

Networking, Cybersecurity, and Privacy for Homes and Small Businesses



Jesse Rocca

This book is a work of non-fiction. All opinions and advice expressed are those of the author and no guarantees or warranties are made of any kind. Although the author has made every effort to ensure that the information in this book was correct at press time, the author does not assume and hereby disclaims any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause. Any fictional names, characters, businesses, places, events, locales, and incidents are either the products of the author's imagination or are used in a fictitious manner. Any resemblance to actual persons, living or dead, or actual events is purely coincidental.

Copyright © 2026 by Jesse Rocca

All rights reserved. No part of this book may be reproduced in any form without permission from the author. To request permission, contact jesse@jesserocca.com.

Cover design by Jesse Rocca using DALL-E 3

All images by Jesse Rocca

Published by Jesse Rocca

www.jesserocca.com

ISBN: 978-1-0679292-1-3

First Edition: August 2026

Table of Contents

1	What You'll Get From This Book... and a Checklist.....	10
2	Introduction.....	17
3	Glossary of Terms.....	24
4	Know The Enemy.....	44
	4.1 Internet Browsing.....	45
	4.2 Email.....	45
	4.3 Installed Software.....	46
	4.4 Hardware.....	48
	4.5 Malware.....	49
	4.6 Internet-of-Things Devices.....	51
	4.7 Mobile Devices.....	51
	4.8 Social Engineering.....	54
	4.9 Denial of Service and Distributed Denial of Service.....	55
	4.10 Survey of Hacking Tools.....	56
5	Computers.....	60
	5.1 Hardware.....	60
	5.2 Application Software.....	108
	5.3 Virtual Machines.....	109
	5.4 Containers.....	112
		113
	5.5 Cloud Services.....	113
6	Home and Small Business Networking.....	122
	6.1 Internet Service Providers.....	123
	6.2 OSI Model.....	125
	6.3 Home and Small Business Routers.....	126
	6.4 Ethernet Switches.....	129
	6.5 Routers and Firewalls.....	131
	6.6 IP Addressing.....	132
	6.7 Dynamic Host Control Protocol.....	138
	6.8 Default Gateway.....	139
	6.9 Static Routing.....	142
	6.10 Public IP Addresses.....	145
	6.11 Network Address Translation.....	148
	6.12 Port Forwarding and Reverse/Application Proxy.....	149
	6.13 Domain Name System.....	152
	6.14 Voice-over-Internet Protocol (VoIP).....	153
	6.15 Wireless Networks.....	156
	6.16 Virtual Private Networks.....	183

7	Security.....	189
7.1	Defense-in-Depth.....	190
7.2	Backups.....	193
7.3	Authentication - Accounts, Passwords, MFA, and Passkeys	201
7.4	Software and Hardware Best Practices and Security Updates.....	212
7.5	Ports, Services, Applications, and Mobile Code.....	217
7.6	Anti-malware Software.....	223
7.7	Portable Media and Peripherals.....	224
7.8	Sandboxing.....	227
7.9	Network Security.....	230
7.10	Advanced Digital Security Concepts.....	246
7.11	Mobile Devices.....	251
7.12	Cyber Attack Detection and Response.....	253
8	Home and Small Business Networking and Security.....	259
8.1	Home and Small Business Network Architecture.....	261
8.2	Self-hosted Services and Applications.....	270
8.3	Remote Hosting.....	274
9	Power.....	277
9.1	Equipment Protection.....	277
9.2	Graceful Shutdowns.....	278
9.3	Backup Power.....	278
10	Privacy.....	281
10.1	WiFi Networks.....	282
10.2	Cellular Networks.....	283
10.3	Personal Privacy.....	284
10.4	Internet.....	286
10.5	Mobile Device Privacy.....	301
10.6	Ad-Blocking.....	302
11	Further Topics, References and Useful Links.....	304
11.1	Artificial Intelligence and Quantum Computing.....	304
11.2	Networking.....	305
11.3	Security.....	305
11.4	Privacy.....	306
11.5	Miscellaneous.....	308
12	Select Software and Tools.....	310
	Bibliography.....	312
	Index.....	314

Table of Figures

Figure 1: Malicious traffic in a random 10 minute window.....	19
Figure 2: Components of a typical PC.....	59
Figure 3: Components of a typical PC.....	62
Figure 4: Older Central Processing Units.....	63
Figure 5: Personal Computer Random Access Memory.....	64
Figure 6: 3.5" Hard Disk Drive.....	65
Figure 7: 2.5" Solid State Drive.....	66
Figure 8: PCIe-Based Dedicated Graphics Card.....	68
Figure 9: USB Audio Interface.....	69
Figure 10: PCIe and PCIe 16x Connectors.....	70
Figure 11: SATA Connectors.....	71
Figure 12: 2.5" mSATA SSD Seated in mSATA Slot.....	72
Figure 13: Female eSATA Connector.....	72
Figure 14: HDMI Connectors.....	73
Figure 15: DisplayPort Connectors.....	74
Figure 16: (a) DVI-I Connectors; (b) DVI-D Connectors.....	74
Figure 17: VGA Connectors.....	75
Figure 18: Older Media Connectors.....	76
Figure 19: 1/8" Inputs and Outputs.....	78
Figure 20: USB Audio Interface.....	79
Figure 21: Audio Connectors.....	80
Figure 22: RJ-45 Connectors for Ethernet Cable.....	81
Figure 23: RJ-11 Connectors for Telephone Cable.....	82
Figure 24: DB-9 Serial Interface Connectors.....	82
Figure 25: USB Connectors.....	84
Figure 26: IEEE1394/Firewire Connectors.....	86
Figure 27: Lightning Connectors.....	87
Figure 28: Thunderbolt Connectors.....	88
Figure 29: PS/2 Connectors.....	89
Figure 30: Worldwide Desktop OS Market Share from March 2025 to April 2026.....	91
Figure 31: Worldwide OS Market Share from March 2025 to April 2026.....	91
Figure 32: Ubuntu Version 24.04.01 Screens.....	93

Figure 33: Linux Mint Version 22 Cinnamon Default Desktop Screen and Launch Menu.....	94
Figure 34: Puppy Linux Bookworm Pup64 Version 10.0.07 Default Desktop Screen and Launch Menu.....	94
Figure 35: PopOS! 24.04 Default Desktop and App Drawer Screens.....	95
Figure 36: Portable Media.....	107
Figure 37: Virtual Machines.....	109
Figure 38: Containers.....	112
Figure 39: Cloud computing.....	120
Figure 40: The Many Functions of the “Home Router”.....	127
Figure 41: Default Gateway.....	140
Figure 42: Static routing.....	142
Figure 43: Port forwarding and reverse proxy.....	150
Figure 44: Typical VPN Use Cases for Home and Small Business Users.....	185
Figure 45: Small network defense in depth.....	190
Figure 46: Network segmentation with a firewall.....	232
Figure 47: Terminal “top” command output.....	257
Figure 48: Gnome System Monitor.....	257
Figure 49: Typical Home Network.....	259
Figure 50: A Better Home and Small Business Network Architecture.....	261
Figure 51: Typical home and small business network architecture vs. a better network architecture.....	263

Index of Tables

Table 1: Glossary of Terms.....	43
Table 2: Hacking Tools.....	59
Table 3: USB Versions, Speeds, and Connector Types [Hill, 2022], [Harding, 2022].....	84
Table 4: IEEE1394/Firewire Versions, Speeds, and Duplex [Teener, 2004].....	86
Table 5: Thunderbolt Versions, Speeds, and Protocols.....	89
Table 6: Benefits and Drawbacks of Microsoft Windows.....	99
Table 7: Benefits and Drawbacks of Linux.....	100
Table 8: Benefits and Drawbacks of MacOS.....	102
Table 9: Smartphone Support Lengths.....	105
Table 10: PCMag 2026 Cloud Service Provider Ratings, Best For and Pros & Cons [Duffy & Muchmore, 2026].....	119
Table 11: OSI Model.....	126
Table 12: IPv4 Address Ranges.....	133
Table 13: Private IPv4 Address Ranges.....	134
Table 14: Canada and US cellular network types, frequencies, and speeds.....	170
Table 15: Bluetooth capabilities.....	171
Table 16: Bluetooth profiles.....	172
Table 17: Bluetooth versions, speeds, and ranges.....	173
Table 18: Bluetooth audio codecs.....	175
Table 19: VPN Types and Their Attributes.....	188
Table 20: Password Vault Comparison.....	206
Table 21: MFA Methods Comparison.....	211
Table 22: Software security controls.....	220
Table 23: Useful netstat commands.....	222
Table 24: Operating System Sandbox Options.....	230
Table 25: WiFi Security Protocols.....	241
Table 26: Bluetooth security features.....	242
Table 27: Bluetooth attacks.....	243
Table 28: Common Attacks, Detection, and Response.....	256
Table 29: Example Power Plan.....	279
Table 30: Similarities Between PIPEDA and GDPR.....	297
Table 31: Differences between PIPEDA and GDPR.....	298

Dedication

This book is dedicated to:

My smart, beautiful, talented, and kind wife and daughters, who make every day a great day, inspire me to do my very best, and allow me to spend my time doing things like writing this book.

My parents for fostering my interest in computers at a young age. For instilling in me a strong work ethic, and a passion for lifelong learning. For providing the encouragement and means to pursue my studies. And for supporting me all along the way.

All of my teachers, academic advisors and mentors who tolerated me, shared their time with me, and helped build my knowledge and skills, preparing me for future academics, and ultimately my career.

My employers for trusting me, and for providing me challenging opportunities of all kinds to grow as an engineer and leader. And for the employment that has allowed me to provide for my family and do all the things we do.

And a special thanks to Mark for his review and feedback. Without Mark's technical and writing expertise, willingness to lend his time, and attention to detail, this book would be much, much worse.

About The Author

Jesse has been using computers since 1987 when his parents bought his family a Commodore 128 computer. Mostly interested in computer games at the time, Jesse studied computer programming in high school and would go on to obtain bachelor's and master's degrees in engineering systems and computing, specializing in intelligent systems.

Following university, Jesse began a career in automation, taking a special interest in cybersecurity. Circa 2006, Jesse began listening to Steve Gibson's Security Now! podcast, where he learned about the Astaro Security Gateway firewall, inspiring him to build one. With the knowledge and experience gained through building, implementing and configuring the Astaro Security Gateway firewall, and combined with his engineering experience, Jesse was offered the opportunity to administer the supervisory control and data acquisition (SCADA) systems of an important and historic group of power generation control centres and plants. Directly responsible for cybersecurity and compliance, administering these critical facilities cemented Jesse's interest and understanding in cybersecurity.

With a long and varied history, interest and experience with computers and networks, Jesse applied his knowledge of securing power generation facilities at home. He has compiled that subject matter into this book, in the hopes that it will help you increase your digital security and privacy.

1

What You'll Get From This Book... and a Checklist

As with many things, when it comes to home and small business networking and cybersecurity you can only pick two of:

1. Good (security and privacy),
2. Cheap (low-cost),
3. Fast (requires little time).

Which leads to the following three scenarios:

Scenario 1: Cheap and Fast, but not Good

This is the average person, let's give them the name Apathia. Apathia has an inexpensive router that has little to no support and is never patched, even though it likely has vulnerabilities. Apathia's network is mostly wireless and was put together quickly, possibly (likely) overlooking important considerations. All of Apathia's devices are on the same network. For Apathia, it would be impossible to tell if any of the devices on her network were hacked. The only way for Apathia to tell if a device was hacked might be to experience performance problems. If any of Apathia's data was leaked there would be no way to know. Apathia might use cloud services for backups of some data. Apathia does not use a password manager, keychain, safe, vault, etc., and mostly uses the same password for

everything, with possibly minor variations. From logging into computers at home and at work, mobile devices, online accounts and even the WiFi, Apathia relies on the same weak password. Apathia hopes that her online digital obscurity is providing cover. Apathia doesn't have any backups. Apathia is not worried about who is using her personal data or for what purposes, it is just not something that Apathia thinks about.

If you're in the same situation as Apathia and you'd like to make improvements, focus on backing up your important data to a couple external hard drives and, ideally, keep one copy at a second location. Then, consider moving toward the scenarios below. Scenario 2 is faster, requiring much less effort, but in the long run costs more. Scenario 3 will take longer, requiring more effort, but costs less and arguably provides more control, privacy, and empowerment.

Scenario 2: Good and Fast, but not Cheap

This is where the cloud integrated users are, let's call them Cloudia. Using mostly mobile devices, Cloudia takes advantage of the mobile devices' hardened operating systems (OS) and app stores for software installation and maintenance. All of Cloudia's backups are safe and sound using an integrated cloud service, ideally encrypted end-to-end. Cloudia uses an email service that encrypts her email end-to-end and uses an integrated cloud-backed up password manager, keychain, safe, vault, etc. Cloudia uses a third-party personal data removal service to outsource the work of tracking and removing her unneeded personal data on the internet. Cloudia is not overly concerned with digital security because she's largely outsourced it to the technology provider.

Scenario 3: Good and Cheap, but not Fast

Where very few vigilant, frugal, dedicated users are, let's call them Valory. Deploying an effective and low cost solution, but using more of her time, Valory uses recycled, low cost or otherwise unused hardware, along with open source software to

create a well segmented network with a strong, supported firewall, and security monitoring tools. Valory has a backup plan and creates local backups with copies stored at a second location. Valory uses a personal cloud server for low-cost modern cloud computing capabilities. Valory serves her own private email server and uses an encrypted email service. Valory employs a local password safe or uses browser-based features to create, store, and change passwords. Valory keeps a list of online accounts and reward program accounts and routinely requests her personal data be deleted from data collectors on the internet. Valory uses other useful privacy tools such as compromised online account detection, passkeys for convenient and strong authentication and email address obfuscation like private duck address generator. Valory may also choose to invest in hardware security appliances for her firewall or other various security related devices.

If you are in scenario 1 the aim of this book is to convince you to head in the direction of scenario 2 or 3 and then to help you understand what is required to realize scenario 3 for yourself if that's your goal. With a modest time commitment and a small budget you can achieve excellent cybersecurity, which is, for lack of a better term "good for you". It is also very rewarding and empowering knowing you are protected, and have the receipts to prove it, which is reassuring.

Below is a home and small business networking and cybersecurity checklist. This checklist lists the actions needed to go from scenario 1 to scenario 3. If the checklist seems daunting, don't be discouraged Dear Reader, this book is intended to help. You are aiming for progress Dear Reader, not perfection. As all good things do, it will take time, but it will be worth it. Be patient with the tech and with yourself! You can do it!

The following is a home and small business networking and cybersecurity checklist:

- Develop a strategy for dealing with all of your data and backing it up. Use backup software such as that included with your operating system or other third-party backup software to help manage all of your backup jobs. Use external drives and move them offsite, or at least put them in a fireproof case, to prepare for the worst. Consider multiple backups of everything. Use cloud services if you care to and consider ones with end-to-end encryption. If you encrypt the files before you upload them you can maintain your privacy without end-to-end encryption. (Section 7.2)
- Use a password manager, keychain, vault, safe, etc. to securely generate and store your passwords. (Section 7.3)
- Uninstall all unnecessary software from all of your devices. (Section 7.4)
- Keep all of your software and hardware patched at the fastest frequency which you are comfortable; you are trading off security for stability and disruption. Monthly patching is really the standard. (Section 7.4)
- Figure out what logical ports should be open and listening on your computers based on your software needs and verify that only those ports are open and listening. (Section 7.5)
- Use anti-malware software on as many hosts as you can. (Section 7.6)
- Lower cost home use: re-purpose a computer with multiple Ethernet cards OR buy a small fan-less computer designed for use as a 4 or 6-port firewall and install a good open source or free for home use firewall operating system on it (e.g., Sophos, Untangle, pfSense, Simplewall, ClearOS, Endian, Zeroshell, Smoothwall, OPNSense, IPFire, IPCop, VyOS, etc.). (Section 7.9.1)

- Higher cost home use OR small business use: buy a good hardware firewall appliance, right-sized for your network (Sophos, WatchGuard, Arista, Fortinet, Cisco, Sonicwall, Ubiquiti, etc.). (Section 7.9.1)
- Use your firewall to create segregated network segments for your internal network (i.e., your most secure network), your general purpose network, your internet facing network (i.e., the network that will contain devices that are directly accessible from the internet), and perhaps a work/school network. Configure the firewall as desired and turn on country blocking, intrusion detection and prevention systems, any advanced threat detection that may be included, any web filtering to suit your needs and be sure to log and alert as desired. (Section 7.9.1)
- Make sure that your router (or firewall) is configured to disable remote configuration. Access to configure your router or firewall should only be allowed from your secure internal network.
- Use vulnerability scanning software to perform scans of your devices. Address any serious vulnerabilities detected such as obsolete or unpatched software or hardware that contains security vulnerabilities, unnecessary open and listening ports, “autorun” features enabled, insecure default settings, default or guest accounts, default passwords, unnecessary drive shares, etc. (Section 7.10.4)
- Consider installing a Security Information and Event Monitoring system (SIEM) to detect and alert on things like failed login attempts on hosts and malicious traffic or websites. (Section 7.10.3)
- Consider installing a honeypot to attract would-be attackers to a safe system on your network that will alert you of an attack in progress. (Section 7.10.6)

- Consider using virtual machines to create some of the suggested security and privacy systems (i.e., Pi-hole, SIEM, Honeypot, possibly even a firewall, etc.) (Section 5.3)
- Consider setting up a personal cloud server, such as NextCloud¹ for a private, personal, feature-rich cloud computing system. A system such as this is similar to the cloud features that Microsoft, Apple, Google, and others provide, allowing you to access your files, photos, videos, calendars, notes, reminders, etc. remotely, along with synchronization across the devices that you connect to your personal cloud server. (Section 5.5)
- Consider setting up an ad-blocking and cybersecurity improving Pi-hole server as your Domain Name System (DNS) server. (Section 6.13)
- Use a virtual private network (VPN) to allow secure remote connections to your home or small business network and ensure privacy. (Section 6.16)
- Look at your power situation. Use surge-protecting power bars to protect your important electronic equipment. Consider purchasing and implementing an uninterruptible power supply (UPS) to allow some of your electronic equipment to remain powered in a power outage, and to give you time to gracefully shut down important systems in an extended power outage. (Section 9)
- Minimize your online personal data so that it cannot be leveraged in unwanted ways by 3rd parties. Do so by keeping a list of all of the online accounts you have, along with any brick and mortar store reward programs you've signed up for. Routinely request your data be deleted. You can outsource personal data removal to a third-party for a fee. (Section 10.3)

1 <https://nextcloud.com/>

- Know what information the apps and software you use have access to (e.g. location, contacts, message log, photos, videos, etc.) and be deliberate about providing that information in return for the functionality. Exercise the privacy features that your OSes, devices, and software provide to limit all such access to the level that suits you. (Section 10.4)
- If all of this seems like too much then consider mostly using mobile devices and integrated cloud computing solutions. You should still observe good password practices, use multi-factor authentication (MFA) and Passkeys whenever possible, make sure everything important is backed up and consider using a 3rd party to help with personal data removal. (Section 7.11)

If any of the above piques your interest then read on Dear Reader. It is the author's hope and intention to entertain at times, encourage, inspire, enlighten, inform or at least remind you of the ways, in which, you can achieve very good digital security at your home or small business. The goal of this book is to make the information as concise as possible, while being approachable and a reference for the technical details.

2

Introduction

There is the idea in cybersecurity that you cannot achieve security through obscurity. That you should not believe that your digital systems are safe just because their security details or digital location are not widely known. The reality is that you cannot rely on your perceived digital obscurity to protect you from an attack.

There was a time, long, long ago, when home users could somewhat rely on their digital obscurity to provide a level of comfort, but this is no longer the case and hasn't been for decades. Hacking tools are sophisticated and have enabled and empowered even the most inept attacker. Automated systems crawl the internet looking for vulnerabilities and machine learning capabilities are being used to lend adaptive behaviors to these systems. Governments worldwide have developed sophisticated Cybersecurity tools with the vast resources they have at their disposal. In the worst cases these cybersecurity tools have been stolen through cyber attacks, leaving a Pandora's box of ridiculously powerful tools available to bad actors. Thanks to the internet, these bad actors are figuratively able to transport themselves across the globe to your very front door (literally, transporting themselves electronically to your router's internet port). From there they can begin to silently take apart your house (again, a metaphor for your router) until they make their way in. This may sound alarmist, but it really isn't far from the truth.

Before computers were connected to the internet, physical access to your home computer was required to hack it. Under these circumstances, most people were justified in not worrying too much about being hacked. In the early days of the internet, and for a very short period of time after, the relative obscurity of how the thing worked and lack of publicized cyber attacks may have weakly justified this apathetic attitude to cybersecurity. However, the situation did not last long. The internet was in use by early adopters in the mid-90's and was adopted by 50% of North American homes by 1999 [History Tools, 2024]. By August 2003 the MS Blaster Worm was circulating around the internet infecting Windows XP computers and using those infected computers to infect more computers, spreading across the internet just like... well, a virus - hence the name.

In August 2004, Microsoft released a Windows XP service pack update (SP2), that installed a firewall into Windows XP. This new firewall effectively stopped the Blaster Worm and marked Microsoft's new focus on security.

Today, the average home or small business user really does have some real cybersecurity risk. Some of the most concerning risks include:

- identity theft
- compromised online accounts including bank accounts
- digital theft of locally stored cryptocurrency or through bank account compromise
- partial or total loss of your important data
- extortion to recover your data or to prevent any sensitive content from being published or distributed
- operational downtime
- loss of customer records or data, possibly necessary for regulatory reasons

It follows that if your situation is such that you don't care about losing or disclosing your data, or the exposure or exploitation of your online activities, identity, online bank accounts etc., then you probably don't need to worry about cybersecurity.

Otherwise, there are some simple and relatively inexpensive steps you can take to drastically decrease your overall cyber security vulnerability and increase your privacy. With online security, most people (that aren't a target of opportunity) can be encouraged by the old adage that "you don't need to outrun the bear, just the guy next to you." That is to say, taking some simple steps to get ahead makes the guy next to you an easier, and more likely target for an attacker and thus, reducing your chances of an attack (only if you're not a target of opportunity for a determined attacker).

The kinds of steps proposed in this book are the cybersecurity analogy of closing and locking your doors, and installing an alarm system and cameras for monitoring. For many people, theft or exposure of the items in their "digital house" may very well be a greater risk to lose than those in their physical house. There is plenty of awesome, open and closed, free and paid software out there to aid in the task of making sure your data is safe and secure. You can do it!

There are two fundamental questions you should ask yourself regarding your cybersecurity and privacy:

- Do you or your small business have any data or online activities that you don't want others to see? Examples might include banking information, health information, intellectual property, sensitive personal data, sensitive personal activities, works of art and inventions in progress, staff records, etc. The list goes on.
- Do you or your small business have any data that you don't want to lose? Examples might include home movies and pictures, personal documents and work, original works of art, cryptocurrency, media libraries, customer

records, financial and tax records, etc. Again, the list goes on.

Are you confident that your data is secure? This book will help you answer that question and help you take steps to improve your digital security.

As a bit more motivation that concern for your cybersecurity posture is warranted, Figure 1 shows a screen capture of the inbound internet traffic from known malicious internet hosts during a random 10 minute period on the author’s home network in September of 2021.

DASHBOARDS

ANALYSIS

ENVIRONMENT

REPORTS

CONFIGURATION

DISPLAYING 1 TO 50 OF THOUSANDS OF EVENTS.

899,983 TOTAL EVENTS IN DATABASE.

☐ EVENT NAME	DATE TIME	SENSOR	CTX	SOURCE	DESTINATION	ASSET S = D	RISK
☒ Sophos UTM: Packet Dropped	2020-09-21 22:38:59	alienvault		192.241.237.80.33116	External-WAN-Address:631	2->2	LOW
☒ Sophos UTM: Packet Dropped	2020-09-21 22:38:31	alienvault		192.35.168.225.39801	External-WAN-Address:12510	2->2	LOW
☒ Sophos UTM: Packet Dropped	2020-09-21 22:37:23	alienvault		174.138.64.163.52575	External-WAN-Address:2273	2->2	LOW
☒ Sophos UTM: GEOIP Drop	2020-09-21 22:36:52	alienvault		193.118.53.210.30294	[REDACTED]	2->2	LOW
☒ Sophos UTM: Packet Logged	2020-09-21 22:36:52	alienvault		193.118.53.210.30294	External-WAN-Address:80	2->2	LOW
☒ Sophos UTM: GEOIP Drop	2020-09-21 22:36:43	alienvault		106.13.41.25.59474	External-WAN-Address:13725	2->2	LOW
☒ Sophos UTM: Packet Dropped	2020-09-21 22:33:40	alienvault		192.35.169.31.14735	External-WAN-Address:1521	2->2	LOW
☒ Sophos UTM: Packet Dropped	2020-09-21 22:33:36	alienvault		192.241.237.249.36770	External-WAN-Address:5964	2->2	LOW
☒ Sophos UTM: GEOIP Drop	2020-09-21 22:33:09	alienvault		3.35.240.145.9709	External-WAN-Address:23	2->2	LOW
☒ Sophos UTM: GEOIP Drop	2020-09-21 22:32:31	alienvault		80.82.64.210.40957	External-WAN-Address:3277	2->2	LOW
☒ Sophos UTM: GEOIP Drop	2020-09-21 22:32:18	alienvault		94.102.51.17.43252	External-WAN-Address:4776	2->2	LOW
☒ Sophos UTM: Packet Dropped	2020-09-21 22:31:48	alienvault		128.1.91.204.32552	External-WAN-Address:8080	2->2	LOW
☒ Sophos UTM: Packet Dropped	2020-09-21 22:31:29	alienvault		146.88.240.4.53144	External-WAN-Address:1434	2->2	LOW
☒ Sophos UTM: GEOIP Drop	2020-09-21 22:31:06	alienvault		45.227.254.30.58496	External-WAN-Address:4404	2->2	LOW
☒ Sophos UTM: GEOIP Drop	2020-09-21 22:30:42	alienvault		185.200.118.66.40312	External-WAN-Address:3289	2->2	LOW
☒ Sophos UTM: Packet Dropped	2020-09-21 22:30:33	alienvault		184.105.139.98.56858	External-WAN-Address:69	2->2	LOW
☒ Sophos UTM: Packet Dropped	2020-09-21 22:30:12	alienvault		162.241.142.103.44311	External-WAN-Address:4311	2->2	LOW
☒ Sophos UTM: Packet Dropped	2020-09-21 22:29:47	alienvault		67.205.162.23.48218	External-WAN-Address:19966	2->2	LOW
☒ Sophos UTM: Packet Dropped	2020-09-21 22:28:30	alienvault		24.53.163.9.44902	External-WAN-Address:23	2->2	LOW

Figure 1: Malicious traffic in a random 10 minute window

Most of the logs are just records that packets have been dropped due to “GEOIP” (as the firewall is configured to drop all incoming traffic from any country other than Canada). However, this is just a random 10 minute sample and there are

19 potentially malicious transactions that could have occurred if the author's home router was vulnerable or misconfigured.

Home routers can be very troublesome from a security perspective. The website routersecurity.org/bugs.php tracks and documents the flaws in routers. It contains a daunting list of security flaws in home and small business routers. Many inexpensive home and small business routers are sold at a price point that cannot sustain its support over long periods of time. Inevitably, security flaws will be discovered and many will not have patches developed for them. Implementing a well supported network router or firewall is a solid plan.

This book introduces a few advanced, but relatively simple to setup and use tools, that increase privacy and security. One such tool is a security information and event monitoring system (SIEM). Implementing a SIEM is the equivalent of putting cameras up around your property. SIEMs collect the logs from all of the networked devices, including routers or firewalls, and provide real visibility into what is happening on the network. In the event that a cybersecurity incident occurs, a SIEM is an invaluable tool for detecting and investigating the attack. Additionally, the use of a personal DNS server, like Pi-hole¹, can help ensure that malicious websites cannot be browsed to (Pi-hole is also excellent at ad-blocking, if that's something you're into). Other DNS tools that provide DNS filtering functionality include Adgard² and Quad9³.

The following are the most important takeaways from this book:

- Bad actors are probing your systems constantly for ways in, and they have powerful tools available to them. If you have data that you don't want to lose, or data or

1 <https://pi-hole.net/>

2 <https://adguard.com/>

3 <https://www.quad9.net/>

online activities that you don't want others to see, then it's good to evaluate your cybersecurity posture and improve it, if needed.

- Your router is your first line of cybersecurity defense. Perhaps surprisingly, the typical home router is more than just a router, it is also a basic firewall, a switch, a WiFi access point, and often a modem and VoIP router. It is useful to understand the various functions that the typical home router performs. Many home routers contain security vulnerabilities. Check yours out at routersecurity.org.
- Upgrading your router to a firewall allows you to segment your network so that you can protect your most important and secure systems from your less secure (and potentially compromised) systems.
- Use strong passwords. Use different passwords for each system, account, website, etc. Use multi-factor authentication (MFA), whenever possible. Use passkeys for a convenient and strong alternative to traditional passwords.
- You don't need to beat the bear, you just need to beat the guy next to you. Good digital security (as opposed to great digital security) may suffice and is better than poor security.
- Very good digital security is within your reach, it does not cost a lot, and is not that hard to achieve. Many of the more important security-related software are open-source or free for home use.
- Your information is valuable; if it wasn't the big data collectors wouldn't be harvesting it at the rate they are. It's good to be aware of the value of your data and to be deliberate in its exchange. It is worth considering the power of the aggregation of this data collection across

society. The value of any individual's data is fairly insignificant. The power emerges at aggregation. You can take simple steps to improve your, and our collective, privacy.

A word of caution, but also encouragement; becoming a more advanced network administrator necessarily comes with the possibility of more troubles. When those troubles arise, please be patient and don't be discouraged. Whether you've temporarily moved a device from one network to another and forgot about the firewall rules being different on the two networks, or an update goes poorly forcing you to restore from backups, there is no doubt that doing some of this stuff will come with challenges. With these challenges, sometimes only you can possibly know how you've painted yourself into this corner and you must use a process of deduction, creativity and most of all patience, to resolve the issue. In many cases, the additional control and options being configured provide the security and privacy benefits that you seek, but may create some kind of unintended consequence, akin to a side-effect. Hopefully the advantages still outweigh the disadvantages, and no doubt it can be frustrating at times, so patience and focus on learning are important to managing the frustration. The artificial intelligence (AI) systems available today can really help to troubleshoot issues and are a massive advantage.

3

Glossary of Terms

*“If you wish to converse with me, define your terms - Voltaire”
- Hiusser*

This section provides a glossary of commonly used terms for the subject matter covered in this book, as defined by the author.

Term	Definition
AGP	Accelerated Graphics Port. Powerful at the time, a now outdated graphics card interfacing port.
AM	Amplitude modulation. An encoding system for radio communication systems that encodes information in the radio signal by modulating the signal's amplitude.
AOSP	Android Open Source Project. An open source operating system for mobile devices, maintained by the Open Handset Alliance. AOSP is the underlying operating system of the more popularly used version made by Google.
API	Application Programming Interface. The manner in which applications access the

Term	Definition
	information and functionality of other applications, via specified and implemented rules, protocols, and procedures.
ARP	Address Resolution Protocol. An important communication protocol that allows the Media Access Control (MAC) address of a given device to be determined from the devices IP address.
AV	Antivirus. Software that scans media or traffic for computer viruses. See Section 7.6.
Bluetooth	An open standard for a low-cost and low power radio network that operates in the 2.4-2.4835 GHz Industrial, Scientific and Medical (ISM) unlicensed frequency band. It allows devices to communicate wirelessly by creating an ad hoc “Wireless Personal Area Network” (WPAN), known as a piconet. See Sections 6.15.3 and 7.9.5.
CAT5/5e/6	Copper cable containing 8 twisted pairs of conductors, usually terminated with RJ-45 connectors, for use on Ethernet networks, but sometimes used for other purposes.
CD	Compact Disc. CDs are data storage media based on the properties of optics and as such are referred to as “optical media”. CD players and drives use lasers that “read” information from the CD by scanning pitted patterns etched onto the CD surface that represent encoded information. CD writer drives are capable of etching (burning) the pitted patterns (representing the encoded information) onto

Term	Definition
	writable CDs. CDs are able to store 700 MB of data.
--CGI	Common Gateway Interface. Often written in a web scripting language, CGIs enable web servers to process HTTP or HTTPS user requests to execute external programs.
CIDR	Classless Inter-Domain Routing. A compact form of denoting an IP address and subnet mask. See Section 6.6.
CPE	Customer Premise Equipment. The equipment provided by the internet service provider that resides at the home or business.
DDR	Dual Data Rate. First introduced in 1996, DDR is a term associated with random access memory (RAM) technology that doubled the data transfer rate by allowing data to be transferred on the rising and falling edge of the clock signal.
dGPU	Dedicated Graphics Processing Unit, a GPU that is a separate, discrete component, having its own dedicated RAM and connecting to the motherboard through a PCIe slot (or formerly AGP or PCI slots).
DHCP	Dynamic Host Control Protocol. DHCP is used to distribute (“give out”) IP addresses to devices on a network. See Section 6.7.
DisplayPort	A prominent video interfacing cable and port. DisplayPort is compatible with HDMI and can also carry audio and Ethernet signals, known as

Term	Definition
	DisplayPort Ethernet Channel (DPEC). See Section 5.1.7.2.
DNS	The hierarchical and decentralized Domain Name System. A naming system for computers, services, and other resources connected to the Internet or a private network. DNS facilitates resolving “domain names” into IP addresses. For most people, the important thing to know is that DNS allows the use of domain names to access websites rather than IP addresses. See Section 6.13.
DPEC	DisplayPort Ethernet Channel. DPEC refers to the Ethernet channel included in some DisplayPort cable interfacing systems.
Driver	Software that is needed to interface with hardware. Sometimes a default driver for a particular piece of hardware will be provided by the operating system that will work, but not optimally. It is usually best to use the latest, correct, manufacturer’s driver for optimal hardware functionality and performance.
DVD	Digital Video Disc. Like CDs, DVDs are data storage media based on the properties of optics and as such are referred to as “optical media”. DVD players and drives use lasers that “read” information from the DVD by scanning pitted patterns etched onto the DVD surface that represent encoded information. DVD writer drives are capable of etching (burning) the pitted patterns (representing the encoded information) onto writable DVDs. DVD

Term	Definition
	technology uses lasers that have a smaller wavelength than CD technology, and the pitting is finer, meaning that DVDs are able to store quite a bit more data than CDs. Single-layer DVDs are able to hold 4.7 GB of data and dual-layer DVDs are able to store 8.5 GB of data.
Ethernet	A computer network architecture consisting of various specified local-area network protocols, devices, and connection methods.
Firewall	Device or software that allows control of Ethernet traffic. See Section 6.5.
FM	Frequency modulation. An encoding system for radio communication systems that encodes information in the radio signal by modulating the signal's frequency.
FOSS	Free and open source software.
GFS	Grandfather-Father-Son. An approach to backups that involves creating and pruning backups on a “rolling” schedule. Something like creating a full backup per day for the last week, a full backup per week for the last month, a full backup per month for the last year, then annual backups for last seven years; then deleting daily backups that are older than a week, the weekly backups that are older than four weeks, the monthly backups that are older than twelve months, the annual backups that are older than seven years.
GNU Linux	The operating system commonly known as Linux is based on the Linux kernel, but all

Term	Definition
	other components that are required to make it function are the GNU operating system. As such, many believe, and the GNU project requests, that the operating system should be referred to as GNU/Linux or GNU Linux. GNU stands for GNU's not Unix, which makes the term a recursive acronym (where one of the letters in the acronym stands for the acronym itself). The GNU project was created for the development of a Unix-like operating system that comes with source code that can be copied, modified, and redistributed. Richard Stallman announced the GNU project in 1983 and, with others, formed the Free Software Foundation in 1985.
GPU	Graphics Processing Unit. The component that processes the graphics and renders them to a display unit, like a monitor or television.
HDMI	High Definition Multimedia Interface. The most prominent video interface port and cable at the time of this writing. HDMI can also carry audio and Ethernet signals. See Section 5.1.7.2.
HEC	HDMI Ethernet Channel. HEC refers to the Ethernet channel included in some HDMI cable interfacing systems.
IDS/IPS	Intrusion Detection System/Intrusion Prevention System. An IDS can be a stand alone system placed somewhere on a network, and it inspects traffic/logs on the network and alerts when it finds something suspicious. A SIEM is an

Term	Definition
	example of an IDS. An IPS not only provides alerts, but can also block traffic based on detection rules. Typically, an IPS is located directly in a network firewall. See Section 7.10.1.
IEEE	Institute of Electrical and Electronics Engineers.
iGPU	Integrated Graphics Processing unit. A GPU that is integrated directly into the motherboard of a computer.
iOS	Apple's iPhone and iPad operating system.
IoT	Internet of Things. The continuing connection of more and more devices and types of devices to the internet, such as thermostats, light switches, refrigerators, etc. These are "IoT" devices. See Sections 4.6 and 5.1.11.
IP Address	Internet Protocol Address. The network address of a device. IPv4 addresses are in the form of four octets separated by a period. E.g., 192.168.0.1. IPv6 addresses are in the form of 8 hexadecimal groups separated by colons. E.g., 2607:f0d0:1002:0051:0000:0000:0000:0004
ISA	Industry Standard Architecture. A very outdated computer peripheral interfacing port.
ISP	Internet Service Provider. Entities that provide internet service by allocating network bandwidth on their network to customers and

Term	Definition
	connecting them to upstream internet servers.
ISM	Industrial, Scientific and Medical unlicensed radio frequency band.
kB/MB/GB/TB	Kilobyte/Megabyte/Gigabyte/Terabyte, 1 kB = 1024 bytes, 1 MB = 1024 kB, 1 GB = 1024 MB, 1 TB = 1024 GB.
LAN	Local Area Network. Devices on the same network in the same geographic area.
Logical Port	An application specific, service specific or process specific software communication endpoint in a host's operating system. Logical port numbers range from 1 to 65535, allowing applications, services and processes to communicate using the same IP address, but using different logical ports. There are well known, registered, applications and ports, see https://www.iana.org/ . See Sections 5.1.7 and 7.5.
MAC Address	Media Access Control address. MAC addresses are hardware encoded addresses of networkable devices. Ethernet switches use MAC tables to determine the MAC addresses (and thus devices) that are connected to its physical ports. Address Resolution Protocol then relates the MAC address to the IP address. It is possible to "spoof" (impersonate) MAC addresses using specialized software.
MacOS	Apple's computer operating system. See Section 5.1.9

Term	Definition
Malware	Malware is software that has malicious intent. See Sections 4.5 and 7.6.
Masquerading (see NAT)	Masquerading is a type of Source Network Address Translation (SNAT). SNAT is used to change the source address in the IP header of a packet. It may also change the source port in the TCP/UDP headers. The most common usage of masquerading is to modify the private source IP addresses of IP packets leaving a private network to the public IP address of the internet connected interface. This allows multiple systems on the private network to access to the internet via the single IP address of the internet connected interface, allowing the internet connected interface to act as the gateway ¹ . Masquerading is a special case of SNAT where the source IP address is not known to the router in advance because the interface connecting to the internet is configured to obtain its IP address via DHCP from the ISP. If the interface connecting to the internet has a static IP address then masquerading isn't necessary, and plain SNAT can be used, which is a faster approach. See Section 6.11.
Microsoft Windows	Microsoft's operating system for personal computers and servers. See Section 5.1.9.
MFA	Multi-factor authentication. Previously called two factor authentication (2FA), this method of authentication requires more than one... factor. Typically following the approach of something you have (token, smart card, etc.), something

¹ See <https://www.rfc-editor.org/rfc/rfc1918>.

Term	Definition
	you know (password, pin, etc.), something you are (fingerprint, retina pattern, etc.). See Section 7.3.
Mobile Device	Small, portable computing devices including Smartphones, tablets, Chromebooks, iPhones, iPads, e-readers, etc., usually running Android or iOS. One day we may have a reliable, popular GNU Linux-based phone, but the Windows phone OS and Blackberry OS are long dead now. See Sections 4.7, 5.1.10, 7.11, and 10.5.
Modem	The word modem is a portmanteau of modulate and demodulate. Modems adapt a local Ethernet network to an ISP network, usually through coaxial cable, phone line, cellular radio, satellite communication, or other wireless technology.
NAND	“Not AND”. NAND is a term used that is used in boolean logic and is a type of boolean logic gate. More commonly, the term NAND is associated with a type of flash memory SSD that is based on NAND logic gates.
NAT	Network Address Translation. A service that operates on routers and firewalls that allows mapping one IP address space onto another through on-the-fly modification of the network address information in the IP packet headers. Perhaps the most common use of NAT is when connecting a private network, like a home or small business network, to the internet and using NAT to modify the IP header of all the

Term	Definition
	outbound private network packets with the IP address of the router's external interface. This allows all of the devices on the private network to communicate with the internet while only requiring one public IP address. See Section 6.11.
NextCloud	Powerful, open source, personal cloud server software.
NFC	Near Field Communication. A wireless personal area network that enables slow, but reliable, and secure communication between two supported devices that are within a very short distance from each other (typically ~2 cm or less). Today, NFC is defined by the ISO/IEC 18092:2013 standard. See Sections 6.15.6 and 7.9.7.
NVMe	Non-volatile Memory Express. NVMe is an interfacing protocol that is used for high-speed data transfer with specific interface ports (M.2, U.2, PCIe add-in cards and Thunderbolt) and NAND flash memory based SSDs.
OEM	Original Equipment Manufacturer. Typically, a company whose products are used and incorporated into another company's products that are sold as finished products.
OS	Operating System, like Windows, GNU Linux, Unix, Android, MacOS, iOS, etc. It is the software that allows applications to run and interact with system components and resources like the Central Processing Unit (CPU), Random

Term	Definition
	Access Memory (RAM), Graphical Processing Unit (GPU) and storage volumes (drives). See Section 5.1.9.
OSI Model	Seven layer model of communication often referred to for Ethernet communications. See Section 6.2.
PC	Personal Computer, usually implies running the Windows OS.
PCI	Peripheral Component Interface. PCI is a standard backplane connection style interfacing slot for connecting peripherals to the motherboard of a computer.
PCIe	Peripheral Component Interface Express. PCIe replaced the former AGP and PCI-X connecting slots. PCIe is a standard backplane connection style interfacing slot for connecting peripherals, mostly dGPUs and SSDs to the motherboard of a computer.
Phishing	A malicious, generic type email, sent out to as many email addresses as possible in the hopes that someone clicks the malicious links, and possibly enters requested information. Traditionally, phishing emails have been pretty easy to spot, the telltale signs being spelling mistakes, poor grammar, weird sending email addresses, general type addressing to the receiver (e.g., Dear Sir/Madam, etc.) and time-pressure or appeal to emotions. However, AI systems are making phishing emails harder and harder to detect.

Term	Definition
Pi-hole	Open source software that runs on GNU Linux that provides a DNS server. Pi-hole acts like a “man in the middle” for outgoing internet requests and fails to serve requests for known ad servers as well as addresses known to be dangerous.
Port Forwarding	A method of specifying which internal host incoming internet traffic should be directed to behind a “NATed” network, based on the logical port that the traffic is communicating on. See Section 6.12.
PoS	Point-of-sales. Cash register systems in retail stores, restaurants, etc.
POTS	Plain-old-telephone-system. Denotes the technology used with traditional analog phone systems.
PQC	Post Quantum Cryptography. Cryptographic methodologies that resist the advantages of quantum computers.
PVR	A Personal Video Recorder is a system for capturing live/streaming content for later playback. PVRs are usually associated with cable and satellite TV services, but there are also various methods to implement a PVR on a computer.
RAID	Redundant Array of Inexpensive Disks. A system consisting of several schemes that facilitate efficient data drive fault tolerance. See Section 7.2.7.

Term	Definition
RAM	Random Access Memory. The memory of a computer that is used in the execution of programs and short term data storage. See Section 5.1.3.
Ransomware	A malicious computer program that encrypts a system's drives to hold the data on the drives ransom. Typically, the goal of ransomware is to extract a monetary ransom to provide the decryption key to decrypt the data. See Sections 4.5 and 7.6.
RF	Radio frequency. Electromagnetic waves that have a frequency of 300 GHz or less.
RFID	Radio Frequency Identification (RFID) is a technology to wirelessly provide information to devices in short proximity, typically through the use of RFID tags. RFID utilizes electromagnetic fields to identify and the track objects. RFID tags have a very small radio transponder, receiver, and transmitter built into them. RFID reader devices emit an interrogation pulse, which then triggers the target RFID tag to transmit digital data. RFID tags can be powered by the reader device's electromagnetic pulse or they can be powered by a battery, which greatly extends the RFID tag's range to upwards of 100 ft. See Sections 6.15.5 and 7.9.7.
Router	An Ethernet networking device that enables communication between different Ethernet networks. However, a "home router" is usually much more than just a router. See Section 6.3.

Term	Definition
SDK	Software development kit. A set of software development tools packaged into a single installation file. They contain a compiler, a debugger and sometimes a software framework and libraries to enable software development.
Sideload	Installing an application from outside of the operating system manufacturer's official app store or repository.
SIEM	Security Information and Event Monitoring system. SIEMs are software appliances or software that collect, correlate, and analyze logs of networked devices. Additional features provided by SIEMs are alarming and alerting on various conditions, cyber incident management and vulnerability assessment. See Section 7.10.3.
SIP	Session Initiation Protocol. A protocol used with Voice over IP (VoIP) communication technology.
Smishing	See Phishing. Similar to a phishing email but delivered via cellular messaging (SMS).
Socket	A combination of an IP Address and a logical port, e.g., 192.168.15.2:32458
Spear-phishing	See Phishing. Similar to a phishing email, but targeted at a particular person or organization. A spear-fishing attack will be more difficult to identify as it may include specific and correct details. The goal of spear-phishing remains to get the user to click a malicious link or provide requested information.

Term	Definition
SSD	Solid State Disk (drive). A type of drive that uses solid state electronics (mostly transistors and diodes) to store data and provide access to that data.
SSID	Service Set Identifier. WiFi routers and access points broadcast their SSID for connecting WiFi devices.
Static Route	An instruction, usually configured in a router or firewall, that specifies how one network should route traffic to another, through an intermediate network, when two networks aren't immediately adjacent to one another. See Section 6.9.
(Ethernet) Switch	A device that connects Ethernet devices to each other creating a network and enabling Ethernet communication. Operating at the Layer 2 level, Ethernet switches use "switching fabric," composed of application specific integrated circuits (ASICs) that implement the ARP protocol allowing the switch to identify which devices (MAC addresses) are connected to which switch ports, and direct traffic accordingly.
Terminal (Emulator)	A program that provides a command line interface to a computer.
TLS	Transport Layer Security. TLS is a security protocol used to encrypt Ethernet communications.
Ubuntu	A very usable and well maintained GNU Linux

Term	Definition
	distribution.
UTM	Unified Threat Management, a concept where firewalls started integrating additional features that “unified” security like intrusion detection and prevention, advanced threat protection, logging, and reporting features, etc. See Section 7.10.2.
UPS	An Uninterruptible Power Supply is a power supply system that provides emergency power to a load when the normal power fails, usually by employing batteries. See Section 9.3.
VGA	Video Graphics Array. VGA is an older, but still ubiquitous video interfacing cable and port. See Section 5.1.7.2.
Virus	A computer or mobile device program, typically malicious in nature, that replicates by copying itself to other computers. See Sections 4.5 and 7.6.
Vishing	See Phishing. Vishing is a form of phishing that uses a voice call, or message and callback, to extract information, money, and more, from victims.
VM	Virtual Machine. A software emulation of a computer system that allows an operating system to be installed and runs as an application on a host computer (which can also be a VM, but there has to be a real computer at the bottom of the chain). Windows includes a virtualization platform. Other popular virtualization platforms include VMWare,

Term	Definition
	VirtualBox, and QEMU. Typically, there are minimum hardware requirements (CPU, motherboard and RAM) to run VMs.
VoIP	Voice over Internet Protocol. A system that allows telephone calls to be made over the internet. VoIP usually requires the use of a VoIP router that will have an RJ-11 connector for connection to an analog phone or phone network, and an RJ-45 connector for connection to an Ethernet network that is connected to the internet.
VPN	Virtual Private Network. A networking technology that facilitates the creation of virtual, logical, encrypted networks for systems to communicate privately. VPNs are commonly used to create a private connection to a home or work network from a remote location or to create private networks between multiple office buildings, over the internet.
VPS	Virtual Private Server. Refers to a full server including the OS and computing resources (CPU, RAM, network adapters, etc.), implemented as a virtual machine in a cloud computing environment. VPS services are available from VPS providers and make standing up servers, for whatever purpose, extremely fast and easy.
WAF	Web Application Firewall, AKA reverse proxy. A WAF facilitates protection of web servers by acting as “man in the middle” virtual server, scanning and filtering incoming internet traffic

Term	Definition
	before sending that traffic to the real web server.
WAN	Wide Area Network. WANs are a home or small business networks' connection to the internet, usually referred to as its WAN connection.
WAP	WiFi Access Point. WAPs allow devices to wirelessly connect to them, usually for the purpose of accessing an upstream internet connection. WAPs can be hardwired to an upstream network, or they may be a wireless repeater, repeating a WiFi signal. WAPs may also be deployed as part of a self-healing wireless mesh network.
WEP	Wired Equivalent Privacy. A now obsolete and insecure wireless network security protocol, WEP provided early WiFi security using a key to authenticate connections to the WiFi network and encrypt the network traffic.
WiFi	The radio-based network technology that allows WiFi-enabled devices to wirelessly connect to a "WiFi access point" or "home router". WiFi does not abbreviate "Wireless Fidelity". It is a marketing brand that marketing company, Interbrand, came up with for the WiFi Alliance. Being connected to the WiFi doesn't necessarily mean you're connected to the internet, just that you are connected to a WiFi router or access point.
WPA / WPA2 / WPA3	WiFi Protected Access, WiFi Protected Access 2 and WiFi Protected Access 3. WPA2 and WPA3

Term	Definition
	are the currently preferred WiFi security protocols for authenticating and encrypting WiFi network connections and traffic.
WPAN	Wireless Personal Area Network. WPAN is a term used to describe the relatively small scale wireless networks that technologies like Bluetooth and Zigbee implement.
Zero Trust	The Zero Trust security model is a methodology for designing and deploying information and operational technology systems. Also known as Zero Trust Architecture (ZTA), or perimeter-less security, the basic principals are to never trust; always verify, and apply least privilege principles. This means that strong user identity verification practices are in place as well as device security compliance prior to granting access, and users and systems only being granted the specific access they require.
Zigbee	A set of communication protocols that comprise an open-source, wireless networking technology that enables the creation of low power, low data rate WPANs.
Z-Wave	An IoT networking technology similar to Zigbee.

Table 1: Glossary of Terms

4

Know The Enemy

There are two main reasons your systems might be subjected to a cyber attack. The first and easiest to thwart is that your systems are easy targets. This is the digital equivalent of leaving your doors open at night. Folks in this category can get a giant boost in their security by doing some very simple things, akin to locking the doors at night.

The other reason your systems might fall prey to a cyber attack is because you or someone in your house or business are a target of opportunity. Average people are not usually targets of opportunity; this is primarily the domain of large or important organizations, people, and celebrities. However, average people can sometimes be targets inside important organizations. Needless to say, those that find themselves targets of opportunity require additional security, likely not only defensive methods, but offensive and proactive ones as well. This is a more difficult scenario to mitigate as an attacker will be persistent in trying to find vulnerabilities in your systems, instead of just moving on to the next hapless victim that has worse security than you. Targets of opportunity certainly require more vigilance, but all the same techniques as those described in this book would be those used to secure their systems as well.

4.1 Internet Browsing

While browsing online, if the wrong link is clicked or in some cases, the wrong content is displayed, your computer/device may become compromised. This can include complete administrative control over your computer/device or a malware infection such as ransomware. The most effective methods of mitigating browsing vulnerabilities are vigilant browsing habits as well as use of sandboxed browsers (see Section 7.8) and anti-malware software that monitors your web activity for malicious links and content. On a computer, it is highly recommended to use a sandboxed browser to view any content that you do not know to be trustworthy.

4.2 Email

The security risks of email are similar to browsing. If you open a malicious email and click a malicious link or display malicious content, your computer/device may be compromised. The types of attacks that come through email are called phishing or spear-phishing attacks. A phishing attack is usually a generic email sent out to as many email addresses as possible in the hopes that someone clicks the links. Usually these emails are pretty easy to spot. The telltale signs are spelling mistakes, poor grammar, weird sending email addresses, general type addressing to the receiver (e.g., Dear Sir/Madam, etc.) and time-pressure or appeal to emotions. Modern email filtering systems automatically filter most of these types of emails out, but in the event that the odd extra crafty one makes it through, it is important to exercise vigilance and delete it without opening it, or especially without clicking any links or attachments.

Spear-phishing emails are like phishing emails in that they contain malicious links or attachments, but they are specially crafted for a particular person, making them more difficult to spot. Extra vigilance is required to spot spear-phishing emails. An example of where you may encounter a spear-phishing

attack is if one of your contacts is compromised and their contact list and email accounts are exposed. In this case, you may receive messages as though they are sent by your contact directly, instead of by the attacker. These types of messages may be very difficult to identify. Artificial Intelligence (AI) is being used to make phishing and spear-fishing emails even more difficult to detect.

If you are a person of any importance, then you should pay special attention for spear-phishing emails. It's best to verify the authenticity of any such message before clicking anything. The best practice is to just not click links or open attachments in emails. If you must, do so inside a sandbox.

Email protection is similar to browsing protection. Sandboxing (see Section 7.8) and anti-malware software (see Section 7.6) help, but personal vigilance is the primary defense.

4.3 Installed Software

Software contains flaws (AKA “bugs”). The complexity of today’s software makes it nearly impossible to ensure that the software is completely free from bugs. Software bugs that have an impact on security are known as vulnerabilities. These vulnerabilities can be exploited in different ways, the worst of which allow complete and total access to, and control of, your system(s). It is critical to remain up to date with security patches, as unpatched software vulnerabilities are entry points into your systems.

An attacker that can get you to install or run a malicious application (downloaded via email attachment, hyperlink, etc.) can do almost anything they wish to your system including establishing a backdoor to access your system remotely, with complete and total access and control. How would anyone even know or detect such activities? Detection of such activities can be accomplished through the use of intrusion detection and prevention systems (IDS/IPS) that can spot known malicious

traffic. Security information and event monitoring systems (SIEMs), that are essentially elaborate intrusion detection systems, can also be used for enhanced alerting, monitoring and correlation of device logs, including monitoring for communication with known malicious hosts. “Honeypots” can be used on your network to lure attackers to attack the honeypot, instead of your actual important systems, and provide you notification. These topics are covered in more depth in Section 7.10.

The following are the most important practices when it comes to securing your software:

- Minimize the number of software vulnerabilities you may have by minimizing the amount of software you have installed - ideally limit installations only to the software you actually use.
- Since all software has flaws it is important that the developer is actively patching any vulnerabilities discovered - ideally only use software that is actively supported by the developer.
- Since vulnerabilities can be exploited, once a patch is available, it is important to apply the patch to remove the vulnerability - keep your software up to date by adopting a monthly patching schedule.
- Software often contains security impacting configurable options. It is good to understand these options and configure them according to your needs. For example, many people install and use remote desktop software. Some remote desktop software include web server functionality to provide remote desktop capability through a browser. Sometimes, this web server based functionality is enabled by default. If browser-based remote access isn't required, perhaps because the client application is preferred, then the best practice is to disable the web server functionality to remove any

chance that it has vulnerabilities - configure your software to support strong security.

4.4 Hardware

Like software, hardware can also have vulnerabilities. Components like motherboards, network cards, video cards, storage drives, and even processors can have vulnerabilities that allow arbitrary exploitation of the affected system. It's not only computer hardware that may contain vulnerabilities, but also, and especially, network hardware, e.g., routers, WiFi devices, etc.

Using hardware that is supported by the manufacturer helps to ensure that patches will be developed for any discovered vulnerabilities in the hardware. Hardware patches are typically applied by installing the latest version of a device's firmware. Many computer Original Equipment Manufacturers (OEMs) provide a consolidated place to get all the firmware updates for the computer hardware they supply. Sometimes, OEMs provide a web-based portal that provides the latest available firmware when a valid computer serial number is entered. Other times, OEMs provide an application to manage firmware versions. Both options really help make it easier to keep hardware up to date.

When building a computer, however, there likely isn't much help available for inventorying hardware and obtaining patches. In this case, it is recommended to have a list of hardware and the locations on the internet where updates are found. Ideally, hardware is checked for security related patches on a monthly basis, and applicable patches applied.

Of particular concern are home routers. Since this is the primary device securing the home network, it is especially important to have a supported router or firewall connecting the network to the internet and to patch it as soon as possible when security updates are available. It is also very good practice to disable any remote configuration capabilities of the

router and to only allow the router to be configured from a trusted, internal network. Configuring the router to alert on any failed or successful login attempts is also a very good idea. See Section 6.3 for more information on routers and firewalls.

4.5 Malware

Software that has malicious intent is known as malware. It comes in the form of viruses, spyware, and unwanted executable code like Visual Basic (VB) and Powershell scripts.

Viruses have the name because once a system is infected the malware then tries to replicate itself onto other systems, akin to a biological virus. Once a device is infected with a virus, the virus can potentially do anything to the system, e.g., deleting or corrupting data, leaking data to a remote server or providing backdoor access to the infected systems.

One of the most pernicious types of malware today is ransomware. This type of malware is contracted like any other malware, e.g., clicking the wrong link in an email or on a website, opening an attachment in an email, installing a malicious application, remote system compromise, etc. Once infected with ransomware, the infected system's drives are encrypted, and the only way to (potentially) decrypt them is to pay a ransom to some bad actor for a decryption key. The bad actors may extort you further to not release your data in some revealing manner. Avoiding ransomware requires all the good computing hygiene practices previously discussed in this section. Additionally, it is recommended to use malware protection software, and to enable malware protection capabilities of your router or firewall, if available. Although popular at one time, dedicated ransomware protection software is no longer a prevalent option. Today, ransomware protection is mostly included as part of antivirus software packages.

Depending on the type of ransomware infection, there may be software tools available to decrypt drives encrypted by ransomware, but it is best to assume the data will be lost, and to rely on backups. Having good backup practices helps to ensure that a copy of the data is available, even in a ransomware attack.

In the event of a virus infection, system operation may be compromised. Anti-malware software or other tools and techniques may be able to help mitigate the impact of a virus. However, it may be best to recover infected systems from a known good backup, or wipe them clean and rebuild from scratch, to help ensure that systems are virus free. This may feel like a daunting task, but with good backup practices it really is the best option. A good backup system includes backing up not only important data, but all necessary software installation files, backed up application data, configuration information, and license information, in order to be able to perform a full recovery.

For important or critical operational environments, having spare hardware on hand in the case of a recovery is important as well. In these environments, a full recovery may require a staged, and very likely painful, process to fully restore the operation. In these environments, it is also wise to test the integrity of the backup data on a frequency as well. Backup files that are corrupt are no help in a recovery. The best way to test the backup data is to attempt to use the backed up data as it is intended to be used. In a test environment, install the installation files, restore the application data and configurations into their test installations, and access the licensing information to verify it will function. This is a lot of work. Mission critical environments will typically undergo such a process annually.

4.6 Internet-of-Things Devices

Internet-of-things (IoT) devices are “things” that are connected to the internet and include appliances, cameras, security devices, sensors, lights and light switches, actuators (switches, levers, etc.) and smart TVs among many other things.

IoT devices present a security challenge as they are often made to be as inexpensive as possible and security may be overlooked or sacrificed. Many times, these potentially insecure devices are placed on the main WiFi network, which can provide a foothold for attackers into the network.

Unless deliberately designed with a security focus and configured properly, IoT devices should probably be treated as potentially hostile devices and isolated from important systems and data.

4.7 Mobile Devices

In this book, the term “mobile device” refers to portable, handheld and relatively small computing devices, e.g., smartphones, tablets, Chromebooks, iPhones, iPads, e-readers, etc. Such mobile devices typically have an operating system that enables them to provide sophisticated functionality. Today, in North America, the most prevalent mobile device operating systems are iOS and Android.

The security of mobile devices is largely in the hands of the manufacturer. Both Android¹ and iOS² have extremely strong security mechanisms built into them. Surely, they both can be used in insecure ways, but fundamentally they are extremely secure operating systems.

1 See <https://services.google.com/fh/files/misc/android-security-paper-2024.pdf>

2 See https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf

For many years, from a security perspective, iOS had a few security advantages over Android:

- iOS has a smaller global user base than Android making it less attractive to attack
- iOS is a closed, tightly controlled platform, a so-called “walled garden,” making it more difficult and less attractive to attack
- The only way to get software onto iOS (without “jailbreaking” it) was via the iOS App Store

However, Apple was compelled by the European Union’s (EU) Digital Markets Act (DMA) in 2023, to allow sideloading of apps on iOS in the EU, which Apple also makes available to other countries. Shortly after Apple was compelled to allow sideloading, in an interesting and somewhat surprising turn of events, in August 2025, Google began to pull back on Android’s fully unrestricted sideloading capability for the security benefits. As of this writing, Google is tightening controls around sideloading and requiring a lengthy process to be executed to allow sideloading in Android. Ultimately, sideloading is now available on both platforms, but you have to be deliberate and pretty determined to use it.

That said, as of this writing, once executing the sideloading enable process in Android, it allows you to install apps from unverified developers. Whereas, iOS doesn’t allow just any old app downloaded from the internet to be installed. iOS only allows for sideloading of apps via alternative “App Marketplaces” that are required to meet certain requirements¹, including notarization and a letter of credit for a minimum of €1,000,000.

1 See <https://developer.apple.com/support/alternative-app-marketplace-in-the-eu/>

Regardless of how an app is sideloaded, a sideloaded app may undergo no security scrutiny at all, and very well may be malicious. Use extreme caution when sideloading apps. There are virus scanners available for Android and iOS that can scan apps before installation.

For mobile devices, the same principles discussed earlier for maintaining computer software security apply:

- minimize apps installed
- only install apps that are actively supported by the developer
- keep apps up to date
- configure apps as securely as possible

Another way of inadvertently installing malicious software is via phishing and spear-phishing attacks. Like computers, email opened on a mobile device carries the same risks with respect to clicking links and opening attachments. Mobile devices have a couple of additional way to be phished, known as “smishing” and “vishing”. Phishing links and attachments may arrive via text message. These are known as Smishing attacks. Here again, don’t click links or open attachments, especially from phone numbers you don’t recognize. Don’t do it! Just DON’T!!Vishing is a voice focused attack that uses a phone call and social engineering to trick a victim into divulging sensitive information.

While extremely secure, mobile devices present a potential stomach churning smorgasbord of privacy concerns. Depending on what applications and options are used, some or all your privacy may be relinquished. This includes pictures, videos, location, likes, preferences, search history, purchase history, app usage, personal information, health information, metadata, the list goes on. There are excellent, privacy respecting, alternatives for many of the popular, but more privacy offending applications.

You can improve your privacy by leaving all of the privacy offending apps off of your mobile device and only using or accessing them from a computer inside your home or from some minimum number of fixed locations. In this way you maintain no persistent connection to the app's servers and your constant feed¹ of data isn't available.

Our data is valuable, both from personal and collective society perspectives. Questions to consider when you engage with privacy offending applications and services are:

- What data are you giving away?
- What are you receiving for your data?
- What does giving your data away cost you personally?
- What does us all giving our data away cost society at an aggregated level?
- Is it a good deal? Is it worth it?

4.8 Social Engineering

Sometimes when attackers want information they will try to extract it from you by communicating with you directly. Attackers may attempt to contact you using any of the forms discussed earlier in this section including by email, SMS, attracting you to put data into a web page or even a direct phone call. Usually these types of attacks would be used to obtain some kind of obviously dangerous type of information disclosure like your username and password, a credit card number or account number, possibly even your social insurance number.

The only defense against this type of attack is personal vigilance. Be extremely cautious giving any personal information to anyone, especially those asking for it

1 See <https://www.techadvisor.com/article/743868/these-popular-apps-collect-the-most-data-about-you.html>

unsolicited. NEVER GIVE AWAY YOUR PASSWORDS, PASSPHRASES OR PIN CODES. EVER. PERIOD. The administrators of any of the systems you log into will never require your password to administer your account. Giving your password to them would only allow them or someone else to impersonate you.

4.9 Denial of Service and Distributed Denial of Service

Denial of service (DoS) attacks come in many different flavours, but they revolve around overwhelming system resources to the point where they fail or become unusable. A DoS attack on a computer could cause it to simply load its processor to 100% until it overheated. A DoS attack on a web server might involve overwhelming it with web requests or malformed web requests to the point where it exhausts its resources and becomes unavailable. Distributed denial of service (DDoS) attacks involve coordinating numerous computers (hundreds, thousands, hundred of thousands...) on the internet to attack their target(s), at once.

Preventing DoS attacks on individual systems requires a broad combination of the best practices covered in this chapter notably:

- only install and run trusted and supported programs
- only run trusted mobile code (shell commands, scripts, executable files)
- apply security patches in a timely fashion
- configure access and applications securely
- close unnecessary logical ports
- Avoid malware and use anti-malware software
- Don't click links or open attachments in emails, etc.

Avoidance of DoS is very important for mission critical systems. It isn't as pertinent to home users, but could be for small businesses running systems critical to their operations.

Mitigating DoS attacks on web servers is difficult. The average person running web servers on their home network would not expect to see a DoS attack against their systems, but if they did, there isn't anything that can really be done locally. However, there are external DDoS protection services available that will filter internet traffic before arriving at your systems, such as CloudFlare, Akamai, AppTrana, Link11, and more. Use of a DDoS protection service will help ensure that your web server will remain usable if a bad actor launches a DDoS attack on it. The DDoS protection service filters DDoS web requests from ever reaching your web server. In turn, your web server will not be overwhelmed with requests and remain functional.

Businesses running systems on the internet that are critical to their business wouldn't want to suffer a DoS or DDoS attack. Traditionally, all that could be done was to provision more bandwidth. Businesses can use external DDoS protection services to pre-filter DoS and DDoS web traffic.

4.10 Survey of Hacking Tools

This section provides a brief survey of common, widely-available hacking tools. The list is not exhaustive, but rather is meant to convey a sense of the power and breadth of hacking tools available, all of them free (keeping in mind that most of these tools are only available to run on GNU Linux).

Tool	Description
Aircrack	A package of utilities for cracking (exposing the encryption keys of) 802.11a/b/g WEP and WPA WiFi networks. Aircrack contains algorithms that allow the user to recover WiFi encryption keys once enough encrypted packets have been

	gathered. The keys can then be used to connect to the WiFi network. Using this type of tool, a nosey neighbour or legitimate local attacker could collect your WiFi traffic undetected for long enough to crack your WiFi password and join your network.
Burp Suite	An integrated platform for attacking web applications. Burp Suite contains several tools with integrations between them for facilitating and speeding up the process of attacking a web application.
Cain & Abel	An extremely powerful, but Windows only password recovery tool. Cain & Abel can recover passwords by network sniffing, dictionary attack, brute-force attack, cryptanalysis attack, recording of VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols.
Ettercap	A suite for facilitating man-in-the-middle attacks on local area networks. Allows for sniffing live connections and content filtering on the fly, among other interesting capabilities. Active and passive dissection of many protocols is supported and features for network and host analysis are available.
John the Ripper	A popular and powerful password cracker.
Kali Linux	The GNU Linux distribution preferred by hackers and security professionals. Kali Linux comes pre-configured with many popular hacking and security related tools.
Maltego	An open source intelligence and forensics

	application. Maltego provides an interface for mining, gathering and visualizing information.
Metasploit	An advanced, flexible, open-source platform for developing, testing, and deploying exploit code used for exploitation research. Metasploit comes with hundreds of exploits.
NIKTO	Nikto is an open source web server scanner that can perform comprehensive tests against web servers for vulnerabilities including, at the time of this writing, checks for over 6400 potentially dangerous files or common gateway interfaces (CGIs), outdated versions for over 1200 servers, and version specific issues for over 270 servers. It also checks for server configuration problems such as presence of multiple index files and poorly configured server options. It will also try to identify installed web servers and software.
Nmap	An extremely popular, open source, multi-platform host and port detection and scanning utility.
OWASP ZED	An open source web application scanner that provides an automated framework for performing numerous tests against web applications, used for identifying potential vulnerabilities. This tool also provides the ability to craft and execute manual tests against target web applications so that the penetration tests can be fine tuned.
Shodan	An online platform that crawls the web looking for accessible services on web servers web and makes them searchable via a website.
Sn1per	The most advanced automated information gathering and penetration testing tool. Sn1per runs on GNU Linux and uses many of the other

	well known hacking/security tools to accomplish its tasks.
THC Hydra	Another tool that is typically run on Kali Linux. THC Hydra is a login cracker that attacks numerous protocols. It can perform rapid parallelized dictionary attacks.
Wireshark	An open source, multiple platform, protocol analyzer and network packet sniffing tool. Supporting hundreds of protocols, Wireshark allows you to capture packets on the network and perform deep packet analysis of the traffic.

Table 2: Hacking Tools

5

Computers

Computers were the first general purpose digital devices that people of the 1980's through the early 2000's were exposed to. Today, most people will likely first encounter a mobile device. Nonetheless, many of us, in the support of our educational and professional activities, as well as our private and leisure activities, will use a computer.

The various computer options and pertinent considerations are explored below. Figure 3 shows the components of a typical PC.

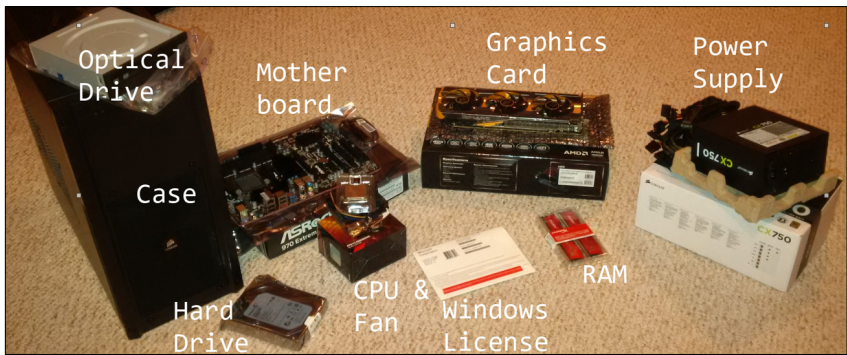


Figure 2: Components of a typical PC

5.1 Hardware

As with many things, the best approach to buying a computer depends on what you want to do with it and what you want to

get out of it. The type of computer you purchase is consequential to your cyber security and privacy.

Today, the computing options available to home users and small businesses largely remain the same as they have for many years, that being the choice of a Windows, GNU Linux or Apple laptop or desktop computer, or a Windows or GNU Linux server. Mobile devices that approach the functionality of a traditional computer include so-called “Chromebooks”, Android tablets and Apple iPads.

Mobile devices usually don’t provide the same level of computing power that a traditional computer does, but they do have some distinct advantages over mainstream OSes including:

- excellent and easy to maintain security by default
- many low cost options
- device usually has a long battery life
- device usually includes a touch screen
- ease of maintenance

An option for the ambitious home or small business user is to deploy Windows or GNU Linux on server, which is typically a different “form factor” than a desktop or laptop computer. Often referred to as a “pizza box,” such a server is usually 19 inches wide (so that it can be mounted in a 19 inch rack, commonly used in information technology (IT) environments) by approximately 21 inches in depth, and a height of 1.75 to 3.5 inches. A previously used server may be a very cost effective method of obtaining serious computing power as servers are made to provide exactly that. Servers typically include multiple CPUs and huge amounts of RAM and storage space.

Windows PCs, whether desktop or laptop, are a traditionally popular choice. Buying a Windows desktop or laptop opens up a very large market of hardware options. From building a desktop yourself from components, to purchasing a pre-built desktop,

the options are vast. Historically, and to this day, the laptop market has only presented pre-built options, but there are movements looking toward open hardware standards and designs for laptops¹. The trend, however, in laptop demand is for thinner and more power efficient devices, which most likely will not come from open, adaptable designs.

Building a desktop computer yourself is a rewarding experience for those looking to squeeze the most power for the least cost. However, a custom built PC requires a bit more effort to keep it completely up to date from a security perspective. On the other hand, buying a pre-built PC is probably a bit more expensive, and may be more restrictive in terms of future upgrade options and compatibility, but may provide a more stable experience, and simplified options for maintaining security updates. Important hardware components to consider when purchasing a computer are described in Sections 5.1.1 to 5.1.10 below.

5.1.1 *Motherboard*

The motherboard is the component that ties everything together. It is a very important component, and when buying one to build a PC, you will want to make sure that it has all of the capabilities that you might need, now and into the future. A motherboard is where you might want to spend a little more for quality, compatibility, options and features. A typical motherboard is shown in Figure 3.

¹ See <https://mntre.com/> for example.

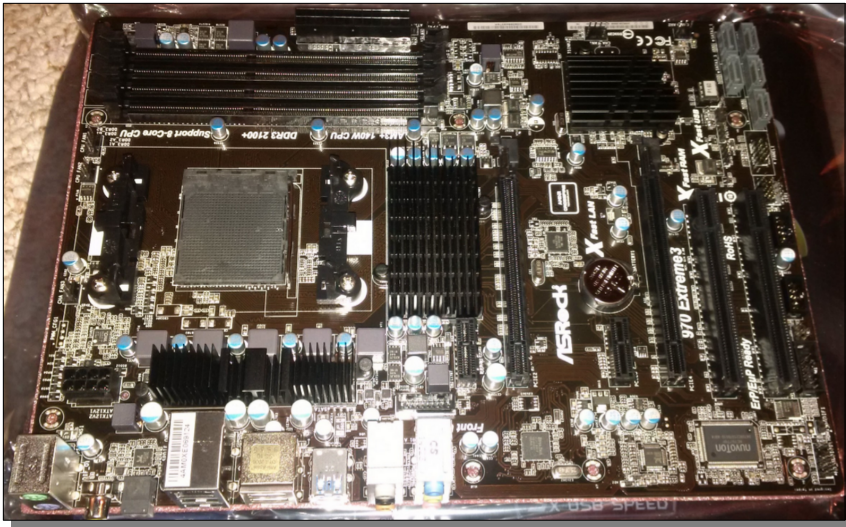


Figure 3: Components of a typical PC

5.1.2 Central Processing Unit (CPU)

The central processing unit (CPU), AKA the processor, is the “brain” of your computer. Generally, the faster the CPU clock speed the faster the processor, but not always. Different processor “architectures” process data differently, which can impact the processing throughput at a given speed. In general though, a faster processor means faster processing, simple enough. Multi-core processing is another story.

Multi-core processing introduces the idea of parallel processing using multiple CPU cores instead of a single CPU core. Applications optimized for parallel processing can achieve a performance boost. However, applications that are not optimized for parallel processing or aren’t conducive to parallelization may actually see performance reduction on multi-core CPUs compared to single core CPUs. This is due to the fact that, for some years, individual CPU cores of a multi-core CPUs were each significantly slower, compared to a faster single core CPU. Today, many applications are optimized for parallel processing and per core processor speeds are such that

it's less of a concern for those applications that aren't optimized for parallel processing. Bottom line, in general more speed and more cores equals faster processing.

The other thing to consider is the amount of cache memory on the processor. This is the fastest memory in your computer and having more of it available to the processor improves performance significantly. This is usually one of the main factors driving the price of the processor.

The processor is one of the more expensive components of the computer and it makes sense to look for a processor's performance to match that of your computing needs, unless money is no object. Then just go for the fastest processor, with the most cores and cache memory. But expect to pay accordingly.

When building a PC you'd want to make sure to match the CPU specifications to that of your motherboard and vice-versa. Motherboards are made for particular CPUs and the combination is made for particular RAM speeds, so it's advisable to pay attention to these factors and select a motherboard, processor and RAM combination that matches and meets your needs.

A few older CPUs are shown in Figure 4.



Figure 4: Older Central Processing Units

5.1.3 Random Access Memory (RAM)

After cache memory, RAM is the next fastest memory in your computer. Having more of it means that you can run more programs at the same time and run more RAM intensive programs smoothly. Not having enough RAM can force your computer to use your system drive as if it were RAM (known as “Virtual Memory”), which is much slower. For good performance it is important to have enough RAM to serve the applications that you need to run at the same time. In general, today, the minimum recommended amount of RAM for a Windows, GNU Linux, or Mac, desktop or laptop is 8 GB. Operating with 8 GB of RAM for a modern operating system with a moderate application load is probably comfortable, where 16 GB of RAM is probably a nice experience for most applications. No one ever said, “I have too much RAM”.

Some applications are extremely RAM intensive, such as video processing applications, video games, engineering applications, Geographical Information Systems (GIS), Digital Audio Workstations (DAWs), virtual instruments and samplers.

A typical “stick” of RAM is shown in Figure 5.

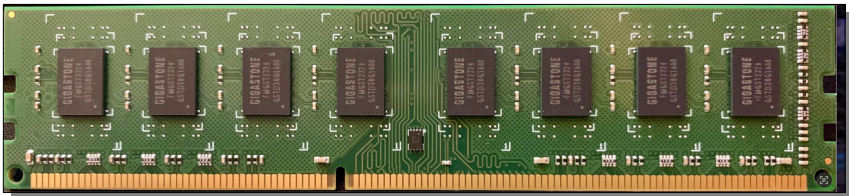


Figure 5: Personal Computer Random Access Memory

5.1.4 Drives

Drives are typically the slowest form of memory and are expected to hold data permanently. Throughout the years, drives have been available in a few technologies, form factors and interfaces. From a technology perspective there has been the following:

Hard Disk Drives (HDDs) - electromechanical devices comprised of magnetic rotating platters. Digital data is written to and read from the disk by a read/write head controlled by a disk controller. Hard disk drives are still quite common as they are inexpensive and can be made to be quite reliable.

A typical HDD is shown in Figure 6.



Figure 6: 3.5" Hard Disk Drive

Solid State Drives (SSDs) - electronic storage devices that store and retrieve digital data electronically through the use of semiconductors. SSDs are typically implemented using non-volatile flash memory. SSDs are much faster, more stable and shock resistant than hard disk drives, but cost more.



Figure 7: 2.5" Solid State Drive

Both HDDs and SSDs are available in 2.5" and 3.5" formats. Historically, desktop computers and servers have been supplied with 3.5" drives, while laptop computers have been supplied with 2.5" drives, though desktops and servers can certainly accommodate 2.5" drives.

HDDs have been around long enough that they've seen a few different types of interfaces. Some of the older ones included the "Industry Standard Architecture" (ISA) and "Integrated Drive Electronics/Parallel Advanced Technology Attachment" (IDE/PATA) drive interfaces for desktop and laptop computers. The "Small Computer System Interface" (SCSI) was the most common hard drive interface for servers. Since about 2003, HDDs have used the "Serial Advanced Technology Attachment" (SATA) drive interface for desktops and laptops. Since about 2005, "Serial Attached SCSI" (SAS) has been used for servers.

At the time of this writing it is common for laptop computers to be supplied with SSDs that are greater than 1 TB in size. HDDs are commonly 3 TB in size or greater.

5.1.5 Graphics Card

A computer's graphics processing unit (GPU), AKA graphics card or video card, determines how much video processing it can do and at what rate. Video cards can come integrated with the motherboard, known as onboard or integrated video (iGPU), or as a separate dedicated video card, known as a discrete or dedicated video card (dGPU). Sometimes iGPUs and dGPUs can be used in parallel to display on multiple screens simultaneously, but not always, it depends on the features of the of the cards. Some dGPUs also support the ability to work together with other dGPUs to display on multiple screens, but again it depends on the features of the cards.

Relevant settings for iGPUs and dGPUs are found in the motherboard's BIOS settings, as well as in the driver software for the graphics card. It is important to use the correct driver software for your graphics card. Often, the operating system will install and use a generic graphics card driver that will work, but will not provide all of the features that your discrete graphics card offers.

Integrated graphics cards are usually pretty limited. They will typically have enough power to play movies and basic videos games, but not much more than that. In order to play modern video games or process significant video content, a dGPU is usually necessary.

The considerations for selecting a dGPU are similar to selecting a CPU. Faster is better and more memory is better. Here again, it makes sense to scale your purchase with your needs, unless money is no object. Then go big! When purchasing a dGPU, since it is one of the more expensive components in a computer, and since many options are available, it makes sense to do a fair amount of research to select the right one.

Modern discrete graphics cards require a PCIe port on your motherboard. Any motherboard you can purchase today probably supplies a PCIe port, but you'd want to ensure

compatibility before purchasing your motherboard and dGPU. You'd also want to ensure your dGPU supports the number of screens that you need to connect and has the types of connectors you need.

An older (but powerful for its time) graphics card is shown in Figure 8.



Figure 8: PCIe-Based Dedicated Graphics Card

5.1.6 Sound Card/Audio Interface

The most basic function of a computer's sound card is to connect the computer to physical speakers to play sound. Like graphics cards, audio cards can be integrated with the motherboard or they can be dedicated. Audio cards can also be external. External audio cards are often referred to as "audio interfaces".

Today, there are many excellent USB 2.0 and Thunderbolt external audio interfaces available. Previously, IEEE 1394/Firewire based external audio cards reigned supreme, but these are now largely obsolete.

Audio cards, integrated, dedicated and external alike, often contain input ports in addition to their output ports. Here again, it makes sense to scale your purchase with your needs.

Do you require an input? Will an eighth inch stereo jack computer microphone input be sufficient or do you require

something with a different input or higher recording fidelity? Will a USB mic work for you? If the onboard audio inputs, outputs or recording/playback fidelity don't meet your needs then look for an external audio interface. Audio interfaces range in quality and functionality. Typically, audio interfaces are used for recording musical instruments such as microphones, guitars, pianos, drums, etc. Audio interfaces can come with several input and output options along with the ability to record a certain number of audio channels simultaneously, ranging from one channel to 24 or 48 channels or more, priced accordingly.

The average user can usually easily be satisfied with their integrated sound card. Recording musicians and other sound hobbyists and professionals likely require an external sound card.

A USB audio interface is shown in Figure 9.



Figure 9: USB Audio Interface

5.1.7 Interface and Communication Ports

It is important to consider what kind of ports and communication options you require. USB 3.0 and USB-C ports are required by most users today. Additionally, most users probably need Bluetooth. Every laptop and mobile device will come equipped with WiFi. Desktop users should consider whether WiFi is required and if so, look for whether it is built into their motherboard or CPU. If WiFi is required, but is not built into your desktop computer then there are WiFi adapters available that can be connected via USB, PCI or PCIe.

It's also important to consider the video connectors you need. The standard option today is an HDMI port, but some graphics cards for desktop and laptop computers may come with other options. Commonly, these are “DisplayPort” and “mini-HDMI”, both related to HDMI, but may require an adapter to connect to your monitor or television.

A listing of common interface and port options to consider, grouped by device type, is provided below.

5.1.7.1 Disk Drive Interfacing

M.2: State of the art (at the time of this writing) port and connector for interfacing laptops and desktop computers with Non-volatile Memory Express (NVMe) SSDs.

PCIe: A standard port included on desktop computer and server motherboards that allows interfacing with high-speed devices like some NVMe SSDs (the PCIe “Add-In Card” type) as well as graphics cards and high-speed networking adapters. Be mindful of the X4, X8, X16 bandwidth lanes when selecting a motherboard and NVMe drive to ensure compatibility.



Figure 10: PCIe and PCIe 16x Connectors

mini-PCIe: A more compact form of PCIe that is used mostly in laptops and tablets to connect WiFi cards, SSDs, and cellular network cards.

SATA: A very common SSD interface available in most desktop computers, servers, and laptops

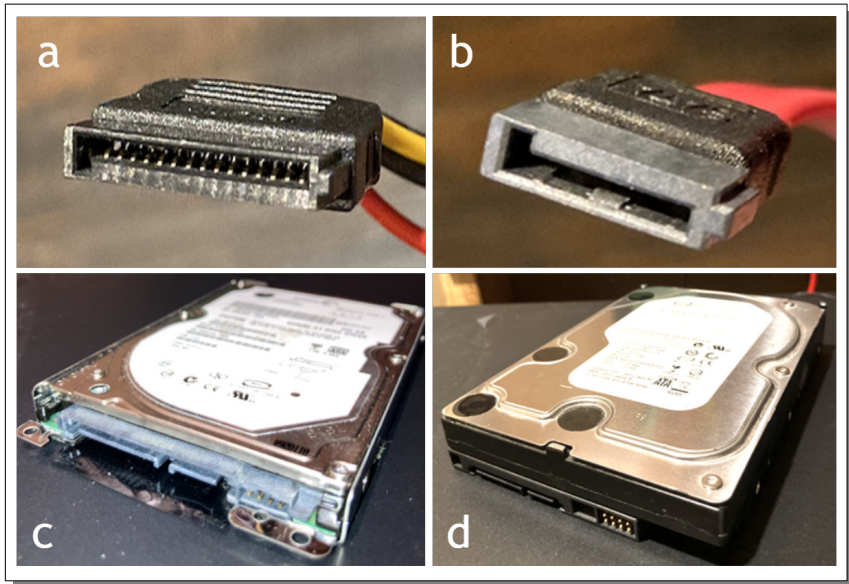


Figure 11: SATA Connectors

(a) SATA Data Connector; (b) SATA Power Connector; (c) 2.5" Hard Drive; (d) 3.5" Hard Drive

mSATA: mini-SATA, a more compact version of the SATA interface used with drives that are also physically smaller than SATA drives.



Figure 12: 2.5" mSATA SSD Seated in mSATA Slot

eSATA: An older, and now practically obsolete, interface for connecting supporting drives to supporting computers. With a transfer rate of 300 MB/s, eSATA allows for faster data transfers than USB 2.0 (35 MB/s), but slower data transfers than USB 3.0 (625 MB/s).

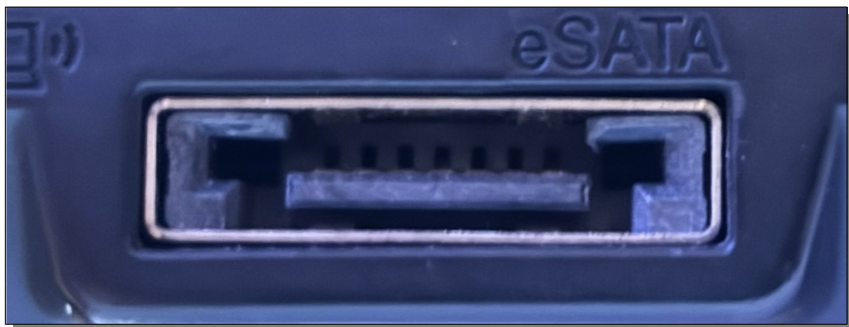


Figure 13: Female eSATA Connector

5.1.7.2 Display Interfacing

HDMI, mini-HDMI and micro-HDMI: Probably the most common video interface at the time of writing. This cable and interface also carries the audio signal and can carry an Ethernet signal as well, known as HDMI Ethernet Channel (HEC).

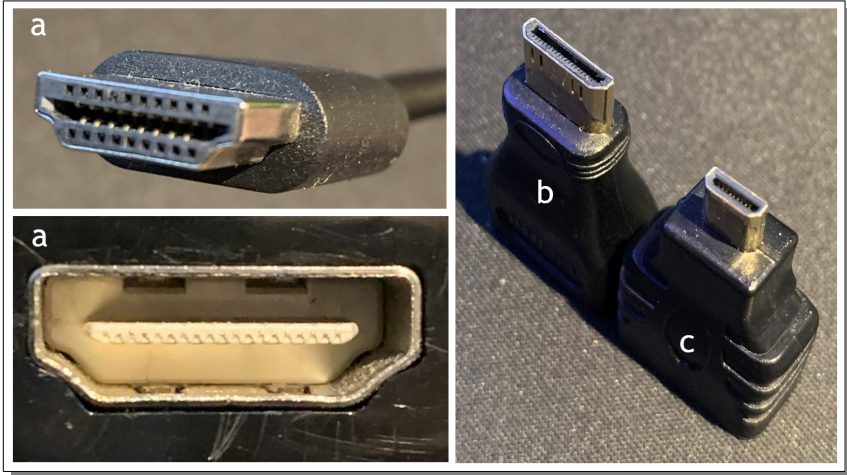


Figure 14: HDMI Connectors

(a) HDMI Connectors; (b) Male Mini HDMI Connector; (c) Male Micro HDMI Connector

DisplayPort and mini-DisplayPort: DisplayPort is commonly supplied on graphics cards for desktop computers, while mini-DisplayPort is sometimes supplied with laptops. This cable and interface also carry the audio and Ethernet signals, known as DisplayPort Ethernet Channel (DPEC). DisplayPort is also compatible with HDMI and vice versa.

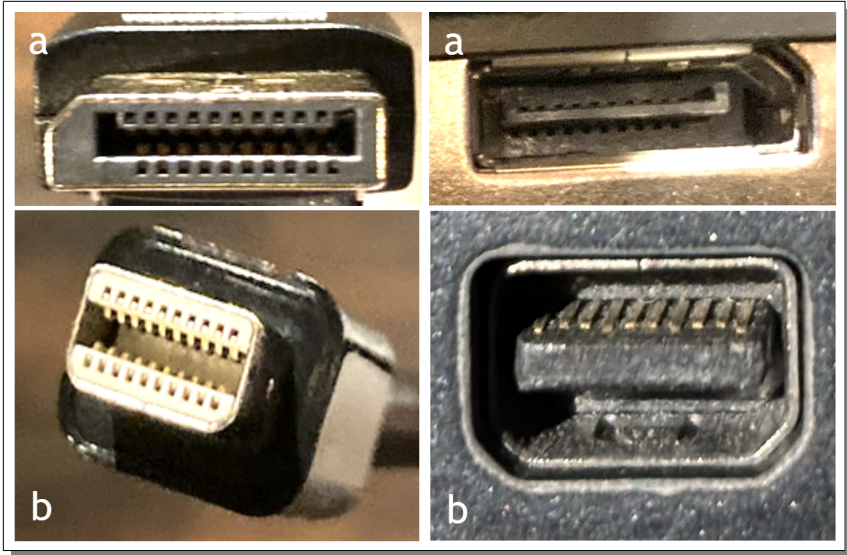


Figure 15: DisplayPort Connectors

(a) DisplayPort Connectors; (b) mini-DisplayPort Connectors

Digital Visual Interface (DVI): DVI is an older type of video cable and connector for connecting computers to supporting monitors and televisions. DVI-A is a fully analog version of DVI. DVI-I supports both digital and analog video, while DVI-D is digital video only. The various DVI types have similar, but different connectors.

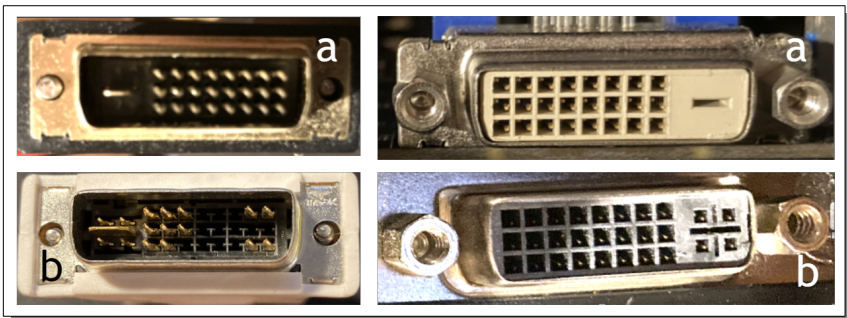


Figure 16: (a) DVI-I Connectors; (b) DVI-D Connectors

Video Graphics Array (VGA): An older, but still ubiquitous, analog display port for connecting computers to monitors. VGA is still very commonly included with the “onboard” graphics on desktop computer motherboards. Many monitors also continue to support it.

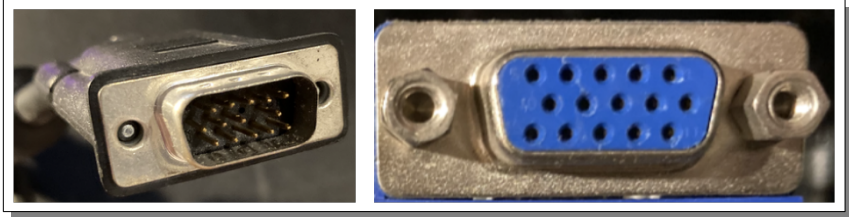


Figure 17: VGA Connectors

RCA, S-Video, Composite Video, Coaxial, and Other Older Video Formats: Older types of audio and video interfaces that are still somewhat in use, but require specialized video hardware, such as a so called video capture card, to interface directly with a computer.

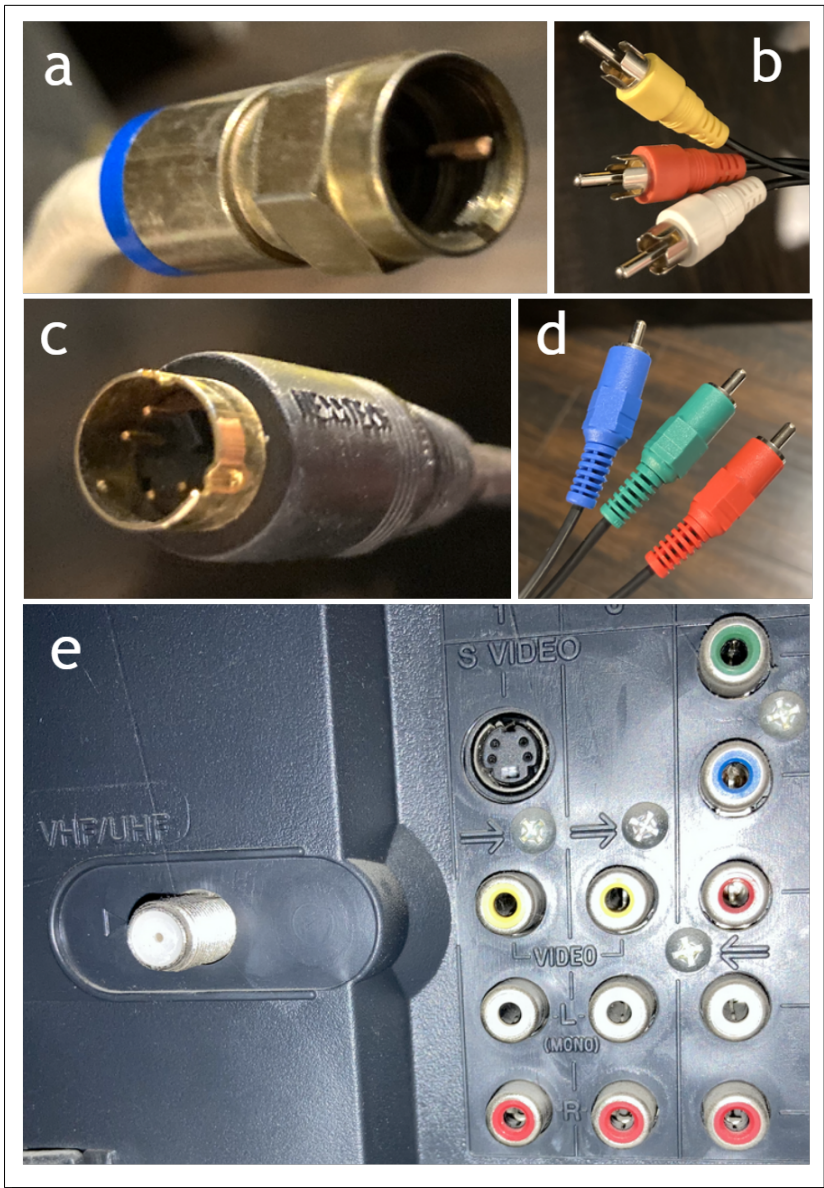


Figure 18: Older Media Connectors

(a) Male Coaxial Cable Connector; (b) Male RCA Connectors;
 (c) Male S-Video Connector; (d) Male Component Video
 Connectors; (e) Television Input Panel with Female
 Connectors of (a) to (d)

5.1.7.3 Integrated Audio & External Audio Interface Interfacing

1/8" Headphone Output: A standard port and connector for connecting analog headphones or powered-speakers to a computer or mobile device. Today, many people opt to use bluetooth headphones, but a good old 1/8" headphone output is still used in professional audio applications, or just to connect older headphones.

1/8" Microphone Input: A standard port and connector for connecting a microphone to a computer. Allows for the analog connection of a microphone, though today most serious applications will use a USB-based microphone or a higher end microphone connected via an audio interface.

1/8" Line Input: A standard port and connector for connecting a line input device, like a pre-amplifier or a digital keyboard's analog output, to a computer.

Typical 1/8" inputs and outputs used with computers are shown in Figure 19.

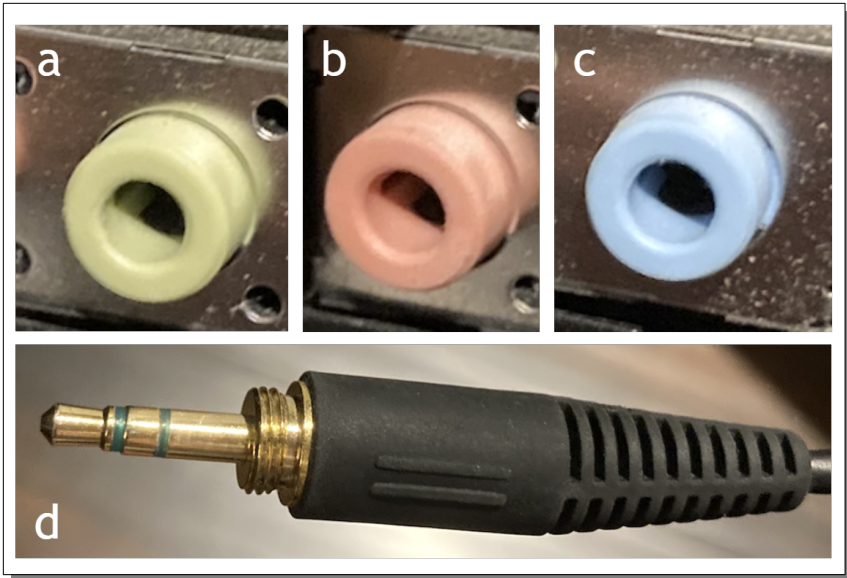


Figure 19: 1/8" Inputs and Outputs

(a) Computer Headphone Output; (b) Computer Microphone Input; (c) Computer Analog Line Input; (d) Headphone Jack

USB or Firewire Audio Interface: A device to expand audio interfacing options, such as 1/4" XLR line and instrument inputs with pre-amplifiers, 1/4" speaker outputs, SPDIF, and RCA audio connectors, 1/4" headphone outputs and more. Audio interfaces today usually connect to a computer or mobile device via USB 2.0 or USB-C.



Figure 20: USB Audio Interface



Figure 21: Audio Connectors

(a) 1/4" Audio Jack; (b) Male XLR Connector; (c) Male and Female MIDI Connectors; (d) Male and Female Toslink Connectors

5.1.7.4 Radio-based Communication Interfacing

WiFi: The standard wireless network interface for computer and mobile device network and internet communications. WiFi is described in more detail in Section 6.15.1.

Bluetooth: A low cost and low power radio network that operates in the 2.4 to 2.4835 GHz unlicensed frequency band. Bluetooth allows devices to communicate wirelessly by creating an ad hoc "Wireless Personal Area Network" (WPAN), known as a piconet. Bluetooth is described in more detail in Section 6.15.3.

NFC: A WPAN that enables slow, but reliable, and secure communication between two supported devices that are within a very short distance from each other (typically ~2 cm or less). NFC is described in more detail in Section 6.15.6.

5.1.7.5 Wire-based Communication Interfacing

Ethernet CAT5+ Cable with RJ-45 Connector: Physical connection to an Ethernet network, common for computers, laptops, servers and other types of devices like printers, video cameras, point-of-sale (PoS) devices, etc.

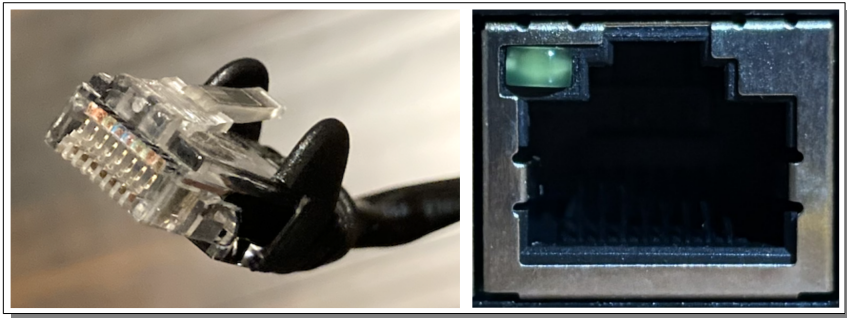


Figure 22: RJ-45 Connectors for Ethernet Cable

Telephone/Fax CAT3 Cable with RJ-11 Connector: A very old technology that is still used for traditional phone land lines. A resilient technology that facilitates communication even when utility power is lost. Still used by some folks that need to send a fax, although faxes can be sent over Voice-over-Internet Protocol (VoIP) systems as well.

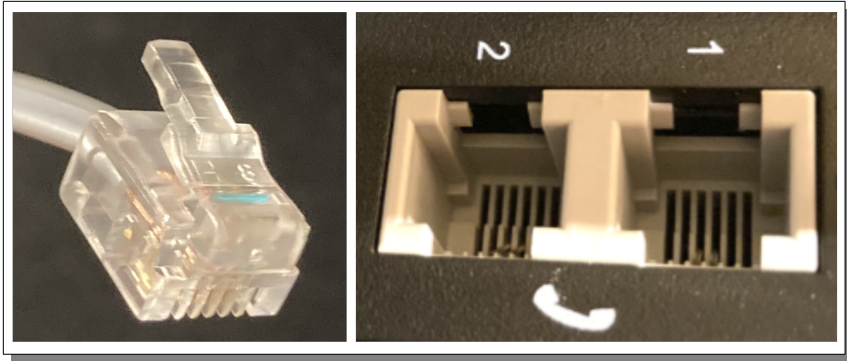


Figure 23: RJ-11 Connectors for Telephone Cable

Serial Interface: An older communication system that is still used to communicate directly with networking and other types of electronic equipment, usually for configuration purposes. It's unusual today to find a consumer grade computer that ships with a serial port. USB to serial port adapters are available for those that need them. Some manufacturers make robust, industrial grade computers and laptops that still ship with integrated serials ports.

Serial communications require the use of a “terminal” application, like Telnet or PuTTY. Serial communications can be a bit finicky to set up and require paying attention to a number of parameters to set up the serial connection. Configuration of managed switches and other network appliances is often accomplished via serial port using Secure Shell (SSH) protocol.

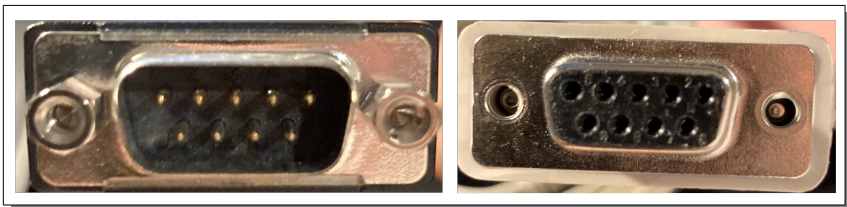


Figure 24: DB-9 Serial Interface Connectors

5.1.7.6 Peripheral Interfacing

Universal Serial Bus (USB): USB has long been the standard interfacing mechanism for peripheral devices including printers, cameras, mobile devices, etc. USB, USB 2.0 and USB 3.0 share the same physical connector at the end of the cable intended for connection to a computer (USB Type-A connector). At the other end of the cable that plugs into the peripheral device is a different type of USB connector. For this peripheral connection, printers typically have employed a USB Type-B connector, whereas smaller devices have employed the USB mini A, mini B, micro A and micro B connectors. USB 3.0 is backward compatible with the previous versions and is what is typically supplied with a new computer or mobile device today.

The various USB versions, speeds, and connectors are listed below in Table 3:

USB Version (s)	Speed	Connector Type(s)
V1.0/V1.1	12 Mbps	Type A, Type B
V2.0	480 Mbps	Type A, Type B, Mini, Micro
V3.0/3.1/3.2 Gen 1	5 Gbps	
V3.0/3.1/3.2 Gen 2	10 Gbps	Type A, Type C
V3.2 Gen 2	2 x 2: 20 Gbps	Type C
V4	20/40 Gbps	

Table 3: USB Versions, Speeds, and Connector Types [Hill, 2022], [Harding, 2022]

Photos of the various USB connectors are shown below in Figure 25.

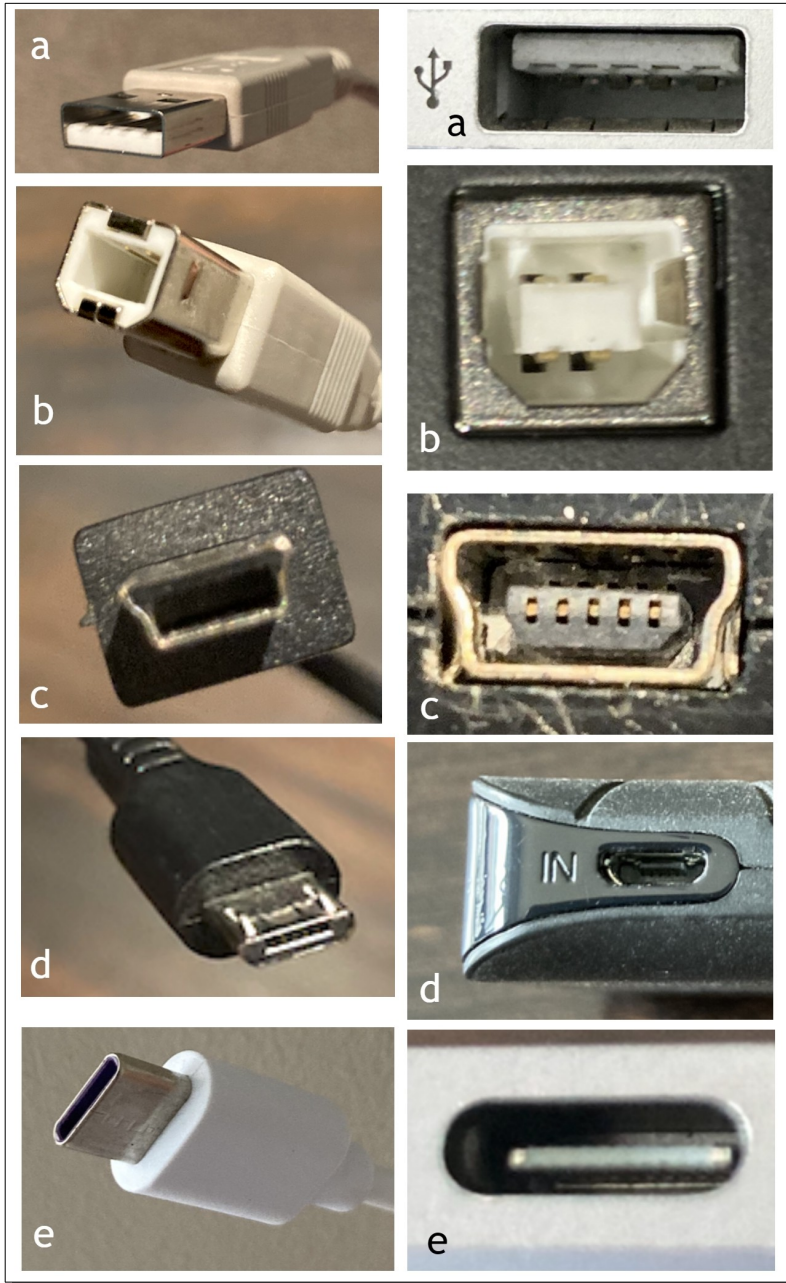


Figure 25: USB Connectors

(a) Type-A; (b) Type-B; (c) Mini; (d) Micro; (e) Type-C

IEEE1394/Firewire: IEEE1394, commonly referred to as Firewire (Apple’s name for it), is a serial bus standard. While quite old now, and essentially obsolete since 2008, IEEE1394 enables high speed data transfer capability and suitability for real-time applications, e.g., real-time virtual musical instruments. IEEE1394 was one of the primary interfaces used to communicate with mini-DV camcorders. Additionally, many of the best audio interfaces of their time employed IEEE1394 to interface with computers. It was a formidable interfacing system for certain.

IEEE1394 has two different connectors, a 6-pin connector and a 4-pin connector. The 6-pin connector is capable of carrying power from the computer to the device. The 4-pin connector does not carry power. Devices that use the 4-pin connector require an external power supply and are usually plugged into the wall using an AC adapter.

The various IEEE1394 versions and speeds are summarized below in Table 4.

IEEE1394 Version (s)	Speed/Duplex
FireWire 400 (S100/S200/S400)	98, 196, 393 Mbps/Half Duplex
FireWire 800	786 Mbps / Full Duplex
FireWire 800T	800 Mbps / Full Duplex
FireWire S1600	1.6 Gbps / Full Duplex
FireWire S3200	3.2 Gbps / Full Duplex

Table 4: IEEE1394/Firewire Versions, Speeds, and Duplex [Teener, 2004]

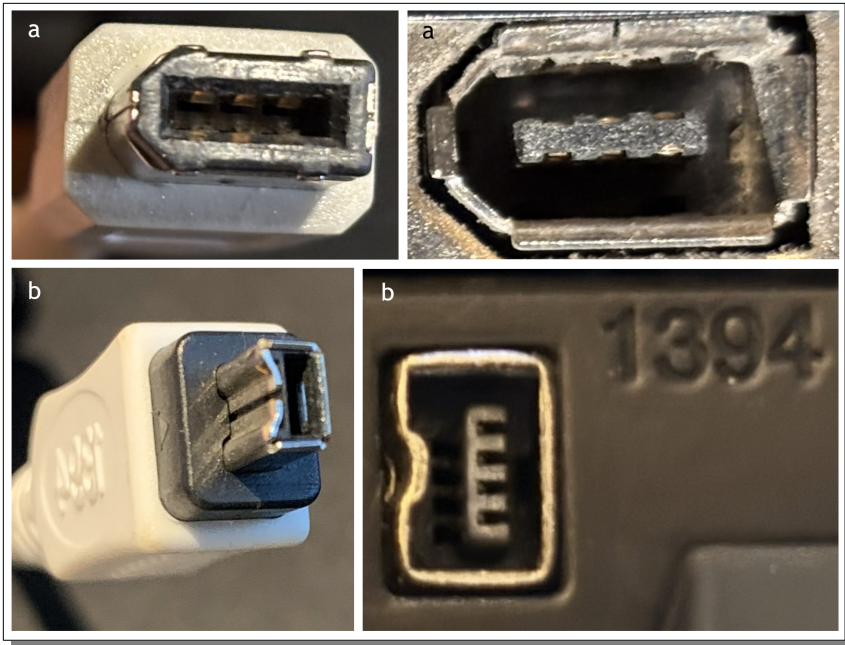


Figure 26: IEEE1394/Firewire Connectors

(a) Type 1 (6 pin); (b) Type 2 (4 pin)

Lightning: The Lightning cable, connector, and port are a proprietary system made by Apple, exclusively for Apple devices. Lightning was introduced by Apple in 2012, for use with the iPhone 5 and by 2018 Apple was transitioning to USB-C. The last Apple iPhone to use Lightning is the iPhone 14 Pro/Pro Max. The last iPads that use Lightning are the iPad 9th generation, iPad Mini 5th generation, iPad Air 3rd generation, iPad Air 2 and iPad Pro 2nd generation. Most Lightning implementations supported USB 2.0 and thus boasted a speed of 480 Mbps. A few iPads came with USB 3.0 capability using the Lightning connector, supporting a speed of 5 Gbps. However, to fully realize this speed, a USB 3.0 camera adapter is required and can only be used with cameras and other peripherals, and not with computers [Apple Fandom Wiki], [Shakir, 2023].



Figure 27: Lightning Connectors

Thunderbolt: Developed by Intel and Apple, Thunderbolt is another type of interface for connecting computers to peripheral devices. Thunderbolt 1 and 2 connectors employed a mini-DisplayPort connector. In addition, Thunderbolt is interoperable with DisplayPort. Thunderbolt 3 and 4 employ the USB-C connector. Thunderbolt versions, speeds, and supported protocols are summarized in Table 5 [Thunderbolt™ Community], [Intel, 2023].

Thunderbolt Version	Speed	Protocol(s)
1 (2 channels)	2 x 10 Gbps	4 x PCI Express 2.0, DisplayPort 1.1a
2	20 Gbps	4 x PCI Express 2.0, DisplayPort 1.2
3	40 Gbps	4 x PCI Express 3.0, DisplayPort 1.2, USB 3.1 Gen 2
4	40 Gbps	4 x PCI Express 3.0, DisplayPort 2.0, USB 4
5	80/120 ¹ Gbps	4 x PCI Express 3.0, DisplayPort 2.1, USB 4

Table 5: Thunderbolt Versions, Speeds, and Protocols

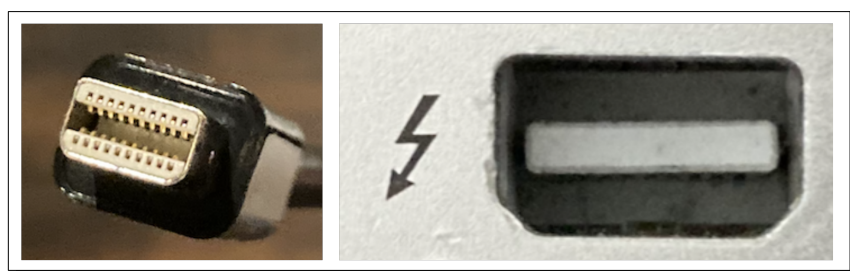


Figure 28: Thunderbolt Connectors

PS/2: The PS/2 interface is a very old, but still commonly supplied, interface for connecting PS/2 keyboards and mice to desktop computers and servers.

¹ Devices with Thunderbolt Bandwidth Boost implemented.

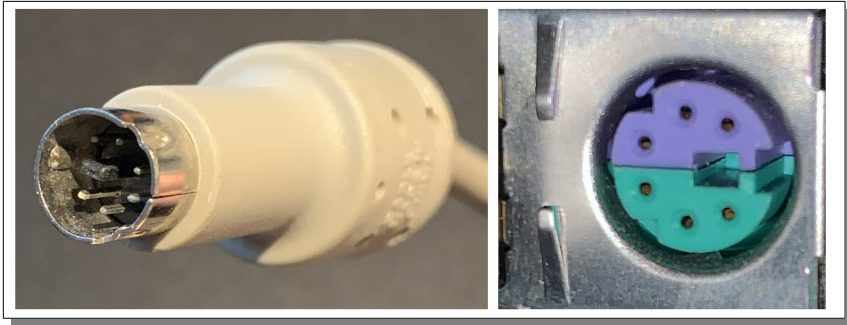


Figure 29: PS/2 Connectors

5.1.8 Monitor

Your monitor is your video interface to your computer, it's a pretty important component. The main things to consider when purchasing a monitor are how large you want the display to be and how high of a resolution you require. Higher resolution means that there are more pixels that make up a given size screen. A pixel is the smallest addressable element on the screen. The smaller the pixel, the more of them fit on the screen. Thus, objects drawn on a higher resolution monitor will appear smaller than the same object drawn on a lower resolution monitor of the same size. This means that higher resolution monitors provide more screen "real estate". That said, even though smaller screens with high resolution allow more content to be displayed, the content may be hard to see. Most operating systems have the option to scale the size of objects in software, to 125% for example, to make things easier to see, but that gives up the very screen "real estate" that warranted the higher resolution in the first place! So then you find that you ultimately just need a bigger screen. But I digress. It's good to have an idea of how the content will look on the screen you intend to use.

Consider the difference between a 24" monitor and a 27" monitor (as measured on the diagonal...). And consider both have a resolution of 1920×1080 (pixels wide by pixels tall).

Because they are the same resolution, getting a bigger screen does not add any “real estate,” it just makes everything bigger. Then consider that same 27” monitor, but with a resolution of 2560×1440. In this scenario, you do get more screen “real estate,” but the screen content does appear smaller.

Other important factors to consider when selecting a monitor include contrast ratio (how black will black look...), refresh rate (smoother video) and physical curvature for a more “immersive” effect.

As always, options are commensurate with price and you get what you pay for. At today’s prices most users, even gamers, will find a good monitor that suits their needs for a very reasonable price. Remember to consider how many displays are needed simultaneously and make sure your graphics card(s) support them.

5.1.9 Computers and Operating Systems

Choice of computer system really starts with choosing an operating system. With Windows there are a lot of hardware options and many of the considerations are provided in Sections 5.1.1 to 5.1.8. Worldwide market share of desktop operating systems in use from December 2023-2024 is shown in Figure 30. For interest, worldwide market share of all operating systems in use from December 2023-2024 is shown in Figure 31.

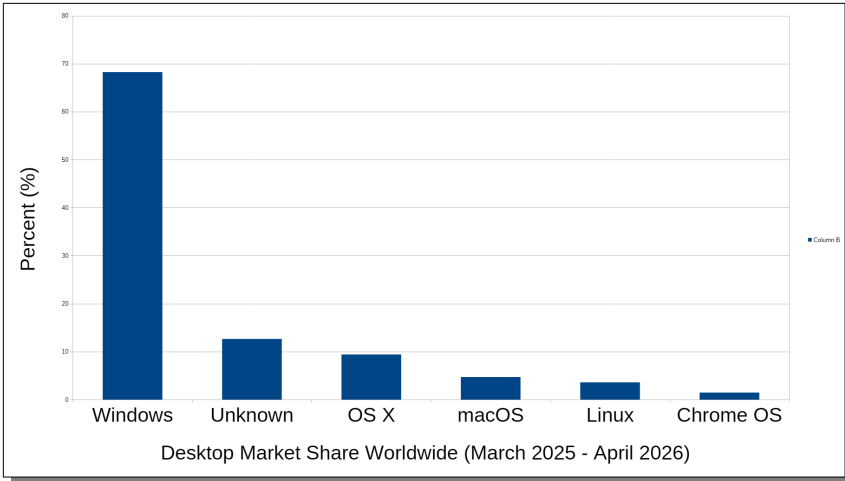


Figure 30: Worldwide Desktop OS Market Share from March 2025 to April 2026¹

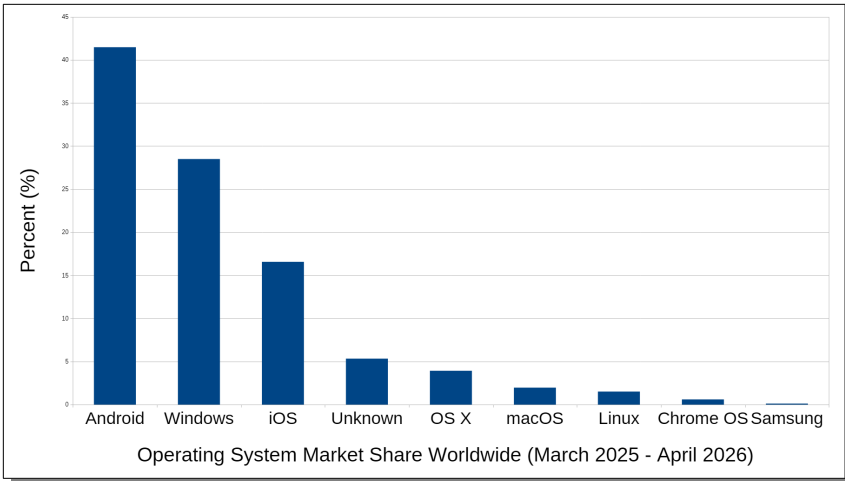


Figure 31: Worldwide OS Market Share from March 2025 to April 2026²

1 <https://gs.statcounter.com/os-market-share/desktop/worldwide>

2 <https://gs.statcounter.com/os-market-share/>

As shown in Figure 30, Windows reigns supreme as the most popular desktop OS worldwide, by a long shot. This makes Windows the largest target for software developers. It also makes Windows the largest target for malware developers. Windows is a mature OS that is extremely well supported and offers a lot of power and flexibility. For computer gaming, Windows offers the most games and the most popular games, by far.

Brand new laptops and pre-built PCs usually come with a Windows license, either “Home” or “Professional” editions. When building a PC, a license must be purchased. Two main features that Windows Professional includes that Windows Home does not are Bitlocker Drive encryption and Windows Remote Desktop.

The GNU Linux OS is an alternative to Windows that can usually be run on same hardware as Windows. GNU Linux is easier to use than ever, and is also very powerful. GNU Linux offers broad hardware support today, which wasn’t always the case (as Gen X and elder Millennial GNU Linux users will remember). There are many “distributions” (AKA “flavours”) of GNU Linux and many of them are very stable. Examples include Ubuntu, Linux Mint, Puppy Linux, PopOS, etc.

New life can often be breathed into an older computer by loading a GNU Linux OS onto it. Typically, GNU Linux will run faster on that older computer than Windows. This is especially true of very light weight GNU Linux distributions, like Puppy GNU Linux, which runs astonishingly fast, on any hardware really.

A nice feature that is available with many GNU Linux distributions is a “Live CD” (Compact Disc) version of the operating system. With Live CDs, the entire operating system can be demonstrated and used without being installed on the computer. Further, these Live CDs can often be installed onto a USB thumb drive in a “persistent” mode that allows persistent

saving to the USB thumb drive so that your work and changes can be saved.

Live CDs are a convenient way to try out different GNU Linux distributions. Live CDs are also just a convenient way to have an entire computer system on a USB thumb drive, requiring only a basic host computer to run it on. Take a look at the default desktop screens and their app menus and launchers for several popular GNU Linux distributions, featured below in Figures 32 to 35.

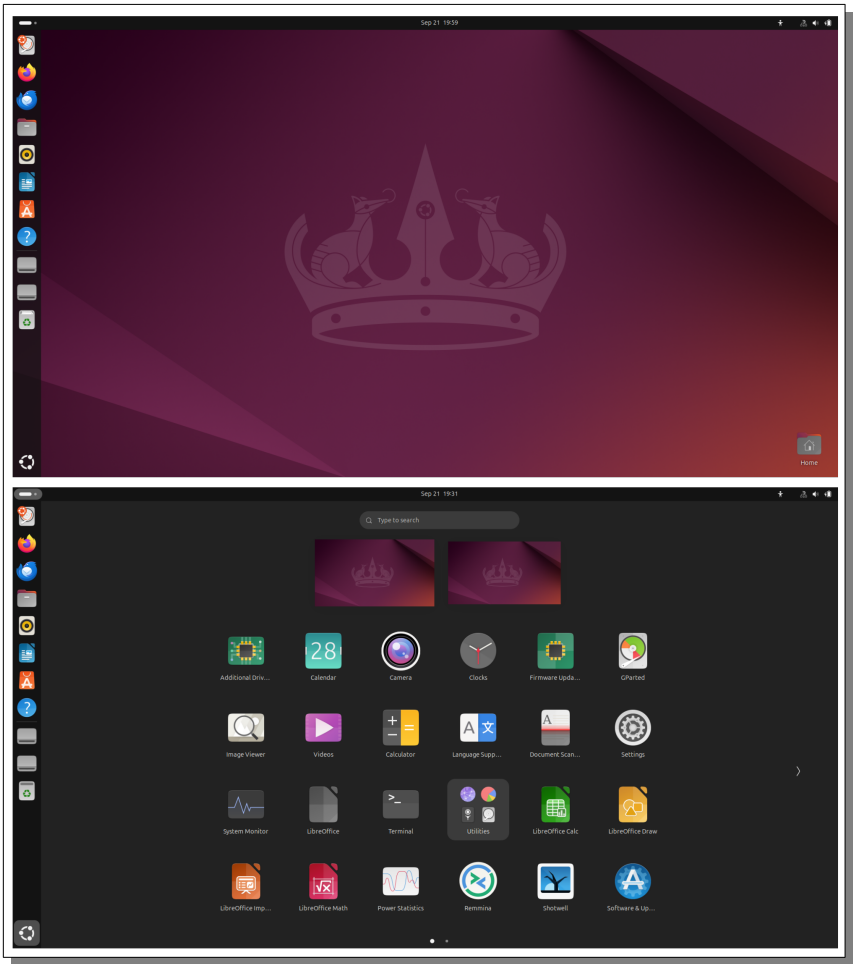


Figure 32: Ubuntu Version 24.04.01 Screens

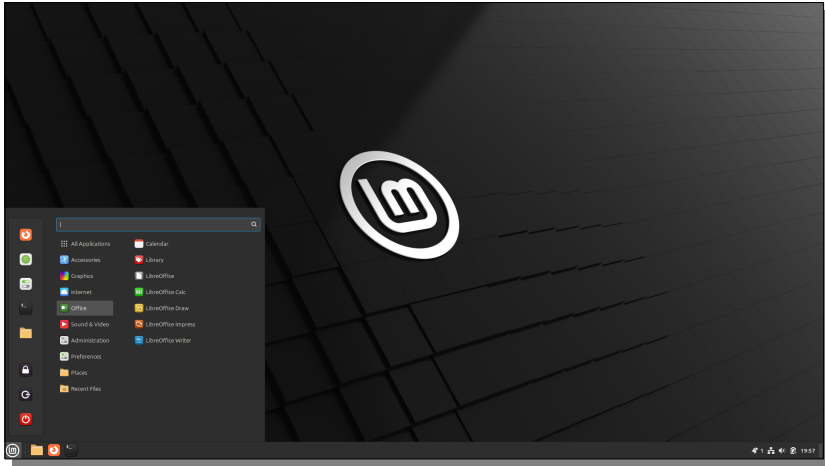


Figure 33: Linux Mint Version 22 Cinnamon Default Desktop Screen and Launch Menu



Figure 34: Puppy Linux Bookworm Pup64 Version 10.0.07 Default Desktop Screen and Launch Menu

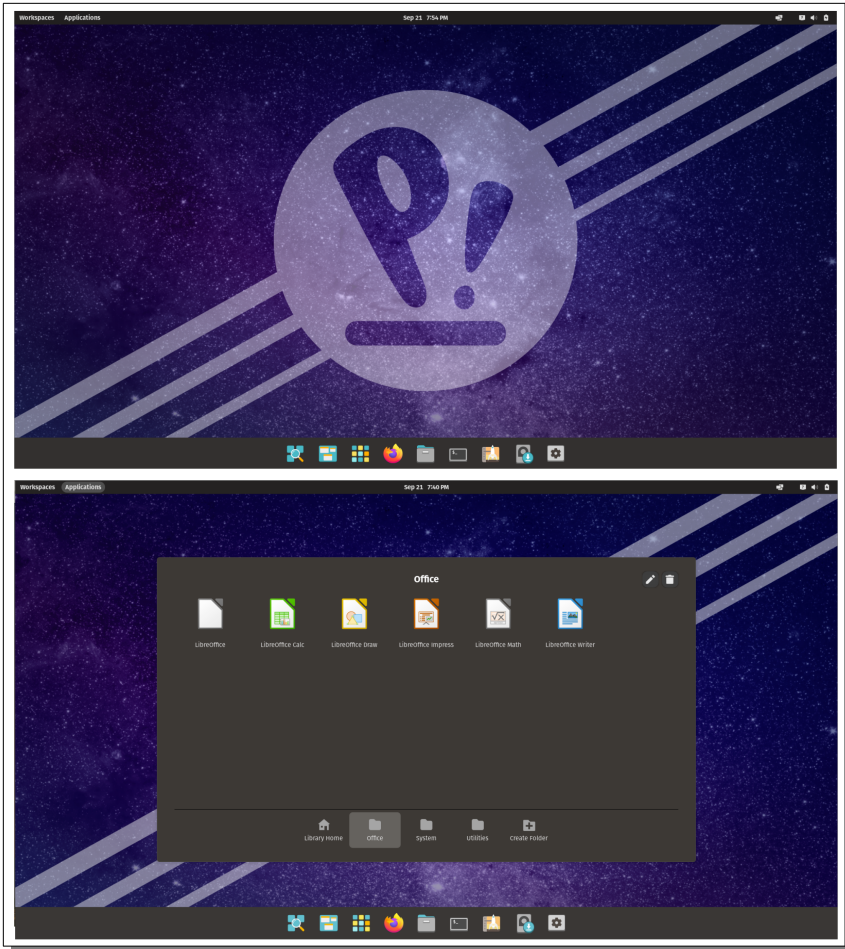


Figure 35: PopOS! 24.04 Default Desktop and App Drawer Screens

And then there's Apple. For those seeking the ultimate stability between hardware, operating system, and application software, there's Apple computers. Historically, Apple computers cost more (though Apple continues to close the affordability gap), but they are always cutting edge technology, stable, and just plain aesthetically pleasing machines. If you can afford an Apple computer and you don't plan to do any serious gaming, then an Apple computer will not disappoint.

It is important to note here again, that for the same hardware, different computer architectures process data differently and may achieve different performance. Hardware specification alone does not entirely determine system performance. It is a combination of the hardware, the OS and the application that determine the user experience.

As of this writing, Apple computers are not ideal for video gaming purposes. There are two main reasons for this. First, there haven't really been any powerful video cards made for Apple computers. The second reason, which is not unrelated to the first, is that there just aren't as many games available for Apple computers. Many folks' favourite games will simply not be playable on an Apple computer without running Windows either via dual boot with Bootcamp, or in a virtual machine (which immediately implies a pretty significant gaming performance reduction). That said, it does appear that as of the Apple M3 CPU, Apple has put a focus on improving gaming performance [Warren, 2023]. Perhaps, over time, Apple will also be able to attract more major game titles.

Cloud services (covered in Section 5.5) enable a client/server model of computing. In this model, a simpler, "terminal" type computer, is able to access a server and its resources, and perform its intensive computing on the server, consuming the server's resources instead. Client/server computing was popular in the days of mainframe computing as it allows for the centralization of resources and reduces costs. The same is true today with modern cloud computing environments as they allow for simpler, less expensive computers to be deployed to users, while still having the ability to consume computing resources, as needed, via the cloud services. Once again, how you intend to use the tool drives the decision on what to purchase. Knowing your options is good, and cloud computing should definitely be a consideration in your computing needs decision making. For example, if you aren't planning to do any serious gaming, and you don't have any specific application needs

driving you to a desktop OS, you can seriously simplify your computing life by going all in on Cloud Services for your data storage needs, and use an iPad or Chrome OS device as a computer.

It makes sense to scale your computing hardware purchases with your needs. The considerations depend on what you are looking for, in terms of simplicity, stability, speed, computing power, form factor, and of course price, and ultimately value. Knowing what you want to do with your computer and what you want in terms of computing power, looks, and efficiency, along with doing research to understand your options and compatibility, will allow you to make the best compromises for your budget.

Tables 6, 7 and 8 describe some of the benefits and drawbacks of the major desktop OSes.

Benefits	Drawbacks
Windows is the dominant desktop platform worldwide.	Windows is not open-source, if you're into that kind of thing.
Windows' popularity and business model make it one of the best supported operating systems available.	Windows costs a non-trivial amount of money to purchase a license.
Windows remains a primary target OS for application developers so plenty, and in many cases, the best types of commercial, freeware, and open-source applications are available.	Being the most popular desktop operating system, Windows is still the most targeted operating system from a cyber security perspective.
There are lots of troubleshooting and performance monitoring tools and ways to "get under the hood" to tweak performance and diagnose problems.	Windows includes a relatively limited set of native applications.
There is a plethora of different hardware manufacturers to buy hardware from.	
It is possible to build and maintain your own PC, if you're into that kind of thing.	
Strong hardware support.	

Table 6: Benefits and Drawbacks of Microsoft Windows

Choose Windows if you:

- prefer it

- want access to the widest range of applications and games
are looking for a lower cost PC
- want a really well supported and flexible OS with plenty of tools for tweaking, monitoring, and diagnosing
- are a serious gamer
- need compatibility with the widest range of hardware
- are a business and want to provide the most familiar experience for your users and administrators

Benefits	Drawbacks
Lightweight and fast.	Less understood by more users than Windows and Apple; it might be harder to find help.
Strongest privacy.	
FREE!!! and awesome.	
Many different distributions or “flavours” to choose from, some for art creation, some for cyber security and everything in between.	Probably a bit harder to use and administer than Windows or MacOS.
Much better hardware support than years ago.	Less hardware compatibility and application software availability than Windows or MacOS, especially true of the newest hardware and software.
Strong repository-based application software distribution.	
GNU Linux is open-source.	
Some of the GNU Linux distributions have really nice desktop interfaces.	

Table 7: Benefits and Drawbacks of Linux

Choose GNU Linux if you:

- Prefer it
- Want the best possible privacy option for a desktop PC
- Have an older PC and want a performance boost over Windows
- Have a PC that needs an OS and want to use one that is free and awesome
- Appreciate and want to support the open-source community
- Have patience and don't mind spending a bit of time learning when you're working with it, which can be downright frustrating at times

Benefits	Drawbacks
Well-supported, user-friendly, productive, OS that focuses on the user experience.	Historically considered more expensive, along with the Apple hardware, but Apple continues to offer more competitive, lower cost options.
Likely the most stable OS due to the strongest coupling between OS and hardware.	Less well-understood than Windows and therefore fewer people know how to troubleshoot, monitor, and diagnose them (ahem, Apple Geniuses?).
Strong application support, especially “creative” software.	Less hardware and upgrade options available.
Able to run on Apple hardware.	Not suitable for serious gaming, at least not at the time of this writing.
MacOS is a derivation of the Unix operating system and that is cool man.	Less abundant applications and games software than Windows.
Some application software is included in the OS (Apple’s version of Office Software, GarageBand, iMovie, etc.).	
Apple continues to demonstrate leadership in increasing privacy and security for its users.	

Table 8: Benefits and Drawbacks of MacOS

Choose MacOS if you:

- prefer it
- are looking for the best stability available
- aren’t looking to do any serious gaming

- don't mind paying a premium price and have the budget (though recently Apple has been closing the affordability gap)
- don't mind fewer hardware and application software options
- don't mind fewer options in general as a user, Apple prioritizes simplicity and consistent user experience over flexibility and customization

5.1.10 Mobile Devices

As described in Section 4.7, “mobile device” refers to portable, handheld and relatively small computing devices, e.g., smartphones, tablets, Chromebooks, iPhones, iPads, e-readers, etc. In an analogy, today, Android is to Smartphones and tablets what Windows has historically been to PCs. This is because it runs on many different manufacturer's devices, whereas, Apple's iOS only runs on their iOS-enabled devices.

One of the main considerations when choosing a mobile phone is whether you prefer the Android or iOS operating system. Other significant considerations may include the phone dimensions, camera(s), battery life, screen, ruggedness, reviews and more. If you prefer iOS then you'll have a choice of iPhones to choose from. If you prefer Android then you'll have many different phone models to choose from, with varying features, specifications and price points, from many different phone manufacturers. If you don't have a preference for Android or iOS then all options may be considered, but your choice of hardware will dictate the mobile OS, which will have security and privacy implications.

There are many Android devices available at a lower price point than comparable iOS devices, though there are certainly premium Android tablets that can make an iPhone or iPad blush, in terms of price. Nonetheless, the price floor is definitely lower for Android devices. Lower end Android Smartphones and

tablets from lesser known manufacturers having similar size screens, storage capacity and battery life as their nearest iOS counterparts are sold for two to four times less than the cost of the most similar iOS device.

That said, one should consider the total cost of investment. In the Smartphone game, this is really about how long you can expect your Smartphone to be supported and how long you intend to use it before replacing it. If you are of the mindset that you replace your Smartphone every two years, then it doesn't matter if it is supported for six years. In contrast, if you are forced to replace your lower cost Smartphone every three years, then it may justify spending a little more for a device that is supported for seven years, if you don't mind using what some may consider to be an older device.

Support lengths of major Smartphone manufacturers ([Mister Mobility, 2023], [Haslam, 2024]), at the time of this writing, are summarized in Table 9.

Manufacturer	Smartphone(s)	Update Support Duration
Google	Pixel	OS: 7 years, Security: 7 years
Apple	iPhone	OS: 5 years, Security: 6 years
Samsung	Galaxy	OS: 4 years, Security: 5 years
Xiaomi	Xiaomi Flagship, Redmi, POCO	OS: 4 years, Security: 5 years
OnePlus	OnePlus Flagship, Nord	OS: 3 years, Security: 4 years
OPPO	Find, Reno	OS: 4 years, Security: 5 years

Manufacturer	Smartphone(s)	Update Support Duration
Motorola	Razr, Edge, Stylus, Power	OS: 2/3 years, Security: 2/3 years
Nokia	All HMD made devices	OS: 2 years, Security: 3 years
Realme	Realme Flagship, GT, C, Note, Narzo	OS: 2 Android Versions, Security updates: 3 years

Table 9: Smartphone Support Lengths

Android device manufacturers design mobile devices for specific Android versions, just as PC manufacturers designed computers for specific versions of Windows. The stability of Apple’s approach to hardware and software integration cannot be beat, though historically it came at a bit of a premium price.

Using Android also comes with the unfortunate disadvantage of being subjected to Google’s pervasive personal data collection and use [Doffman, 2025]. There are ways to “de-Google” Android devices, but this typically requires advanced, and somewhat risky techniques, to “unlock” and “root” the device, and then install an aftermarket Android “ROM” on the device. That said, there is a thriving community of users that do exactly that and install third-party ROMs. Installing a third-party ROM can be a rewarding experience, but often it is a pretty good pain and it comes with some risks. ROMs may also be less stable and require more effort to maintain. To some, dare I say most, it simply will not be worth it.

Years ago, users could turn to Blackberry for an alternative to Android and iOS. Although Blackberry was one of the strongest and earliest mobile device manufacturers, they are no longer in the mobile device business. Now, the only other alternative to Android is iOS. While iOS is an excellent option, there are lower cost Android options. Choose wisely dear mobile device user.

5.1.11 IoT Devices

This category of “smart” devices includes smart TVs, security systems, security cameras, doorbell cameras, thermostats, light switches, power outlets, garage door openers, automobiles, refrigerators, laundry appliances, pool control systems, etc. With IoT devices, manufacturers have been prioritizing functionality and price over security and privacy. As such, IoT devices may have poor security and privacy. What’s worse is that one of the basic functionalities expected of IoT devices is that they are connected to, and accessible via the internet. This accessibility is usually for the purpose of being able to access the smart device using a mobile device application. It is this expectation of IoT device accessibility from the internet where IoT devices present a real security risk. This is because they can be easy targets for hackers, and provide a “foothold” into your network. If an IoT device on your network is compromised, then that device can provide an attacker with ongoing, continuous access, to that compromised IoT device. If that compromised IoT device is connected to the same LAN as your more important devices and data, then only the security defenses provided to the hosts themselves will be able to help protect those hosts from an attacker. Using a defense in depth strategy (See Section 7.1), all hosts on the LAN should have the appropriate host-based security defenses deployed, which should help to protect the hosts from any attackers. Still, segregating the IoT devices from the more important hosts through the use of a firewall makes a lot of sense as it provides another layer of security (ahem, “peace of mind”).

IoT device users would be wise to survey the market for the available manufacturers of the types of products they need, and to research those products and manufacturers. If the IoT device manufacturers prominently highlight information about their device security and privacy features, and ongoing security updates, then it may be worth paying a bit more. Otherwise, prioritizing functionality and price is fine, and you can learn

about ways to protect your more important hosts from your IoT devices in Sections 7.9.1 and 8.1.

5.1.12 *Portable Media*

Portable media are data storage media devices that can be conveniently connected to a computer or compatible electronic device, in an ad hoc manner, for writing and reading data, to and from, that media. Modern forms of portable media include Secure Digital (SD) cards, mini SD cards and micro SD cards. Older portable media formats still in minor use include compact flash, Digital Video Discs (DVDs) and Compact Discs (CDs). While even older forms of portable media are completely obsolete including digital video (DV) tapes, Mini Discs, Zip disks, Jazz disks and floppy disks.

SD, mini SD and micro SD cards are a very attractive form of portable media because they are physically very small and lightweight, but have the ability to store a massive amount of digital information. Because of this, today, SD, mini SD and micro SD cards are the preferred portable media for mobile devices, cameras, and all types of other digital devices that need to store audio, video or files in general. Some laptops and desktop computers come equipped with SD card readers. For computer that don't have integrated SD card readers, USB-based card readers are available.

Other types of modern portable media include USB thumb drives, external hard drives and tape drives. Photos of various portable media are provided in Figure 36.



Figure 36: Portable Media

(a) SD card; (b) Mini SD card; (c) Micro SD card; (d) Compact Flash; (e) DVD Disc; (f) CD Disc; (g) MiniDV Tape; (h) Minidisc; (i) 2.5" Floppy Diskette; (j) Portable Hard Disk Drive; (k) USB Flash Drive

5.2 Application Software

Today's operating systems have application repositories, or "stores", that consolidate the application discovery and installation process. From a security perspective this is an excellent approach as it allows vetting of applications for any

malicious behaviour. Another advantage to application repositories is that they allow security updates to be distributed to all installed applications, in a simple manner. The downside is that it puts the store owner in a monopoly position over the applications available for installation on the systems they sell, holding both consumers and application developers hostage, paying whatever price the store owner demands. Still, from a security perspective it is preferable.

Installing applications outside of the official OSes application repository is known as sideloading. Many times, the only way to install an application is by sideloading it. Sideloading comes with two main considerations, security of the installation package and maintaining ongoing updates. If you are sideloading applications, and especially if the installation files are acquired via the internet, it is important to scan the files with a virus scanner before installing them. It's also best if you acquire the installation files from a reputable software developer.

5.3 Virtual Machines

A virtual machine is a software emulation of an entire computer system that runs as an application on another computer. A virtual machine is a computer made entirely of software, not hardware. Virtual machines have been around for a long time, and are very common and useful.

In standard IT parlance the “guest” is the virtual machine itself, being run as an application on the “host”. The host is another computer, usually a physical machine, but may also be a virtual machine. Figure 37 graphically depicts the concept of a virtual machine.

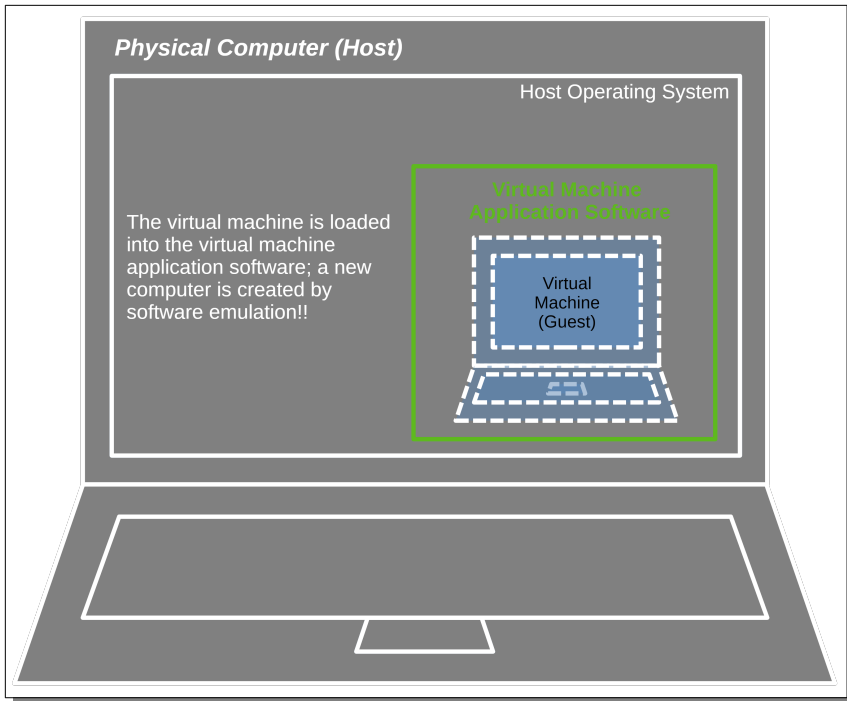


Figure 37: Virtual Machines

Why would anyone want to do this virtual machine stuff?

1. Virtual machines provide a very convenient way to setup the configuration of a complete computer, and then make that computer super portable and backup-able. This means that if the host computer hardware fails, it is very easy to get everything up and running on a new host.
2. If the software loaded on a virtual machine becomes problematic, due to a misconfigured application or perhaps file corruption, a backup image of the virtual machine can be used to quickly recover.
3. Starting each computing session with a fresh, hardened, virtual machine image can be ideal, when desiring the highest privacy and security. This is because all system changes and data are discarded after each use. Data can

be transferred carefully from the VM to the host, as needed. This approach ensures that a clean computer is used each and every computing session.

4. Virtual machines also provide a way to take full advantage of powerful computer hardware in an ideal way. Rather than loading many applications onto a single operating system, you can load many operating systems via virtual machines, with fewer applications each. This allows for each of those individual virtual machine to be more stable, as they each have fewer applications running that could become problematic. One powerful virtual machine server (host) can run many virtual machines (guests) allowing for the full resources of the computer hardware of the server to be utilized, while also creating a more stable environment, albeit incurring the overhead of the VM infrastructure..
5. Virtual machines have also been used to make applications that are portable across the major OSes. Java is a virtual machine environment that has been around for a very long time. Many people have bumped into the “Java Runtime Environment” (JRE) and probably didn’t realize that it was creating a virtual machine and that java applications were being run on that virtual machine. This allows Java applications to be portable across the different operating systems like Windows, GNU Linux, and Mac. This is because the Java Runtime Environment is what is running the application, not the host operating system. The developers at Java make the Java Runtime Environment for each of the major OSes, then Java applications can be run in the Java Runtime Environment on those major OSes.
6. Redundancy and fault tolerance. For mission critical applications, virtual machines, and their hypervisor environments provide, unparalleled flexibility for setting up fault tolerant applications efficiently.

7. There are probably more reasons than above, but these are good enough for the discussions in this book.

Perhaps surprisingly, the average home and small business can probably benefit from leveraging virtual machines. The main use case is to use older hardware, or to buy a server, and use it as a host for several key virtual machines, such as a self-hosted cloud server or security appliance. There is excellent free software for creating and running virtual machines. Virtual machines are also much easier to get up and running than most people think, and are much more useful than most people realize.

5.4 Containers

Containers, or “containerized applications,” provide a method of bundling up all that is necessary to get an application running on an OS and making that bundle portable, drastically simplifying the installation and configuration process. This is an extremely useful feature as it allows rapid deployment of applications. However, this convenience does sometimes come at the cost of flexibility. This is because sometimes containerized applications do not have the same configuration flexibility as the same applications installed using the full and proper installation and configuration process. Regardless, application containers are really useful and popular because they save a lot of time.

Probably the most popular multi-OS container platform today is called Docker, which supports Mac, Windows, and GNU Linux. Another popular container-like platform, exclusively for GNU Linux is the Snap package manager. Snap is popular for packaging GNU Linux applications, which can be notoriously difficult to setup and configure. For example, a Snap package has been created that can be used to set up a NextCloud personal cloud server by executing one command and entering input to a few subsequent questions, immensely simplifying the

setup process. A graphical depiction of how containers work is shown in Figure 38.

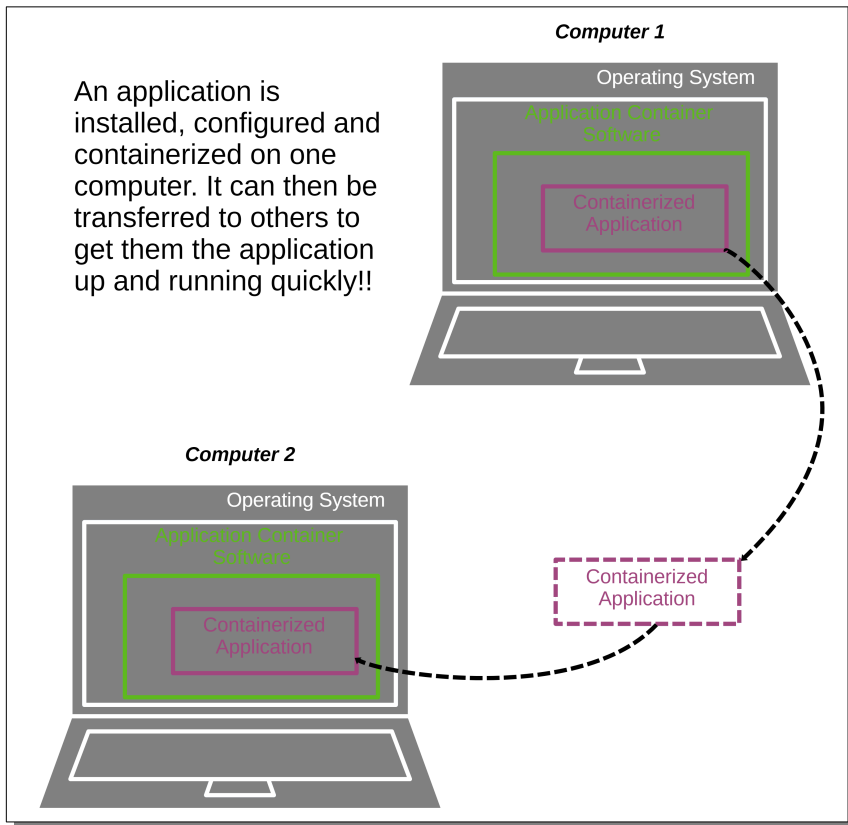


Figure 38: Containers

5.5 Cloud Services

Cloud Services allow you to run applications and store data on somebody else's computers. To you it's just "the cloud". You don't need to know where specifically the applications are running, or specifically where the data is stored, it's just "in the cloud," and you have continued access to it.

Web infrastructure has enabled rich digital features to be delivered through browsers and mobile applications. Cloud service providers build integrated platforms that allow you to

run their applications on a computer via native applications, in a browser via web applications, or on a mobile device via mobile device applications. Cloud services provide a familiar experience in each supported environment and seamless access to data. The data does not need to be stored on your computer and it is conveniently accessible in computer, mobile and web applications.

Cloud services perform multiple functions that people have already gotten very accustomed to including:

- safe, secure, and reliable storage of your data “in the cloud”
- convenient web, mobile, and computer applications that integrate with the cloud data and provide access and features
- synchronization of the cloud data across your devices
- easy sharing of data with other online users

The major information technology companies like Apple, Microsoft, Google, and a few others, provide cloud services with varying degrees of functionality. At the time of this writing, Microsoft is providing the pinnacle of cloud services. Their Office 365 product is extremely functional in web browsers, mobile device applications, and native applications, and everything is seamlessly integrated. Their applications are cross-platform and hey, they are MICROSOFT. That said, because Microsoft is not making mobile devices, while their applications are extremely functional and solid, it would stand to argue that their applications may not be as tightly integrated with another manufacturer’s digital “ecosystem”. For users that have gone all the way with the Apple or Android ecosystem, it is natural and convenient to use Apple’s or Google’s cloud services, though Microsoft provides more comprehensive cloud products.

PCMag tested and rated Cloud Service providers in 2026 [Duffy & Muchmore, 2026], the results are summarized in Table 10.

Cloud Service Provider	PC Mag Rating	PC Mag Selected Best For	Pros & Cons
Microsoft OneDrive	5	Overall	Excellent interface. Clients for Android, iOS, macOS, and Windows. Seamless Microsoft 365 and Windows integration. Strong online photo presentation and management. Powerful file sharing and collaborative editing. Many new features are available only for organizations.
Google Drive	4.5	Google Workspace Users	Generous free storage space. Excellent productivity suite collaboration. Includes desktop-to-desktop file syncing. Many third-party integrations. Cross-platform apps. No password protection for shared files. Multiple apps required for related functions. Some privacy concerns.

Cloud Service Provider	PC Mag Rating	PC Mag Selected Best For	Pros & Cons
iDrive	4.5	Price	Excellent value. Unlimited devices per account. Strong security options, including password-protected shared files. 10GB of free backup. Backs up mobile data, plus cloud data from third-party platforms. Complete disk imaging is only available for Windows PCs. Android app has more backup options than the iOS app.
Proton Drive	4	Privacy & Security	All files fully encrypted. Flexible sharing options. Data protected by Swiss privacy laws. Free tier available. Not the best value per gigabyte. Somewhat slow upload speeds. Lacks GNU Linux app.

Cloud Service Provider	PC Mag Rating	PC Mag Selected Best For	Pros & Cons
Sync	4	Simple, Straight-Forward Syncing	Extremely easy to use. Client-side encryption means Sync can't access your files. Multiple file-sharing options. GDPR and HIPAA compliant. No file size limits. Not the best price per gigabyte. Mobile apps lack scanning and OCR features. Lacks local area network syncing.
Apple iCloud Drive	3.5	Apple Users	Tightly integrated with Apple products. Surprising security options. Lets you edit files in a browser. Useful Windows PC desktop app. Only lets you share files with people who have an Apple ID. Expensive high-end plans. Lacks Android and GNU Linux apps.

Cloud Service Provider	PC Mag Rating	PC Mag Selected Best For	Pros & Cons
Box.com	3.5	Integrations	Flexible web app that can open files using desktop software. Many security options, including HIPAA compliance. Integrations with more than 1,500 applications. Pro plan supports versioning. Mobile apps with OCR. Offline file access. Pricey for the amount of storage offered. Low file-size limit. Longstanding issue with Google accounts prevents logins. Can't configure location of desktop syncing app.

Cloud Service Provider	PC Mag Rating	PC Mag Selected Best For	Pros & Cons
Dropbox	3.5	Useful Extra Tools	Hundreds of integrations. Mobile apps back up phone files and have OCR. File Request feature lets people without Dropbox accounts share files. Comes with a few useful Dropbox productivity tools. Free version only lets you install it on three devices. Not the best per-GB value. Syncing issue with Macs.

Table 10: PCMag 2026 Cloud Service Provider Ratings, Best For and Pros & Cons [Duffy & Muchmore, 2026]

In addition to using a cloud service provider, there is also the option of setting up your own personal cloud server. There are free, open-source, products available to conveniently set up your own cloud server at home. While this set up wouldn’t quite have the same integration, maturity, security, and reliability of a cloud service provider, it is extremely functional, convenient, inexpensive, and you gain total control over your information. For some users, this is great solution for cloud computing. However, running your own cloud server does take some personal investment to stand up, and you need to be concerned about security and backups. A personal cloud server is most useful if it is exposed to the internet so that your data is accessible, conveniently, from anywhere. Since a personal cloud server is really just a web server, the security and

backups of your personal cloud server, that likely has your personal or small business data on it, needs to be taken very seriously.

For many, it would be just fine or preferable to pay a cloud service provider for the convenience, integration, and stability of their cloud services. Potential drawbacks to using a third-party cloud service include:

- it can get expensive, especially for a family
- some of the cloud service providers are not interoperable with each other, locking you into their digital “ecosystem”
- privacy of your data may be compromised, though some Cloud Service providers are now offering end-to-end encryption and do not have access to your information (remember, you can overcome this by encrypting your data before uploading, but this is certainly not convenient or ideal)

A graphical depiction of cloud computing is shown below in Figure 39.

Your 3rd party cloud service data is stored remotely, on a diverse set of servers, for data backup and resiliency. Your devices that have your cloud service synchronization software installed, and are logged into your cloud service account, can synchronize the data in your cloud drive and store the data locally on the synchronized device. You can also separately have a personal cloud server, hosted on your own network.

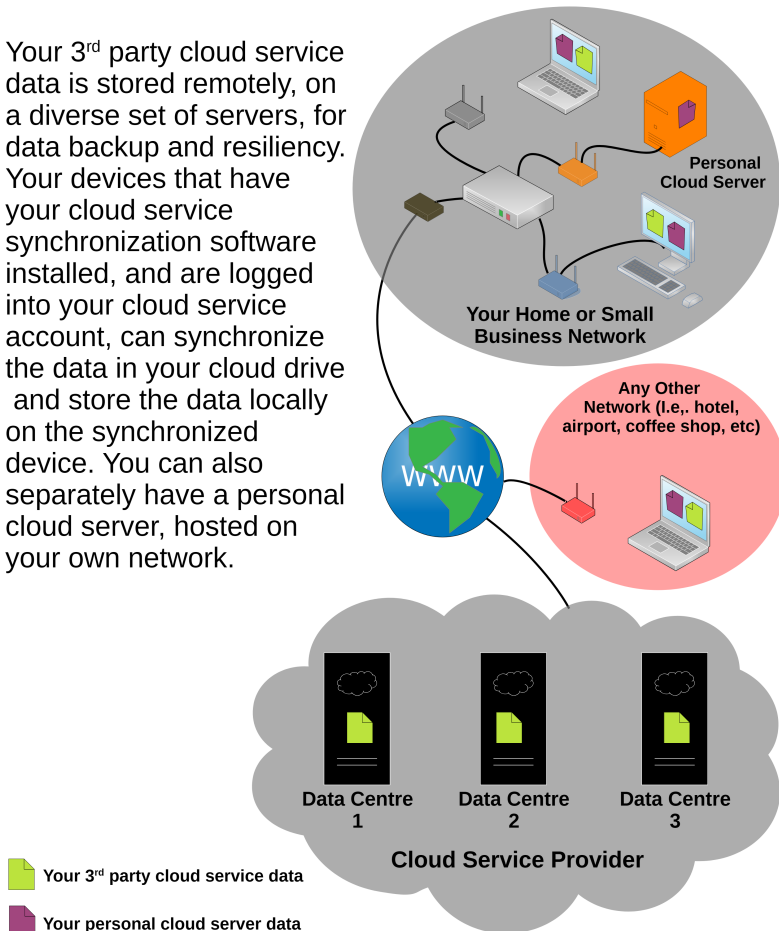


Figure 39: Cloud computing

6

Home and Small Business Networking

This chapter dives into home and small business networking. Section 6.1 jumps straight into internet service providers. This is because most homes and small businesses are primarily concerned with connecting to the internet, not necessarily with the overall networking of their devices. Starting with how homes and small businesses connect to the internet provides the opportunity to clarify some key misunderstandings right at the outset.

Section 6.2 introduces the Open Systems Interconnect (OSI) model. This model helps to visualize how the various communication layers and their attributes map to their physical and logical realizations that are discussed throughout the remainder of Section 6 covering:

- Home and small business routers (Section 6.3)
- Ethernet switches (Section 6.4)
- Routers and firewalls (Section 6.5)
- IP addressing (Section 6.6)
- Dynamic Host Control Protocol (Section 6.7)
- Default gateways (Section 6.8)
- Static routing (Section 6.9)

- Public vs. private IP addressing (Section 6.10)
- Network Address Translation (Section 6.11)
- Port forwarding and reverse/application proxies (Section 6.12)
- Domain Name System (Section 6.13)
- Voice-over-IP (Section 6.14)
- Wireless networks (Section 6.15)
- Virtual Private Networks (Section 6.16)

6.1 Internet Service Providers

Your network connects to the internet through an internet service provider (ISP), who provides just that to you, the internet. What makes them an ISP you ask? Good question, inquisitive reader. At least two things. First and foremost, you need to be able to connect your communication equipment to the internet, physically. Your ISP either owns the communication lines between your connection point and their upstream connection to the internet. Alternatively, your ISP may lease those lines or bandwidth on those lines, and resell it to you. Second, your ISP issues you an IP address on the public internet, or otherwise shepherds your connection to a public facing IP address somewhere in their network. In summary, two critical things your ISP does are that they provide your physical connection to the internet and your logical connection to the internet.

The IPv4 protocol, still in dominant use today, only accommodates approximately 3,702,258,432 IP addresses for public use. Your ISP likely provides your home or small business network with a public IPv4 address. However, some ISPs may issue home or small business networks an IP address on the ISPs private network, instead of a public IP address. Section 6.10 discusses public IP addresses further. IPv6 is a newer protocol

and it accommodates 340,282,366,920,938,463,463, 374,607,431,768, 211,456 addresses, but today, a home or small business network will usually only be issued one IPv4 address from its ISP, and it needs to suffice for all the various devices on the network. A technology called “network address translation” (NAT) was developed to allow all the various devices on a typical home or small business network to work with the internet, while only having one public IP address. NAT is discussed further in Section 6.11.

The move to IPv6 is happening very slowly and for good reason. It is a different technology that introduces a raft of new considerations for security and privacy and needs to remain interoperable with IPv4. In the future, expect that your ISP will likely issue IP address spaces for your networking needs instead of a single IP address.

ISPs range in size and the services they provide. Many TV cable companies have become ISPs and offer bundling of their services including TV, phone, internet, and sometimes even cellular services. While bundling does help lower the bill, sometimes going with a smaller ISP can be more cost effective, especially if you don’t need any bundling.

Home phones are nice in the case of emergency, but if your ISP is only providing you a voice over internet protocol (VoIP) service, as opposed to an analog telephone service, then that VoIP service is also unavailable when the internet is unavailable. Additionally, all the devices involved in the VoIP system need to be connected to a battery system or they lose power when the power goes out too. Older analog phone lines still exist today, but they are less and less popular. Still, analog telephone service, while relatively expensive, is available when the power or internet is out. It really is a valuable service that most people overlook today. The less expensive VoIP option does provide a “home phone” option, but it has questionable value today when most people already have cell phones and it

may cease to work in a power outage anyway, when it may be most valuable.

6.2 OSI Model

Ethernet communication can be conceptualized in layers. Starting with the physical connections at the first layer and stacked on top of that are the communications between two nodes (data link layer), then multi-node network communications (network layer), etc. These layers are characterized by the OSI conceptual model of communication systems and are summarized in Table 11 ([China, Goodwin, 2024], [Code Academy], [Raza, 2024]).

	Layer	Target	Data Unit	Function	Example Network Protocols
7	Application	Host	Data	End user applications	HTTP, HTTPS, FTP, IRC, SSH, DNS
6	Presentation	Host	Data	Formatting of data for viewing by user	SSL, SSH, IMAP, FTP, MPEG, JPEG
5	Session	Host	Data	Establishes and terminates connections between two hosts	NetBIOS, NetBEUI, RPC, SMB
4	Transport	Host	Segment, Datagram	Connections, transmissions, and error handling	TCP, UDP, NetBIOS, FCP
3	Network	Media	Packet	IP addressing, routing	IP, ICMP, ARP, RIP, OSPF, IPSEC
2	Data Link	Media	Frame	Physical addressing, switching	Ethernet, ARP, MAC, WiFi, Frame Relay, L2TP, VLAN, STP
1	Physical	Media	Bit, Symbol	Physical medium	Telephone, USB, Ethernet physical layer, DSL, T1

Table 11: OSI Model

6.3 Home and Small Business Routers

The basic piece of equipment that is required to connect your home network to your ISPs network is called a modem. In many cases this is a device that has only two ports, one Ethernet port to connect to your router and one port to your ISPs network (cable, DSL, satellite, etc.). The modem itself is performing the functions that are required to adapt your physical and logical Ethernet connection to their physical and logical network. It is typical to buy or lease your modem from your ISP. Equipment supplied by your ISP, is often referred to as customer premise

equipment (CPE). Beyond your modem, you need a router as well, to enable devices on your network to communicate with devices on other networks, and ultimately, the internet.

Today, ISPs are providing, leasing or selling devices that perform more than just the modem function. Often, ISPs are now providing devices that perform the functions of a modem, router, firewall, multi-port Ethernet switch and WiFi access point. Most people just refer to this device as their “router,” though it does much more than just routing.

The reason it is important to distinguish these features from one another is so that security and functionality can be described more precisely. Additionally, you may consider segmenting your networks for a better security architecture (see Section 7.9.1), and then it is necessary to consider these functions separately (e.g., modem, router, firewall, multi-port Ethernet switch and WiFi access point). This is because all the aforementioned mentioned functions are usually discrete components in a segmented network. The many functions of the “home router” are illustrated in Figure 41.

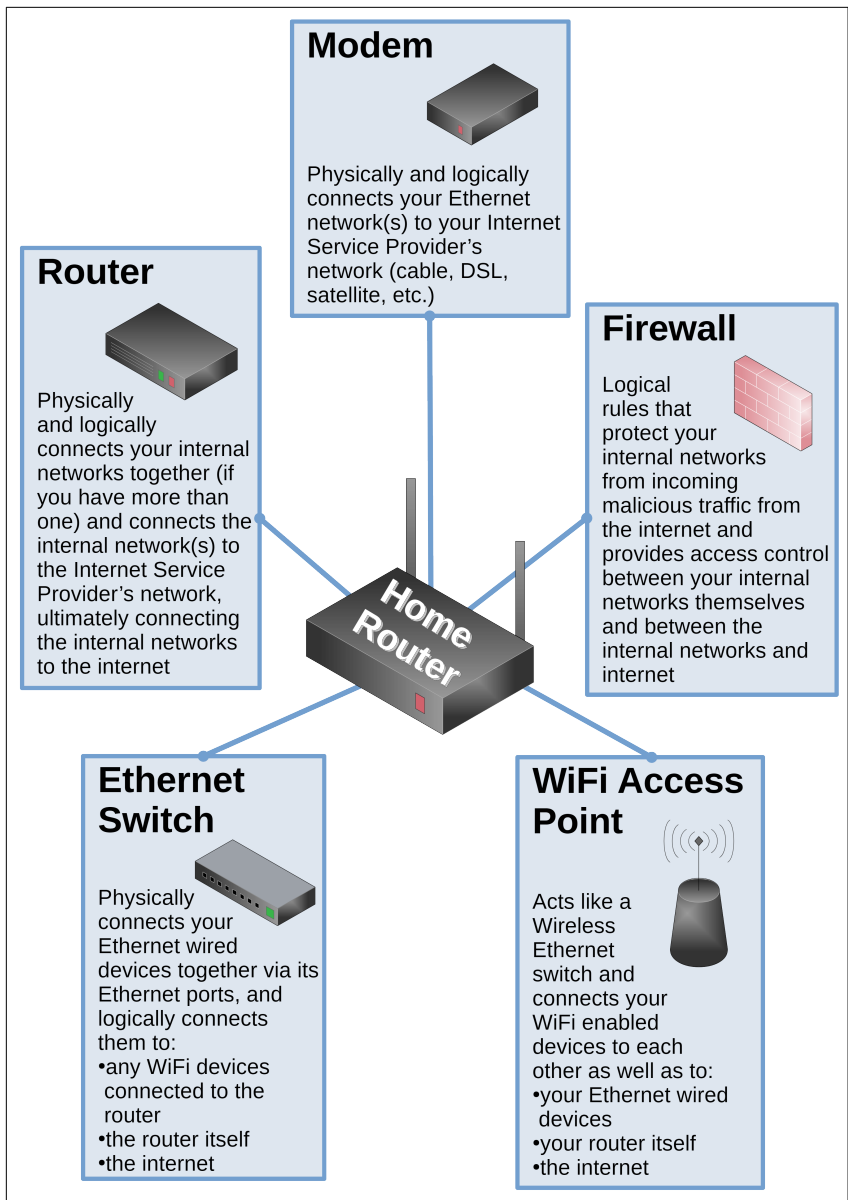


Figure 40: The Many Functions of the “Home Router”

Though your ISP may provide you with an all-in-one style router, there are some of us that really prefer to administer our own router. Administering your own router provides more flexibility,

privacy, and quite possibly security. It is certainly possible to purchase or otherwise implement a router or firewall that provides far superior security to one provided by the ISP. And honestly, it's a bit creepy in the author's opinion, that the ISP would have access to their the author's private networks to that degree. Worth a think for sure.

Should you desire the ability to administer your own router, you will have to:

1. Ensure that any "router" provided by your ISP is only operating as a modem, not a router
2. Purchase, acquire, or otherwise build, configure and deploy a router or firewall yourself

Regarding item 1 above, you can usually restrict your ISP supplied router into functioning only as a modem by configuring it to operate in "bridge mode". In "bridge mode," the routing and WiFi capabilities of the router are disabled. You will likely need to call your ISP to have them enable "bridge mode" (in their supplied "home router") for you.

Regarding item 2 above, for many years people were used to purchasing their own router and would avail themselves of the ever popular consumer grade WiFi router, of which there were, and still are, many different types and brands to choose from. Should you choose to administer your own router (which, to be clear, the author certainly thinks you should) then this book attempts to convince you to consider going beyond a consumer grade (WiFi) router and implementing a firewall or unified threat management device instead (for reasons covered in Section 7.9.1).

6.4 Ethernet Switches

With reference to the OSI model from the introduction of Section 6, Ethernet switches, in general, operate at the data link level, or OSI layer 2. This layer is where individual nodes on

a local network communicate. Ethernet switches allow the physical connection of multiple Ethernet devices to their ports. On home and small business networks, the connections are usually made with copper Ethernet cables of the CAT5/5e/6 type with RJ-45 connectors.

Each Ethernet device that connects to an Ethernet switch has a Media Access Control (MAC) address that is assigned by the manufacturer, and that is embedded in the Ethernet communication module of the device. This MAC address is what the Ethernet switch is “listening” for when the device is connected to the switch. Using Address Resolution Protocol (ARP), Ethernet switches learn the IP addresses associated with the MAC addresses of the devices that are connected its physical ports. The switch then forwards traffic to the intended device(s) without needing to broadcast the traffic to all the devices connected to its ports, like Ethernet hubs do.

Now long obsolete (but still in use for specific purposes!), before Ethernet switches there were Ethernet hubs. Contrary to Ethernet switches that effectively operate at the OSI layer 2 level, Ethernet hubs operate at OSI layer 1. This is because with Ethernet Hubs, traffic that originates on any one port is copied to all of the other ports (AKA broadcasted). This copying function requires no further processing by the hub than that present at OSI layer 1. One significant drawback to Ethernet hubs was that since all packets are sent to all hosts there is no privacy offered, at all. Another significant drawback to Ethernet hubs is that they implement half-duplex communication, which only allows devices to send or receive information at any given time, but not both. As such, Ethernet hubs create networks that are not as fast as those that implement Ethernet switches.

Most Ethernet switches purchased by homes and small businesses are the “unmanaged” type. Unmanaged switches require no configuration and don’t provide any configurable options. On the contrary, “managed” switches have

configurable options for enhanced functionality including fault tolerance, logging, alerting and monitoring features. The configurable options of a managed switch may be available via telnet or SSH using a serial cable or Ethernet, or via a web interface. Most homes and small businesses probably do not require the use of managed switches, but they can provide additional network visibility and diagnostics.

6.5 Routers and Firewalls

Routers and firewalls operate at the network layer, or OSI layer 3. This communication occurs using IP addresses. As described above, nodes that are on the same network (as indicated by their IP address and subnet mask) communicate through Ethernet switches at the OSI layer 2 level. But when two devices on separate network segments communicate, they must use a routing device to do so.

Routing devices transfer IP traffic from one network to another. In order to do so they require information about how to get from one network to another, and they use that information to forward the traffic appropriately. These defined communication paths are known as routes and can be established a few ways:

1. By default, known as default routes or,
2. Manually, known as static routes,
3. Dynamically, known as dynamic routing. Static and default routes are configured manually, whereas dynamic routing utilizes routing protocols, such as Border Gateway Protocol (BGP) and Routing Information Protocol (RIP) to establish routes. Static and default routing will be discussed further, however dynamic routing is outside the scope of this book, as it is seldom required for home or small business networks.

6.6 IP Addressing

IPv4 IP addresses are conceptualized in two parts: the network part and the host part. IP addresses are made up of four sections, referred to as octets, that are separated by a period (e.g., 192.168.0.15). Valid values for each octet range from 0 to 255. Each octet represents one part of the address and can be used to identify the network part of the address or the host part of the address. The “subnet mask” is used to indicate which parts of the address represent the network and which parts represent the host.

In an analogy similar residential addressing, part of the IPv4 address represents the network address and would be akin to the country, province, city, and street portion of the address and part of the address represents the host number itself, akin to a house number. As an example, consider the following example that shows the analogy between the home address: 25 Blarkon Ave., Slamilton, Ontario, Canada, and the “Class C” IP address 192.168.0.15.

	Country, Province, City, Street/Network			House # /Host #
Home Address	Canada, Ontario, Slamilton, Blarkon Ave.			25
IPv4 Address	192 (Octet 1)	168 (Octet 2)	0 (Octet 3)	15 (Octet 4)

Although the example above shows the first three octets as the network portion of the address with only the last octet representing the host portion of the address (which is extremely common for homes and small businesses), this does not have to be the case. The subnet mask indicates which portion of the IPv4 address represents the network and which portion represents the hosts by indicating a binary “1” for the network portion and a binary “0” for the host portion. This is the traditional long form of a subnet mask that represents a binary “masking” digit for each bit in the IP address. There is a

second, more common and more compact, form for indicating the subnet mask, known as CIDR notation. We'll take a look at both forms.

IP address format and use was specified long ago in [RFC 1020](#) [Romano, Stahl, 1987] and is summarized in Table 12.

Class	Address Range	Network(N) vs. Host(H) Parts in Address	CIDR	# of Networks	# of Hosts/ Network
A	1.0.0.0 - 127.255.255.255	N.H.H.H	/8	128	16,777,216
B	128.0.0.0 - 191.255.255.255	N.N.H.H	/16	16,384	65,536
C	192.0.0.0 - 223.255.255.255	N.N.N.H	/24	2,097,152	256

Table 12: IPv4 Address Ranges

As shown in Table 12, three IP ranges, or Classes, were defined. The Class A IP address space is a group of 128 networks, each with 16,777,216 hosts, and starting with a first octet value of 1 - 127. The Class B IP address space is a group of 16,384 networks, each with 65,536 hosts, and starting with a first octet value of 128 - 191. Finally, The Class C IP address space is a group of 2,097,152 networks, each with 256 hosts, and starting with a first octet value of 192 - 223. The Class A, Class B and Class C network ranges are known together as “classful networks.”

There are three specific network addresses within the classful network ranges that have been reserved for “private” use, and for this reason are not routable on the public internet. These private network addresses are defined in [RFC 1918](#) [Rekhter, Moskowitz, Karrenberg, de Groot, Lear, 1996] and summarized as in Table 13.

Private Class	Network	IP Address Range	# of Addresses	Notes
A	10.0.0.0/8	10.0.0.0 - 10.255.255.255	16,777,216	Class A networks 10.X.X.X
B	172.16.0.0/12	172.16.0.0 - 172.31.255.255	1,048,576	16 contiguous Class B networks from 172.16.X.X through 172.31.X.X
C	192.168.0.0/16 ¹	192.168.0.0 - 192.168.255.255	65,536	256 contiguous Class C networks from 192.168.0.X through 192.168.255.X

Table 13: Private IPv4 Address Ranges

One thing to note, is that on any given network, the first and last addresses (i.e., the .0 and .255 addresses) are not usable, as they are reserved for the “network address” and “broadcast address,” respectively. Thus, the usable range for the last octet in an IP address is 1 to 254.

These private IPv4 address ranges are used by homes and small businesses alike to create local, private networks. They are private because they are behind your router. As a result, your ISP and others on the internet do not see these private addresses in the IP traffic going to and from your router as these private addresses are only used on your local network². Your ISP and others on the internet only see packets from your

- 1 Note that most available consumer and ISP supplied routers will default to this IP address space and will implement a Class C network at 192.168.0.0/24. Another popular default IP address space that consumer and ISP supplied routers implement is 192.168.1.1/24.
- 2 That said, if your ISP provides your router, and you don’t put the router in “bridge” mode and install your own router, then your ISP can probably still monitor all of the traffic through logging, but these are different things, and your ISP is probably not doing that, just that it’s likely possible.

network’s public IP address, and as briefly mentioned in Section 6.1, and discussed in further detail in Section 6.11, NAT is used to enable all of the devices on your network to communicate with the internet using only a single public IP address.

When selecting and configuring your network’s private IP address space it is best to use the IP address spaces defined for private networks. The defined private IP address spaces support a huge number of networks and hosts (256 networks with 256 devices on each network), and using them should create the fewest issues. Keep in mind that there is nothing technically enforcing the use of the defined private IP address spaces. Private networks that don’t use the defined private IP address spaces will probably work just fine. Regardless, it is wise to use the defined private IP address spaces on the off chance that things don’t work quite as expected.

A couple examples are provided below to further illustrate how IPv4 addressing works. In the examples the network parts of the address are red in colour and the host part is black.

Example 1:

Take for instance a typical IP address of 192.168.1.15 and subnet mask of 255.255.255.0.

	1st Octet	2nd Octet	3rd Octet	4th Octet
Subnet Mask	255	255	255	0
Address Part	Network	Network	Network	Host
Network Address	192	168	1	0
Broadcast Address	192	168	1	255
Host IP Address	192	168	1	15

To understand why a subnet mask octet value of 255 means that the whole octet is part of the address, we have to look at the

binary representation of the numbers. Here we use the same address, but represented in binary number format:

	1st Octet	2nd Octet	3rd Octet	4th Octet
Subnet Mask	1111 1111	1111 1111	1111 1111	0000 0000
Address Part	Network	Network	Network	Host
Host IP Address	1100 0000	1010 1000	0000 0001	0000 1111

As shown, for each binary digit in the IP address, the subnet mask digit being a 1 indicates that part of the address is for the network. Likewise, the subnet mask digit being a 0 indicates that part of the address is for the hosts.

In the case of Example 1, the first three octets represent the network, and the last octet represents the host. Thus, in this case, the hosts are only indicated by the last octet, whose usable range is from 1 to 254.

A binary subnet mask uses a string of 1's and 0's to differentiate the network part of the address from the host part of the address, and then each octet is converted to a decimal number for a more compact form. The classic private Class C network, as in Example 1, has a binary subnet mask of 11111111.11111111.11111111.00000000 or 255.255.255.0 in decimal, which is much shorter and easier to read.

Classless inter-domain routing (CIDR), a successor to classful network architecture, provides a more granular method of creating subnets that does not observe the classful networks structure. CIDR notation is yet a shorter form to write the IP address and subnet mask, that uses a forward slash and the number of 1's in the binary subnet mask, to indicate the network portion of the address. Once the network portion of the IP address is established, deducing the host portion of the address is trivial. In Example 1, the CIDR notation for the host is 192.168.1.15/24 and the CIDR notation for the network itself is 192.168.1.0/24. The /24 is because there are 24 1's in the binary subnet mask.

To illustrate the point further, let's consider another example.

Example 2:

Again, let's say we have chosen to use the private IP address space 192.168.1.0 - 255 for our network. While perhaps a little unconventional for a home or small business network, we've decided we want to break our network into 2 subnets using only the last octet. In this example, network 1 spans the IP addresses 192.168.1.0 to 192.168.1.127, and network 2 spans the IP addresses 192.168.1.128 to 192.168.1.255. The subnet mask can be used to create these two networks. Once the two networks are implemented, communication between the two networks requires a router. So what would this look like?

Example Network		Octet			
		1 st	2 nd	3 rd	4 th
1	Network Address	192	168	1	0
	Usable Host IP Range	192	168	1	1-126
		1100 0000	1010 1000	0000 0001	0000 0001 - 0111 1111
	Subnet Mask	255	255	255	128
		1111 1111	1111 1111	1111 1111	1000 0000
	Network CIDR Notation	192.168.1.0/25			
2	Network Address	192	168	1	128
	Usable Host IP Range	192	168	1	129-254
		1100 0000	1010 1000	0000 0001	1000 0001 - 1111 1110
	Subnet Mask	255	255	255	128
		1111 1111	1111 1111	1111 1111	1000 0000
	Network CIDR Notation	192.168.1.128/25			

This example illustrates the concept of how the subnet mask is used to break networks into subnets. In the case of Example 2, a Class C network consisting of 254 usable IP addresses, is

broken into two subnets each with 127 addresses. In practice, with homes and small businesses, subnetting at this granular a level is not usually necessary, but the example illustrates an important concept.

6.7 Dynamic Host Control Protocol

Dynamic Host Control Protocol (DHCP) is a protocol that routers employ as a “DHCP service.” DHCP servers issue IP addresses to devices that request them. DHCP enables the IP address distribution process to be done dynamically, as the name suggests, such that whenever a device connects to the network and requests an IP address, the router automatically determines an IP address for the device and issues it to the device. Many routers also offer the ability to manually assign IP addresses using a “DHCP reservation”. With DHCP reservations, the DHCP server is configured to issue a specific IP address to a specific device when it requests an IP address. The DHCP server does this by having a table that relates the MAC address of the target devices (i.e., those using DHCP reservations) to the desired IP addresses for those devices.

Many readers will know that it is also possible to manually configure IP addresses directly on the end device. Using a DHCP reservation is a better approach to setting static IP addresses, rather than manually configuring IP addresses directly on end devices. This is because DHCP reservations allow you to set the end device to “automatically obtain IP address,” and the DHCP server will issue it the desired IP address. DHCP reservations are easy to implement and ensure that DNS settings can be automatically set (see Section 6.13). Further, since the DHCP server is aware of the reserved IP addresses, it will not inadvertently give it to another device. This can happen if you manually set a static IP address on an end device and your DHCP server gives another device the same IP address (because it has no idea that you manually set it in another device).

It makes sense to setup DHCP reservations for most of the devices on your home and small business networks if you intend to manage them. Likewise, DHCP ranges for automatic distribution of IP addresses should be setup for guest devices and for connecting spontaneously, when needed, to the various networks.

6.8 Default Gateway

An important concept in routing, which is especially relevant to home users, is the idea of a default gateway. A gateway is the “next hop” router (the next router upstream), and the default gateway is the one used when a direct route is not known. A route may be known to a router because:

1. The target networks are directly connected to the router or,
2. A static route has been defined or,
3. The route was determined by a dynamic routing protocol.

When none of these options are available, and therefore a route is not known, the default gateway is used. For example, if a static route is setup that allows the router to know what the next hop router is for a particular network, then that route would be chosen. However, if no static routes are defined, or the target network isn’t directly connected, or a dynamic routing protocol isn’t used, then the default gateway will be used.

For a simple private network connected to the internet there are at least two default gateways that are important to consider. First, all of the devices on a private network require a default gateway, and that is usually set to be the router. As an example, if a network uses 192.168.0.0/24 for its IP addressing (so a “Class C” network with a host IP address range from 192.168.0.1 - 192.168.0.254 and a subnet mask of

255.255.255.0) then an arbitrary device may have an IP address 192.168.0.5 and the default gateway for that device will be set as the IP address of the router, which in this case would usually configured to be 192.168.0.1.

This configuration implies that if the device doesn't know a route to a particular host, like a server out on the internet for example, then it should forward those packets to the router and let the router figure out where to send them. The default gateway is a very subtle, but powerful feature that allows your device to communicate with devices outside of your local network. Usually, the default gateway is set automatically by the DHCP protocol when your network adapter is configured to receive its IP address automatically by DHCP.

Since most devices are configured by default to obtain their IP address via DHCP, all of this goes unnoticed by most users. On a Windows PC, the default gateway configuration is found by going to Settings..Network & Internet.. Change Adapter Options, then right-clicking on the desired network adapter then selecting Properties, then selecting "Internet Protocol Version 4 (TCP/IP)" and clicking the Properties button.

The other important default gateway is the default gateway for the router itself. A home router typically connects two networks together, the private home network and the ISP's network. Those are the only two networks that the router is directly connected to, and as a result, will "know" about. What will the router do when a host says "hey router (ahem default gateway), I need to send this traffic to this IP address, but I don't know where it is!". Well, the router does the very same thing, it says "I don't know that IP address either so I'll send it to my default gateway" (that being the default gateway of the router itself). And so home routers are also configured with a default gateway. In the case of most home networks, the default gateway for the router is configured to be the ISP's router, i.e., the "next hop" router getting your traffic out to its final destination.

Figure 41 illustrates some important concepts associated with the default gateway.

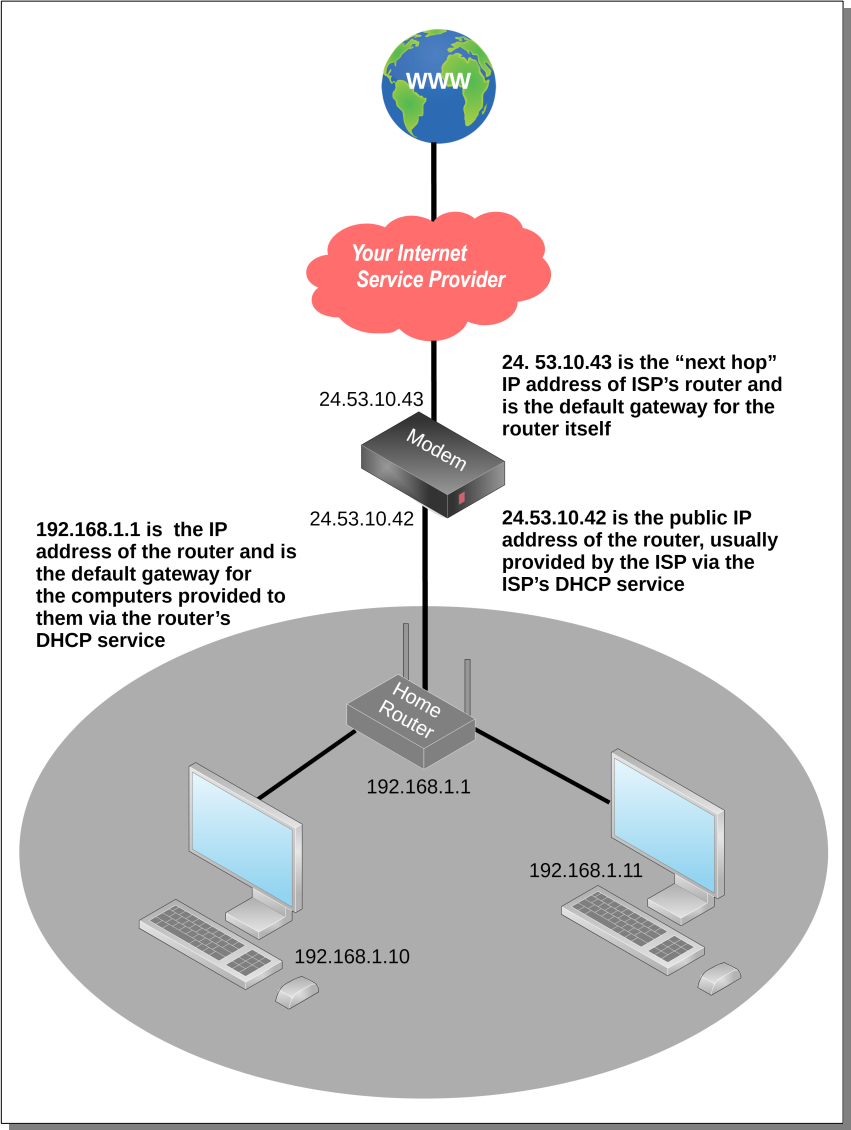


Figure 41: Default Gateway

6.9 Static Routing

As mentioned above, dynamic routing is outside the scope of this book and not typically necessary for home and small business users. However, some small businesses may elect to set up multiple network segments, and depending on the architecture static, routing may be useful. Disinterested readers can very safely skip this section.

Most home and small business network users can take the concept of routing for granted. This is because their network setup is very simple and only consists of a single router. The typical home or small business network only has two networks being connected together by their router, the ISPs network and the home network itself. In this simple setup, all the traffic from the internal network is headed to the same place - to the router (ahem, default gateway), and ultimately to the internet.

By contrast, on networks where multiple routers are networked, in some configurations the routers cannot know about the internal LANs of the other routers without somehow being explicitly told about those LANs. Telling the routers about the internal LANs of the other routers can be done manually using “static routes”. It can also be done by the routers dynamically, but again, that topic is outside the scope of this book.

Entering static routes into a router is how that router will know how to forward packets from its connected hosts to their destination network, via another specific router. Figure 42 illustrates a possible use of static routing. Setting up a network like this is not typical, especially for homes or small businesses, but it illustrates how static routing works.

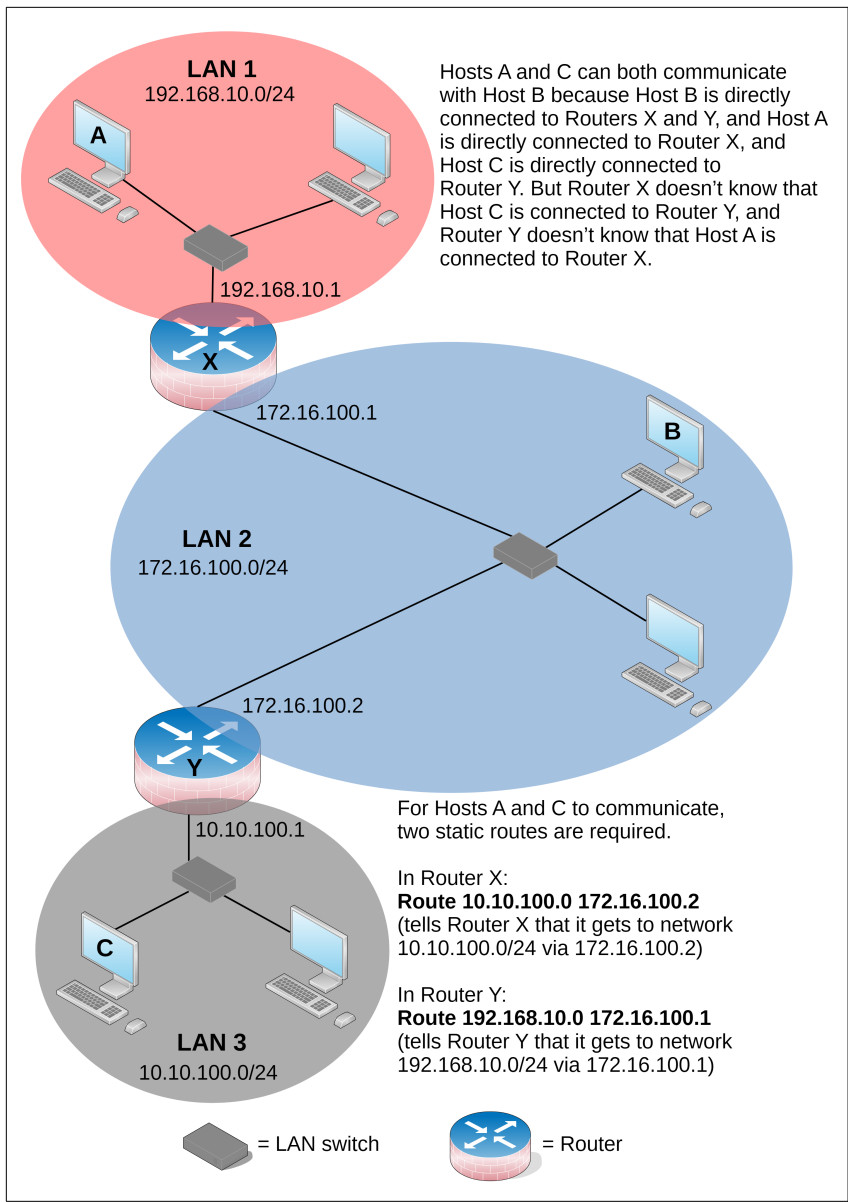


Figure 42: Static routing

In the example shown in Figure 42, Router X does not know anything about the networks connected to Router Y and vice versa. Both Hosts A and C can communicate with Host B, and

vice versa, but if Host A wants to communicate with Host C, or vice versa, then two static routes are required, as shown. Router X requires a static route to tell it that LAN 3 (10.10.100.0/24), where Host C is located, is found through interface 172.16.100.2. And likewise, Router Y requires a static route in to tell it that the LAN 1 (192.168.10.0/24), where Host A is located, is found through interface 172.16.100.1. The two routers can both reach each other's interfaces on LAN 2 (172.16.100.0/24) because they are directly connected through through a LAN switch. The intermediate interfaces belonging to Router X and Router Y (172.16.100.1 and 172.16.100.2, respectively) then become "gateways" for one network to reach another. And returning to the concept of the "next hop," defining static routes is defining the "next hop" interface for one network to communicate with another network that it isn't directly connected to.

The example can be extended further to the LAN3 switch. Imagine, for example, yet another router connected "downstream" of Router Y on LAN 3, call it Router Z. Consider further that Host A wants to communicate with a host on Router Z's LAN. Again, a static route would be required in Router X to indicate that Router Z's LAN can be reached through Router Y (interface 172.16.100.2). From the perspective of Router X, interface 172.16.100.2 still represents the "next hop", or "gateway," to Router Z's LAN. However, since Router Y is not directly connected to Router Z's LAN, a static route would also be needed in Router Y to tell it that Router Z's LAN can be reached through Router Z's interface on LAN3. It would be a good exercise to sketch out this scenario.

Finally, routers will use a static route if one exists, and if none exist they will forward the traffic to the default gateway. In the case of most homes and small businesses, the default gateway, will be the ISP's upstream router. In a small to medium business that has more than one network, the default gateway for each

router is usually the interface of the upstream router that connects to the internet.

6.10 Public IP Addresses

If your network has a public IP address then that IP address is your network's unique, public address on the internet. A public IP address is globally routable on the public internet and is the address that other devices on the internet:

- see associated with ALL requests from devices on your network (e.g., a device on your network requesting a web page)
- return responses to (e.g., delivering requested web page content to the requesting device on your network)
- send direct requests to your systems to (e.g., hosting a game server on your network and a player on the internet wants to connect).

Home and small business networks typically only have one or maybe two connections to the internet. For a typical home or small business network the internet connection is usually made between the modem's Ethernet port and the 'internet' port of the router. The 'internet' port on the router is also known as the wide area network (WAN) port or interface. The WAN port is issued its IP address from the ISP (usually via DHCP), and this IP address is referred to as the network's public IP address. There are some cases where an ISP will provide more than one public IP address, but it is uncommon these days for homes and small business to require, and acquire, more than one public IP address. As discussed in Section 6.8, the router usually receives its public IP address from the ISP through the DHCP protocol. The router then routes the internet requests from the "internal" network to the ISPs network, via its WAN port and public IP address.

Public IP addresses are unique and as described in Section 6.1, there are only a total of approximately 3,702,258,432 IPv4 addresses available for public use. This is not a sufficient number of IP addresses to uniquely identify every device that is communicating on the internet. It's no longer even enough IP addresses to guarantee that every home and business can have their own public IP address. When a public IP address cannot be provided, ISPs will issue homes and small businesses an IP address on the ISP's private network, and will perform network operations to shepherd the customer's connection to the internet. There is a security benefit to not having a public IP address, as your network(s) are not directly accessible from the internet. However, not having a public IP address can also make some internet activities more difficult to accomplish, like hosting your own web server or game server. In these cases, network address translation (NAT - covered in Section 6.11) is likely required to be implemented by your ISP to allow you to perform these functions.

Like your physical address, you want to exercise some caution with providing your public IP address to the public (i.e., to the systems on the internet). First, consider that in the physical world you wouldn't send mail to someone with your return address on it, if you didn't want them to know your physical address. There are good reasons for this. Perhaps you don't want someone to know where to find you. Or perhaps you don't want someone to have your physical address enabling them to send you junk mail. The exact same analogy exists with your public IP address. When you visit a website or otherwise interact with the internet, your public IP address is carried with the digital packets, like your return address on the envelope. Interacting with the internet with your public IP address is like sending physical mail with your physical address on it. And just like in the physical analogy, the receiver now has your digital address. That information may not only enable those internet systems you've interacted with to target ads at you, but also to mount more sophisticated attacks against your router.

Knowledge of your public IP address would be interesting to a “bad actor” that wanted to attack your network.

With this in mind, you want to guard your public IP address to some degree. Ideally, only visit trusted, or otherwise “low risk” websites with your public IP address. Also, it wouldn’t make sense to just give out your public IP address to someone if they asked for it.

Traffic originating from your home or small business network router is tagged with the router’s public IP address. The communication methods used by modern networks use your public IP address to work properly and knowledge of your public IP address will be available to the various internet resources you interact with. This is the nature of the beast. When knowledge of your public IP address is combined with other personally identifying information you may provide to websites, say like, googleamazonfacebooktwitterreddit instagrameamartiktoketc.com then your public IP address can be married to your identity. Pretty powerful stuff really.

Additionally, as described in Section 2, many home routers have vulnerabilities that can be exploited. A bad actor having knowledge of your public IP address and a vulnerable router are not a good combination. It’s good to keep knowledge of your public IP address away from bad actors, to keep your router up to date for security updates, and to replace your router when it is no longer supported and receiving security updates.

You can hide your public IP address through the use of a Virtual Private Network (VPN) service. VPNs are covered in Section 6.16.

Finally, a note on the “tagging” of packets leaving your network with your public IP address; this is not a routing function, but NAT, described further in Section 6.11.

6.11 Network Address Translation

As mentioned previously (not unlike a broken record), IPv4 makes available only approximately 3,702,258,432 public IP addresses. This is nowhere near the number of IP addresses that would be necessary for all of the Ethernet devices of the world to communicate with each other if they were given public facing IP addresses. This is a shortcoming of the design of IPv4. The new IP protocol IPv6 is slowly replacing IPv4, and once implemented, every internet connected will device be able to have its own public IP address as IPv6 offers 340,282,366,920,938,463,463,374,607,431,768,211,456 unique addresses. The implementation of IPv6 will bring a different security landscape, but for now IPv4 continues to dominate the internet.

How do all the devices connected to a private network communicate with the internet if there is only one public IP address? Through a little piece of technology called, you guessed it, network address translation (NAT). Although there are other uses for NAT, the most common use is to provide a way for all the devices on a private network to effectively communicate with the internet using only one public IP address.

Obscuring the technical details as to how it actually works under the hood, NAT allows for all of the IP packets from the devices on your “internal” network to be “tagged” with the network’s public IP address when the packets leave your router’s WAN port. To other devices on the internet, every outbound packet leaving your network will appear as though that packet originated from your router directly (although it actually originated from a device inside your network). Through the use of a “NAT table”, the router keeps track of which systems made which internet requests so that when packets are returned the router knows which internal device to forward the returned packets to.

For many years NAT has enabled most of the Ethernet-enabled devices of the world to effectively communicate on the internet while existing on internal private networks behind routers that have only one public IP address. Regardless, the world is determined to move to IPv6 eventually and the IPv4 address limitation will no longer be an issue.

Another benefit of NAT is that it allows for hiding the IP address details of the devices on the internal network when communicating with devices on the internet. Exposing only a public IP address is better from a privacy and security perspective than having to expose a bunch of internal IP addresses. For this reason, this type of NAT is also known as masquerading as it allows for masking the internal IP addresses with the public IP address.

As IPv6 proliferates, it seems that it will be an option, or may even be necessary, that ALL of our devices will use their own public IP address. This concept seems to fly in the face of privacy and security. That said, given the right amount of hardening, having a device like a smart watch communicate with its own public IP address could really simplify some things.

Along with NAT comes the concept of port forwarding. With only one public IP address, in order for devices on the internet to be able to reach a device inside your internal network (e.g., a web server or gaming server that you host), port forwarding is needed.

6.12 Port Forwarding and Reverse/Application Proxy

Most Ethernet communications occur not only with an IP address, but also with something known as a “logical port”, or simply, a port. The combination of an IP address and a port number is known as a socket.

Ports are assigned to applications and processes so that those applications and processes can be uniquely identified. The port

number assigned to an application is used to direct Ethernet packets arriving at the router's WAN port to the correct device inside the internal network. For this to work, the router's "port forwarding" settings are configured such that all traffic received on its WAN interface bearing a particular logical port number will be forwarded to the IP address of the chosen internal system. E.g., a gaming server with IP address 192.168.1.10 is waiting for connections (i.e., listening) on port 7070. In order to facilitate connections from requesting gaming clients on the internet, the router is configured to forward all incoming traffic received on its WAN interface bearing port 7070 to IP address 192.168.1.10 (the IP address of the gaming server). Figure 43 provides graphical depiction of this scenario.

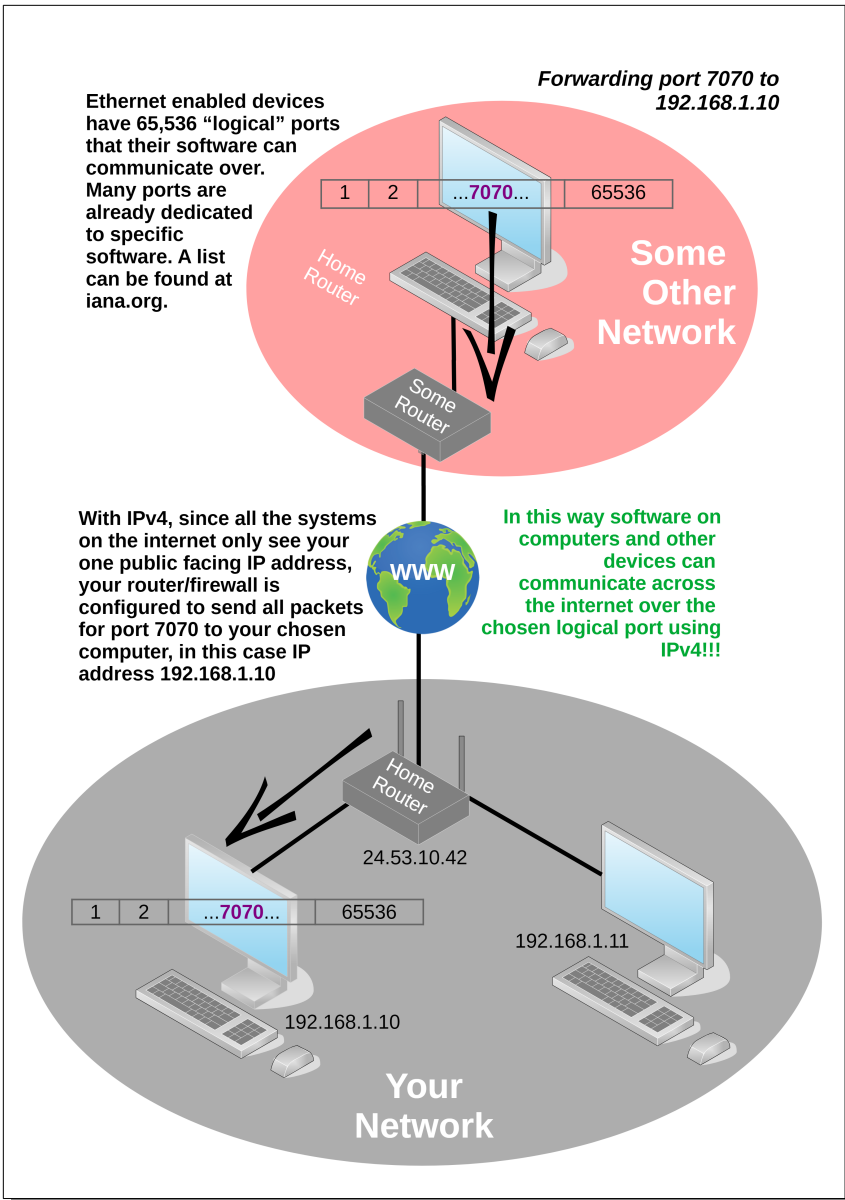


Figure 43: Port forwarding and reverse proxy

Port forwarding is another form of NAT. Thus, NAT not only provides a method for all devices on a private network to be able to communicate with the internet through a single public

IP address, but also provides a method for devices on the internet to initiate communication with devices on private networks through port forwarding. Pretty slick.

Port forwarding is one method of allowing devices on the internet to initiate communication with devices on your private network. Another method is by using a “reverse proxy”, also known as an “application proxy” or “web application firewall” (WAF). Reverse proxies work similarly to port forwarding in that they use the logical port to determine the internal system to forward the packets to. However, the key difference is that reverse proxies intercept the packets and apply additional security measures before forwarding the packets to your internal device. This is a better security configuration than port forwarding alone.

6.13 Domain Name System

The Domain Name System (DNS) is how the internet converts or “resolves” the public IP addresses across the internet to their registered domain names. Domain names are easier to remember than IP addresses and can be used as part of branding. Domain names are registered with various domain name registrars like GoDaddy, Hostinger, HostGator, etc. The book “DNS and Bind (Liu, Albitz)” is recommended as further reading on the subject of DNS.

Typically, home and small business networks have their devices configured to obtain their IP addresses automatically through DHCP, as previously described in Section 6.7. When a connecting device requests an IP address of a router via DHCP, the router is configured (usually by default) to provide the DNS server address along with the issued IP address. Usually the router will provide its own IP address as the DNS server, such that when DNS requests are made by devices on the local network, those DNS requests go to the router, and the router forwards those requests to the ISP’s DNS servers. The ISP’s DNS servers then forward those requests on to the their upstream DNS servers

and so on until a so called “Authoritative DNS Server” is found. Authoritative DNS servers hold the DNS records and can finally resolve the domain name to its actual public IP address. This really is fundamental internet stuff.

You can change the DNS server used by your various devices and there is good reason to consider doing so. Usually the DNS server can be changed at the device level, but doing so also requires manually setting the IP address details for that device, which is usually not ideal. A better approach to consider is to change the DNS server address provided by the router’s DHCP service to connecting devices. Even better, using “DHCP reservations” in the router means that connecting devices obtain their IP addresses automatically, while being provided a specific DNS server address (as configured in the router’s DHCP service), which is ideal.

Why might you want to use a different DNS server address than your ISP’s DNS server(s)? Speed, reliability, and security. Some publicly available DNS servers are better than others so if you’re considering changing your DNS server it’s worth doing a bit of research to figure out the one that suits you.

There are also interesting DNS products available, like the free and open source Pi-hole software. Pi-hole acts like a DNS server for your local network and maintains list of known advertising servers, and other potentially dangerous internet addresses, and filters traffic requests to those addresses. This can effectively cut down a lot of advertising on your home network and provide another security layer in a defense in depth strategy. The concept of defense in depth is further described in Section 7.1.

6.14 Voice-over-Internet Protocol (VoIP)

VoIP systems allow phone calls to be made over the internet, rather than over traditional Plain-Old-Telephone-System (POTS) technology. Today, there are all kinds of VoIP implementations,

but one of the original use cases and one that is still prevalent to many homes and small businesses, is using an analog phone or phone network with VoIP (i.e., an old school home phone but over the internet). This can be done with a VoIP router, which has both female RJ-11 connectors to connect an analog phone or phone network, and female RJ-45 connectors to connect to an Ethernet network and the internet.

Your ISP is usually quite happy to sell you VoIP services. Getting your VoIP services from your ISP is usually a pretty convenient option as VoIP capabilities are often built into the router your ISP supplies which simplifies the setup. However, you may find that you want to use a 3rd party VoIP provider. There are many 3rd party VoIP providers on the internet and often they are lower cost.

Using an analog phone or phone network with a 3rd party VoIP provider requires you to get and deploy your own VoIP router. With this arrangement you'll get the "Session Initiation Protocol" (SIP) settings from your VoIP provider (usually just a username, password, and server addresses) and enter the settings into the VoIP router, usually via a web interface.

Also, when deploying your own VoIP router, you need to decide if the VoIP router is connected to the main router's LAN (and the main router is directly connected to the ISP), or alternatively, the main router is connected to the VoIP router's LAN (and the VoIP router is directly connected to the ISP). Generally, your home router is more powerful than your VoIP router so it usually makes sense to place the VoIP router on the main router's LAN, and let the VoIP router obtain its IP address from the main router's DHCP service¹. That said, in this case, because your VoIP router is now "behind" your main router,

1 When the VoIP router is connected to the home router's internal network, you probably don't *need to*, but it's likely a good idea to turn off the DHCP server on the VoIP router. Unless you're connecting devices on the internal network side of the VoIP router, then you should not require the DHCP server be enabled.

ideally you are able to configure your main router's "Quality of Service" (QoS) settings to prioritize your VoIP traffic, to help ensure the best phone call quality possible. If you place your VoIP router behind your main router, and you are experiencing problems with phone calls, and you don't have QoS capability on your home router to help prioritize the calls, then you might have to consider putting your main router behind your VoIP router. Yuck though.

The other alternative is that your ISP provides you with more than one IP address and both your main router and VoIP router are directly connected to the ISP. In that case, neither is behind the other, which is probably the best case scenario.

Today, rather than using analog phones with VoIP routers, you can also purchase IP phones that work directly with VoIP providers. IP phones include rechargeable, cordless or corded handsets that cradle into base stations that connect over WiFi, or hardwired Ethernet, to the network and then directly to the VoIP service provider. If you have the need for a home or small business phone or phone network then WiFi IP phones are a slick solution. There are also Bluetooth handsets available that can be paired with cell phones to provide a "home phone" like experience.

Finally, just a note on power and emergencies. POTS works when the power is out, but there is a very strong probability that any kind of VoIP solution you deploy will not. Even if you have a good backup power solution, it is unlikely that your ISP will continue to serve internet for very long in a power outage (unless advertised). Additionally, depending on your VoIP provider, you may not have reliable 911 service either. These shortcomings should be considered when determining what kind of phone system you require. Recently, iPhones and Android smartphones have started including a feature to connect to a satellite network to send and receive messages, which may be very handy in a power outage.

6.15 Wireless Networks

Wireless networking has become a key method of connecting networks due to its obvious convenience - no cables required! Most wireless networks employ radio technology to implement the communication. Such radio communication occurs over specific radio frequencies (RF). Rather than sending electrical pulses down a cable, radio systems communicate over airborne electromagnetic waves. The same waves that traditional radio stations emit, but harnessed and directed for bidirectional Ethernet communication. An overview of popular wireless networking technologies is provided below.

6.15.1 WiFi

WiFi is a weird name. It was a creation of a marketing group and doesn't mean anything in particular, least of all "wireless fidelity," as the moniker seems to suggest (from the term "HiFi" that was common with high fidelity stereo systems). WiFi is the name of an extremely popular wireless networking technology that most people know and use in their homes, workplaces, and countless other locations. The specifications for WiFi are defined in the IEEE 802.11 standards that describe the characteristics of the devices that WiFi device manufacturers adhere to in order to produce WiFi devices that talk to each other "wirelessly."

WiFi is a communication technology that uses radio waves to wirelessly transmit and receive digital signals that represent Ethernet networking traffic. Radio waves are a type of electromagnetic radiation that behave like physical waves that people are more familiar with, such as the waves produced when a stone is thrown into a pond. Such waves can be described by the periodicity of the peak of the wave that they produce, which is denoted as its frequency. More precisely, frequency is how many times the complete waveform (one cycle) is produced per second. The unit of measurement for

frequency is cycles per second and denoted as “Hz”, named after Heinrich Rudolph Hertz who was the first person to prove the existence of electromagnetic waves.

The types of waves used in many applications, including radio waves, have a very high frequency, so it is common to express the magnitude along with the unit of measurement. For example, the WiFi radio spectrum expressed in units of Hz would look like 2,400,000,000 Hz and 5,000,000,000 Hz. This is much more succinctly written as 2.4 GHz and 5 GHz (gigahertz - billions of Hz). To contrast, the AM radio frequency range is 535 to 1705 kHz (kilohertz - thousands of Hz) and the FM radio frequency range is 88 to 108 MHz (megahertz - millions of Hz).

Electromagnetic radiation with a frequency of 3 kHz to 3000 GHz is considered the radio spectrum. When a time-varying electrical current is applied to an antenna electromagnetic radiation occurs. This property can be leveraged to develop schemes for wireless communication technologies. Today, RF electronics are used as radio transmitters that produce the required time-varying current signal (according to the communication scheme). When this signal is connected to an antenna it radiates through free air, allowing a complementary receiver system to receive the RF signal, enabling communication.

WiFi is a low power RF system that allows bidirectional digital information to be “piped” through an analog radio transmission system. By contrast, amplitude modulation (AM) and frequency modulation (FM) radio systems are higher power and unidirectional. AM and FM radio stations broadcast a strong, one-way, radio signal that is received by radio receivers, known to most people as “radios”. AM and FM radio systems transmit and receive encoded, analog, audio signals. WiFi systems transmit and receive encoded digital information, such as Ethernet packets.

As mentioned, the WiFi standards call for two specific RF bands: 2.4 GHz and 5 GHz bands. The RF spectrum is a whole topic on its own, and entities that wish to communicate over portions of the RF spectrum often have to obtain a license to do so. This licensing process is important to ensure that various entities don't unintentionally communicate over the same frequencies in the same physical space and interfere with one another. There are, however, certain bands of the RF spectrum that are reserved for unlicensed use. Communicating in these bands does not require obtaining a license to do so, but the implication is that nothing will prevent another transmitter from interfering in your band.

The two specific frequency bands used for WiFi are reserved for unlicensed use. This means that any use of WiFi does not require any licensing, but also means that interference is possible. In order to limit such interference, WiFi radio transmitter strength is regulated and limited in most devices. Additionally, the WiFi frequency band is broken down into specific frequency channels that provide a way of changing the WiFi channel to another that may be less used in the vicinity of your WiFi router. There are applications, typically for mobile devices, that can help identify which WiFi channels are less "busy" than others in a given physical space.

In order to communicate Ethernet traffic over WiFi, Ethernet packets originating from wireless devices connected to a WiFi network are "modulated" from their digital format into the appropriate radio signal using a modulator and the radio signal is then amplified and broadcasted into the air with a transmitting amplifier and antenna. From there, the radio signal propagates through the air where a reciprocal receiving antenna and amplifier receives the signal. From there, the signal is demodulated, using a demodulator, back into its original digital format Ethernet packet. In order to implement bidirectional communication, WiFi radio systems consist of both transmitting and receiving components.

In most cases, only a single antenna is required for transmitting and receiving Ethernet packets because an automated electronic switch is used to switch access to the antenna between the transmitting and receiving electronics. All of these electronics are implemented in WiFi adapters. WiFi routers have WiFi adapters implemented in them. Laptop computers and mobile devices have WiFi adapters installed. Some desktop computers today also come with WiFi adapters installed, but they can also be installed separately either in a PCI slot or a USB port. There are odd times when there is a need for a laptop to have a second WiFi adapter and USB WiFi adapters are good for this purpose.

There are various ways, historically, that radio signals have been generated, but today's WiFi enabled devices use microprocessors and microcontrollers (programmable chips) to generate the signals that are fed into amplifiers and then into antennas, and likewise to receive and demodulate the signals from other WiFi transmitters.

WiFi enabled devices usually have options to enable and disable the device's WiFi capability, as well as change the device's WiFi parameters. Normally, enabling the WiFi capability on an end device will cause the device to automatically search for available WiFi networks to connect to. At home, the available networks that most people see in their neighbourhoods are their own WiFi router along with their neighbours' WiFi routers. However, sometimes the available WiFi networks include WiFi access points (WAPs). From the perspective of connecting to an available network, there is no noticeable or material difference between connecting to a WiFi router or a WAP. Both WiFi routers and WAPs facilitate connections to the WiFi network, but only the WiFi router routes the traffic to the internet. When connecting to a WAP, the WAP is shepherding your connection to an upstream router in the network. It's a pretty mundane detail, but a detail nonetheless.

Acting as a WiFi repeater, WAPs are often used to extend the range of a WiFi network. Other times, WAPs are deployed to specific physical locations and hardwired back to the main router, providing a WiFi connection for WiFi devices near the WAP.

You can configure a typical router by logging into its web interface (i.e., the website that is presented when you enter the router's IP address into a web browser's address bar). Typically, for a brand new router, a computer that is configured to "obtain IP address automatically" (i.e., is DHCP enabled) can be physically connected by Ethernet cable to any of the Ethernet LAN ports on the new router. The router will then issue the connected computer an IP address on its LAN, and the computer will be able to communicate with any other devices on the LAN, including the router itself. The web interface of the WiFi router can then be opened in a web browser on the connected computer.

It is very typical that "out of the box", a new WiFi router will have its web interface available at <https://192.168.0.1> or <https://192.168.1.1> (sometimes http instead of https for older devices). You can tell by looking at the IP address that the router issued your connected computer (again, for a computer that is configured to "obtain IP address automatically", which is usually the default setting). In Microsoft Windows this is done by opening the Ethernet adapter properties from the Control Panel or using the command prompt and executing the command: `ipconfig`. Similar methods are available for Apple and GNU Linux computers to display the computer's IP address. Once you see the computer's IP address, you'll be able to tell what the IP address of the WiFi router's web interface will be. For example, if a router issued the connected computer an IP address of 192.168.100.10, then it is very likely that the web interface will be found at <https://192.168.100.1>. Every router will have a different looking web interface, but once logged in

the user can configure all the various parameters and routers usually offer similar options.

WiFi routers and access points can be configured to allow unauthenticated connections to the WiFi network (i.e., without the use of a password), so called “open” networks. Allowing unauthenticated connections to your WiFi network permits any arbitrary device to connect to your network. Imagine someone connecting to your WiFi network and surfing very seedy, or even illegal websites, on your network. Unauthenticated WiFi connections also do not encrypt the network traffic. This means that WiFi devices on the network can intercept and inspect each other’s Ethernet communications (with a network adapter in “promiscuous” mode). Open WiFi networks don’t encrypt the network traffic so it’s advised to simply not connect to them, and not to set them up yourself for your own network. If you do need to connect to an unauthenticated WiFi network, consider using a VPN (see Section 6.16). As usual, it’s best to configure your router to require a strong password to connect to your WiFi network. An older WiFi security protocol that should be avoided is WEP as it contains significant security flaws and is considered broken and insecure. WPA is also no longer recommended for use. Instead, better WiFi protocols to use for WiFi security are WPA2, and WPA3.

When a WiFi enabled device finds available WiFi networks to connect to, it is because nearby WiFi routers or WiFi access points are broadcasting their service set identifier (SSID). The SSID is usually configured in the WiFi router’s web interface. The SSID is the literal character string broadcasted by the WiFi router that will allow devices searching for available WiFi networks to list the router and allow initiation of WiFi connections to it. The ability for WiFi routers to broadcast their SSID so that client devices can search for it and initiate a connection by clicking on it is very convenient. In general, it isn’t considered to be too dangerous to broadcast your SSID, as long as the connection uses WPA2 or WPA3.

It is often possible to disable SSID broadcasting via the WiFi router's web interface. If you disable SSID broadcasting, then it is necessary to know the SSID of the WiFi router and to manually create the connection to the WiFi router. Some people perceive disabling SSID broadcasting as increasing their privacy and security, and it does, in a very weak and limited way. There are tools that attackers can use to provide insight into wireless transmissions that can report back SSIDs. Attackers may perceive additional value in targets that are going out of their way to superficially hide their SSIDs. It's generally advised to just go ahead and broadcast your SSID.

The typical steps for configuring an off-the-shelf WiFi router include:

1. Calling your ISP to ensure your ISP supplied modem/router is in bridge mode (if needed).
2. Opening the box, plugging the router into power, powering on the router, physically connecting a computer (configured to obtain its IP address automatically) with an Ethernet cable to one of the router's LAN ports.
3. Determining the WiFi router's web interface IP address by reading the router's manual or by looking at the computer's obtained IP address.
4. Using a web browser to open the router's web interface by entering the IP address of the router into the browser's address bar, typically `https://192.168.0.1` or `https://192.168.1.1`. (sometimes older routers use `http://`).
5. Logging into the WiFi router's web interface by entering the default username and password into its login page. The default username and password are usually found in the manual, but also very often can be found online (a very good reason to change it as soon as possible).

6. Changing the admin account password to a strong one. Better yet, see if you can add another administrative account with a username (not “admin” or “administrator”!) that you choose and give it a good password. Verify that you can login with your new administrative user account and consider deleting or disabling the default admin account.
7. If desired, reconfigure the LAN IP address range from its default. This is done in the DHCP service settings of your router. Perhaps the default is 192.168.0.1, but you’d like to change it to 192.168.150.0/24. If you choose to do this you’ll need to pay attention to the IP address of the web interface as it needs to be on the same network, e.g., if you did change the LAN to 192.168.150.0/24 then it’s pretty customary to have the router’s IP address be 192.168.150.1. This too can be changed though very few people choose to. If you do choose to change it you’ll just have to remember what you changed it to for when you want to connect to it again. Heads up that when you change the LAN network address space from its default and apply the change, your computer will lose its connection to the router. Your computer will need to get a new IP address on the new network address space, which is usually done automatically, and then you’ll need to enter the new IP address of the router into the web browser address bar again, and then reconnect and re-login. Phew. I mean, that sounds like a lot, but it’s not.
8. While you’re looking at your DHCP service settings, consider changing the DNS server IP address that your router issues to DHCP clients. Your router distributes DNS server IP addresses when it issues IP addresses via its DHCP service. OpenDNS and CloudFlare are both excellent publicly available DNS servers to consider using in place of your router’s IP address.

If you implement a Pi-hole server on your network that acts as a DNS server, then you would enter the Pi-hole server's IP address into the primary DNS server settings of your router's DHCP service. For the secondary DNS server you have the choice of your own router's IP address (and in turn your ISP's DNS server), or a publicly available DNS server. With this Pi-hole setup, your DHCP clients forward their DNS requests to the Pi-hole server and the Pi-hole server filters them before forwarding them on to another DNS server. The Pi-hole server itself still needs to be able to forward DNS requests from the clients (and itself!) to authoritative DNS servers on the internet. Thus, the Pi-hole server's DNS server setting should be set to your router's internal IP address or a publicly available DNS server's public IP address.

9. Opening and configuring the WiFi settings in the web interface:
 1. Enable WiFi.
 2. Provide an SSID for the WiFi network.
 3. Enable/disable broadcasting of SSID.
 4. Enable WPA2 or WPA3 and configure it with the desired password.
10. Confirming that the WiFi router's WAN port is configured to obtain its IP address automatically, which it will obtain from the ISP by its connection to the modem that is connected to the ISP's network.
11. Connecting the WiFi router's WAN port to the network port on the modem.
12. Physically disconnecting (unplugging) the computer from the LAN port of the WiFi router and connecting the computer to the WiFi router wirelessly instead, using the configured SSIDs and passwords.

13. Verifying the computer can access the internet by opening websites in a browser.
14. Verifying that the router is configured to only allow configuration from the internal LAN so that it cannot be configured from systems on the internet.
15. Configuring logging and alerting, if available. You might want to know whenever anyone logs into the router. It doesn't hurt to log everything you can to help diagnose issues, should they arise. If you have a "remote syslog server" or some other kind of log aggregation server then you'd configure your router to send its logs to your log aggregation server.

If your WiFi router has both 2.4 GHz and 5 GHz capability, then your various devices can connect to either WiFi network. Most commonly, once the devices are connected to either the 2.4 GHz or 5 GHz WiFi radios they will all be on the same logical network.

While it is common that devices on the same network need to be able to communicate with each other, sometimes there is no need at all. For example, guests in a hotel or rental property, passengers on a plane or train, etc. For this case, many WiFi routers and access points have the ability to use a feature called "host isolation mode," where even though, logically the devices are on the same network, they are prevented from being able to communicate with each other. This is a really nice, simple, and secure feature for some applications.

Why would one connect to the 2.4 GHz vs. the 5 GHz WiFi radio? The 2.4 GHz frequency is slower than the 5 GHz frequency and it is known to be more susceptible to noise, but it provides longer range and is able to work through walls and obstacles better. These characteristics arise from the fundamental properties of the waves. The preferred use of the 2.4 GHz vs 5 GHz WiFi radios depends on the application.

Typically, 2.4 GHz WiFi is deployed for general use, while 5 GHz is used for applications that have high bandwidth requirements like video streaming and gaming. There are applications that can help determine what speeds are available from the WiFi networks at various locations away from the antenna.

It is useful to know that if there are multiple WAPs in your network, if all the WAPs are configured with the same SSID then the WiFi clients will roam between the WAPs and automatically connect to the that provides the best connection. Just broadcast the SSID and configure the access points with the same WiFi network login credentials and you should be able to roam between access points.

There are also WiFi mesh network systems available. WiFi mesh networks implement a WiFi router and use a series of physically distributed WAPs to create WiFi coverage in a physical area, using the WAPs as repeaters. These types of networks provide seamless WiFi coverage for an area and have the intelligence to reconfigure how the WAPs repeat the WiFi signal in the event that one or more of the access points fail.

6.15.2 Cellular Networks

When we are away from our homes and offices most of us use cellular networks to make phone calls and to access the internet. Like WiFi, cellular networks utilize radio communication. However, unlike WiFi, cellular networks utilize licensed radio frequency bands to help ensure the integrity of the radio communications. Licenses to communicate on the licensed radio frequency spectrum are typically granted by a regional radio spectrum authority. In Canada, the Government of Canada's "Innovation, Science and Economic Development" branch issues radio spectrum licenses. In the US, the Federal Communications Commission (FCC) issues the radio spectrum licenses. The licensing process typically involves providing information about the physical locations of the transmitting and receiving antennae and communication path, along with the

operating frequencies and safety related information. Radios emit non-ionizing electromagnetic radiation that can be a danger to humans (and other animals) that find themselves in the path of the radiation of powerful radio transmitters. Being in the physical path between two powerful cellular tower-type systems can be dangerous. This is why safety related information is supplied to radio spectrum licensing bodies during the application process, to ensure the public is not put at risk by the cellular system.

Your mobile device has a cellular radio transmitter and receiver allowing it to communicate via radio signals to cell towers. The radio signals that your cell phone transmits and receives are generally considered not powerful enough to be dangerous to humans. Certainly, the radio signals that your cell phone transmits and receives are nowhere near as powerful and dangerous as the point-to-point microwave radio systems that make up the backbones of cellular networks.

The settings of your mobile device allow you to configure the parameters of the cellular connection including whether “cellular data” is turned on or off, which cellular networks are allowed, and whether mobile hotspot is turned on or off. For example, on iOS, the cellular settings can be found under Settings..Cellular.

Cellular communication has two forms, “cellular” proper, which allows phone calls and SMS messages to be made without consuming “data”. The other form is “cellular data,” which is for interacting with the internet, like browsing, instant messaging, using internet-enabled apps, etc. In a way, this breakdown of services is just marketing, but nonetheless many cellular service providers sell cellular plans that have these three options listed separately. I.e., phone calls, SMS messaging, and data. Ideally, you can find a plan that suits your needs at a price that you can afford. Today in Canada, cellular plans (including “unlimited” plans) have become considerably more affordable than in days past, especially from the so-called

“Mid-level Tier” cellular providers (also known in the industry as “Tier 2”).

Smartphones typically offer the ability to create a mobile hotspot, which allows the smartphone to become a WiFi router, allowing other WiFi devices to connect to it and access the internet via the smartphone’s cellular connection. A common use of mobile hotspots is to provide mobile internet for devices that can only connect with WiFi, i.e., the device does not have cellular capability or does not have an active SIM card or cellular plan.

As previously mentioned, cellular communication occurs over the licensed band of frequency spectrum. Cellular communication service providers will acquire and license, typically from a government agency, portions of the frequency spectrum in whatever locations they are serving.

The Canada and US cellular network types, speeds and frequencies are summarized in Table 14.

	Type	Speed (Mbps) ¹	Operating Frequencies (MHz)	
			Canada ²	USA ³
2G	GPRS	0.1	GSM 850, GSM 1900	
	EDGE	0.3		
3G	3G Basic	0.3	UMTS 850 UMTS 1700 UMTS 1900	UMTS 850
	HSPA	7.2		UMTS 1900
	HSPA+	21		UMTS 1700
	DC-HSPA+	42		UMTS 2100
	LTE Cat 4	150		
4G	4G+ LTE- Adv. Cat 6	300	LTE 700 (12, 13, 17, 4, 29)	
	4G+ LTE- Adv. Cat 9	450	LTE 1700 (4, 66) LTE 1900 (2) LTE 2100 (4)	LTE 700 (12, 13, 17) LTE 1700 (4, 66) LTE 1900 (2, 25)
	4G+ LTE- Adv. Cat 12	600	LTE 2300 (40) LTE 2500 (7) LTE 2600 (7, 38)	LTE WCS 2300 (30)
	4G+ LTE- Adv. Cat 16	979	LTE 3500 (42)	

1 <https://kenstechtips.com/index.php/download-speeds-2g-3g-and-4g-actual-meaning>

2 <https://www.gsmarena.com/network-bands.php3?sCountry=CANADA>

3 <https://www.gsmarena.com/network-bands.php3?sCountry=United+States>

Type	Speed (Mbps)	Operating Frequencies (MHz)	
		Canada	USA
5G	1000 - 10,000	5G 2600 (38, 66)	5G 2500 (41)
			5G 39 (260)
			5G 28 (260)
			5G 600 (71)

Table 14: Canada and US cellular network types, frequencies, and speeds

6.15.3 Bluetooth

Bluetooth itself is an open standard that describes a low cost, low power radio network, that operates in the 2.4-2.4835 GHz Industrial, Scientific and Medical (ISM) unlicensed frequency band. Note, this is the same frequency band that WiFi operates in. Bluetooth allows devices to communicate wirelessly by allowing the ad hoc creation of “Wireless Personal Area Networks” (WPAN), known as a piconets.

Bluetooth enables a number of useful wireless capabilities, they are summarized in Table 15.

Bluetooth Function	Example(s)
Cable Replacement	Audio cables - Wireless headphones, speakers, and microphones
	USB cables - Keyboards, mice, printers, cars, gamepads, smart watches, hearing aids, etc.
Internet Connectivity	Using an internet connected (WiFi or wired), Bluetooth enabled device to share internet with other Bluetooth enabled devices.
	Using a smartphone to share cellular

Bluetooth Function	Example(s)
	data with other Bluetooth enabled devices.
File Sharing	“Piconets” established between Bluetooth devices allow files to be transferred between them.
Device Synchronization	Bluetooth devices can synchronize information between them, like contact information.

Table 15: Bluetooth capabilities

The earliest versions of Bluetooth were version 1.0 and 1.0B and they were initially announced in 1998, formalized by the “Bluetooth Special Interest Group,” (SIG) consisting of companies such as Ericsson, IBM, Intel, Nokia, and Toshiba, among others that joined later. Version 1.1 was issued as IEEE 802.15.1-2002, then version 1.2 as IEEE 802.15.1-2005. Increasing versions have been released, up to version 5.3 at the time of this writing (released by the SIG in 2021) with increasing functionality. A couple important points are that devices implemented with Bluetooth version 2.0 and lower had limited sound capabilities and were mostly geared toward voice communications, like “hands free” calling. Bluetooth Version 4.0 included Bluetooth Low Energy (LE), which brought significant energy consumption reductions.

Early Bluetooth implementations allowed the “pairing” of a bluetooth enabled mobile headphone, headset, speaker, or car speaker system to a smartphone to provide “hands free” communications, typically for driving purposes. Today, implementations of Bluetooth have expanded to include the ability to stream audio, not just voice communications, but audio like mp3s and streaming services (i.e., Apple Music, Spotify, Tidal, etc.).

Bluetooth is specified with “profiles” and the implemented profiles determine a given device’s capability. The Bluetooth profiles are summarized in Table 16.

Bluetooth Profile	Description
Hands-free (HFP)	Allows a paired device (headphone, car, speaker, etc.) to make phone calls and use phone features
Headset (HSP)	Allows a paired device to receive phone calls, hang up phone calls and adjust the volume
Advanced Audio Distribution (A2DP)	Allows streaming of audio from one paired device to another
Advanced Video Remote Control (AVRCP)	Allows a paired device to control media playback (play, pause, stop, skip track)
Phone Book Access (PBAP)	Allows one paired device to access the contact information stored in another device for use with the “Caller Announce” feature that allows users to retrieve and dial a phone number by speaking the name of the contact.

Table 16: Bluetooth profiles

Table 17 summarizes the speeds and ranges of the Bluetooth versions.

Version	Speed	Range
1	732.2 Kbps	10 meters (~33 ft)
2	2.1 Mbps Enhanced Data Rate	30 meters (~100 ft)
3	24 Mbps (via Wi-Fi)	30 meters (~100 ft)

Version	Speed	Range
4	24 Mbps (EDR)	60 meters (~200 ft)
5	50 Mbps (EDR)	240 meters (~800 ft)

Table 17: Bluetooth versions, speeds, and ranges

Connecting or pairing your Bluetooth enabled devices typically requires that the devices be placed in “pairing” mode. While in pairing mode, Bluetooth devices listen for connections from other Bluetooth devices that are searching for listening devices to connect to. A very typical example is pairing headphones. Usually there is a button on the headphones that provides multiple functions including power on/off, playback start/stop and if held down long enough will enable the device’s Bluetooth pairing mode. Once the headphones are in pairing mode they show up as available to other searching Bluetooth devices. A similar process is used to connect all types of Bluetooth devices. Sometimes a passcode will presented by the Bluetooth device that needs to be confirmed or entered into the mobile device, laptop, car, etc.

When Bluetooth devices are operated in the “Advanced Audio Distribution” profile, they use a protocol to do so, which in turn uses an audio “codec.” Audio codecs encode and decode audio signals using compression techniques in order to reduce the amount of information that needs to be processed. In the case of Bluetooth audio this enables audio signals to be transferred wirelessly and efficiently, at established audio quality levels. The most important characteristics to consider with an audio codec are sampling rate (kHz), bit depth (bits), bit rate (Kbps) and latency (ms).

For sampling rate, bit depth and bit rate, increasing values indicate increasing audio quality. For latency, the lower the value, the closer to “realtime” the audio is played. Very low latency is important when playing virtual musical instruments

for example, typically requiring latency to be less than 6 ms. For gaming, anything under 40 ms is considered acceptable. Whereas, waiting 100 ms for audio to start playing after the play button is pressed is probably perfectly acceptable.

Common Bluetooth audio codecs are:

- Subband Codec (SBC): the most common and supported codec, can approach Compact Disc (CD) quality under ideal conditions. SBC has high latency and is not suitable for gaming.
- Advanced Audio Codec (AAC): this codec is used by Apple devices and is not to be confused with Apple's digital audio file format. Like, SBC it has a higher latency and wouldn't be suitable for gaming.
- Audio Processing Technology X (AptX) and its Low Latency (LL) High Definition (HD), Adaptive and Adaptive Live: Developed by Qualcomm, AptX comes in several variations to suit specific needs including a low latency version (LL) suitable for gaming and a higher quality version (HD) for higher quality audio.
- Low Latency Audio Codec (LDAC): Part of the Android Open Source Project and developed by Sony, LDAC offers very high quality Bluetooth audio streaming, but is also high in latency and not suitable for gaming.
- Low Latency High Definition Codec (LHDC) and its variants LHDC Low Latency and LHDC Lossless: Developed by Savitech and Huawei, LHDC is a competitor to LDAC. LHDC dynamically adjusts bit rate and has low latency (LHDC Low Latency Audio Codec (LLAC)) and high audio quality (LHDC Lossless Audio) versions. LHDC is suitable for gaming.

The sampling rates, bit depths, bit rates and latencies of the Bluetooth audio codecs are summarized in Table 18.

Codec	Sampling Rate	Bit Depth	Bit Rate	Latency
SBC	44.1 kHz 48 kHz	16 bit	328 Kbps	High
AAC	44.1 kHz	24 bit	Up to 320 Kbps	
AptX				High
AptX LL	44.1 kHz 48 kHz	16 bit	352 Kbps (44.1 kHz) 384 Kbps (48 kHz)	Low
AptX HD			576 Kbps (48 kHz)	High
AptX Adaptive	44.1 kHz 48 kHz 96 kHz	16 bit 24 bit	279 - 420 Kbps	Low
AptX Adaptive Live	44.1 kHz	16 bit	Up to 1.2 Mbps	
LDAC	44.1 kHz 48 kHz	16 bit	Up to 990 Kbps	High
LHDC	96 kHz	24 bit	Up to 1 Mbps	
LHDC Low Latency		24 bit	600 Kbps	Low
LHDC Lossless Audio	48 kHz	16 bit	Up to 1.6 Mbps	High

Table 18: Bluetooth audio codecs¹²

1 <https://www.pcmag.com/how-to/what-are-bluetooth-codecs-a-guide-to-everything-from-aac-to-sbc>

2 <https://en.wikipedia.org/wiki/AptX>

“Multipoint Bluetooth” is available on some Bluetooth devices. This technology allows several “source” Bluetooth devices to connect simultaneously to one “playback” Bluetooth device. For example, the ability for a smartphone and a computer to be connected, simultaneously, to Bluetooth headphones, or the ability to connect two smartphones to a car simultaneously. Basic Multipoint Bluetooth is limited to two source devices connecting to one playback device, however there is a version of Bluetooth Multipoint, known as “Triple Connectivity”, that allows for three source devices to connect to one playback device.

6.15.4 Apple's AirDrop & AirPlay

Apple computers and devices offer two proprietary short range radio communication features called AirDrop and AirPlay. Much like Bluetooth, AirDrop offers a mechanism to transfer files between Apple devices. AirDrop uses transport layer security (TLS) to encrypt communications.

Additionally, like Bluetooth, AirPlay has the ability to transmit audio and perform media control functions. In addition to transmitting audio, AirPlay can also transmit video and includes screen mirroring capability.

6.15.5 Radio Frequency Identification

Radio-frequency identification (RFID) tags are used to wirelessly provide information from one RFID-enabled device to other RFID-enabled devices within short proximity. Built into an RFID tag are a very small radio transponder, receiver, and transmitter. RFID reader devices emit an interrogation pulse, which then triggers the target RFID tag to transmit digital data. RFID tags can be powered by the reader device's electromagnetic pulse, or they can be powered by a battery, which greatly extends the RFID tag's range to upwards of 100 ft. RFID tags have a wide variety of uses including:

- inventory management, shipping, and logistics to track products
- asset management to track assets within organizations
- access control to implement low-grade physical security measures
- a plethora of healthcare uses including, but not limited to, tracking of medication, assets, staff, surgical instruments and more; some of these applications use “high security” RFID tags
- library and document management systems to track documents
- ticket systems to implement access measures at events, amusement parks, etc.
- animal management to track livestock and pets

There are also a large variety of different types of RFID tags including, but not limited to, those that are waterproof, antimicrobial, resistant to high temperatures, micro-sized, temperature sensitive, data-logging capable, tamper evident, flexible, printable, and high security.

6.15.6 Near Field Communication

Evolving from RFID, Near Field Communication (NFC) is a radio-based (13.56 MHz frequency) WPAN that enables slow (46 Kbps - 1.7 Mbps), but reliable, and secure communication between two supported devices that are within a very short distance from each other (typically 2 cm or less¹). NFC is defined by the ISO/IEC 18092:2013 standard.

NFC applications include, but are not limited to:

- tap-to-pay credit card, debit card and smartphone-based payments

1 <https://nfc-forum.org/learn/nfc-technology/>

- more secure access control than plain RFID
- automotive (unlock, start, and manage)
- more secure healthcare applications than plain RFID
- hospitality and customer engagement (wearable or smartphone-based tap to enter hotel room, pay for services, access services, loyalty programs, etc.)
- personal identification (driver's license, passports, etc.)
- setup and management of IoT devices
- public and private transportation (accessing and paying for services)
- Probably the most prevalent and useful NFC application for the average user is mobile payments, both paying and receiving. Mobile applications, like Apple Pay and Google Pay, along with many major bank mobile applications, enable smartphone-based "tapping" to pay at cash registers, instead of using a physical debit or credit card. Within the mobile pay applications, user debit and credit card information is added via secure authentication methods. NFC payments can then be enabled, taking the place of a physical debit or credit card. This can be useful in helping to reduce the amount of cards that must be carried.

RFID protection enabled wallets and sleeves are available to hold NFC enabled payment cards to prevent them from communicating. While it can't really hurt to have such protection, in practice it is probably not necessary as someone would have to get quite close to you (~2cm or less) and hope that your wallet, clothing, etc. wouldn't block the signal.

6.15.7 Zigbee, Z-Wave and Home Automation

Zigbee is developed, maintained, and promoted by the "Connectivity Standards Alliance (CSA)," formerly the Zigbee

Alliance. As of the time of this writing, the CSA purports Zigbee to be “The Full-Stack Solution for All Smart Devices” and that “Zigbee is the only complete IoT solution – from mesh network to the universal language that allows smart objects to work together.” The CSA advertise that Zigbee is globally adopted, interoperable, reliable, low power, and secure¹.

Based on the IEEE 802.15.4 standard, and supported by the CSA, Zigbee is a set of communications protocols that comprise an open-source, wireless networking technology that enables the creation of low power, low data rate, WPANs. Targeted at wireless battery powered devices, one of the largest applications of Zigbee is home automation, but it is clear that Zigbee is positioning itself as the IoT solution platform.

Zigbee devices use radio transceivers (a portmanteau of transmitter and receiver) to communicate. The most frequently used frequency band worldwide for Zigbee is 2.4 GHz, which supports a 250 Kbps data rate and 16 channels (11-26). The United States and Australia also utilize the 915 MHz frequency band with a 40 Kbps data rate and channels 1-10 and 13, while Europe additionally uses the 868 MHz frequency band, with a data rate of 20 Kbps and only a single channel. Because the 2.4 GHz Zigbee network shares the same frequency band as WiFi, interference with WiFi networks is possible. In such cases it is useful to use Zigbee channels 15, 20, and 26, which utilize specific frequencies within the band that are not used by WiFi.

Zigbee networks consist of devices that have Zigbee chips built into them that allow them to perform a Zigbee “role” of Coordinator, Router or End-Device. Zigbee networks are star, tree or mesh types. Zigbee networks commonly include a “hub” that performs the role of the coordinator (of which there can only be one). The hub also facilitates the connection to the “outside world,” most commonly by connecting it via Ethernet to your router so that it can communicate with other devices on your network, or other devices on the internet (e.g., via mobile

1 <https://csa-iot.org/all-solutions/zigbee/>

application to view cameras, control light switches, lock doors, close garage doors, change the house temperature, change the pool temperature, etc.).

Zigbee supports both device authentication (to authenticate devices joining the network) and data authentication, using AES encryption. Zigbee utilizes three security keys: 1. a master key is used to protect key exchange between two devices, 2. a link key is used to secure the communications between two specific devices, and 3. a network key is used to secure broadcast messages on the network. The security keys use AES 128-bit encryption. The Zigbee network coordinator (most commonly the “hub”) also acts as the “Trust Center” and manages the distribution of the network keys to the various devices.

Centralized and distributed security models are implemented in Zigbee. The distributed model is simpler in that it is only made up of routers and end devices. In the distributed model, any router can allow another router to join the network by providing the network key (encrypted by the pre-configured link key). With the centralized model, a third type of device is implemented, the Trust Center, that distributes the Network Key that is used to communicate on the network. The Trust Center can refresh the network key to help build resiliency to cyber attacks. The Trust Center also distributes a Link Key to devices as they join the network. The Link Key is used to secure communications between the end-devices and the Trust Center.

In various Zigbee configurations there are times when the Trust Center will very briefly send unencrypted keys to new devices joining the network. During this brief moment, an attacker with sufficient “listening” capabilities may be able to ascertain the keys and use them to join devices to the network. Such an attacker may also decrypt network traffic, or craft malicious, but valid, network packets and inject them into the network (perhaps to open a door or disable a camera). Some Zigbee products can be purchased that avoid this problem, but the

unencrypted messaging is thought to be so fleeting that it's not an issue.

Most Zigbee installations will have applications to control and monitor them. Many of those applications will be made available to the internet in some way, or at least on a local network. Some of these types of applications require ports to be forwarded to the Zigbee hub in order to provide remote access from the internet. As with all internet connected applications served on home and small business networks, there are some risks associated with making a Zigbee hub or system remotely accessible. The applications used to communicate with the hub will usually require some form of user authentication by password or better, MFA. Use of strong passwords, and even better, MFA is strongly advised to prevent attackers from gaining access to your system from the internet.

When port forwarding or application proxying is used to allow devices on the internet to communicate directly with your hub, the security of the hub becomes more important. This is because if the hub has a vulnerability, it is directly accessible from the internet. As always, remaining patched is very important and any security features that are available should be used including, but not limited to, strong passwords, password aging, MFA, logging, and alerting.

Some Zigbee hubs may be remotely accessible without the use of port forwarding. These implementations use a client/server approach that requires no inbound traffic ports to be opened or forwarded in your router. This is good because the hub does not need to be exposed directly to the internet via forwarded ports or application proxy. These types of client/server implementations require the hub to communicate outbound to a server on the internet, and that server on the internet is helping to shepherd your application's connection to your Zigbee hub.

Discussed in Section 7.9.1, it is a good idea to segment your networks appropriately, via a firewall. It make sense to put all of your Zigbee devices on their own network “firewalled off,” from the rest of your networks. This is especially true when using forwarded ports because the target devices are exposed directly to the internet, and if exploited can become a foothold into your network.

An alternative to Zigbee is Z-Wave. The following comparisons can be drawn and considerations offered between the two technologies:

- Zigbee is faster
- Z-Wave has better battery life performance
- Zigbee 2.4 GHz signaling is more susceptible to WiFi interference, though this can be mitigated by using channels WiFi 15, 20, and 26
- All devices used on a Z-Wave network are compatible while Zigbee versions have various compatibility requirements that must be considered
- Z-Wave supports up to 232 devices on a network simultaneously, while Zigbee supports 65,000 devices
- Both technologies support specific manufacturers and devices
- Ultimately, it seems that Zigbee is likely the better choice for most applications

It is also possible to build a fully functional home automation system with WiFi-only capable devices that have their own mobile applications and integration capabilities (as opposed to a Zigbee or Z-Wave network and compatible devices). For example, WiFi-only light switches, light bulbs, garage-door openers, camera systems, home security devices, pool control systems, etc., that each have their own mobile application for configuration and monitoring, but also have the ability to be

integrated and unified into other mobile applications such as Google Home or Apple Home. These WiFi-only devices usually have a built-in, temporary, WiFi access point that you first connect to with a mobile device. Once connected, the home automation device will ask you, in turn, to connect it to your network, and once connected, will disable its own WiFi access point capability. Then applications such as Apple Home and Google Home allow you to integrate your home automation devices into one mobile interface. Sweet!

6.16 Virtual Private Networks

Virtual private networks (VPNs) are quite important. VPNs create connections between specific devices and allow encrypted communication between those devices. These encrypted connections are called tunnels and allow the creation of private networks, layered virtually on top the existing internet communication technologies.

There are three main reasons why a home or small business user would need to think about the use of a VPN, they are:

1. Remote Access VPN (also known as Client-to-Site VPN): to connect to your home or small business network from a remote location. For example when on vacation, away from home, at a hotel, etc. Availability of cloud services to provide convenient access to data has somewhat supplanted the need for remote access VPNs, but remote access VPNs can still be very handy.
2. Site-to-site VPN: to connect, secure, and encrypt the networks of two or more homes or small businesses, together.
3. VPN Service Provider: to connect to a VPN service provider and encrypt your network traffic immediately as it leaves your network card or router (if your router has the capability and is setup to connect a VPN service

provider). VPN Service Providers are useful in a least a couple cases:

- When you are connected to a network that you don't trust and want to ensure the traffic is encrypted. For example, when you are connected to a hotel network, coffee shop network, or any "open", free WiFi.
- When you want to enhance your privacy by hiding your IP address as you go about your business on the internet. That said, keep in mind that if you are deliberately trying to hide your IP address you may want to be careful about any online services that you are logged into as then you're authenticated at that IP address anyway.

Remote access and site-to-site VPN capability is often included in firewalls and more sophisticated home routers. Setting these features up can take some patience, but the functionality is often very worth it.

VPN service provider services are usually acquired through the use of a free or paid online service and involves the installation of VPN "client" software to connect your computer, mobile device, router or firewall, to the VPN service provider's network. Note that many people are skeptical of the privacy provided by free VPN service providers.

The three typical VPN use cases for home and small business users are shown in Figure 44. The Remote Access VPN example shows a laptop connected via a hotel WiFi to the internet. The VPN client software on the laptop is used to create the VPN connection (tunnel) to the home or small business router or firewall. Once connected, the rules inside the firewall dictate what the connected VPN user/device can do. One of the most typical things one might want to do with this type of VPN connection is to enable a secure connection to "remote desktop" to a permanently connected system at the home or

small business, or to securely access a network attached drive. As can be seen in Figure 44, in the case of the Remote Access VPN, a typical scenario is to be at a hotel, or otherwise away from the office/home, and wanting to connect to your home or small business network. Perhaps you want to do some stuff on your home or small business computer through a remote desktop session. Perhaps you want to access some data stored on those systems.

The usual steps to setup this type of remote access VPN are to enable and configure the VPN capability in your router or firewall, and then use your router or firewall VPN client software (or your devices native VPN client software, or some other VPN client software...) to launch and establish the VPN connection from your device to your router's or firewall's public IP address. Once the connection is established, the configuration of the router or firewall determines the access that VPN connected devices have to the devices behind the router or firewall. When setting up a remote access VPN, a smartphone with a hotspot can be useful to test out the ability to connect to the VPN. For example, a laptop can be connected to the cellular hotspot and then a connection to the remote access VPN can be initiated to test the functionality of the VPN.

Site-to-site VPN connections are configured in the main site router/firewall and the "branch" routers/firewalls to establish VPN connections between those devices, protecting the communications of all the devices behind them and between them. All the "branch" communications will emerge onto the internet at the main router/firewall site, and via the main site router/firewall's ISP supplied IP address.

Connecting to a VPN service provider typically requires installing the VPN service provider's VPN client software and then using that software to connect securely to their servers, typically offered in many different global locations.

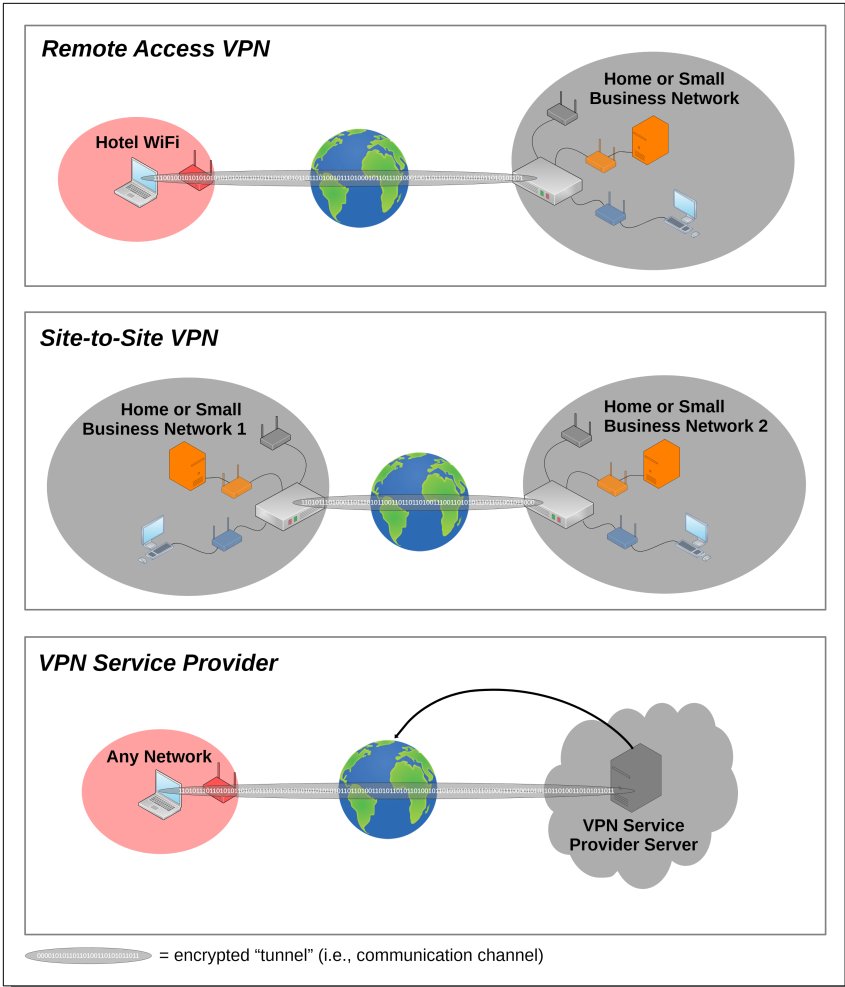


Figure 44: Typical VPN Use Cases for Home and Small Business Users

There are typically several VPN protocols that routers or firewalls will offer to serve their VPN services. Table 19 presents a list of common VPN protocols along with their attributes.

VPN Protocol	Max Key Length	Encryption Standards	Authentication	Security & Privacy	Comment
PPTP	128	MPPE	username/ password	Very poor	Easy to setup, but not secure
L2TP over IPsec	256	3DES or AES	username/ password + pre-shared key	Good/?	Possibly compromised
SSTP	256	AES	username/ password	Good/?	Microsoft proprietary
IKEv2/ IPSec	256	AES, Blowfish, Camellia	username/ password + X.509 certificate	Good	Very fast, secure, and reliable
OpenVPN	All key lengths and encryption standards supported by OpenSSL		username/ password, certificate, and/or smart cards	Excellent	Can be slower and difficult to configure
IPsec	256	DES, 3DES, AES, Blowfish	username/ password + pre-shared key	Good/?	Possibly compromised
SSL	256	SSL/TLS	username/ password, certificate	Good	Implemented at the OSI layer 4 level, somewhat limited

VPN Protocol	Max Key Length	Encryption Standards	Authentication	Security & Privacy	Comment
Wire-guard	256	ChaCha20	Public/private keys	Excellent /Good	New. Fast connections. Open-source, simplified code base compared to OpenVPN. Linus Torvalds, called it a “work of art”.

Table 19: VPN Types and Their Attributes

Security

This section covers various aspects of security. Some of the concepts covered in this section are also introduced and covered to some degree in other sections, but this area concentrates on network security and summarizes the concepts.

Much of what is in this section amounts to system hardening including, but not limited, to the following activities:

- Employing a “defense-in-depth” strategy to make it as hard as possible for any attackers
- Having good backups
- Using strong authentication methods, removing all unused and unnecessary device and online accounts, and configuring all accounts with the least privileges necessary
- Removing all unused and unnecessary software, keeping all software and hardware current for security updates, and configuring all hardware, software, and services in the most secure manner available
- Closing all unused and unnecessary logical ports and services
- Using antivirus software
- Using portable media (such as USB drives, SD cards, etc.) securely

- Using sandboxing to create temporary operating or application running environments that can be quickly deleted, if infected with malware

7.1 Defense-in-Depth

An important concept in cybersecurity is defense-in-depth. It is leveraging security controls and tools at each access level to create as many barriers as possible for an attacker, to prevent them from gaining access to your systems and data. A graphical depiction of the typical measures of defense available to home and small business users is shown in Figure 45.

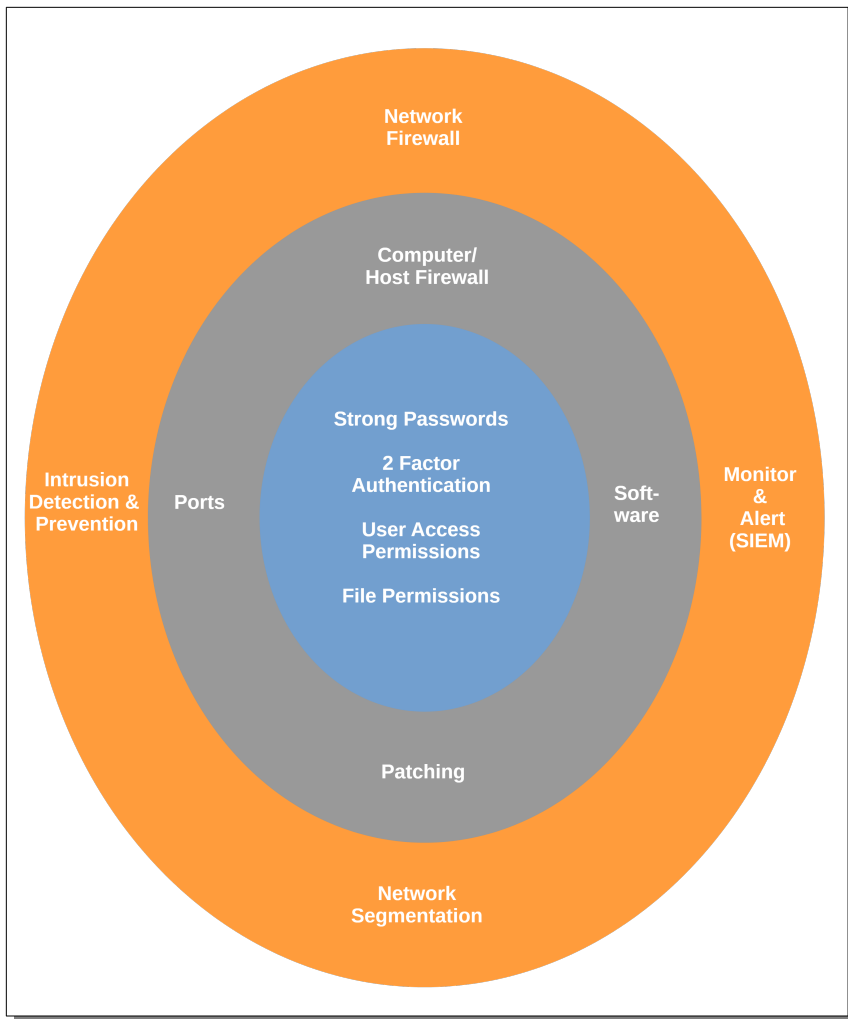


Figure 45: Small network defense in depth

From a defense-in-depth perspective, an attack on one of your networked devices may include an attacker:

- Gaining access to your network, facing your Layer 3 defenses
- Gaining access to your devices, facing your Layer 2 defenses

- Gaining access to the accounts, resources, and files on the devices, facing your Layer 1 defenses

The goal is deploy defenses at each layer. If we assume that the defenses at each increasing defense layer will be breached then we are motivated to use whatever defenses we may have available at each decreasing defense layer. I.e., Once our network is breached (Layer 3) then we'd like to rely on our host defenses (Layer 2); once our host defenses are breached then we'd like to rely on our account, resource, and file access defenses (Layer 1). The defense-in-depth layers in Figure 45 are further described below:

Layer 1 focuses on internal security controls of the hosts and includes:

- Using strong password practices
- Using MFA, whenever possible
- Deleting unused and default user accounts
- Changing passwords for default accounts that cannot be deleted
- Configuring user accounts, resource, and file access with the least permissions necessary (the so-called “least privilege” approach)

Layer 2 focuses on the mitigation of software vulnerabilities and limiting host communications to only that which are necessary by:

- Ensuring only necessary software is installed
- Ensuring installed software is configured as securely as possible and remains up to date with security patches
- Disabling unused operating system services/daemons and ensuring that only the required logical ports are listening/open

- Installing and configuring a host-based firewall to further control host communications, especially inbound communications

Layer 3 focuses on secure network design, configuration, and monitoring including:

- Use of network segmentation to better protect the most important systems and data by deploying a well configured network firewall to:
 - create network segmentation
 - allow the required traffic flows to occur, as defined by the firewall rules
 - monitor network traffic for malicious or suspicious activity
 - provide alerts and notifications
- Use of intrusion detection and prevention systems (IDS/IPS) to inspect network traffic for malicious and suspicious activity, and provide alerts and notifications
- Use of a security information and event monitoring (SIEM) system to consolidate and correlate log files and other sources of system information, along with raw network packet analysis into one system that allows sophisticated monitoring, searching, and reporting as well as custom rules for alerting and notification

7.2 Backups

Probably the most basic and effective thing that can be done to improve your security posture is to have reliable, immutable, backups of important data and systems. There is rule of thumb in the IT industry referred to as the 3-2-1 rule. The idea is that for any data that you want to safely back up, you should:

1. Have three copies (3) of the data; this includes the original working copy, a local backup and a remote backup.
2. Copies of your data should be kept on at least two (2) different physical media; ideally these would be different types of media like magnetic disk and tape, or magnetic disk and SSD.
3. At least one (1) copy of your data should be stored at an alternate location.

7.2.1 Data Backups

There are several types of backups. The simplest is data backup. If you don't need to recover any systems in the event that something happens to them (physical, electrical, cyber attack, etc.) then just backing up your data may be a good option. For data backups, software can be used to create different kinds of backup jobs that can be triggered a number of different ways including manually, on a timer, or on a schedule.

The types of backup jobs that are typically available in data backup software include full backup, incremental backup and differential backup. The typical data backup types and their attributes are described below.

Full Backup

All target files are copied from a source location to a backup location. Using "separated" backups, typically timestamped, the entire file set is copied to the destination location, in a new folder named, named by the time-stamp. If separated backups are not used, then the files in the backup location are overwritten with the versions of themselves from the source location. Full backups can be very time consuming.

Separated (timestamped) backups create multiple copies of the data, which can provide resiliency in the face of file corruption, but of course costs disk space. When not using separated, timestamped backups (i.e., overwriting the same files and directories instead of creating a fresh, new copy in a new timestamped folder) minimizes the amount of disk space used and simplifies the restoration process. However, if the source files are corrupted then they will be used to overwrite the destination files leaving the backup corrupted.

Incremental Backup

All new files and files that have changed since the last backup are copied from the source location to the backup location. Incremental backups are smaller and faster than full backups.

Using separated (timestamped) backups with incremental backups, while more resilient, creates a more complicated recovery process.

Where full backups are vulnerable to copying corrupted files from the source location to the destination location, incremental backups are vulnerable to becoming corrupted and not being overwritten by the source (because the source may not have appeared to have changed).

Differential Backup

All new files and files that have changed since the last full backup are copied from the source location to the backup location.

Differential backups are faster than full backups but slower than incremental backups. Fewer steps to required restore data than incremental backups.

Differential backups that don't use separated, timestamped backups suffer the same weakness as incremental backups that don't use separated timestamped backups, where corrupt files in the backup may not be detected as changed from the source

and thus are not overwritten by the good source files, as would be desired.

With the backup types listed above it should be noted that the software used and media being backed up to can affect how the backups work. In the simplest form, the software is just copying the files from one disk to another, and the recovery process simply involves locating the backed up files on the backup disk. It can get a bit complicated if using separated (timestamped) backups and incremental or differential style backups as the most recent files will be distributed among the backup folders. But still, it's just logistics.

Some backup software, on the other hand, uses chunks of data and must be recovered using the software through some kind of process, as would be the case if using tape. Another consideration for these kinds of backups are that it takes longer to recover incremental and differential backups as compared to full backups, because there are processes needed to reconstruct the data from the incremental or differential data chunks.

Finally, there is the mirror style backup, which is basically one-way file synchronization. With mirror backups, the intent is to keep an exact mirrored copy of some file set. This can be a really tempting idea as having a perfect mirror of the file set means that the recovery process is as simple as possible and takes up the least amount of disk space. However, a consequence of mirror style backups is that files that are deleted from the source location are automatically deleted from the backup location as well. When done deliberately this can help prune the backup, keeping space usage down, and making the recovery process a simple one. However, if files are accidentally deleted from the source location then they will be automatically deleted from the backup location just the same. And files that are corrupted will be copied over just the same. As such, extreme caution should be exercised when implementing mirror style backups. In the author's experience

it can be useful to run mirror backup jobs manually to prune a backup, in a very deliberate way, and just not to run them automatically on a schedule.

Backup software will have options to trigger the backups manually, on a timer, on a schedule, or possibly on an event (like startup). Some thought can be given to when the backups will occur to minimize any disruptions, and to stagger the backups to some degree so that they occur on the intended schedule - since it is typical that only one backup job will execute at a time, and any jobs that were triggered before the previous job(s) are completed will just build a queue.

With all of these options there are several different strategies that can be employed to back up data. From simply mirroring the data to having a more complex scheme that duplicates the data several times to provide resiliency from corruption.

A common backup approach is the so-called “Grandfather-Father-Son” (GFS) approach, where “rolling” full backups (i.e., a snapshot on a particular day) are automatically refreshed and deleted. Something like the idea of a full backup per year, then full backups per month for the last year, then full backups per week for the last month, then full backups per day for the last week. With this type of plan, the total storage space required is relatively large as there is a lot of duplication, but the space required is predictable. This plan enables restoring a snapshot of the data from any previous year, any month in the last year, any week in the last month or any day in the last week. This is a very comfortable place to be with data backups. Especially if you then store a copy of all of that data at a second physical location or in the cloud; very comfortable indeed. Small businesses might consider using a system like this to backup the data for their business.

There are other, more complex, methodologies that exist to optimize backup times and storage requirements, such as the Tower of Hanoi and weighted random distribution methods.

Unless you're into huge amounts of data stored on tape, the complexity of implementing one of these schemes is likely not worth it. Given the storage needs of most homes and small businesses and the relatively low cost of storage media and cloud storage, a GFS scheme is likely a better option for serious resiliency. Otherwise, a few copies of your critical/important data, following the 3-2-1 method, using scheduled full, differential and incremental backups, would be just swell.

7.2.2 Software and Device Configuration Backups

With data backups, sometimes the data can include configuration files and application data for recovering systems and applications. In this case, the data is recovery data and may be worth treating separately from user files. Keeping up to date versions of configuration files and application data may be important.

7.2.3 Operating System and Device Backups

Another type of backup involves backing up a whole computer system. This type of backup is well suited to quickly restore a computer that is performing a specific function. The software to backup a complete system is typically provided by the operating system itself, but third-party software is often available as well.

Windows provides backup tools that are used to create recovery files. Recovery files can be used with Windows recovery facilities to restore an entire system to the point in time when the recovery files were made. Apple's Time Machine software is used to backup Mac computers. Time Machine requires a dedicated drive to function. Android and iOS devices have backup mechanisms built into the OS. Android and iOS backups can be stored on a computer or in the cloud. The rsync and cron commands in GNU Linux can be used to perform scheduled full, differential and incremental backups.

7.2.4 Image Backups

Imaging software is used create images of entire disks that can be restored to new media. Entire operating systems, and their associated data, can be backed up using an image backup. Some imaging software provide the ability to restore an OS from one hardware platform onto a different hardware platform, a so-called “bare-metal” backup. Imaging software is available in paid and open source versions.

Image based backups can be finicky. When relying on them, it’s best to test the restoration processes well.

7.2.5 Standard Builds

An alternative to OS and image based backups is to use standard builds. With standard build tools, the installation, configuration, and hardening of the OS can be done quickly and in a predefined manner, which is preferable to just using the installation media. Once the new system is built using the standard build process, application software can be installed and configured.

7.2.6 Backup Plans

If you have any appreciable amount of data, with the various backup options and methods it can quickly get confusing and difficult to track all the data and backups. It’s a good idea to make an inventory of all your important data that you have and make a backup plan. A basic backup plan could be laid out in a simple table consisting of the following headings:

- Backup Item #
- Backup Description
- Backup Task Name
- Source Location

- Destination Location
- Backup type (ex., full, incremental, differential, mirror)
- Backup frequency (ex., manual, daily, weekly, monthly, etc.)

There are certainly a few more columns that could be added that would be useful, but those listed are a good start.

7.2.7 Drive Fault Tolerance and RAID

Drive fault tolerance is the ability to withstand the failure of a drive. Fault tolerance is usually accomplished via a technology called “Redundant Array of Inexpensive Disks” (RAID). RAID uses several drives in a computer, and a RAID controller, to read and write from those disks, as a system. RAID allows for efficiently copying data to more than one drive, and some RAID schemes optimize disk storage. RAID includes a number of schemes of which “RAID 1” and “RAID 5” have been most popular.

Throughout the years, RAID has been popular with server owners as it has allowed for their servers to continue operating while suffering the loss of a single drive. A very popular configuration is RAID 5, used with three drives. In this configuration, one of the three drives can fail, yet all of the data is retained and the computer continues operating until a new drive can be installed to replace the failed one. In many cases, the new drive can be installed while the computer continues operating, and the RAID controller takes care of the synchronizing the new drive.

Today, RAID is also popular with homes and small businesses that deploy “Network Attached Storage” (NAS) systems in a RAID 1 configuration. This setup allows for data to be written to both drives, at once, ensuring that there is an exact mirror, efficiently and seamlessly. Many people see this approach as maintaining a backup. While very convenient in the event of a drive failure, it would still be good to have a least one copy of

important data offsite. A RAID 1 NAS system with cloud storage could be the ideal solution from a convenience perspective.

7.3 Authentication - Accounts, Passwords, MFA, and Passkeys

Most computers and some mobile devices allow multiple accounts to be created. Accounts will typically be associated with user profiles and will include the creation of specific disk locations for the user's digital content like documents, pictures, videos, music, downloads, favourites and power settings. Access permissions are included with user profiles to restrict access to the user's profile to only the user themselves and the administrators. User accounts themselves are also created with system access levels, such that some users are "guests", while others are normal users, "power users", and then full blown administrators.

Traditionally, securing user accounts has been done with login credentials, consisting of a username and a password, that are used to "authenticate" the user, granting them access to the account along with its resources and privileges. Other authentication mechanisms may also be available on a given device including biometric mechanisms like fingerprint, face, retina, and voice "scanners," or other devices like smart cards, tokens, and fobs.

It is good practice to harden accounts using the following principles:

- only create accounts that are needed
- configure accounts with the least privileges necessary for the accounts to perform their functions
- remove accounts when they are no longer required

Accounts are entry points into your systems allowing human to machine interaction to take place, once authentication has occurred. All accounts provide some form of access, and the

required access increases as more administrative tasks are required of a particular user. In alignment with the principles of defense-in-depth, all user accounts should be properly managed and removed when no longer required. Accounts of increasing privilege, and especially administrative accounts, should be managed with the utmost care, as they provide increasing access to resources and privileges.

While the above comments are targeted mostly at OS accounts, It is general advice for many types of accounts that may exist within applications or web-based systems; the same principles should be observed.

As mentioned, passwords have traditionally been the primary mechanism to secure accounts. In many cases very predictable usernames are used and the only mechanism that is really securing an account (i.e., preventing unwanted or unauthorized use) is the password. What that means is that the only thing really securing your accounts is that only you know your passwords and that your passwords are hard to guess. Thus, it is important to:

- Not share your passwords
- Use strong passwords
- Use alerts for your accounts, whenever available, to warn you about attempts to access your accounts
- Use account login delay and lockout mechanisms for multiple failed login attempts

At the time of this writing, Microsoft recommends a minimum password length of 14 characters and the Canadian government recommends 15 characters. This attribute is known as password length.

Using a mix of uppercase and lowercase alphabetical characters, along with numeric, and “special” characters, and randomness, will help ensure the password has more “entropy,”

and is more difficult to guess. This attribute is known as password complexity.

Traditionally, it has been considered important to change your passwords periodically to limit the use of any accounts that are compromised. This is known as password aging. Recently, this practice has been somewhat discouraged in favour of just very long, hard, random passwords. The idea is that changing passwords too often encourages people to prefer simpler passwords. It is argued that using one really good password (per account, per system!) is all that is needed. The debate continues.

In many cases systems can be configured to automatically require (AKA “technically enforce”) a minimum password length, minimum complexity and maximum age. It is good to use these features, if they are available, to make good practice automatic!

In order to accomplish all of these objectives for generating good passwords it is useful to employ a strategy. A few approaches that work well to generate strong passwords in a somewhat easy way include:

1. Come up with a somewhat random, or at least complex, bunch of characters that you can remember, and use this bunch as part of each password you generate; combine it with something about the thing you are accessing in a way that you can remember as this will provide uniqueness as well as more length and ideally complexity. The downside to this method is that if one of your passwords is compromised, it may be relatively easy to guess the passwords for your other accounts.
2. Use long sentences (that too may incorporate the thing you want to access in a way) that you can remember.

3. Some novel algorithm that you come up with that suits you.
4. Use a password vault/safe/keychain/secure document.

In all four cases, it still makes sense to incorporate upper case and lower case letters, numbers, and special characters, into all passwords and to shoot for at least 14-15 characters in length. You can also replace letters with numbers and special characters like “a” becomes “@”, “E” or “e” becomes 3, etc. Replacing only some of the letters this way would help make it harder to guess your other passwords if one were compromised.

Probably, the best way to manage passwords for most people is through the use of a password vault/safe/keychain. With a password vault a password is still required to access the vault. Your password for your password vault should be really hard, because if it compromised, then all of your passwords are compromised.

There are a multitude of password vaults available. Table 20 provides a summary of the various options.

Password Vault Type	Advantages	Disadvantages
Simple document: Password protected and encrypted text document or spreadsheet	Simple	May require software to password protect and/or encrypt
	Easy to get started Easy to maintain Probably free or already have the necessary software	No automatic backups No automatic synchronization across devices (but could be used with a cloud solution) No advanced features
Browser based: Password storage features inside most browsers	You're probably already using a browser that has password management features Conveniently integrated with internet browsing Some browsers provide synchronization across devices Some browsers have additional features like accounts compromise checks Usually free Strong encryption and password protection	Not all browsers provide all of the desired password storage and synching capabilities May become dependent on the browser Potentially vulnerable to breach

Password Vault Type	Advantages	Disadvantages
Software: Purpose made application software	May be free depending on the product and features	May not be free depending on the product and features
	Advanced features to help track password changes, generate strong passwords and keep a history of password changes	Possibly no automatic backups
	Strong encryption and password protection	Possibly no automatic synchronization across devices (but may work with a cloud solution)
Cloud based: Password management cloud service	May be free depending on the product and features	
	Advanced features to help track password changes, generate strong passwords and keep a password change history	May not be free depending on the product and features
	Automatic backups	Potentially vulnerable to breach
	Synchronization across devices	
	Strong encryption and password protection	

Table 20: Password Vault Comparison

Regarding brute-forcing of account login credentials, many systems offer login rate limiting to limit the number of logins (username/password combinations) that can be tried in a given time, and a forced waiting period in between allowed login attempts. It is advisable to enable such mechanisms, when available. Some systems can also be configured to alert when login activity is detected, which should also be used, when available.

It is highly recommended to have different passwords for all your various online accounts, and ideally your devices as well. This is to avoid the situation where an attacker compromises one device or account and has effectively compromised others as well.

There are facilities available through browser features, websites (e.g., haveibeenpwned.com) and mobile apps that help determine if any of your account login credentials have been compromised.

Finally, many people have all kinds of online accounts using various passwords. It is easy to forget that you created an online account that reuses a password, and then that online account is compromised. Ideally, you might keep a list of all online accounts you create. As mentioned before, deleting unused accounts is always a good idea. Employing one of the password vault methods mentioned is perfectly suited here as well.

In summary, for generating and maintaining passwords:

- Use a minimum password length of 15 characters
- Use a minimum password complexity that includes uppercase and lower case characters, as well as numbers and special characters
- Use different passwords for every online account and device account

- Change your passwords periodically; as a possible alternative, just use really hard passwords
- Employ the security features in your systems to automatically enforce password length, complexity, and age, if available
- Make password management simpler by using a password vault/safe/keychain/secure document
- Use the features of a password vault to craft passwords to your needs or come up with a “personal algorithm” for generating strong passwords that you can remember
- Use login rate limiting and login alerts to mitigate brute force attacks
- Use mechanisms to check if your online accounts have been compromised
- Keep a list of every online account you make or use a password vault to store them all

MFA adds a very substantial improvement to simple username and password protection, as it introduces a second factor to the authentication method.

There are at least three factors that can be used to provide authentication, they are:

- Something you know (e.g., password, passphrase, pin, etc.)
- Something you have (smart card, soft token, fob, MFA code via SMS or email, etc.)
- Something you are (fingerprint, handprint, faceprint, voiceprint, retina pattern, iris pattern, etc.)

It is becoming more and more common that interactive systems, especially online systems, require this second authentication factor. Most often, after entering a username

and password into a login prompt, a prompt to enter a so called “one time password” (OTP) is required. OTPs are usually delivered via SMS, email, authentication application or hardware token.

The OTP MFA method employs the something you know (password) and something you have (OTP) factors¹. While the OTP approach can still be thwarted in various ways using somewhat advanced attack methods, it nonetheless drastically increases the security of the authentication mechanism. MFA should be used whenever it is available for the obvious additional security that it provides.

Table 21 compares the advantages and disadvantages of the MFA options.

MFA Method	Advantages	Disadvantages
SMS OTP	Requires only a cell phone to receive a code	Vulnerable to a number of attacks that can intercept the authentication codes (“SIM Swapping” and SS7 vulnerabilities)
	Very easy	
	Fast	Cellular network must be available to receive authentication codes, especially bothersome if you’re traveling without cell service
	Dependable	
	“Free” assuming you already have a cell phone	Vulnerable to physical theft

1 Some people argue that OTP methods aren’t true MFA because once the OTP is known it’s still “something you know.” It is argued that biometrics are the only true second authentication factor, albeit biometrics are “something you are”.

MFA Method	Advantages	Disadvantages
Email OTP	Requires only an email account to receive an authentication code “Free” assuming you already have an email account Not required to be connected to a cellular network, as in the case of the SMS delivery Very easy Fast Dependable	Vulnerable to email account compromise; email accounts are usually used to reset passwords for online accounts, such that if your email is compromised then an attacker can take over your online accounts using the MFA codes sent to your compromised email address
Authenticator Application OTP	Not required to be online Fast Dependable Many free authentication applications available for Android and iOS	Vulnerable to physical theft Requires an app to be installed and managed Arguably not as easy as receiving an SMS or email

MFA Method	Advantages	Disadvantages
Hardware Token OTP	Considered the most secure option due to immunity to the attacks that SMS, email, and authentication applications suffer Not required to be online Fast Dependable	Vulnerable to physical theft Requires purchasing an additional device Requires carrying an additional device
Biometrics	Convenient Not required to be online	Vulnerable to “false accepts,” where different people have similar enough biometric signatures, as detected by the biometric scanner, that they are accepted inadvertently Privacy concerns around the need to store biometric-related information Once a biometric signature is compromised it can no longer be used

Table 21: MFA Methods Comparison

Passkeys are a relatively new form of authentication that many experts and users like. Passkeys use a public key and private key that combine to make your passkey. The public key is stored by the system you wish to authenticate against and the private key is stored on your device. While the private key can be associated with an actual password, it can also be associated with a biometric signature, like a Faceprint or fingerprint, making it very attractive to users that don't like to bother with passwords. Additional benefits of passkeys are that they can't be shared or guessed, they provide some resistance to phishing (as they are uniquely generated on a per site basis), but most importantly, your Passkeys cannot be stolen in a data breach. Passkeys will certainly become more and more popular as times goes on, and are an elegant and security-enhanced approach to password replacement.

7.4 Software and Hardware Best Practices and Security Updates

All software has “bugs,” hardware may as well. Some bugs are security impacting, and it is usually only a matter of time before some combination of feature, options, configuration, hardware, system state, etc. leads to some element of the system being vulnerable to attack. Such vulnerabilities lead to unwanted capabilities and behaviours including providing would-be attackers the ability to remotely and completely control your system(s) and steal your data, use resources, install ransomware, sow chaos, etc.

With this in mind, as always, the idea is to minimize the attack surface. In this case, that means only installing and using the trusted hardware and software that you need, and making sure to configure hardware and software in the most secure manner possible. This includes the software that may be included with your OS!

When it comes to selection and ongoing maintenance of hardware and software, a security conscious consumer would:

- Use only supported hardware and software from reputable vendors (i.e., regular and emergent security updates provided by the vendor)
- Use the official app store for your OS and official hardware update systems for your hardware, performing file integrity checks on any downloads using file hashes
- Patch hardware and software for available security updates on a monthly basis or more frequent as required, including emergent patches for serious threats
- Regularly review installed hardware and software to ensure only what is continued to be needed remains installed
- Regularly review “startup programs” and “scheduled tasks” to verify that no unwanted applications, scripts or other unwanted software are being launched

Cybersecurity researchers work to discover software and hardware vulnerabilities. Some cybersecurity researchers are employed directly by manufacturers, others are employed by cybersecurity research companies and others yet still are self-employed. Often, large companies like Apple and Google will offer security researchers a “bug bounty” to encourage research and responsible reporting.

The idea of responsible reporting is to provide software manufacturers notification that a vulnerability has been discovered in their product and time to develop a fix, usually released as a software patch. The patch can come in many forms, but more often than not it’s a file or “update” that is installed the way files, programs or updates are installed on a given system. As mentioned, OS, and sometime hardware platform updates, come through a unified update interface, which should be used, when available.

Prior to a software patch being released it is possible that bad actors knew about the vulnerability and were using it. This is

known as a “zero-day” exploit. It’s also possible that governments knew about the vulnerability as well. This is bad enough, but once the vulnerability has been discovered and reported, and a software patch is released to the public, then anyone and everyone can know about it, including bad actors that will reverse engineer it to uncover the vulnerability that it’s fixing and start exploiting it before people patch it.

Needless to say, it is important to stay patched. However, there are times when the rush to release a patch has broken things too. In mission critical applications the goal is to test patches in a “sandbox” environment that is representative of the production environment, then implement the patches once the necessary testing is completed and is resulting in acceptable behaviour post-patching. Another approach could be to deliberately delay patching a bit to allow the rest of the world to test out the patches a bit more and then deploy them a few weeks or months (shudder) later. Again, it’s a race to patch, given that bad actors will reverse engineer patches once they are publicly available, so it’s best to just stay patched and rely on backup and recovery processes in case the worst happens. In mission critical applications, or even just applications where you really cannot tolerate interruptions, consider implementing a “sandbox” environment, probably in a virtual machine environment, to test patches before deploying them in the production environment.

There are at least three kinds of security patches that should be kept in mind:

- OS
- third-party software
- hardware

Modern OSes have mechanisms for distributing their updates. It is usually straight forward to locate the update mechanism for

the OS for your computer or mobile device and use it to update or schedule updates for a device.

Manufacturer's of third-party software often release software patches containing security updates. These too should be applied as soon as practical. Many installed applications will include mechanisms to check for updates either on system boot, or when the software is run. These mechanisms are useful to help keep software up to date.

Package managers are very useful for consolidating the update process for third-party software and can be used, perhaps on a monthly basis, to keep third-party software up to date. Without a package manager, or an automatic update mechanism of some kind, there may be nothing checking for updates and software can get out of date pretty quickly.

The simplest and most dependable way of keeping track of updates is just a good old list of patch sources to check. A spreadsheet makes a great security update tracker.

Most people expect that OSes and third-party software will have security updates released at some point in their life cycle, however many people do not realize that hardware often receives security updates as well. For mobile devices and Apple and Microsoft-branded computers, hardware updates are typically delivered through the OS update process. For other PCs the situation is more complicated. For those PCs purchased as complete units from a manufacturer, like a laptop or fully assembled PC, sometimes hardware updates will be delivered through a manufacturer website or through a dedicated manufacturer provided update application. For PCs that are assembled from parts (i.e., a custom built PC) the process is more difficult, where the manufacturer for each component needs to be checked for updates.

A patching plan is a good idea to write down. A patching plan includes:

- an inventory of systems
- update sources for each system's OS, hardware, and third-party software
- a description of how updates are applied
- update frequency

That said, if all updates can all be automated through the use of package manager then even better.

Free and open source software (FOSS) has the advantage of being open for all to see the source code, and in a perfect world that should make it more secure, because more, interested eyes, have reviewed the code. This may be true of very mature software, but it is nowhere near guaranteed and much less true of newer and less popular software. Further, with FOSS, no one has anything to say about the necessary qualifications of code reviewers, nor whether any such reviews are necessary prior to the release of the software, just that the code is available for review if any qualified reviewers care to. FOSS is very much buyer beware and hard to truly consider for a “production environment,” unless, as mentioned, it is a mature, trusted product (and even then...).

Supporting reliable, high-quality software and its long term maintenance and evolution requires dedicated programmers (that presumably need to make a living). It follows that paying for your important software helps foster its continued development including its security updates. Paid software, however, is usually closed source, meaning its code cannot be inspected.

Whether free or paid, open or closed source, software that is audited for security by third parties provides the most assurance that the software isn't doing anything malicious or unwanted.

7.5 Ports, Services, Applications, and Mobile Code

All communications into and out of a digital device using the TCP/IP protocol utilize a logical port to do so. Introduced in Section 6.12, logical ports allow for multiple applications on a single device that only has one IP address to communicate with multiple systems on a remote network. This is because each application communicates over a specific port. Traffic arriving from the internet can be directed by port, using port forwarding (or a web application firewall or reverse proxy), to the target internal device.

The configuration of logical ports, particularly the “open” and “listening” ports, along with the security state (patch level and configuration) of the software “running” behind that port, are pivotal to the security of the device. The term “open” port implies that nothing is explicitly preventing a connection from taking place on a particular port. The term “listening” refers to the software “running” behind the open port, waiting to accept connections.

Most modern operating systems come with a built-in or pre-installed host firewall that is used to control connections. It is common for host firewalls to block ALL connections except for those that are explicitly accepted. Host firewalls usually come configured with a series of default rules that allow the normally expected connections to take place. It’s definitely good to use your host-based firewall, **ESPECIALLY AT A HOTEL OR OTHER PUBLIC NETWORK**, where it may be the only thing protecting your device.

Depending on your system’s role in a particular application, your system may initiate the connection to some other system on the internet to create a connection. This is the case when your browser creates a connection to a search engine’s website on the internet. Other examples include a gaming PC or console reaching out to an online gaming platform, or mobile

application reaching out to its online platform server (e.g., online banking application, nutrition database, mobile game, etc.).

Conversely, your system's role may necessitate that it waits for connections from other systems on the internet, or possibly just from other systems on your local network(s), as would be the case if you were hosting a web or game server. As mentioned, allowing other systems to initiate connections with your systems requires your system to be "listening" for connections, and it does so by having an "open" port with a "running" application or service behind it, poised to respond to a connection request from a requesting system. Because open and listening ports are entry points into your systems, there are serious security considerations when using them. It is important to know which ports should be listening, if any. It's also important ensure that the software "listening" behind those open ports is promptly patched for security updates, as any unpatched vulnerabilities are directly exposed and waiting for connections. Patching may be the only thing preventing a full system compromise if the internet exposed software contains a vulnerability. Once a system is compromised, other systems on the same network are in the direct line of sight for attack, which is why segmentation is so important (see Section 7.9.1).

SIEMs and IDS/IPSeS can really be useful to provide mitigating measures, as SIEMs and IDS/IPSeS can be tuned to spot the indicators of attack and compromise, and in some cases prevent the attack from occurring. Other mitigations for unpatched vulnerabilities might include manually monitoring logs, tweaking a firewall rule, or disabling specific vulnerable functionalities that you can live without. There are certainly more mitigating measures that can be conceived. Sometimes creativity may be required to come up with a good mitigating measure to buy you time to test patches and patch up.

Table 22 summarizes the software types and security controls to consider.

Software Type	Description	Security Measures and Controls
Applications	Software installed “on top of” the OS, usually very deliberately by the user; may be third-party, but may be optionally installed with the OS; usually requires “launching” by the user or may be configured to “auto start” with the OS or possibly to start with a “scheduled task”	Know what applications should be installed and review them periodically using the OSes add/remove software utility or “app store,” along with the configuration of the autostart programs and scheduled tasks
Services/ Daemons	Software built into or installed on the OS that runs in the background (Windows services, GNU Linux daemons, etc.)	Know what services should be present and what their configuration should be (manually or automatically started) and review them periodically Windows services are configured using the services “snap-in” (run services.msc) or execute “sc” in a command prompt

Software Type	Description	Security Measures and Controls
		MacOS/GNU Linux services can be viewed in a terminal using the following commands: <pre>"top"</pre> <pre>"sudo launchctl list"</pre> <pre>"ps -ef grep /Library/StartupItems"</pre>
Mobile Code	Code that does not come built into the OS and that does not need to be installed, but is triggered to run somehow, usually relying on a command-line shell, a scripting environment (Vbscript, Visual Basic for Applications) or a virtual machine environment (java, Python)	Keeping antivirus software and definitions up to date to help detect malicious code Periodically review the configuration of the autostart programs and scheduled tasks Use the operating systems' process monitor to look for unexpected processes Use network and host intrusion detection systems to help identify malicious traffic Use host and network firewall rules to explicitly only allow desired connections (e.g., maybe only allow connections to systems in specific countries and deny all others)

Table 22: Software security controls

Given that listening ports allow incoming connections to be created by remote systems, it is important to know what listening ports are needed to be open and to check that only those ports are listening. While not quite as crucial from a security configuration perspective, outbound ports can be checked and monitored for malicious or unexpected outbound connections, as well.

Checking for listening ports can be done internally within the OS and externally from another, trusted, system. The internal method uses a shell command (`netstat`) to query the OS as to what ports it thinks are listening. The external method involves using an external system to perform a port scan on the target system using specialized port scanning software (e.g., Nmap). For additional assurance, it is good to employ both methods. The internal method allows for more detailed information about listening ports, but could potentially report inaccurate information if the system was compromised. Conversely, using the external port scanning method allows a secondary, trusted device to be used, overcoming the idea of a compromised system reporting inaccurate port information. Using an external port scanner does do a very good job of detecting open ports, however, comprehensive port scans can be lengthy in duration, and sometimes report ambiguous results.

On all systems, running a simple “`netstat`” command provides an ongoing list of current connections and their status. This connection information can be used to verify if any malicious or unwanted communication is occurring.

Table 23 below provides useful `netstat` commands and their description.

Operating System	Netstat Command	Description
Windows	<code>netstat -nab</code>	Output requires interpretation, but provides process and filename, when accessible
	<code>netstat -ano find "LISTEN" find /v "[::]"</code>	A list of listening ports and the Process ID (PID)
MacOS/ GNU Linux/ Unix	<code>netstat -an grep LISTEN</code>	A list of listening ports and the PID
	<code>lsof -iTCP -sTCP:LISTEN</code>	A list of listening ports and the process name

Table 23: Useful netstat commands

In summary, when it comes to ports, services/daemons, applications and mobile code:

- Know the software that you want to have installed and keep it patched for security updates, as per Section 7.4
- Know the services/daemons that you want running (because you want to know if any are listening for connections that are unwanted or unexpected. It's good to be deliberate about any listening services/daemons.
- Periodically review the configuration of the autostart programs and scheduled tasks to see if any unexpected applications are being launched
- Use a host firewall to block all ports for inbound connections except those that you specifically allow; get to know the ruleset of your host firewall

- Use the netstat commands to get a report from your OS on ports that are listening and use connection information to spot any unwanted connections
- Use Nmap or similar software on a trusted external computer to perform port scans on target systems to help verify that only the ports you expect are listening, are in fact, listening

7.6 Anti-malware Software

Anti-malware software is another important tool in maintaining security and privacy. Anti-malware software scans and analyses the files on a device's disks, along with the device's network traffic, to look for malicious files and data, and block execution of them. Often, signatures for known malicious files and programs are used by anti-malware software, but they will also often use "heuristics" to detect what may be malicious files or behaviour.

Anti-malware software can be configured to exclude files, folders, and programs. Sometimes files or folders that are frequently used by your applications or OSes can cause serious performance lags if anti-malware is scanning the application disk activity. If you suspect that an application's performance is being unacceptably affected by your anti-malware software then you can configure your anti-malware software not to scan that application's executable file and the disk locations it uses. Bear in mind, in making such exclusions, there is the risk of those applications or disk locations introducing undetected malware. As such, exclusions should be applied judiciously and sparingly.

Windows comes with Windows Defender, which is a solid and easy to use anti-malware program. There are third-party alternatives to Windows Defender. Some of the available third-party options offer additional features to those provided by Windows Defender alone. For most people these additional

features are probably not necessary, but one really nice feature to consider is a central administration system offered by some anti-malware software vendors. With a central administration system, the family or small business administrator can see the state of all connected devices in a dashboard and can initiate scans remotely.

MacOS comes with a series of security features that help protect the device right out of the box, but it does not come with anti-malware software. MacOS is not immune to viruses. It's really anyone's guess on any day whether a security vulnerability on any system will be discovered. So it's probably a good idea to run an anti-malware program on any of your Mac computers as well. There are plenty of paid and free options to suit your needs.

Android and iOS mobile products do not come equipped with anti-malware software. Although there are some features about Android and iOS products that make them a bit less susceptible to malware, they are nonetheless still susceptible. There are high quality anti-malware applications available for Android and iOS products that are worth considering to gain an extra layer of defense.

7.7 Portable Media and Peripherals

Portable media refers to external, mountable drives such as:

- Portable USB drives (magnetic, rotating hard disks or solid state drives)
- Flash memory drives including compact flash, SD, mini SD, micro SD, etc.
- Optical discs including compact discs (CDs), digital video discs (DVDs) and Blu-ray discs
- Older formats including jazz drives, zip drives and floppy diskettes

Portable media is a classic attack vector and requires deliberate consideration. If portable media can be introduced into a network, the network firewall cannot help (well, it can still block any undefined outbound connections) and only host-based controls will be effective.

Portable media is a very serious cyber attack vector. The classic scenario is that an infected USB drive is left somewhere conspicuous for a hapless person, possibly an employee, to pick it up and plug it into a computer, where it can wreak untold havoc. A portable media based attack is what is thought to have been behind the Stuxnet Iranian nuclear enrichment facility attack in 2010. Stuxnet was an extremely sophisticated virus, suspected to be inserted by a double agent. Once introduced, Stuxnet “slept” inside the nuclear facility’s network until its deployment conditions were met. It then proceeded to cause nuclear centrifuges to destroy themselves. At the same time, Stuxnet used specific knowledge of the control systems deployed at the nuclear facility to “seed” information into the monitoring facilities making everything look like it was operating normally¹.

Older style USB attacks included USB Hacksaw and Switchblade that provided methods of gathering system information, exfiltrating data and replicating itself. Other USB type attacks include the ability to launch malware, USB device overflow, RAM dumping, pod slurping, and social engineering combined with a USB type attack. BleepingComputer.com provides a list of 29 different types of USB based attacks².

It’s not just the good old days that saw USB style attacks. According to BleepingComputer.com, USB based attacks were spiking in 2023³. BleepingComputer refers to a “Sogu Campaign” that requires users to execute a file that appears legitimate,

1 <https://en.wikipedia.org/wiki/Stuxnet>

2 <https://www.bleepingcomputer.com/news/security/heres-a-list-of-29-different-types-of-usb-attacks/>

but instead exfiltrates data, sets up a reverse shell, and copies itself to any connected portable media. Another very similar campaign BleepingComputer.com describes is “Snowydrive,” that provides similar capabilities.

The bottom line with USB devices is that they bypass many network-based controls, as well as many host-based controls, and provide enormous capability. Serious portable media based attack campaigns continue today. As such, portable media should be taken seriously and treated with appropriate precautions.

Consider the following mitigating measures with respect to portable media:

- Don’t insert unknown USB drives or devices into your computer. If you must see the contents of such a drive it would be best to inspect it using an offline system that has up to date anti-malware protection and autorun turned off; be sure to scan the test system again after disconnecting the target USB drive.
- Don’t stick your trusted USB devices or drives into any other untrusted devices or charging ports as malware can be copied to your device or drive, which can then be further propagated into the other devices you connect.
- Turn off autorun on all your systems.
- There are ways to restrict the ability to mount portable media on Mac and GNU Linux computers, but it’s a little complicated; a determined user will be able to figure it out.
- In Windows, ability to mount portable media can be configured for all users or just specific users using local group policy (Windows Professional and above editions) or registry key edits (all editions).

3 <https://www.bleepingcomputer.com/news/security/usb-drive-malware-attacks-spiking-again-in-first-half-of-2023/>

The following group policy keys can be modified:

User Configuration -> Policies -> Administrative
Templates -> System -> Removable Storage Access

Computer Configuration -> Policies -> Administrative
Templates -> System -> Removable Storage Access

OR

The following registry key can be created:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\
Windows\RemovableStorageDevices

Followed by creating the following DWORD and
setting it equal to 1:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\
Windows\RemovableStorageDevices\Deny_All

While a little less concerning than portable media, peripheral devices connected via USB can still be problematic. Borrowing a friend's mouse may not be an issue, but connecting a device from a stranger could be. For example, a USB device called the Rubber Ducky hotplug acts as a key logger and virtual keyboard that can issue commands without an actual keyboard and keystrokes being necessary. Use caution and common sense whenever considering connecting any peripherals via USB.

7.8 Sandboxing

Sandboxing is the practice of doing something that may be dangerous, but in a safer way. With computers, the idea is to isolate the system resources that are being used to execute whatever it is you are trying to do and then controlling how that those resources interact with the host. The objective is to prevent interactions with the host system's resources unless very explicitly allowed or directed by the user. This makes it very easy to erase/undo/back out of whatever it is and doesn't affect the host system. Common uses of sandboxes are:

- opening emails and attachments
- browsing the internet, particularly untrusted sites
- downloading and executing untrusted files from the internet
- working with potentially infected or dangerous files
- testing new applications
- testing OS updates

Sandboxie-Plus is a very handy third-party Windows application that enables users to quickly and easily run applications in a sandbox. Sandboxie-Plus makes it very easy to “empty” the sandbox and to get content out of the sandbox, should you choose to do so, brave user (probably scan any such content with a virus scanner). Today, Windows also comes with a sandboxing program, Windows Sandbox. Both Sandboxie-Plus and Windows Sandbox are great options for sandboxing in Windows. There are other software options for sandboxing.

The other very robust option for creating a sandbox environment is just to run a second OS in a virtual machine on whatever host OS you are using (see Section 5.3 for more on virtual machines). You can use the tools of the virtual machine software to decide what level of access you want between your virtual machine sandbox and your host OS, along with being able to just delete the virtual machine if any security concerns arise.

Sandboxing is a very strong security improvement measure that protects users from unexpected harmful consequences of their digital activities and is just very highly recommended.

For Apple’s Mac¹ and iOS² products, apps distributed using the Apple app store must employ Apple’s App Sandbox technology. There is nothing that the user needs to do to reap the benefits. Android automatically runs all apps in a Sandbox as well³. However, with Windows, GNU Linux or sideloaded MacOS apps, additional steps need to be taken to implement sandboxing. As mentioned, with Windows, sandboxing is implemented using third-party sandboxing software such as Sandboxie-Plus or by enabling Windows Sandbox, or by using a virtual machine. MacOS’s App Sandbox can be invoked by executing the “sandbox-exec” command.

Table 24 below summarizes the Sandboxing options for the major OSes.

Operating System	Sandbox Built-in?	Options
Windows 10+ Pro, Enterprise, and Education Versions ⁴	Yes	Launched like an app, Windows Sandbox is built in and provides a lightweight Windows VM Can also use an alternative VM, which may provide some additional privacy assurance Can also use Sandboxie-Plus and other software to quickly and easily sandbox applications

1 <https://developer.apple.com/documentation/security/app-sandbox>

2 <https://support.apple.com/en-ca/guide/security/sec15bfe098e/web>

3 <https://source.android.com/docs/security/app-sandbox>

4 Not available for Windows Home version.

Operating System	Sandbox Built-in?	Options
Windows 8 and before	No	Don't use these OSES anymore because they aren't supported, but if you do and you need to sandbox then use a VM
iOS iPadOS	Yes	Sandboxing is built into all applications installed from the official app store
MacOS	Yes	Sandboxing is built into all applications installed from the official app store MacOS Sandbox is available for launching any side-loaded applications, but it's a bit complicated to setup Can also use other VM software, which may provide some additional privacy assurance
Android	Yes	All applications are run in a Sandbox
GNU Linux	Sort of	There are very complicated ways of sandboxing processes in the various GNU Linux distributions, but it's just easier to use a VM

Table 24: Operating System Sandbox Options

7.9 Network Security

Much of what has been covered in this section until now has focused on host-based security and what can be done at the device level to increase security. This section focuses on what

can be done at the network level to improve security. It discusses network architecture as well as the security considerations around the common types of wired and wireless networks found in homes and small businesses.

7.9.1 Network Firewall and Segmentation

It is smart to place important and sensitive devices and data on separate networks from more exposed devices. This is to prevent compromised devices from inadvertently providing safe harbour and passage to the golden jewels. For homes and small businesses this might look like three or more networks:

1. A high exposure network for internet facing and internet integrated stuff like web servers, game servers, IoT devices, security systems, camera systems, smart appliances, etc. It is expected that because of their deliberate exposure, or short support period, these systems are more prone to exploitation and steps should be taken to protect more sensitive systems from them.
2. A medium exposure network for general purpose use like smartphones, laptops, PCs, supported Smart TVs, etc. These devices are not expected to be listening for connections or otherwise accessible from the internet, so they are less exposed. Given the more general purpose nature of this network, the greatest risk is likely a user themselves unwittingly launching malware, so further steps should be taken to secure even more sensitive systems and data from them.
3. A low exposure network for safe data storage and access to the most important and sensitive systems and data. This network is deliberately the least exposed in order to provide the safest environment. For this reason, systems on this network are ideally further hardened, per the means described in the preceding sections of this chapter.

Segmenting networks can be accomplished in a few ways. A series of home routers can be arranged to create tiered networks that usefully facilitate restriction of access. A more robust and convenient solution is to implement a supported, multi-port, network firewall. This can be done nearly for free using open-source or “free for home use” software installed on an unused PC that has several network cards (adapters) installed in it. This is a starting point for many people introducing themselves to the wonderful world of better network security. Alternatively, very slick, small, fanless, power efficient, single-board computers are available with multiple Ethernet ports that are perfect for, and in some cases even marketed as, an ideal hardware solution for a powerful firewall.

A diagram showing how networks are segmented with a firewall is shown below in Figure 46.

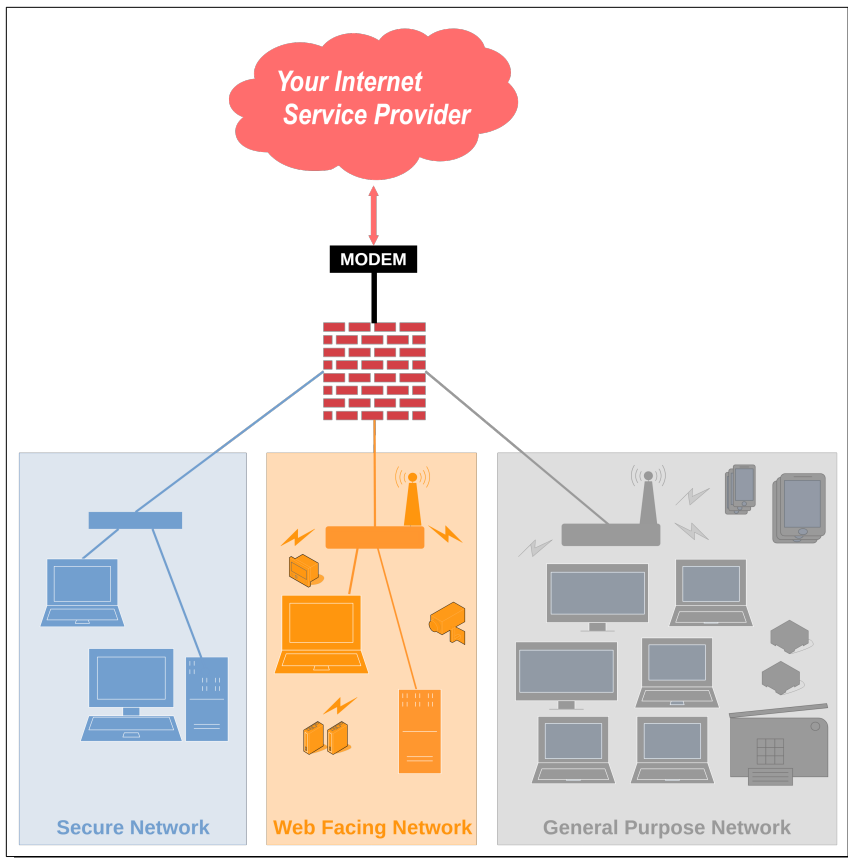


Figure 46: Network segmentation with a firewall

The benefit to segmenting your networks is that you can then control access across the networks. Any such access across the networks implies some form of security risk, but these are risks that you can assess and choose to take. You can also have measures to mitigate the risks as well.

A common example might be a printer that is located on the general purpose network that you want accessible from the other networks. In the case of our example, we might configure the firewall to allow incoming traffic from the other two networks to that printer alone, over the specific ports that are used to enable printing. Even better, we can define a group of hosts and only allow that group of hosts to communicate with

the printer. This arrangement allows for tightly controlled resource sharing across the networks, which can be very effective.

Some planning is a good idea before implementing such a firewall. Consider how many different wired and wireless networks you might need, and where devices will be placed. Firewall devices on the market allow you to create an arbitrary number of wireless networks, and that joining a specific wireless network (SSID) will associate your device with a specific network. This is very useful to create segmented wireless networks, but not all devices will be used in a wireless fashion. Therefore, consider planning how the wired and wireless devices will be connected, and what networks they will be placed on. Depending on the firewall you choose, and its capabilities, you may find that you are limited by physical ports. A physical port is needed to connect wired devices to a particular WiFi network. Ethernet switches can be used to connect more devices to a given network, but the number of physical ports on the firewall device limits the number of networks that can be created with wired devices to connected to them.

Upfront planning, combined with some understanding of the capability of the firewall is ideal. Once you know how the wired and wireless networks will be configured then the IP addressing for the networks can be determined. Once the physical and logical details are determined then the firewall can be implemented. Depending on the firewall you purchase, you may be able to take it directly out of the box and follow the instructions to begin configuring it. If you're going with the open-source or "free at home" firewall solution then you'll likely have to install the firewall OS onto your chosen device. This device, as mentioned previously, may be:

- A PC loaded up with as many network cards as physical networks are needed

- A small, fanless, single board computer
- A virtual machine loaded on some other computer's host OS
- Some other kind of purpose-made computer or device

Once the firewall is ready to be configured, the following is a list of general steps and considerations required to configure it:

1. Define the physical and virtual interfaces; assign names and IP spaces to the physical ports.
2. Specify how the firewall's external physical interface port gets its IP address, usually "automatically".
3. Specify, which physical interface is the default gateway; usually the one connected to the ISP.
4. Configure DHCP.
5. Configure DNS (usually points to your ISP's DNS server, but can alternatively point to others like CloudFlare or possibly your own DNS server, like a Pi-Hole, see Section 6.13).
6. Configure NAT.
7. Define the hosts.
8. Configure the firewall rules (try to make them as point to point as possible, and use network groups to simplify rules by applying them to the groups instead of specific hosts). Firewall rules typically execute from top to bottom, and the first rule that matches "wins". This means that any second matching rule will not be executed. The order of rule execution is important to keep in mind during rule construction. Some firewalls have the ability to monitor how often the firewalls rules are executed and it's always advisable to put the "busiest" rules at the top. This is so that the firewall

executes the shortest scan of the rule base possible before the matching rule is found, saving CPU cycles.

9. Enable and configure country blocking, if available and desired.
10. Enable and configure IDS/IPS, if available and desired (include whitelisting of hosts, domains, etc. and exclusions, as needed).
11. Enable and configure any other advanced threat detection, if available and desired (include whitelisting of hosts, domains, etc. and exclusions, as needed).
12. Enable and configure local and remote logging (e.g., sending logs to a SIEM or syslog server), as desired.
13. Make sure that the last rule in the firewall rule base is a deny all and that it is configured to log.
14. Enable and configure notifications as desired, particularly, successful and failed login attempts.
15. Make sure to change any default passwords and remove any unused accounts (it is better to create your own admin accounts, test them, then delete any default accounts to force any attacker to have to determine the username in addition to the password).
16. Enable and configure any port forwarding and application proxy features, if available and desired (prefer application proxy for the security benefit of not directly exposing ports, as is the case with port forwarding).
17. Enable and configure any desired and available VPN features (don't use PPTP as it is not secure).
18. Make sure to perform regular security updates.
19. Review and update the firewall configuration whenever the actual network configuration changes so as to not

leave any unneeded firewall rules or object definitions behind.

20. Backup the configuration and have hardware spares if you want to be able to recover quickly in the event the device fails.
21. Migrate to another supported device once the device is no longer supported.

7.9.2 Cabling Security

In many cases copper and fiber optic cabling is still preferred for connecting networks and devices together. Wired connections have the benefit of being able to physically restrict where the connections take place. That said, physical cabling and connections can be tampered with. If your data is very sensitive then you may want to consider physically securing the cabling. In a home it's hard to imagine needing to secure cabling, but in a small office environment it may be more desirable. In such cases this would normally be done by installing the cabling inside conduit and securing the rooms where cabling breaks out. In extreme cases the conduit can also be pressurized and monitored for intrusion attempts by pressure sensing. This level of physical security is usually not necessary and would only be warranted in the most secure applications. But always bear in mind that physical access may imply complete loss of security.

There are some electronic measures that can be taken to mitigate physical access to cabling. With “managed” Ethernet switches, the following measures can be taken:

- Disable all unneeded physical switch ports
- Enable MAC address filtering to restrict physical connections to only the MAC addresses of specified devices (MAC address spoofing is still possible but this is another barrier in a defense-in-depth strategy)

- Use mechanisms to monitor the up/down status of the various physical ports on the switch and send alerts if the status changes, possibly indicating someone attempted to connect or disconnect a device

Interestingly, from a security perspective, since wireless networks are entirely encrypted and the only way to gain access to them is to wirelessly connect to them with knowledge of a password in advance, this may represent a security enhancement relative to physical cabling, as long as the password being used is strong. The potential downside of wireless networks is that they use radio communication, albeit encrypted, that can be detected by those in the proximity. It is to say, the radio signals may extend beyond the walls of the building and thus cannot easily be physically restricted. Again, as long as strong passwords are used there is almost no consequence to this or reason to prefer physical connections. And even that said, for the most paranoid of paranoid, WiFi signals could be collected for future decrypting. With the advent of quantum computers, decrypting today's WiFi protocols could become trivial.

For homes and small businesses, both physical cabling and WiFi are generally perfectly good options to use.

7.9.3 WiFi Security

From a security perspective WiFi is fairly straightforward. At the home or office just ensure that your WiFi networks are configured to use WPA2 encryption or better with a strong password (15+ characters using a mix of lower case, upper case, numbers and special characters) and that your networks are segmented properly. Broadcasting your SSID may appear to be a security risk, but remember obscurity is not security. As previously mentioned, it is generally advised to go ahead and broadcast your SSID.

Most people don't have their WiFi router configured to alert them whenever anyone attempts to connect to it so they wouldn't know if someone was trying. Anyone in proximity could try as many attempts as they wanted and you wouldn't know. So you want to choose a password that will make it unreasonable for them to try. Also, if you can configure your WiFi router to alert you whenever someone attempts to connect, that could be useful.

Although it is generally advised to go ahead and broadcast your SSID it would be a mistake to include any useful information in the SSID. Your address, personal details or information about your WiFi router would not be particularly wise to choose. Sometimes manufacturer's will provide a default SSID that includes the router's model number. Why? WHY??? That information can be used to exploit known vulnerabilities in the WiFi router. Yet another reminder to keep your router up to date for security patches.

It is typical that WiFi routers and access points have the ability to serve a separate guest WiFi network. Such guest networks can be used to provide a separate password to guests than that used for the primary WiFi networks and also provides segmentation from the primary WiFi networks. This is a good security measure to use.

WiFi networks can be configured so that all the devices that connect to them are automatically isolated from each other. This is known as "host isolation" mode. The connected devices, though connected to the same network, will not be able to communicate with each other. On a home network this can be useful to ensure that any device that may become infected with malware will not be able to affect the others. While very useful, host isolation isn't suitable for in all cases, e.g., printing to a WiFi printer, using your smartphone to control a smart TV or to access a local media server. If you do not need these types of features then host isolation is a tidy, simple solution to drastically increase the security on your WiFi

network. WiFi routers, if equipped with this feature, will typically have an option to enable host isolation or “AP Isolation”. If it suits you, use it!

In some WiFi routers and access points MAC address filtering is available, which can be used to restrict WiFi connections to only specified devices whose MAC addresses are entered into the router in advance. This is a worthy measure worth considering, but it should be noted that it is not difficult to defeat. Simple approaches exist to sniff MAC addresses from other devices in the area (via the WiFi radio), and then “spoof” the MAC addresses by using specialized software to change the apparent MAC address of the attacker’s WiFi card. Using a strong WPA2 /WPA3 password is still the best measure to prevent unwanted connections to your WiFi network(s).

A comparison of the WEP, WPA, WPA2, and WPA3 WiFi security protocols is shown in Table 25.

Protocol	Description
WEP	Uses 64 or 128 bit key length, the RC4 protocol, and a 24-bit initialization vector that makes it particularly vulnerable. Does not have strong authentication mechanisms. Widely considered unsafe for use as it can be deciphered relatively easily using well understood methods.
WPA	Improves on WEP security by using a 256-bit initialization vector and dynamically changing keys using the Temporal Key Integrity Protocol (TKIP). Incorporates stronger authentication methods IEEE 802.1x and Extensible Authentication Protocol (EAP). Generally not recommended for use.

Protocol	Description
WPA2	Improves on WPA security by using Advanced Encryption Standard (AES) instead of the RC4 protocol and using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) instead of TKIP. Recommended for use.
WPA3	Improves on WPA2 security by introducing Protected Management Frames (PMFs), enhanced CCMP, stronger cryptographic handshake, Opportunistic Wireless Open (OWE) and Enhanced WiFi Open technology that protects clients from each other on public hotspots. Recommended for use.

Table 25: WiFi Security Protocols¹²

7.9.4 Cellular Network Security

When you are connected to a cellular network using “cellular data,” you will be given an IP address on your cellular service provider’s network. Cellular networks isolate connected devices from each other (via NAT!), meaning your device has no direct exposure to other devices on the cellular network or the internet. This is ideal from a security perspective. Theoretically it is possible that a misconfiguration by a cellular service provider could lead to direct exposure, but in reality, it would be vanishingly rare.

7.9.5 Bluetooth Security

A high level summary of Bluetooth security features is provided in Table 26.

- 1 <https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2>
- 2 <https://www.link-pp.com/knowledge/wep-vs-wpa-wireless-security.html>

Security Feature	Description
Authentication	Uses the Bluetooth address of the device to verify identity. Note that user authentication is not provided by Bluetooth.
Authorization	Ensures that access and resource control is only provided to devices that are authorized.
Confidentiality	Prevents other Bluetooth devices from eavesdropping or compromising information by only allowing access to and viewing of data by authorized devices.
Message Integrity	Verifies that there has been no alteration of a message sent between two devices.
Pairing/ Bonding	During the connection process, allows the forming of a trusted pair of Bluetooth devices, through the use of a shared, stored key that is used in future connections.

Table 26: Bluetooth security features

From a security perspective, there are several types of Bluetooth attacks and prevention mechanisms, they are summarized in Table 27.

Attack	Description
BlueSmacking	A denial of service type attack where an oversized Bluetooth packet is sent to a Bluetooth enabled device in order to disrupt or degrade its performance.
BlueJacking	“Discoverable” Bluetooth devices are able to receive unsolicited messages and files from other Bluetooth devices. Bluejacking is when that capability is harnessed for less than desirable purposes, ranging from spam to denial of service to full on phishing and device compromise.

Attack	Description
Bluesnarfing	A more serious type of attack that involves exploiting vulnerabilities in the object exchange (OBEX) protocol that Bluetooth uses in its implementation. Once exploited an attacker would pair their Bluetooth device to the target device and attempt to steal available information.
Bluebugging	Another serious type of attack that uses the “discoverable” mode of Bluetooth-enabled devices to install malware and create a persistent backdoor, providing overall compromise of the device. In the case of a smartphone, this type of attack would extend to listening to phone calls, reading text messages and stealing contact information.

Table 27: Bluetooth attacks

Bear in mind, these types of attacks need to occur within the Bluetooth proximity range so they are relatively easy to avoid by not using, or at least pairing, Bluetooth devices in heavily populated settings, where an attacker may be camping.

Some tips for securing Bluetooth-enabled devices include:

- Turning off Bluetooth when not using it
- Using a strong password on your Bluetooth-enabled device
- Refusing to accept pairing requests from devices that you didn’t initiate a connection to or aren’t expecting
- Limiting the storage of sensitive information on your Bluetooth-enabled devices
- Configuring your Bluetooth-enabled devices to require approval for connection

- Avoiding pairing Bluetooth devices for the first time in a public setting
- De-activate Bluetooth discovery mode on your Bluetooth-enabled devices
- Keep track of the whereabouts and status of your Bluetooth-enabled devices
- Use MFA where possible to limit the extent of damage a Bluetooth attack may pose
- Keep your Bluetooth-enabled device up to date with security patches

Refer to NIST Special Publication 800-121 “Guide to Bluetooth Security” for a comprehensive review of how Bluetooth works and is secured.

7.9.6 Apple’s AirDrop and AirPlay Security

AirDrop has some security advantages. First, the communication it enables is performed over a TLS encrypted session. Additionally, it does not require any ports to be open (listening) and doesn’t leave any files around as would be the case using email or cloud servers. Finally, it allows for restricting communications to only known contacts. A very strong and useful communication technology.

AirDrop also includes a setting to allow receiving files from “Everyone for 10 minutes,” meaning that any device within range can send your device files. This can be very useful if say, a stranger took a very nice photo of something you were looking at and you wanted a copy. Apple restricts this mode to only being available for 10 minutes at a time so that you can’t forget to put it back in “Contacts Only” or “Receiving Off” mode so that you don’t receive unsolicited file transfers from strangers.

One interesting thing to note is that AirDrop can be a method of “exfiltrating” data. While many small businesses probably

consider blocking USB capability on laptops and PCs they provide to users, some may not have considered that AirDrop provides file transfer capability. Microsoft Intune and Apple Business Manager provide “Endpoint Management” solutions that provide organizations with capabilities and features to manage devices. While well outside the scope of this book, these tools are mentioned as they provide a means for organizations to disable AirDrop along with many other useful operations for securing their employee’s devices and their data.

7.9.7 NFC and RFID Security

From a security and privacy perspective, there is not much to worry about with NFC. Disabling NFC if you’re not using it can’t hurt from a security perspective. That said, it would be quite inconvenient to disable NFC if you do use NFC regularly, and you don’t gain much, if anything, in the way of security or privacy by disabling it. Just a nice little piece of tech.

7.9.8 Zigbee, Z-Wave and Home Automation Security

Zigbee is an IoT technology. As always, with such technology it is important to keep it up to date with security patches. When purchasing IoT devices it would be desirable to target products that have a support life cycle that meets your needs, from companies that have a track record of transparency and taking security seriously, and fixing bugs quickly after they are discovered. Zigbee may be different than some IoT devices in that the damage that may be inflicted via, say a light bulb or television, could be no big deal at all. But if a system incorporates the ability to, say open a door, turn off a freezer, monitor cameras, HVAC systems, etc. then security and privacy become a serious issue.

A summary of security tips for Zigbee devices is provided below.

- Zigbee automatically distributes strong security keys, but be aware that certain systems and configurations may have moments of brief vulnerability for key sniffing
- Be conscious of the capabilities of your Zigbee devices and scale your security accordingly
- Consider segmenting your Zigbee network from your important data networks, so your important data networks are not vulnerable to any vulnerabilities in your Zigbee network, but consider that your Zigbee network may still need to be strongly secured as your Zigbee devices may be quite important themselves (e.g., door locks, freezers, HVAC systems, cameras, etc.)
- If your Zigbee network has devices that are sensitive from a capability or privacy perspective, buy devices that have a support life cycle that meets your needs from companies that have a strong track record of fixing bugs quickly after discovery
- Use strong passwords and better, MFA for authenticating users on associated mobile or web applications
- Consider the capabilities of the devices on the network and scale security accordingly, e.g., cameras and door opening mechanisms are arguably more important to secure than light switches.

7.10 Advanced Digital Security Concepts

Taking all of the security measures discussed in this chapter creates a strong security architecture with defense-in-depth in mind. This section presents some additional, more advanced measures that can be taken to improve security even further.

7.10.1 Intrusion Detection and Prevention Systems (IDS/IPS)

Intrusion detection and prevention systems (IDS/IPS) are hardware or software solutions that monitor network traffic for known malicious packet types, IP addresses, hostnames, along with malformed packets.

These types of systems inspect all of the traffic that enters and exits the desired network interfaces and take action if they find something suspicious. Traditionally, IDSeS have been colocated with a group of devices connected to a LAN switch, that is connected to a router (or firewall), where the LAN switch ports connecting the router (or firewall) are “mirrored” onto another port on the switch, that is then connected to the IDS. That is a mouthful, but it just means that ALL the traffic entering and exiting the router is “copied” to the IDS. This allows all raw network traffic to be monitored and analyzed. While this method can be very useful for detecting and alerting on malicious traffic, it cannot take any preventative action.

Preventative action can be built into firewalls or other inline security appliances that can inspect all of the traffic inline and actually block any further communication if it detects malicious traffic. While these systems are very effective, taking automatic action on “false positives” blocking network traffic can be problematic depending on what the communicating systems are being used for. Accordingly, approach IPSeS carefully if you have high availability systems behind the IPS. Using just an IDS and alerts may be a better approach. Additionally, enabling IDS/IPS features may be resource intensive and may limit the throughput of the IDS/IPS system, so such features should be judiciously deployed. Using whitelists or exceptions should also be considered to eliminate scanning of expected activity, and freeing up system resources.

7.10.2 Unified Threat Management (UTM)

Unified threat management is the idea of a single device, software or system that provides multiple security related services. This often looks like a supported, multi-port hardware security appliance that incorporates an object-based firewall, country blocking, IDS/IPS, application proxy/web application firewall, enhanced NAT options, user web access and bandwidth controls, VPN options, logging, monitoring, alerting, dashboards, and charts along with other advanced security features. UTM devices are extremely powerful and convenient, and offer a massive improvement in security.

There are several fully featured commercial UTM products available that home users can enjoy for free. They are often licensed only for home use and only support a limited number of IP addresses. As such, small businesses usually need to purchase a supported hardware appliance and business license. A supported, commercial, small business UTM appliance is not free, but cost effective options are available and worth it. Alternatively, small businesses may consider deploying an open source UTM device, which there are several strong options available. The open source options available are excellent, but it is nice to have support. If your small business has high availability needs then you may consider support for your UTM device quite important.

7.10.3 Security Information and Event Monitoring Systems

Security information and event monitoring systems (SIEMs) are able to ingest log files from a wide variety of devices, along with raw network packets to correlate and analyze the logs, then alarm and alert accordingly, based on a configurable rule base. Not only are SIEMs able to look for known malicious or malformed traffic, but they can look for user activity, like failed login attempts, system and file accesses, rogue systems, etc. They also provide mechanisms to manually look through

the logs and raw packet information, along with opening and closing security incident and investigation tickets and facilitating vulnerability assessments. SIEMs are invaluable in detecting anomalous traffic and activities, and providing mechanisms for figuring out what is going on quickly. SIEMs do for digital security what camera systems with object detection and video recording do for physical security.

There are both open source and commercial SIEMs available, such as Wazuh, IBM's Qradar commercial and community editions, Security Onion, Elk Stack, SIEMonster, LogRhythm, Graylog, Splunk, and more. Some SIEM solutions have an open-source or community edition that is free to use, along with a commercially supported version. However, when considering implementing a SIEM, be aware that the computing requirements can be hefty. SIEMs can also be somewhat complicated to setup, and to maintain over time, so they should be considered an investment. That said, SIEMs are truly the pinnacle of being able to detect, monitor, and investigate anomalies on networks and providing confidence (and evidence!) that all is well.

7.10.4 Vulnerability Scanners

Vulnerability scanners are tools that have a database of known vulnerabilities and are used to perform a vulnerability assessment by probing your systems to see if they contain any of the vulnerabilities in the database.

An authenticated scan allows the vulnerability scanner a chosen user's level of access by providing that user's login credentials. If an admin user's credentials are provided then the scanner will have admin privileges over the system and will be able to glean the most information about the machine, including known vulnerabilities in the operating system, missing security updates, disk shares, netstat based port scan, etc. This is really useful in helping to find vulnerabilities and take measures to

mitigate them or at least know they exist, and perhaps tune the SIEM to look for related indicators of compromise.

An unauthenticated scan will not provide the same level of detail as an authenticated one. It will include an external system type port scan to detect any listening ports, and it will likely also include looking for known services that may provide information to a remote system, such as the Windows Management Instrumentation, Windows Remote Management or SNMP services (configured with a default network string).

7.10.5 Penetration Testing

Penetration testing is the active process of trying to hack into a network. Whereas a vulnerability assessment provides details of whatever vulnerabilities may exist penetration testing takes it a step further and attempts to exploit any such vulnerabilities.

Software like Kali Linux and Metasploit make the exploitation process much simpler. In general this involves finding an open/listening port, determining the software listening on that port, then attempting to exploit a vulnerability in that software to deliver a “payload” to the target system.

Once the listening port and vulnerable software have been identified Metasploit offers a range of payloads that can be deployed to the target system via the exploit and a mechanism to launch the whole attack. The payloads include such fun things as the remote attacker being able to execute arbitrary commands, creating new administrative users, deploying a reverse shell (proper backdoor) and even things like making a vulnerable iPhone vibrate.

Usually the reason an exploit works is because the listening software has a vulnerability that just has not been patched. If a patch does not even exist for a vulnerability then there is little that can be done other than monitor and block access, which usually means disabling service.

Sometimes, latent vulnerabilities are known only to adversaries who can then be poised to attack with little or no warning and with no defense in place. As previously mentioned, these are known as zero-day exploits. The goal of security researchers is to find these kinds of vulnerabilities and then disclose them quickly and privately to the software owner so that a patch can be developed, and a responsible disclosure to the public can take place.

7.10.6 Honey Pots

In Aesop's fable, the Flies and the Honey Pot, flies are attracted to the honey pot where they eat greedily, but then find their feet and wings covered in honey. Unable to fly or get away they perish [Aesop, 1867].

In the digital version of a honey pot, some kind of vulnerable device is deliberately made available for would-be attackers to find. The goal is to bait the attackers to hack the honey pot device, which will in turn provide indication to the network administrator that suspicious or malicious activity has been detected. With such information the network administrator can know their network is under attack and can then take the necessary steps to secure the network.

While it is possible to make a do-it-yourself (DIY) honey pot, such a solution will not be overly easy to administer over time. Luckily, there are a number of open source and commercial products available to simplify and enhance honey pot capabilities. Honey pots are a very effective way to improve threat detection.

7.11 Mobile Devices

For most users, mobile device security is fairly straightforward as the app stores of the mobile platform are used to load software safely onto the device. Additionally, strong measures are taken by the mobile operating systems to provide a very

malware resistant environment. As a result, most people don't need to think much about the security of their mobile device beyond using the official app store, only installing needed apps, keeping apps up to date for security patches and practicing good online hygiene.

Today in North America, there are really only two mobile platforms available and they are Google's Android and Apple's iOS. Android is an open source mobile operating system, and an open source project, known as the Android Open Source Project (AOSP). The AOSP continues to be maintained and can be installed on compatible hardware. While AOSP is a very functional mobile operating system, it does not contain Google Services that play a very key role in most people's experience of Android. That is to say, when it comes to Android there are two versions to consider, the Google proprietary version and the open source AOSP version, for which Google still leads the project [Triggs, 2024].

AOSP allows side-loading of applications, and without support for the Google Play Store, it is likely considered that all applications are side-loaded on AOSP. Side-loading is inherently more dangerous than using the official app store as there is no vetting of the software. There are "app stores" available for AOSP that can be used to at least help keep the software up to date, but with side-loading it really is buyer beware. The Android app store F-Droid hosts only open-source software and although it is awesome most users will likely find that it feels quite limited.

The proprietary version of Android comes with Google Services integrated and can access the Google Play Store, Android's official app store. Again, in both the case of Apple's iOS and Google's proprietary Android, simply using the official app store goes a long way to ensuring that you don't introduce malicious software onto your device. As always, more software means more potential vulnerabilities, so it is wise to follow the approach of only installing the needed software. Both Android

and iOS offer the ability to completely encrypt the data on the mobile device. They also have auto-locking features that lock the device after a period of inactivity and contain mechanisms to detect their location and to remotely wipe them if they are lost. Below is a summary of security measures for mobile devices:

- Use supported operating system versions
- Use the official app store to install software
- Only install the software you need
- Keep everything up to date
- Practice good online hygiene
- Encrypt the device's storage
- Enable the device's auto-lock feature
- Enable lost device tracking capability
- Enable and learn how to use remote wipe capability
- Keep backups of your device

7.12 Cyber Attack Detection and Response

Most of the attacks that you'll likely encounter were covered in Section 4. Here we'll briefly cover some aspects of detecting attacks and what to do in response. Table 28 summarizes a number of common attacks, how they come about (attack vector), how they are detected and recommended response.

Type of Attack	Common Attack Vectors	Detection	Response
Exploited Software or Hardware Vulnerability Leading to Remote Access and/or Malware Infections	Internet exposed software or hardware that contains unpatched vulnerabilities	Anti-malware software SIEM System Monitoring Diagnostics Performance degradation Honeypot	Use firewall to identify attacking IP addresses and create/tweak firewall rules to block the attack and remote access. Restore data and systems from backups. Try to use anti-malware software to remove malware, but verify with online scanners or using offline tools (see Section 12). Change all passwords.

Type of Attack	Common Attack Vectors	Detection	Response
Malware	Hyperlinks		
	Internet downloads	Anti-malware software	Restore data and system from backups.
	Email attachments	SIEM	Try to use anti-malware software to remove malware, but verify with online scanners or using offline tools (see Section 12).
	Phishing	IDS/IPS	
	Smishing	System Monitoring/	
	Exploited software or hardware vulnerability	Diagnostics	
	USB/portable Media	Performance degradation	Change all passwords.
Ransomware	Hyperlinks	This one should be pretty obvious as the attackers will encrypt your data and demand a ransom	Restore data and systems from backups.
	Internet downloads		Pay the attackers? Well, the idea is that paying them just encourages them, depending on your situation you won't be the first or last to just pay if you can afford to and the alternatives aren't feasible or better.
	Email attachments		
	Phishing		
	Smishing		
	Exploited software or hardware vulnerability	Ideally, if you have a honeypot they will find your honeypot first and try to attack it	
	USB/portable Media		Change all passwords.

Type of Attack	Common Attack Vectors	Detection	Response
Persistent Remote Access/ Data Leak	Hyperlinks		Use firewall to identify attacking IP addresses and create/tweak firewall rules to block the attack and remote access.
	Internet downloads	Anti-malware software	
	Email attachments	SIEM	Restore data and systems from backups.
	Phishing	IDS/IPS	
	Smishing	Monitoring/	
	Exploited software or hardware vulnerability	Diagnostics	Try to use anti-malware software to remove malware, but verify with online scanners or using offline tools (see Section 12).
	USB/portable Media	Performance degradation Honeypot	Change all passwords.
Denial of Service	Serving an online service	Performance degradation	Use a third-party service to validate web requests like CloudFlare.
		SIEM	
		IDS/IPS	Buy more bandwidth.

Table 28: Common Attacks, Detection, and Response

Restoring systems from backups is often the best course of action to recover from a cyber attack. As per Section 7.2, in the ideal case, you’ve recently backed up your important OSES and data so you can reasonably quickly restore your systems to a

convenient state. Sometimes just reinstalling the OSes is the best approach if you don't have recent backups. Sometimes important information and even backups are on live drives and it is possible that these drives could become compromised or encrypted as part of an attack. That's why the best situation is to have offline backups. Maintaining such backups takes a strategy and the help of some software. But it's worth the effort.

When it comes to identifying attacks, having a SIEM is super valuable. Having all of the various system logs in one place to sift through with charts to help indicate frequencies across the systems is very powerful. The ability to group logs and then drill down deeply into them provides efficiencies. The SIEM is really the ideal tool for detecting cyber attacks.

When it comes to computer systems, i.e., Windows, GNU Linux, Mac, there are monitoring and diagnostic tools built in that can help you see if anything unusual is running on the computer. Windows Task Manager, Resource Monitor and Performance Monitor provide detailed insights into the operation and performance of Windows computers. The Windows SysInternals tools also provide excellent information about Windows. E.g., Process Monitor provides detailed process information that can be very helpful in tracking down a malware's process and executable file(s). MacOS has the Activity Monitor that can be used to monitor system performance. The Gnome System Monitor can be used to monitor GNU Linux systems along with many other utilities. The "top" terminal command can be used for both MacOS and GNU Linux to monitor resources.

The "top" terminal command is shown in Figure 47, and the Gnome Activity Monitor is shown in Figure 48.

```
Processes: 798 total, 2 running, 796 sleeping, 3577 threads 16:12:09
Load Avg: 2.50, 2.29, 2.11 CPU usage: 2.50% user, 1.8% sys, 96.41% idle
SharedLibs: 1182M resident, 143M data, 84M linkedit.
MemRegions: 0 total, 0B resident, 0B private, 3926M shared.
PhysMem: 270 used (3389M wired, 1646M compressor), 5149M unused.
VM: 29T vsz, 4955M framework vsz, 5795322(0) swpins, 5898058(0) swapouts.
Networks: packets: 6871894/6200M in, 8709273/8303M out.
Disks: 8375237/145G read, 4474630/91G written.

PID COMMAND %CPU TIME #TH #WQ #PORT MEM PURG CMPRS
656 firefox 19.6 02:13:10 89 2 825 1712M+ 23M 152M
14262 plugin-conta 13.6 66:49.09 30 1 124 75M- 0B 2760K
31166 top 8.4 00:21.48 1/1 0 35 9944K 0B 0B
159 WindowServer 5.9 02:53:29 16 7 4632 965M 4736K 140M
0 kernel_task 1.5 64:25.21 300/16 0 0 536M 0B 0B
152 bluetoothd 1.3 19:51.25 9 5 409 7380K 384K 1144K
354 TouchBarServ 1.0 12:27.13 4 1 364 42M 6272K 5996K
31218 screencaptur 0.7 00:00.34 3 2 67 5360K 620K 0B
31158 Terminal 0.5 00:06.77 9 4 323 25M+ 840K+ 0B
456 sharingd 0.4 06:51.67 4 2 370 12M 0B 3280K
458 soffice 0.3 34:02.87 8 1 472 1595M 1724K 391M
403 rapportd 0.3 04:53.27 2 1 240 5812K 0B 508K
466 nearbyd 0.2 03:58.71 8 6 108 3984K 0B 1716K
306 mds_stores 0.2 26:19.16 4 2 117 56M+ 0B 6016K
117 mds 0.2 13:59.75 6 3 446 24M 0B 5844K
333 BTLEServer 0.2 00:55.50 2 1 50 1916K 0B 404K
402 milod 0.2 03:04.55 2 1 122 7640K 1920K 1964K
31212 mdworker_sha 0.2 00:00.08 4 1 53 1668K 0B 0B
```

Figure 47: Terminal “top” command output

Processes						
Process Name	User	% CPU	ID	Memory	Disk read total	Disk write
gnome-system-monitor	ubuntu	1.91	3862	152.9 MB	13.3 MB	
gnome-shell	ubuntu	1.15	2127	213.9 MB	38.2 MB	
Xorg	ubuntu	0.00	1898	30.6 MB	28.0 MB	
mutter-x11-frames	ubuntu	0.00	2164	22.1 MB	3.8 MB	
update-notifier	ubuntu	0.00	3441	6.8 MB	11.1 MB	
tracker-miner-fs-3	ubuntu	0.00	2621	10.4 MB	2.3 MB	
gvfsafc-volume-monitor	ubuntu	0.00	2514	1.0 MB	38.9 kB	
gsd-xsettings	ubuntu	0.00	2336	7.7 MB	313.3 kB	
seahorse	ubuntu	0.00	3764	15.5 MB	1.7 MB	
(sd-pam)	ubuntu	0.00	1854	1.9 MB	N/A	
at-spi-bus-launcher	ubuntu	0.00	2011	786.4 kB	180.2 kB	
at-spi2-registryd	ubuntu	0.00	2174	786.4 kB	64.5 kB	
dconf-service	ubuntu	0.00	2231	524.3 kB	56.3 kB	
evolution-addressbook-factory	ubuntu	0.00	2506	4.1 MB	2.3 MB	
evolution-alarm-notify	ubuntu	0.00	2305	15.4 MB	2.5 MB	
evolution-calendar-factory	ubuntu	0.00	2482	3.5 MB	1.1 MB	
evolution-source-registry	ubuntu	0.00	2225	8.3 MB	3.9 MB	
gcr-ssh-agent	ubuntu	0.00	2027	655.4 kB	28.7 kB	
gdm-x-session	ubuntu	0.00	1894	524.3 kB	120.8 kB	

Figure 48: Gnome System Monitor

Online and offline virus scanning tools and offline boot CDs can be very useful in identifying, removing, and providing validation of malware removal.

8

Home and Small Business Networking and Security

This chapter discusses aspects of home networking. A typical home network is presented and its drawbacks are discussed. A more secure home network design is presented that can be implemented using a firewall, and the advantages are described. To begin, Figure 49 depicts a typical home network, where all the devices are logically on the same network, and are thus immediately exposed to each other.

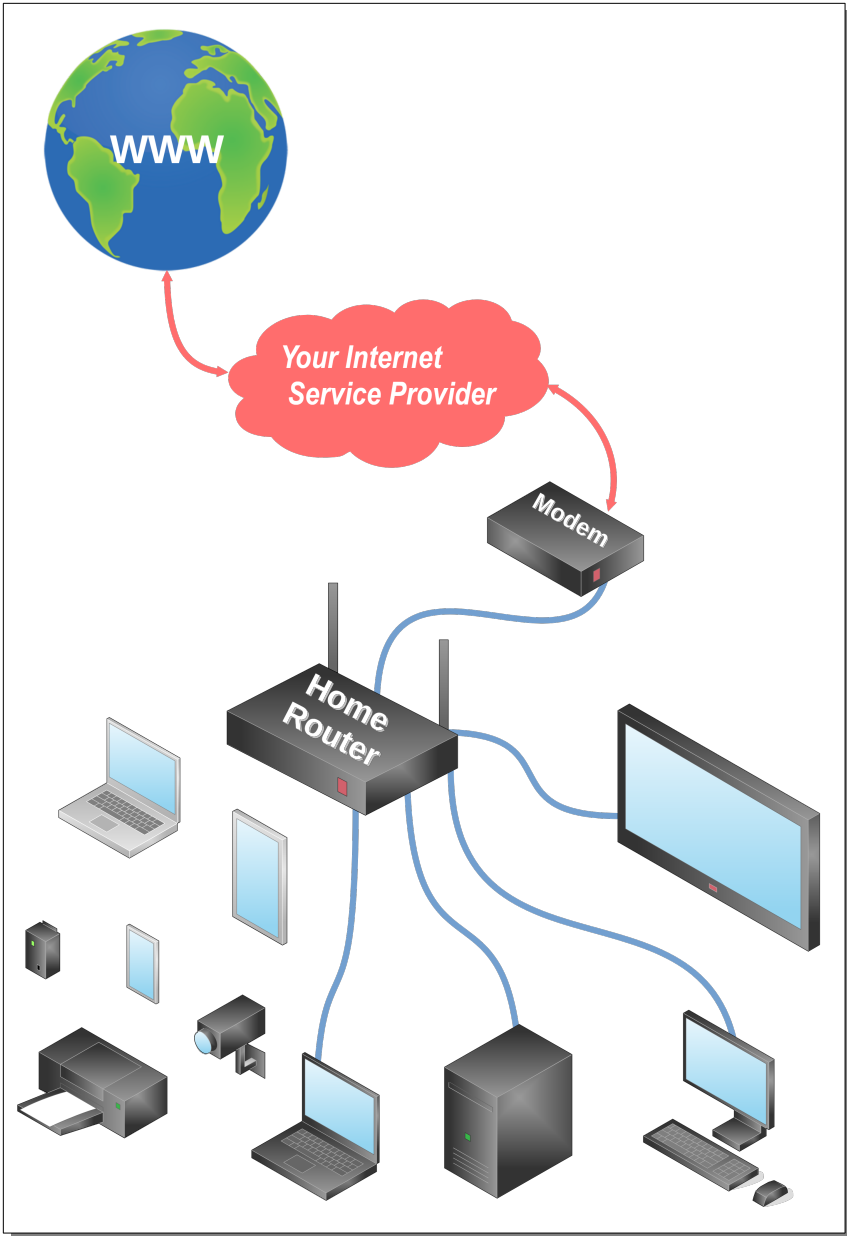


Figure 49: Typical Home Network

8.1 Home and Small Business Network Architecture

It is very common that homes and small businesses have all their devices on the same network. A better architecture segments the network into “enclaves”. With segmentation, important and sensitive devices are placed on their own network segment. This is done so that any compromised devices on other segments cannot access the more important and sensitive devices and data. An ideal home or small business network architecture is shown in Figure 50.

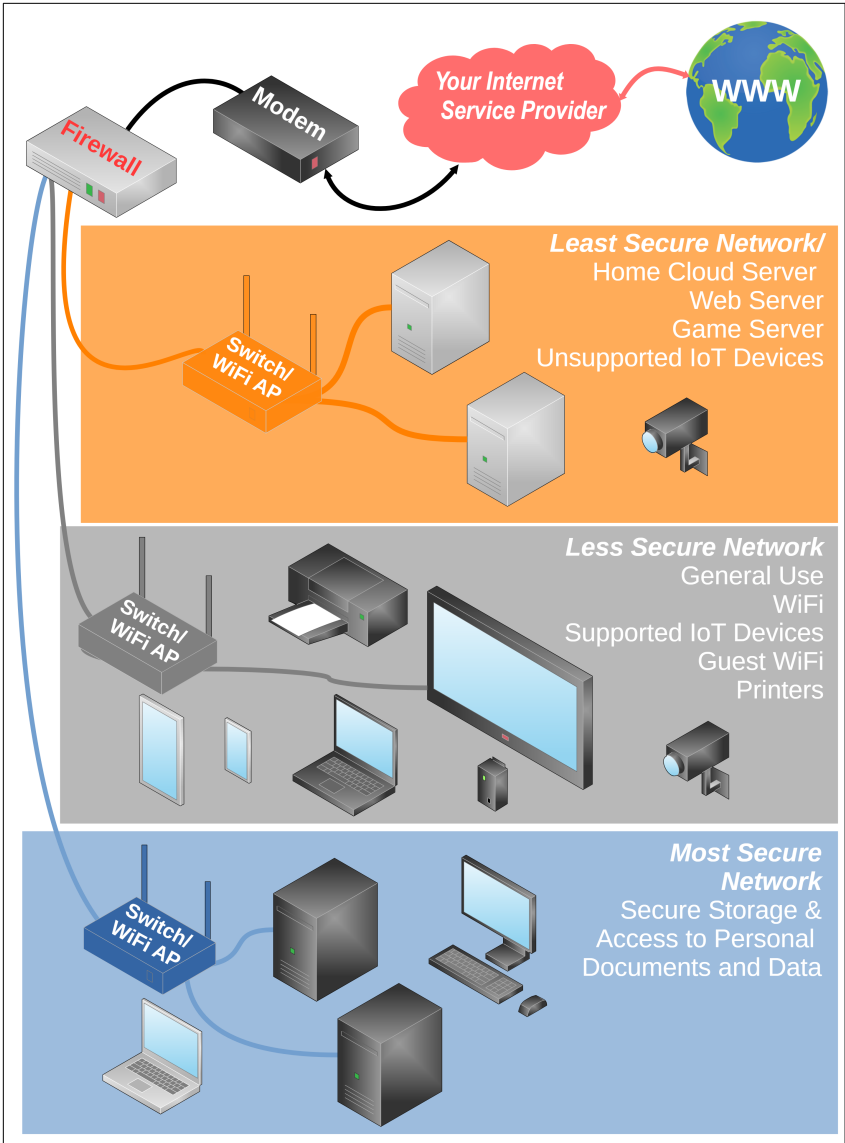


Figure 50: A Better Home and Small Business Network Architecture

The home network shown in Figure 49 depicts a router with only one network and two connections; one connection to the internet and the other to the internal network. The home network shown in Figure 50 depicts a home network with a firewall has four connections; one to the internet and three

others, each connected to a separate internal network. The orange coloured network is where the most exposed and least secure devices are placed. The grey coloured network is for more general purpose use by less exposed devices. Finally, the blue network contains the most important and least exposed devices and data. It can certainly be arbitrary how the networks are segmented, but the principle is to keep the most exposed and vulnerable devices on different segments than the most important and sensitive devices and data.

Figure 51 depicts two types of networks under attack by two attackers. Attacker 1 is targeting a computer and Attacker 2 is targeting some kind of IoT device. In the case of the typical home network, as is shown, once either Attacker 1 or Attacker 2 accomplish their goal of exploiting their chosen device to gain access that device, they ultimately gain access to the rest of the network. Once one device is compromised then the attacker is operating directly on the network with all the other devices on that network, and the only thing protecting all those devices is their own host-based security controls and vulnerability/patch status. However, on the segmented network, it is shown that because of the segmentation, the attackers only have direct exposure to the devices on that particular network segment. The devices and data contained on the most secure network segment remain secure against the attackers. This is because if either Attacker 1 or Attacker 2 succeed in compromising their target, they must still face the firewall to be able to get through to the segment that contains the important devices and data. Of course, if the firewall itself has a vulnerability that can be exploited then it could be reconfigured to provide such access. As always and especially with your firewall, it is important to stay on top of security patching.

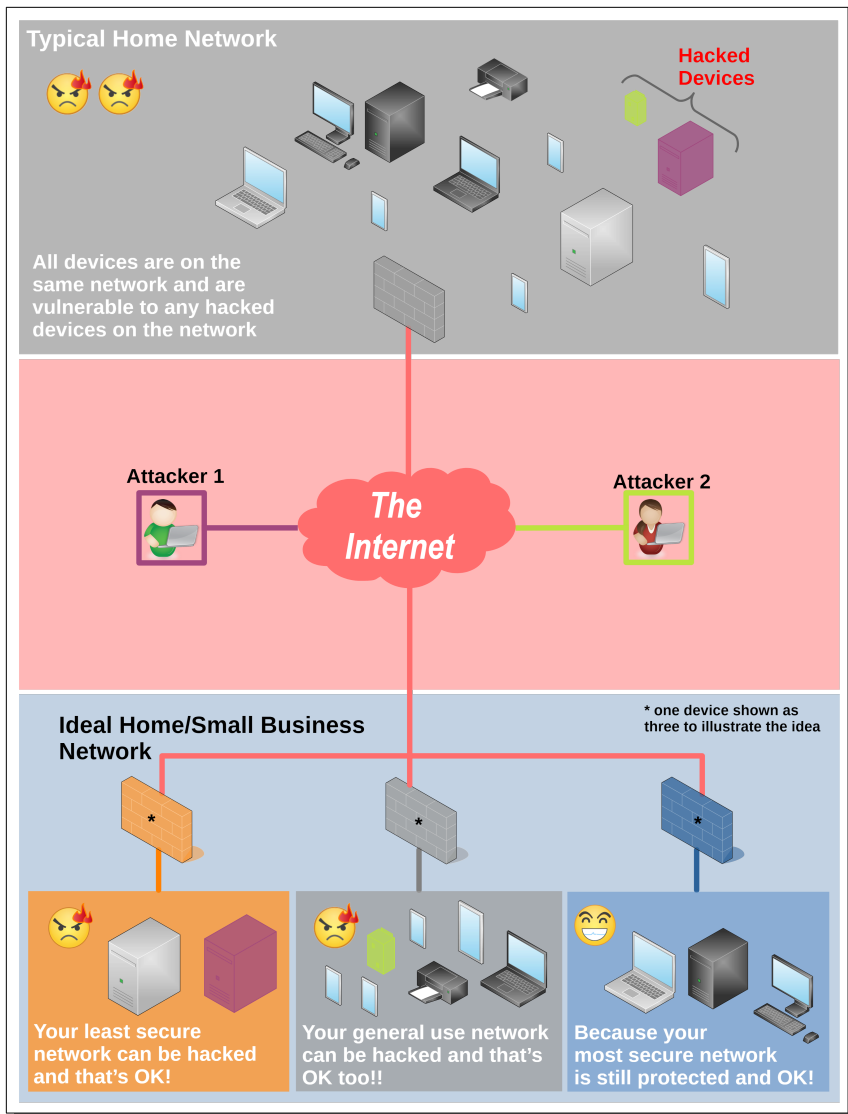


Figure 51: Typical home and small business network architecture vs. a better network architecture

The network architecture presented in Figure 50 can provide the ideal setup for a home or small business network. This architecture provides excellent capability to do all the things a person, family or small business might want to do with their networks. It does so while providing peace of mind with respect

to security and privacy. It also provides the flexibility to allow access between the networks, as required.

To implement the firewall there are several options. Some higher end consumer grade routers will allow for the implementation of some segmentation, and it is likely that these capabilities will increase over time. Another relatively low-cost solution, that is very effective from a security perspective, is to purchase a single-board computer that has multiple Ethernet ports available, and install firewall software on it. From a hardware perspective there are several options for implementing a firewall:

- Purchase a higher end consumer WiFi firewall router that contains some or all of the segmenting and security capability required (e.g., the Ubiquiti Dream Machine)
- Purchase or re-purpose a computer that has several spare I/O ports available and install Ethernet cards into them
- Purchase a fanless, single-board computer made for the purpose
- Purchase a suitable firewall from a firewall manufacturer

For the home user a very nice option is to purchase a low power, fanless single-board computer equipped with 4-6 Ethernet ports, RAM (typically 8-16 GB) and a SSD (typically 128-256 GB). Today, there are many makes and models of such systems that are made for the purpose.

There are also several options for highly effective firewall software ranging from truly free and open-source (e.g., pfSense, IPFire, OPNSense, Smoothwall, Endian, etc.) to closed source, but free for home use (e.g., Sophos UTM and XG Firewalls, NG Firewall, etc.) to paid feature sets that are activated through a licensing arrangement on hardware or virtual appliances. It is somewhat common for vendors to

provide an open source solution that is installed on a PC as “software,” whereas their business, licensed, version is provided as part of a solution, with either a hardware or virtual appliance.

Finally, there are a couple other architectures that can achieve similar goals as that shown in Figure 50. Products are now becoming available that allow WiFi segmentation. If your network consisted mostly of WiFi enabled devices with limited need to physically connect via Ethernet cable, then there are now powerful devices to create segmented WiFi networks, similar to that of Figure 50 (e.g., Ubiquiti Dream Machine).

A firewall allows for the connection of multiple networks and controls the traffic flow between them, among other things that it can do. Unlike a network switch where all devices connected to it are on the same network and share the same IP address space, the ports on a firewall are used to connect together entirely separate networks, from different IP address spaces. Each port on the firewall is configured with an IP address on each of the networks it connects, and is usually the default gateway for the devices connected to that port and network. Each port on the firewall can usually be configured to host network services for the devices connected to that port/network as well, most notably DHCP and DNS, so that devices connected to that port will receive an IP address and DNS server address, automatically. One of the ports of the firewall will be connected to the internet modem and configured to get its IP address from the internet service provider dynamically, as discussed in Section 6.8. That port will usually also be configured as the default gateway for the firewall itself so that any traffic originating on any of the internal network ports, destined for an IP address that the router doesn’t have a route for, will be forwarded by that port to the next-hop router (i.e., your ISP’s router that connects your network to the internet).

Once your networks are configured in your firewall, and the networks are connected to the correct firewall ports, firewall rules can be defined in the firewall to allow traffic to flow between the networks and out to the internet. Most firewalls will, by default, implement a “deny all” rule set where all access between networks is denied by default and must be explicitly configured otherwise. For example, it’s typical for many devices connected to any of the networks to require access to the internet. To allow this communication to occur, a rule is set up in the firewall that allows the flow of network traffic originating from any of the desired internal networks or devices destined for the internet over port 80 (HTTP) or port 443 (HTTPS).

Rules in firewalls can be very granular and will often allow for rules to be made for individual hosts. Very specific firewall rules are often useful when you only want to allow specific hosts, or groups of hosts, to communicate with other specific hosts, or groups of hosts. An example could be that you have a laptop, which is often connected to the “general use” network, but sometimes you need to launch a remote desktop or SSH session to another system on another network. In cases like this, a granular firewall rule, AKA “a pinhole,” can be set up to allow such communication. From a security perspective this set up severely restricts the communications and is the superior approach, than say, allowing the entire network to communicate. The more “point-to-point” the rule set can be, the better it is from a security perspective, as it represents the minimum set of connections that should be allowed and minimizes the attack surface. To aid with this process, many firewalls include the ability to define objects and groups to contain those objects. This helps make the system more manageable, allowing rules to be applied to the groups. Once rules are defined then objects can be added or removed from the group, as required. This approach makes managing rules a lot easier.

As further described in Section 7.9.1, firewall rules are usually set up in an ordered list somehow, either through a web interface served by the firewall or through the editing of a configuration file. Firewalls typically execute their rule matching routine from top of the list to bottom, and the first rule that matches “wins,” or executes. Even if there is another rule that matches, since the first one that matches is the one that is executed, the second rule will never be executed. This makes sense as from a logic perspective; the second rule isn’t necessary. It’s important to be aware of this firewall behaviour when crafting rules as they could be redundant. It’s good practice to remove unneeded firewall rules, or better yet, not to create them in the first place, because redundant rules are still needlessly processed, wasting the firewall’s resources. Many firewalls have a mechanism to report the frequency of rule execution, allowing administrators to move the most used rules to the top of the list to speed up execution. Firewall rule execution frequency also allows you to quickly identify redundant firewall rules as the redundant rules will indicate zero executions.

Another important security consideration is that the firewall’s configuration capabilities, usually available via web interface (HTTP (port 80), HTTPS (port 443), SSH (port 22) or telnet (port 23)), should not be exposed to the lower security network segments, and especially not to the internet. If an attacker can gain access to a lower security network segment, and then access a configuration interface for the firewall, they may be able to login to the firewall and reconfigure the firewall rules. Use of a strong password and MFA (if available) to login to the firewall is recommended, along with limiting its configuration access to only the more secure network segment(s). Enabling login notifications will help you catch anyone trying to login to your firewall. You probably don’t log into your firewall very often so you might as well just enable notification for all logins, not just failed logins, so that you can monitor ALL firewall login activity. Why not?!

If you really think you need to be able to reconfigure your firewall remotely, you'd be better off setting up a VPN connection on your firewall. With a firewall VPN connection you can remotely and securely login to your network and then access your firewall configuration. You can configure the firewall so that your VPN-connected host can configure the firewall directly. However, a better method is to configure the firewall to allow a remote connection to a trusted system on the secure internal network (via remote desktop or SSH). The firewall can then be configured by the trusted system instead. This approach of first connecting to an internal trusted system forces another layer of authentication as the remote user has to login to the trusted internal system.

Interestingly, the network segmentation shown in Figure 50 can be achieved with a series of regular WiFi routers in a specific configuration. Because most home and small business WiFi routers deny “unsolicited” traffic on their WAN ports, three WiFi routers can be connected in series, by their WAN ports, to create segmentation. The first WiFi router, including its WiFi networks and physically connected devices, is connected by its WAN port to a LAN port on the second WiFi router. Then the second WiFi router's WAN port is connected to a LAN port on the third WiFi router and the third WiFi router's WAN port is connected to the internet. All of the routers will be configured to obtain their WAN IP addresses from their internet service provider, and they will all each be configured to host a DHCP server for their internal network. Each router's DHCP server will provide IP addresses to each device connected to its LAN ports or via WiFi. This implies that the WAN port of router 1 will get its IP address from router 2's DHCP server and likewise, router 2 will get its IP address from router 1's DHCP server. Router 1 will get its WAN IP address from the actual internet service provider. The devices connected to router 1 would be similar to the devices on the blue network, completely segmented from the devices connected to router 2 and 3. Likewise, the devices connected to router 2 would be similar to the devices on the

grey network, completely segmented from the devices connected to router 3, but not necessarily from the devices connected to router 1, so that would be a small, but likely insignificant difference. Finally, the devices connected to router 3 would be similar to the devices on the orange network, except that they too are also potentially exposed to the devices connected to routers 1 and 2, which again, likely doesn't matter. While this multi-router approach can be used to create network segmentation, a full-featured firewall or UTM solution is likely easier to use, more-flexible and has more security features.

8.2 Self-hosted Services and Applications

There are many reasons why homes and small businesses may consider hosting their own applications that are served to the internet. Common examples include self-hosting web servers, personal cloud servers, gaming servers, media servers, etc. As these servers are deliberately exposed to the internet, it is important to ensure they are placed on different network segments than any important systems and data, that they are hardened properly and that they remain up to date for security patches.

There are several things to contemplate when considering self-hosting an application:

- How much cybersecurity exposure is there?
- How will cybersecurity be dealt with?
- How much power will be consumed?
- How much internet bandwidth is required?
- How much computing power is required?
- With answers to the above questions, how much does it cost?

In the case of a web server, usually the entire point of the thing is to make it something that is available publicly on the internet. In general a website will be relatively easy to find using a search engine and will pose a fair security threat to any networks they are connected to. It may be reasonable to self-host a few websites to get them up and running to serve a small group of users, but it may quickly become unwieldy for the average home user or small business to maintain if the web sites get a lot of traffic.

From a security perspective, the traffic from a popular website would undoubtedly bring some unwanted malicious attention to your web server and network and the administrator needs to be prepared to deal with it. This would primarily be accomplished by ensuring that the web server is placed on a different network segment than any important systems and data, along with hardening the web server properly, remaining up to date for patches, and ideally having a way to detect and defend against attacks.

A popular website also needs to be available, which drives the need to keep the server up and running as well, which consumes electric power. In the case where the expected traffic to the site is low then it may be hard to justify leaving the server running. Likewise, if the traffic grew big enough it may demand more computing power and consume that much more electric power. From a computing resources and bandwidth perspective, a web server serving a small group of users does not require much computing power or bandwidth, but as the site grows it continues to require more resources to remain responsive to users.

Consider self-hosting a website if you:

- Need to host a website that is mostly for personal or infrequent use
- Want to save a few dollars a month (the cost of remote hosting)

- Aren't expecting to generate much traffic
- Already have an appropriate computer running that can be leveraged to implement a web server or otherwise can afford to build and run one permanently for the purpose
- Have the cybersecurity infrastructure to at least segment the web server from any other important systems and data, but also ideally detect and help defend against any attacks
- Don't mind the additional exposure to your home or small business network's public IP address; from a cybersecurity attack perspective, a web server makes a very handy "front door" for would be attackers, if that web server is not properly secured and managed appropriately

Another popular option for self-hosting is a media server. A media server typically allows for any home videos and pictures along with any downloaded mp3s, television shows and movies to be served for consumption via web browser or mobile application. There are several products available ranging from free and open source to "freemium" with the option for a relatively low-priced monthly subscription. The idea is to install the media server software on a computer, configure the media server with "libraries" that point to your media sources, and connect the media server to one of your networks, and ultimately to the internet. From there, the media server can be accessed via a browser or a mobile application.

From a security perspective, since a media server is not intended to serve a large audience and is typically set up for individuals, families, and friends, they are less concerning than web servers. They do typically have some logical ports exposed to the internet, and so if they are misconfigured or the software has a vulnerability then they can present a security concern. For this reason, it probably makes sense to place your

media server on a different network segment than those that contain important devices or data. And as always, keep the software up to date for security patches.

From a resource perspective, a media server isn't exactly trivial. It probably needs to run 24/7, and while running it consumes some power. In order to play large video files, transcode videos or serve multiple users simultaneously, a media server can require a moderately powerful computer as well.

Finally, another popular self-hosted application is a game server. A game server probably doesn't have as much exposure as a web server as it usually requires special software to access it. However, a game server probably has more exposure than a media server. Usually within the game, users can search and find your game server, which could attract some unwanted attention to your servers and network. As usual, the advice is the same; locate your game server on a different network segment than that of your important systems and data and keep your software up to date for security patches. You get the drill.

It may be tempting for gamers to run game servers on their primary gaming computers, as they are typically fairly powerful to play the games in the first place. For gamers, this could be their day to day computer as well, where their most important data is accessed. It would be wise to avoid the temptation to run a game server on your day to day computer. Instead, install the game server on a separate computer, to reduce the cybersecurity exposure and risk to the important data. Another option could be to gain some security by installing the game server in a virtual machine and connecting the virtual machine to the "web facing" network. Physical separation is still better, but virtual separation is better than nothing.

Whether it's a personal web server, media server, gaming server or some other self-hosted application, homes and small businesses typically use port forwarding to facilitate the

connection between the requesting system on the internet and their server. Port forwarding an application exposes it to the internet directly, which makes the security posture of the server critical. A better option, if available, is to use a reverse/application proxy or web application firewall, which sits in between the server and the clients and can respond to malicious activity. See Section 6.12 for more information.

8.3 Remote Hosting

Given the computing, networking, security, and power resources required to perform the various hosting activities one might want to pursue, it is often more advantageous to pay someone else to provide those hosting resources. For a nominal monthly fee, the required resources can be obtained, relieving you of trying to set it all up and maintain it yourself. Web hosting service providers have automated tools to make provisioning a web server very simple, for them and for you. Your web servers are typically provisioned as virtual servers, hosted on hardware servers in a server farm. So called shared hosting services are exactly that, virtual servers running on a hardware server, shared with other virtual servers. Dedicated hardware server hosting is available as well, naturally at a higher cost. If you are hosting a popular website then you may need dedicated hosting.

For the reasons mentioned above, it is common to purchase web hosting services from a web hosting service provider. Most home users and small businesses will find it simple, and cost effective, to purchase web hosting services. Web hosting service providers typically sell multiple tiers of hosting packages, from a single website with limited features (design tools, email, backup options, etc.) to practically unlimited websites with a full feature set that might include enhanced design tools, backup, and E-Commerce features. Typically, web hosting service providers scale your average monthly cost with the time commitment. The deals offered are usually one, two,

three or four year time commitments, paid for up front vs. paying monthly as you go. The savings when purchasing a multi-year plan can be very large. Beware, it is common for web hosting service providers start charging the “normal” fee after the initial term expires. The “normal fee” is usually quite a bit more expensive than the initial offer. While not insurmountable, changing your web hosting service provider is a pretty good pain in the butt, but it’s pretty much the only option to keep costs low. It does seem that the best way to keep web hosting costs low is to purchase the longest initial period as possible, while expecting to pay for the entire term up front, and then plan to go through the trouble of changing service providers at the end of the terms. Repeat. Ugh.

Web hosting service providers will also typically sell domain name registration services as well. It is not necessary, in any way, that your domain name service provider be provided by your web hosting service provider, but it can be quite convenient. If your web hosting is provided by a different service provider than your domain name registration, then you just need to provide the DNS nameservers for your web hosting provider to your domain name service provider. This is usually as simple looking up the IP addresses of the DNS nameservers from your web hosting service and entering them into the DNS nameservers field of the domain name configuration page of your domain name, with your domain name service provider. Your service providers will be able to help with this, if needed.

In addition to web hosting services, more general server hosting services are available as well, known as Virtual Private Servers (VPS). A VPS can be used to host a web server, but it can also be used to do other things like a hosting a media server or game server. Again, because hosting web services requires computing, networking, power, and security resources, sometimes it may be most effective to host such services with a VPS service provider. In either the case of a web hosting service or a VPS service, most often you are still left with security

considerations and tasks. For example, if you are hosting a Wordpress site with your web hosting service it is usually your responsibility to ensure that Wordpress, along with any installed plugins, is kept up to date for security patches. Some VPS services include options for assistance in maintaining the security of the VPS operating system(s), as well as maintaining backups, but some don't.

In summary, web hosting and VPS services can:

- Help you avoid unwanted attention to your home or small businesses public IP address
- Relieve you of needing to purchase computing hardware, power and network bandwidth
- Relieve you of standing up the hardware, OSes and web hosting services
- Get you up and running quickly and reliably
- In some cases relieve you of maintenance work

Web hosting and VPS services can do all of this for you for a modest monthly fee. Paying for hosting is a strong choice. Choose wisely between self-hosting and remote hosting.

9

Power

It's no fun when the power goes out for at least a few reasons related to your network. First, there is the matter of protecting your equipment when the grid power is abnormal. Second, there is the idea of shutting your systems down gracefully, so they can be brought back up reliably, with little concern of file corruption, component failure, etc. Finally, there is the idea of having the internet available for as long as possible when the power is out, particularly as the cellular networks get very slow during power outages (presumably because most of the people around you are using the same cell towers and they have no internet either). These items are elaborated further below.

9.1 Equipment Protection

There are two main devices commonly used to electrically protect electronic equipment in homes and small businesses, they are the surge suppressing power bar and the uninterruptible power supply (UPS). Surge suppressing power bars are inexpensive and great for providing basic electrical surge (increased incoming voltage) protection to electronics that can be safely powered down instantaneously. They do not, however, provide brown out (decreased incoming voltage) protection and they also do not provide any backup power. For these additional features we look to the UPS, which is basically a fancy battery with power receptacles, that devices can be plugged into. UPSes help protect electronic equipment, provide

time to gracefully shut down systems and provide backup power to keep important systems alive longer during a power outage.

9.2 Graceful Shutdowns

During a power outage there are some electronics that can definitely withstand instantaneous loss of power, and that you may not worry about in brown out conditions. A surge suppressing power bar is all that is needed to protect this type of equipment. But there are also some electronics that it would be better to shutdown in a controlled fashion, to avoid things like file corruption. UPSes provide time for gracefully shutting systems down in the event of a power failure by providing battery backup power.

9.3 Backup Power

Finally, when the power goes out, some cellular networks may get very slow. This is likely because most homes do not have a UPS and so the power to their home internet equipment is lost. In this situation, since people don't have access to the internet via their home internet connection, they will likely be relying on their cell phones. Because of this it would be wise, or at least convenient, to try to extend the power to your home networking equipment for as long as possible during a power failure. It might also make sense to prioritize shutting down systems connected to the UPS, that aren't necessary during a power outage, to reserve more UPS battery life for the communication devices.

In light of the above objectives, it would be a good idea to develop a strategy for connecting your various devices to power, and what is planned to happen in the event of a power outage.

Table 29 provides an example of a power plan.

System	Description	Plan	Power Supply
Modem	Needed for comms, instantaneous shutdown OK	Sustain	UPS
Firewall	Needed for comms, graceful shutdown preferred	Sustain	UPS
Secure Network Switch	Preferred for communication until the Desktop PC is shut down, instantaneous shutdown OK	Sustain & Unplug	UPS
Family Network Switch 1	Needed for comms, instantaneous shutdown OK	Sustain	UPS
Family Network Switch 2	Instantaneous shutdown OK	Shutdown	Power Bar
Pi-Hole Laptop	Graceful shutdown preferred	Shutdown	AC w/ Laptop Battery
Desktop PC & Monitor	Graceful shutdown preferred	Shutdown	UPS

Table 29: Example Power Plan

It is great to have a plan yourself to extend the power of your communication devices for your internet connection, but your efforts are futile if your ISP does not have the same or longer duration of backup power available, and you lose internet service anyway. Admittedly, in the author's experience, your ISP may not provide internet access for very long during a power outage. If this is important to you then it would be good to know up front and you may want to inquire with your service provider.

It seems that many of us may have to rely on potentially unreliable cell phone service during power outages, which is not reassuring. For emergency purposes the case for the classic home phone line is still strong. That said, smartphone manufacturers are now integrating emergency satellite communication capabilities into their smartphones, which is quite reassuring.

When purchasing a UPS, consider how much load you will require it to carry and how long you'd like to have backup power available. Bear in mind that you will have to replace the UPS batteries every so often (typically every 2-3 years), so it would be good to identify the replacement costs up front and keep that in mind when buying.

10

Privacy

“What is collected, for what purposes, with whom information is shared, are all matters of policy choice, not technological determinism... Man cannot escape his social or moral responsibilities by murmuring feebly that ‘the machine made me do it.’” - Allan F. Westin, 1973 [Westin, 1973]

“...my point here is, as I've observed since, unregulated data brokers - just by their very existence, just the aggregation of what is available on the Internet, that aggregation itself represents a clear and present danger to society at large.” - Steve Gibson, 2024¹

Webster’s dictionary describes the word privacy as follows:

- “the quality or state of being apart from company or observation: seclusion”
- “freedom from unauthorized intrusion”

Privacy covers a wide-ranging set of topics from the technical ways to improve digital privacy to the implications of sharing data with social media networks. A series of privacy related topics are discussed in this section.

1 Steve Gibson spoke these words on the Security Now! Podcast, episode #1004, which was released on December 10, 2024. A transcript can be found at <https://www.grc.com/sn/sn-1004.txt>.

10.1 WiFi Networks

When out and about, you may come across open WiFi networks (typically free), perhaps at the hotel, mall, coffee shop, etc. The problem with open WiFi networks is that they do not encrypt the WiFi connection and allow anyone on the network to see your network traffic, unencrypted by the WiFi connection. Specialized tools allow malicious actors on the network to see the contents of those communications in “plain text,” unless the communications are encrypted at a subsequent stage in the communication channel. Even if the WiFi connection itself is not encrypted, the communications may still be encrypted by the communication protocol. For example, most modern web servers only allow encrypted connections, e.g., <https>. Most web services (apps, email, etc.) are encrypted, as well. Nonetheless, unencrypted communications on open WiFi networks are susceptible to being intercepted and viewed by others. If it’s necessary to connect to an open WiFi network, then the easiest way to encrypt all of your traffic is through the use of a VPN. As described in Section 6.16, a VPN allows your device to create an encrypted tunnel to a VPN server at home or on the internet where your connection will “emerge” onto the internet. Since your connection is encrypted to the VPN server, all the traffic is encrypted and the devices on the open WiFi network will only see encrypted traffic.

Finally, be mindful of the fact that when that when you are walking around with your mobile device’s WiFi radio enabled, your mobile device will be communicating to some degree with all of the WiFi routers that are in its range. These types of WiFi radio interactions may even possibly leave records behind in logs of the various interacting WiFi routers. If this is not desirable for you, you may want to turn off your mobile device’s WiFi radio if you’re not intentionally using it.

10.2 Cellular Networks

Your location can be ascertained with some accuracy just by carrying your cellular device around. Your device's cellular radio signal "bounces" off of cell towers (radios) in range, which not only includes cellular carrier towers, but also other things like cellular enabled advertising billboards. That cellular radio signal interaction information can be used to locate you, in real time or historically. As in, you were in a certain place, at a certain time.

It is interesting to know that your cellular location information combined with your identity information from the apps you use can be used to personalize the ads on a nearby billboard for you. The billboards in Times Square, New York, for example are optimized for content based on who's in Times Square at that moment.

If you don't like this kind of invasive advertising then the best defense is to limit the software that you use that provides identity information to third parties. You can't stop the location of your cellular device from being known to cellular radios in the area and still have use of cellular services, but you can do your best to limit third parties from knowing that your cellular device is used by you.

You can place your smartphone in a "Faraday cage" to physically prevent it entirely from transmitting and receiving radio communications, but unfortunately, doing so would mean you cannot receive phone calls. Invented in 1836 and named after its inventor, Michael Faraday, a Faraday cage is an enclosure that blocks electromagnetic fields (like those emitted by cellular and WiFi radios). Interestingly, a simple and effective Faraday cage is a stainless steel cocktail shaker, although it could make for an interesting explanation at a traffic stop!

10.3 Personal Privacy

Personal privacy is important. If you trust everything, and everyone, then you have nothing to worry about. If you don't, then you should be concerned with privacy, at least a bit. But you absolutely should not trust everything, and everyone. Even if you trust the governments and corporations that are trying to track more and more of your life, and society at large, inevitably it's only a matter of time before that information falls into the hands of less well intentioned actors, like hackers and hostile governments. And even if you don't care about personal privacy for your own sake, consider the amount of data that is collected about all of us through our interactions on the internet. Imagine the powerful insights that can be drawn from the data that is collected across the globe today. Further, consider how easily humans can be manipulated en masse based on that data. Now add AI and quantum computers.

All of these data collection systems are connected together so that what you do in one system can be known to all the other systems, for whatever uses they may have with it, subject to the terms of service, of course. Physical stores with rewards programs can upload data to social media networks that are associated with your social media account, without your knowledge (well, you agreed to the terms of service when you started using the rewards program...). And that data can then be associated with your social media account when they determine the uploaded data is associated with your identity.

Websites that you interact with can do the same. Your physical location, as ascertained in a number of ways by your cell phone, can then be used to target physical advertising at you.

Advertising, while often creepy, annoying, and generally unappealing, is not very concerning, but aggregated across an entire economy of spenders; wow, that is powerful information. Combined with social media posts, clicks, likes, reactions, etc. This is unbelievably powerful information, and it is used to

build finely detailed models of your social behaviours, and social groups at large. Those behaviour models are then used to draw your attention to whatever the social media network wants to. Mostly to make money through advertising, but who knows; some think to swing elections. It's certainly plausible.

The data flow between consumers and data collectors is very asymmetrical. The data collectors have ALL THE DATA and all we, the users have, is the use of their websites and apps. For the most part, we really have no idea how our data is being used. Some uses of our data are described, at a high level, in the data collectors' privacy policies. Thankfully, some control of your data is often provided now (thanks to privacy laws). Consider that the data collectors are multinational organizations. These organizations are collecting more behavioural data about us than any of our governments could ever hope for. Then again, how much of our collected data might just be shared with the government(s) anyway?

Our relationship with data collecting apps and websites like Google, Facebook, Instagram, LinkedIn, Reddit, etc. is a weird and somewhat twisted one. Surely there is an exchange of value for us to use their services, or they wouldn't provide them. However, we don't pay with money, but with our data and attention. The apps and websites the data collectors provide are like a siren call we just can't seem to resist. With all the great open source and paid options that don't spy, it's worth a think to look elsewhere for your computing needs.

Consider the amount of data that Google Classroom has amassed about school children, with all the various school boards embracing Google Classroom. This is yet another digital siren call, targeted at school boards and children. Consider what could be done with such data, in the hands of people with positive or self-serving interests, never mind those with nefarious intentions that may gain access to the data through nefarious means.

The main point is that your data is valuable; if it weren't, the data collectors wouldn't exist to harvest, aggregate, and harness the power of that data, for a handsome profit, none of which is shared with you. Even if you are apathetic to your own personal privacy and the value of your data, consider that the power of the aggregation of our data is much greater than the sum of our individual personal data.

10.4 Internet

Most of your internet traffic originates inside your internal networks on your devices and then “emerges” onto the internet when your router forwards those packets to the next-hop router, toward their destination. Once those packets leave your router, if they aren't protected in some way, then devices along the path to the destination may be able to see the contents of those packets and perhaps even modify them. Such internet communications occur over communication protocols. The internet protocols are paramount in protecting your internet privacy and rely on encryption techniques to make the data unknowable to devices that relay your packets along their path, to and from, their destination.

As previously mentioned, most browsers today use HTTPS. You don't have to think much about this. Modern browsers go to great lengths to make it difficult, if not impossible, to use plain HTTP. You can pretty well take for granted that your internet browsing traffic uses HTTPS and is safe from snooping by conventional computers.

Many of the encryption techniques used today are not safe from fast decryption by quantum computers. Quantum computers work differently than conventional computers, and are particularly well suited to decrypting information that was encrypted using conventional encryption algorithms, practically instantly.

For example, some encryption algorithms, such as RSA¹, rely on the idea that it is trivial to multiply two very large numbers together for a result, but that same number is extremely difficult to factor to determine which two numbers were originally multiplied together. In the case of RSA-2048 encryption, it is estimated that it would take 300 trillion years for a conventional computer to break the encryption². However, quantum computers promise to be able to do so in mere moments.

Post quantum cryptography (PQC) is available and in active development so there is a path forward for encryption. However, until PQC is in widespread use, your privacy may already be entirely compromised with a future, retroactive analysis once quantum computers are prevalent.

10.4.1 Virtual Private Networks

Use of a VPN service can be used to gain an additional layer of privacy, even anonymity if done properly. This is because the IP address that the internet sees associated with your traffic is only a temporary one, provided by the VPN service provider. In theory, the only thing connecting you to the traffic associated with that IP address is your VPN user account and any logs the VPN service provider keeps (so use one that doesn't keep logs if that matters to you...). This is pretty strong privacy, but it does require you to trust, and usually pay for, a VPN service provider.

All of this said, true anonymity requires that you are not logged into any of your website accounts or services, or otherwise have any apps communicating with internet servers. This is because whatever systems you are logged into can then log your temporary VPN-based IP address and associate it with the logged in user account, exposing your identity. This includes

1 <https://www.historytools.org/concepts/rsa-encryption>

2 <https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art>

being logged into any cloud services, OS based connections “back to the mothership”, social media websites and apps, online retail websites, along with any other websites you log into to access. In reality, true anonymity requires some effort to make sure you aren’t exposed somehow. A GNU Linux based VM is probably the simplest option. The idea would be to launch and use a “bares bones” GNU Linux VM that is, and has never been, logged into anything. Then install your VPN client on your GNU Linux VM, launch your VPN client on your Linux VM, and proceed to interact with the internet from the VPN-connected GNU Linux VM.

The Onion Router (TOR) and proxy chaining also provide methods of anonymizing your internet traffic to varying degrees of effectiveness. Some combination of VPN services, TOR and proxy chaining may provide the most confidence of anonymity. Still, unless quantum resistant cryptographic protocols are used, the traffic may still be decrypted trivially at some point in the future.

Remote access VPNs allow you to connect from a remote location to your home or office network to access its resources, like file shares, email servers, intranet sites, etc. Similarly, site-to-site VPNs can be used to connect two or more houses/office branches/sites together, in a secure and private way. Use of remote access and site-to-site VPNs ensures that any traffic flowing across these networks cannot be snooped on, even though the packets are flowing across the internet.

10.4.2 Online Interactions

The online systems that you interact with like websites (search engines, online shopping, social networks, etc.) and online applications (maps, documents, streaming services, etc.) can leverage your connection and interactions with them to track your activities across the internet. Such activities might include your spending habits, browsing habits, location, possibly your health status, exercise patterns, eating habits, and more

depending on the apps and services you use. Some of this information can also be correlated with your offline activities through things like reward programs. Most of this type of information exchange is necessary to gain the functionality that users want and cannot be avoided other than limiting use of those systems. It's good to be mindful of what data you're deliberately sharing and what that data is being used for.

Thanks to advances in privacy laws, data collectors are required to provide transparency into the data they are collecting and to provide users some control over the continued storage of their data. Often steps can be taken to limit the amount of data collection an app or website performs through options they provide. It's good to find out about the privacy improving features available on your devices. Many times the default settings of these kinds of options are not in favour of your privacy so it is good to get to know the options and to exercise them accordingly.

As is the case with software security, not installing apps on your mobile device that are not needed improves your privacy as well, as it eliminates another application from collecting data, whether deliberately or through mis/poor-configuration.

10.4.3 Online/Offline Accounts

Online accounts, and even offline accounts you have with brick and mortar stores, can be a source of privacy concern. It has to be assumed that any and all online databases can, and probably will be hacked, at some point. If you would be embarrassed, or unacceptably exposed if a database that has information about you were publicly disclosed, then it's something to be mindful of and act accordingly. Remember that use of rewards programs can link your "offline" activities with your online identity.

10.4.4 Cookies

A lot has been said, and made, of cookies. Most people have heard of cookies and have the sense that they are used to track

your actions across the internet. And that is exactly what they are for. Cookies are text information stored on your device, placed there by the online websites. Cookies are used to make your online experience more convenient by enabling the websites that you interact with to identify you, and the state of their interaction with you. For example, to allow you to continue your online web shopping session and restore your shopping cart. How convenient?! Cookies are a powerful mechanism for enabling web servers to provide the most convenient experience possible.

For this convenience, there are some issues to be aware of with cookies. Using a shared computer to access websites that use cookies may leave them behind on that computer. Those cookies may be leveraged by another user of the shared computer. In a possible worst case scenario, if you were to make online purchases on that shared computer, another user with access to those cookies may be able to make online purchases from the online stores you purchased from.

In terms of the ability for cookies to store state information conveniently, they cannot accommodate one person using multiple computers. This kind of convenience usually requires an account to be created with a given website so that it can store state information in a database for retrieval when you log back in.

An irritation to many users, is when temporary internet files (including cookies) need to be deleted when troubleshooting computer issues. Cookies are not a perfect solution for creating a convenient internet experience, but they can still be very useful.

There are two types of cookies, first-party and third-party cookies. Both types of cookies are encrypted. First party cookies can be accessed only by the website that created them. But third-party cookies, also known as tracking cookies, are placed on the users device by a website other than the one the

user is visiting, and thus the cookie can be accessed by websites other than the one that originally stored it. This behaviour allows the third-party cookie provider to track your online activity across the sites you visit, providing much more powerful insights. Mostly for the purposes of targeted advertising, tracking cookies will store information about the websites you visit, product pages/web elements you've interacted with, your online purchases, your IP address and your geographic location. This information allows them to present you with the most targeted advertising that they can. Is this bad? It depends on how you feel about privacy and advertising.

10.4.5 Social Media & Gaming

The privacy implications of social media are pretty well known to most people by now (the time of this writing). Social media sites are meant for sharing content, messaging, etc., and by their nature, are not really meant to be private. It's part of the deal. It's just important to be aware that all of your interactions on social media are stored and meticulously leveraged by the algorithms on the platforms to optimize content delivery to you. The documentary "The Social Dilemma" paints a pretty dismal picture of how unhealthy this content delivery can be in terms of the emotions that the algorithms try to tap into, to capture your attention.

Social media networks retain all the information that you provide to them, if you let them. Social media networks store your information to maintain your personal profile, as you wish, but also to leverage that information to feed their content delivery algorithm. Thanks to recent advancements in privacy laws, social media networks, along with all other personal data storing websites, have to provide citizens of those countries where the privacy laws apply, with options to understand what data is being collected, how that data is being stored and what the data is being used for. In addition, data collectors are

required to provide some control over how that data is used, the ability to request copies of the information and the ability to request its deletion. It's good to be familiar with the privacy options available from the social media networks you use, and to configure and exercise those options according to your personal preferences.

Some social media sites provide information to their users about what other data third-parties have uploaded to them, about their users. The social media sites take bulk uploads from other third-party websites and sources, and correlate them with the accounts of their own users. They then use those correlations to target advertising at you. Facebook provides this information at:

https://www.facebook.com/off_facebook_activity.

At one time Facebook provided information about what brick and mortar store rewards programs uploaded data to them, like Canadian Tire's Triangle program. The information no longer seems to be available, but the author remembers that it once was and then used that information to request the data be deleted from the companies that uploaded it. It would be good to be aware of any such options in any social media and gaming platforms you use, and to exercise those options to minimize those correlations, if privacy is your thing.

Roblox and Snapchat are two social networks that have aspects worth discussing specifically. Roblox is an online social gaming platform that allows its online user base, of mostly kids, to develop games within its software environment. Those games can then be played by other users. There is a reward system that allows Roblox game developers to receive some compensation in the form of Robux, Roblox's own online currency of sorts, that can be used to buy digital content within Roblox. Robux can also be purchased from Roblox directly or through official sales channels. While prohibited by Roblox, Robux can often be bought and sold on aftermarket websites. The good folks at the People Make Games Youtube channel have

done some investigating and released two very eye-opening videos documenting concerning aspects of Roblox. We learn from these videos that the trouble is that Roblox is mostly used by kids and their parents don't realize that, via Roblox, their kids may have access to very unsavory content. Additionally, the development aspects of Roblox have evolved to teams of developers, essentially creating an unregulated online workplace. Finally, the digital marketplace in Roblox, along with the prohibited third-party marketplaces and Robux exchanges, provide potentially dangerous incentives and outlets for kids.

Certainly Roblox can be used responsibly, but it does seem that it needs to be used deliberately so, and a lot of parents don't realize it. The People Makes Games videos are definitely worth watching, especially if you have children using the platform. They are easy to find on Youtube and their titles are "Investigation: How Roblox Is Exploiting Young Game Developers" and "Roblox Pressured Us to Delete Our Video. So We Dug Deeper".

Snapchat is another social network that requires special consideration for parents. Snapchat is your basic social media network complete with content feed, but the more concerning part about Snapchat is its deliberate approach to automatic disappearing messages and keeping no records. The trouble with Snapchat is that it allows mass private communication, that automatically disappears from all devices that receive them, within a short period of time. So its mass communication with zero accountability. Zero. When screenshots are taken of a "snap", the original poster is notified that a screenshot was taken. Even this feature discourages people from taking a screenshot as they are immediately exposed. This type of functionality just lends itself to abuse and it can really be used to create toxic environments for kids. One kid can communicate privately and silently sending a hideous message to hundreds of other kids and within moments of viewing it the message

disappears forever. And if anyone takes a screenshot they are immediately exposed. It's just a perfect tool for cyberbullying.

It's not that Snapchat is inherently bad, it's just encourages a zero accountability culture and since it's user base is mostly kids, it's just ripe for abuse as a cyberbullying tool. Plain and simple. Snapchat also has a location sharing feature that kids don't seem to mind using to let all their contacts know where they are at all times. Why anyone would willingly use this feature is beyond fathom to the author.

The moral of the story is, if you have kids using Snapchat, be wary of what they may be exposed to or creating themselves. The zero accountability environments tempts the worst behaviour in the best of people. Even if your child doesn't use Snapchat it's good to be aware of what they might be encountering in their day-to-day with others that do.

10.4.6 Televisions and TV Boxes

Today, for home television and entertainment, many people use streaming services. In order to enable those streaming services, most modern televisions are sold as "Smart" televisions and come with some kind of operating system built in allowing them to offer apps for streaming. There are also 3rd party streaming systems available that can be plugged into the input ports of a television, such as the Amazon Firestick, Google Chromestick, Apple TV and the various Roku streaming devices. When it comes to privacy, many of these devices are brutal, just read their privacy policies, seriously. They monitor what you watch and when you watch it. They listen to you through the voice activation features. Some of them include algorithms that try to determine what you are watching on the installed channels that they can't explicitly access. They store all of it. They sell all of it. Many of them are starting to insert a sickening amount of advertising into their content delivery. It's really just sad.

Unfortunately, there are not that many great options to retain your privacy when it comes to televisions and TV boxes. The most privacy retaining option appears to be setting up a GNU Linux computer as a streaming device, but this would likely not be slick enough for many folks. The next best option may be an Apple TV as Apple seems to be more privacy forward than the others available, but that is just the author's opinion.

Finally, a note on Android TV boxes. These TV boxes look similar to an Apple TV or Roku streaming devices, but they have Android loaded on them. While extremely convenient and cost-effective, many of them come pre-hacked with a malware called "BAD BOX" and need to be treated with severe caution when introducing them onto your network¹. Basically, don't use an Android TV box.

10.4.7 Privacy Laws

Since the 1990s, when the internet started to see increasingly popular use, the privacy laws have been playing catch up. It should be clear at this point in the book how valuable your data is to the companies that want it, and how powerful a tool it is for them to influence consumer behaviour, in aggregate. Increasingly, consumers are unable to escape using the internet in their day to day lives. Interacting with the online systems that consumers interact with inevitably leaves their data available for collection, aggregation, and exploitation. Privacy regulations are essentially the only tool that consumers have to maintain their privacy.

At the time of this writing the US does not have federal data protection laws and only five states have some form of them. Canada has had its Personal Information Protection and Electronic Documents Act (PIPEDA) since April 13, 2000, and Europe has had its General Data Protection Regulation (GDPR) since May 25, 2018. The power of these laws are felt everyday

1 <https://securityaffairs.com/172191/malware/190000-android-devices-infected-by-badbox.html>

by people all over the world as we all explicitly accept cookies when sites ask us to, as they must now, to be in compliance with the laws.

Both PIPEDA and GDPR generally aim for the same goals, but there are some differences. Tables 30 and 31 provide some interesting similarities and differences between PIPEDA and GDPR.

Privacy Area	Description of PIPEDA and GDPR Similarity
Data Protection Principles	Fundamental data protection principles including things such as the need for businesses to obtain consent for data processing, to process data fairly and lawfully, and to maintain data accuracy.
Individual Rights	Granting individuals specific rights over their personal data. Including things like the right to access, rectify, and delete their information, and to request information about how their data is being used.
Accountability and Transparency	Organizational accountability and transparency for data processing activities, including things like having clear privacy policies and ways for individuals to contact the organization if they have concerns over their privacy.
Data Minimization	Encouragement for businesses to only collect and retain the personal data that is necessary to accomplish the purpose that it was collected for, aiming to minimize potential privacy risks associated with the collection of excessive amounts of personal data.
Cross-Border Data Transfers	Regulation of cross-border data transfers to ensure that personal data is protected adequately when transferred outside the respective jurisdictions.

Privacy Area	Description of PIPEDA and GDPR Similarity
Privacy By Design	Promotion of the idea of “privacy by design,” encouraging businesses to concern themselves with data protection from the beginning and when new products, services, or processes are developed.

Table 30: Similarities Between PIPEDA and GDPR

Privacy Area Difference	PIPEDA	GDPR
Data Protection Officers	Every organization with compliance scope must appoint privacy officers.	GDPR outlines specific situations when a Data Protection Officer is required.
Legal Basis for Processing Data	PIPEDA contains ten lawful bases for processing, they are: accountability, identifying purposes, individual’s consent, limiting collection, limiting use, disclosure, retention, accuracy, safeguards, openness, individual access and challenging compliance. Data controllers must choose a lawful basis as justification for using the information of a data subject.	The GDPR outlines six lawful bases for processing the data, they are: consent, contractual necessity, compliance with a legal obligation, necessary to protect vital interest of data subjects, public interest, the legitimate interest pursued by the controller or by a third-party. A lawful basis must be used as justification for using the information of a data subject.

Privacy Area Difference	PIPEDA	GDPR
Reporting Data Breaches	At the earliest when there are circumstances of significant harm to the individual organizations; must notify the Federal Privacy Commissioner and the affected individual(s) regarding breaches involving their personal information.	Organizations have to report a data breach within 72 hours.
Damages/ Fines	Fines can be up to \$100,000 depending on the severity of the violation.	Fines can be up to €20 million or 4% of annual global revenue, whichever is higher for the most serious offenses.

Table 31: Differences between PIPEDA and GDPR

These privacy laws are important and while it can sometimes be annoying to always have to explicitly agree to methods of data collection, these obstacles are there for your protection and they should be guarded and cherished.

10.4.8 Your Information on Their Systems

Regardless of whether you truly like and trust the business that you're giving your data to or not, there are privacy risks worth considering when interacting with their systems. It is usually only a matter of when, not if, a website will be hacked and the data it contains leaked or otherwise leveraged. All of your data can be leveraged in some way, and even if it seems innocuous,

you are party to these transactions. If you could be paid to provide your data, that would be one thing, but just to have it leaked or leveraged by others? The author contends it's better to minimize situations where your data can be leveraged by others and that the best way to do this is to be aware of, and minimize, the amount of your data that is online and available to data collectors.

There are times when you might deliberately want to store your data on someone else's systems. For example, email, and cloud services for storing your files/data, photos, backups, etc. In these cases having your data on someone else's systems is the very service you are seeking. Even in these cases it's important to remember that when your data is unencrypted on someone else's system you will not have privacy. Encouragingly, there are increasing options for encrypted cloud storage.

There are email services available, such as Protonmail, that ensure your email is encrypted end-to-end, and that your data is encrypted while on their systems, ensuring that they have no access to it. Email delivered this way is more costly to deliver, particularly because it is not leveraged for advertising. While free services are available, excellent ones at that, be advised that you may find them with limited access only to browser-based or mobile applications and may require a subscription to use with email clients like Microsoft Outlook, Mozilla Thunderbird, Apple Mail, etc.

With regards to cloud services for photo and video storage, documents, data backups, etc., you can choose to use a service that ensures the files are encrypted and that **ONLY YOU HAVE THE KEY**. If anyone else has the key then there is no way to know that the data isn't being decrypted and used. There are some cloud services available that provide end-to-end encryption and the decryption keys are unknown to them. If this is important to you, it is excellent privacy, super convenient and reliable. It just costs some money. The other mitigation is to encrypt your files before uploading them. This

wouldn't necessarily work for photos and videos or other files created contemporaneously and uploaded to the cloud by a mobile device, but for a set of data that just requires backing up to a cloud server, then encryption before uploading could be a good solution if your cloud service provider doesn't offer encryption.

10.4.9 Opting Out

Among the privacy conscious, there is the idea of opting out. Opting out is essentially telling businesses that you don't want them to collect your data, to remove any of your data that they have, and to be conscious and deliberate about what data you give to who, online, and in real life.

It is ideal to keep a running list of all of the websites that you make accounts with, as well as brick and mortar stores that you interact with, so that you can contact them to remove your data should you wish to. If you are careful and conscious about what websites and businesses that you interact with then you may have a tight list of data collectors that you must let have your data so that you can interact with them as you wish to. This is good situation to be in. It's the best you can do. You can still contact these businesses routinely to remove any unnecessary information they may have. Perhaps a transaction history, list of calls, post interactions, etc. Unless the data is relevant and valuable for you then you may consider asking them to delete it. Diligently using a password safe to log your account creations and generate strong passwords is an excellent way to keep track of your online accounts. You could also put "dummy" entries into a password safe to keep track of reward program accounts and other physical type accounts.

The website <https://simpleoptout.com/> has compiled a long list of opt-out options from many of the companies you may use and want your data removed from. The website also highlights some of the worst parts of their privacy policies and uses of your data.

In addition to taking personal action to have your data removed there are services available that are able to find your online data and request its removal, and then persistently track and follow up on removal progress. Thanks to privacy laws, many of the online businesses that you interact with are more and more compelled to comply with data removal requests. Often it is a somewhat painful process and requires ongoing effort to track and follow up on progress. Data removal services typically cost a fee, but they provide a valuable service by relieving you of the effort to catalog the data brokers that have your data, initiate the data removal process, track, and follow up on data removal requests.

10.5 Mobile Device Privacy

Mobile devices, as they are largely used on the internet, suffer all of the same issues described in this section, but from a privacy perspective they add the element of your location history. Additionally, most people use their mobile devices in a much more intimate way than other devices, and so they usually contain a lot of private, personal information.

The location features of mobile devices make them extremely potent for targeting advertising. Depending on the applications you use, sufficiently sophisticated businesses are able to use the cell radio in your phone combined with attributes of your identity to target billboards at you. Turning off location services for applications that you don't require to have it, and only turning on location services when you need it will help.

From a privacy perspective, there isn't much you can do about cellular communications because you need to be able to make and receive phone calls. In the event that you do want to completely disable your cellular communications, remember that you can put your cell phone into a Faraday cage.

10.6 Ad-Blocking

Ad-blocking is a bit of an ethical dilemma that everyone must face for themselves. On one the one hand, websites and apps are providing a service “for free” in the hopes of achieving some form of revenue via advertising. The moral case is that it costs human effort and money to run a good website or app and the businesses should be able to recover their costs. For both themselves and the consumer, they have decided the way they can and will recover their costs is via advertising, as opposed to say, asking for an explicit subscription fee. On the other hand, the consumer gains access to the free service, but is subjected to sometimes ugly, creepy, non-uniform, disproportionate and even, at times, downright dangerous advertising. In the middle is an obnoxious fight over the features of how the internet works and services it provides. Today, the fight is coming to a head and many sites are refusing to load content if ad-blocking technology is used. Youtube is continuing to increase the number of ads you must watch while decreasing the length of video between ads, and making the ads un-skippable. Browser plugins are responding in kind as much as they can. It is a full on “arms race” for ads in browsers.

There are different kinds of advertisements. Typically, there are the kind that are loaded into your browser or mobile application, integrated with the displayed content and then there are the kind that are loaded into video players or embedded directly into video streams. Systems such as “Pi-hole” act as a DNS server so that all of the internet requests made by the devices in your home or office first make the request to the Pi-hole, and the Pi-hole decides whether to forward the request or not. You configure the Pi-hole as the DNS server for your devices. This will not only block out advertising, but also known malicious sites. This type of ad blocking is effective for the kinds of ads that load into websites, but less effective for embedded video type advertising from Youtube.

The other option is to use a browser plugin, mainly Firefox, loaded with an ad-blocking plugin. This method can be very effective and even works with video advertisements, but again, it's like an arms race and sometimes it breaks. It's probably only a matter of time before it breaks permanently. It seems that advertising is going to be a part of human fabric for the long term. It's how we get ideas off the ground that people aren't willing to pay for. People won't pay for Gmail it seems, not with money anyway, only with loss of privacy, and in turn get advertising. It seems it's what we, as a consumer collective, insist on - the advertising approach. But there has to be a better way.

Further Topics, References and Useful Links

This section provides some further topics for the interested reader along with some references and useful links to explore.

11.1 Artificial Intelligence and Quantum Computing

Powerful AI is here. It's still early days, but we are all witnessing its power unfold before us. These are pattern seeking machines and they are very good at it. Perhaps not great quite yet, but on its way. The ability for artificial intelligence to comb through data to draw deep insights will be astonishing.

Quantum computers have been talked and research has proceeded for a long time, since about 1980, but have never been a reality. Today, it seems they will become a reality before long. While not all applications will be able to exploit the benefits of quantum computing technology, some applications will see unthinkable productivity improvements. As mentioned previously, one area that is under active threat and development is cryptography and post-quantum encryption.

The combination of AI and quantum computing will yield unbelievable computing power with unbelievable pattern recognition capability, “the likes we have never seen before”.

Without proper regulation, AI and quantum computing have the potential to be absolutely devastating to security and privacy. Essentially limitless power to collect, comb through and leverage all the data. From developing advanced and adaptive malware to pre-crime and thought crime. It will all be possible. In the right hands, its just technology to be deployed to the benefit of humanity. In the wrong hands, your imagination is insufficient to envision what it could be used for.

Folks, this is pretty serious. Take your privacy seriously now before it's too late. Demand government regulation because its the only thing that will limit this capability and power and it is not in your favour. Realistically, because there are hostile entities in the world that will not curb their enthusiasm for these technologies it is another arms race. Unfortunately that implies that we probably cannot afford to slow down the development of these technologies, but we need protections over how they will be used against consumers and citizens.

11.2 Networking

The following are a series of interesting online resources related to networking:

The book “DNS and Bind” by Liu and Albitz

Industrial Ethernet University:

<https://www.industrialethernetu.com/>

11.3 Security

The following are a series of interesting online resources related to cyber security:

Security Now Podcast: <https://twit.tv/shows/security-now>

Gibson Research Corporation: www.grc.com

Cybersecurity for Gamers 101: Gaming Malware and Online Risks: <https://heimdalsecurity.com/blog/cybersecurity-for-gamers-101-malware-risks/>

NIST Special Publication 800-121 “Guide to Bluetooth Security”: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2-upd1.pdf>

Guidelines for Securing Wireless Local Area Networks (WLANs): <https://csrc.nist.gov/publications/detail/sp/800-153/final>

Guidelines on Firewalls and Firewall Policy: <https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final>

NIST Small Business Cybersecurity Corner - Securing Network Connections: <https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/securing-network-connections>

11.4 Privacy

The following are a series of interesting online resources related to privacy:

New York Times Article ‘You’re Tracked Everywhere You Go Online. Use This Guide to Fight Back’:

https://www.nytimes.com/2019/11/24/smarter-living/privacy-online-how-to-stop-advertiser-tracking-opt-out.html?utm_source=pocket-newtab

Jscrambler Article ‘Beyond Analytics: The Silent Collection of Commercial Intelligence by TikTok and Meta Ad Pixels’:

<https://jscrambler.com/blog/beyond-analytics-tiktok-meta-ad-pixels>

Inc.com Article ‘Secret Consumer Scores’ Explain Why Some People Get Much Better Service Than Others. Now, You Can Finally Request Your Data and Get Your Information’:

<https://www.inc.com/bill-murphy-jr/secret-consumer-scores-explain-why-some-people-get-much-better-service-than-others-now-you-can-finally-request-your-data-get-your-file.html>

BleepingComputer.com Article ‘LinkedIn secretly scans for 6,000+ Chrome extensions, collects data’:

<https://www.bleepingcomputer.com/news/security/linkedin-secretly-scans-for-6-000-plus-chrome-extensions-collects-data/>

PrivacyGuides.org:

<https://www.privacyguides.org/>

Simple Opt-Out:

<https://simpleoptout.com/>

Sift’s Data Rights Request Page:

<https://sift.com/data-request>

Zeta’s Global Privacy Request Page:

<https://privacyportal-cdn.onetrust.com/dsarwebform/bc2d3301-11a5-4de5-b15e-ce796187a352/d0720d0f-d427-4a7d-a773-5d6793229f15.html>

Electronic Frontier Foundation Article ‘Google Says It Doesn’t

'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits It.'

<https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and>

PressFarm article 'Tim Cook Privacy Stance: Apple's Commitment to User Security':

<https://press.farm/tim-cook-privacy-apples-commitment-user-security/>

Internal Association of Privacy Professionals article 'Apple's Tim Cook: Protection Privacy 'most essential battle of our time':

<https://iapp.org/news/a/apples-tim-cook-protecting-privacy-most-essential-battle-of-our-time/>

Paper titled "third-party Tracking in the Mobile Ecosystem" by Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, Nigel Shadbolt:*

<https://arxiv.org/pdf/1804.03603>

Forbes article 'Google Starts Tracking All Your Devices In 6 Weeks—Forget Chrome And Android':

<https://www.forbes.com/sites/zakdoffman/2025/01/11/google-starts-tracking-all-your-devices-in-6-weeks-forget-chrome-and-android/>

BBC Article 'Gmail messages 'read by human third parties':

<https://www.bbc.com/news/technology-44699263>

Proton Article "Outlook is Microsoft's new data collection service" by Edward Komenda:

<https://proton.me/blog/outlook-is-microsofts-new-data-collection-service>

11.5 Miscellaneous

Summary of various data transfer rates:

<https://www.cmd-ltd.com/advice-centre/usb-chargers-and-power-modules/usb-and-power-module-product-help/data-transfer-rate/>

12

Select Software and Tools

This section provides a list of software that may help implement some of the concepts in this book and be evaluated by users for suitability in their environments and applications.

Anti-malware Software: Malwarebytes, ESET, BitDefender, Windows Defender

Backup Software: Paragon Backup & Recovery, VEEAM, Synchredible

Network Firewalls: Sophos UTM Home Firewalls, PFSense, IPFire, OpnSense, Arista (formerly Untangle), Ubiquiti Dream Machine/Router, Smoothwall, Endian

Office Suite: LibreOffice, Open Office

Encrypted Email and Private Cloud Computing: proton.me

Security Tools: Kali Linux, Metasploit, NMAP, OpenCanary

Media Server: Jellyfish, Kodi

Network Monitoring: PRTG Network Monitor, Nagios, Zabbix

Password Management: Password Safe, BitWarden

Windows Security Audit: Bel Arc Security Advisor, ESET SysInspector

SIEM: Security Onion, Wazuh, Splunk, Elk Stack

Windows Utilities: Easy Service Optimizer, Balena Etcher, PuTTY, Sysinternals, WinSCP

Vulnerability Assessment: OpenVAS, Nexpose, W3AF, OpenSCAP

Virtualization and Sandboxing: VirtualBox, VMWare, Sandboxie, QEMU

Patch Management: OS App Stores, OEM Hardware Websites, OEM Patching Tools, Patch My PC (Windows), Ninite (Windows)

Free Online Scanning Tools: ESET, Malwarebytes, VirusTotal

Free Offline Scanning Tools: Windows Defender Offline, Dr. Web LiveDisk, Hiren's BootCD PE, ESET SysRescue Live

Bibliography

History Tools, 2024: History Tools, The Evolution of the Internet: From Early Networks to Today's Global Phenomenon, 2024, <https://www.historytools.org/concepts/internet>

Hill, 2022: Hill, Brandon, USB Decoded: All the Specs and Version Numbers, 2022, <https://www.tomshardware.com/features/usb-decoded-all-the-specs-and-version-numbers>

Harding, 2022: Harding, Scharon, Breaking down how USB4 goes where no USB standard has gone before, 2022, <https://arstechnica.com/gadgets/2022/09/breaking-down-how-usb4-goes-where-no-usb-standard-has-gone-before/>

Teener, 2004: Teener, Michael Johas, Technical Introduction to IEEE 1394, 2004, https://www.ieee802.org/802_tutorials/04-July/NewTechIntroTo1394.pdf

Apple Fandom Wiki: Apple Fandom Wiki, Lightning (connector), 2012, [https://apple.fandom.com/wiki/Lightning_\(connector\)](https://apple.fandom.com/wiki/Lightning_(connector))

Shakir, 2023: Shakir, Umar, A history of Apple making us buy new cables, 2023, <https://www.theverge.com/2023/9/12/23859659/apple-cable-history-iphone-15-usb-c-lightning-mac-thunderbolt>

Thunderbolt™ Community: Thunderbolt™ Community, Technology Brief: Thunderbolt™ 5, 2023, https://www.thunderbolttechnology.net/sites/default/files/Thunderbolt_5_TechBrief_2023_09_12.pdf

Intel, 2023: Intel, Intel Introduces Thunderbolt 5 Connectivity Standard, 2023, <https://www.intel.com/content/www/us/en/newsroom/news/intel-introduces-thunderbolt-5-standard.html?wapkw=thunderbolt%20version%20compare#gs.fx8ula>

Warren, 2023: Warren, Tom, Apple's new M3 chips have big GPU upgrades focused on gaming and pro apps, 2023

Mister Mobility, 2023: Mister Mobility, How Many Years Of Updates Do Android Phones Get? A Helpful Guide, 2023

Haslam, 2024: Haslam, Karen, How long does Apple support iPhones?, 2024

Doffman, 2025: Doffman, Zak, Google Starts Tracking All Your Devices In 6 Weeks—Forget Chrome And Android, 2025

Duffy & Muchmore, 2026: Duffy, Julie, Michael, Muchmore, The Best Cloud Storage and File-Sharing Services for 2024, 2026

China, Goodwin, 2024: China, Chrystal R., Goodwin, Michael, What is the OSI model?, 2024,
<https://www.ibm.com/think/topics/osi-model>

Code Academy: Code Academy, The OSI Model, Year Unavailable, <https://www.codecademy.com/article/osi-model>

Raza, 2024: Raza, Muhammad, OSI Model: The 7 Layers of Network Architecture, 2024, <https://www.bmc.com/blogs/osi-model-7-layers/>

Romano, Stahl, 1987: Romano, S., Stahl, M., "Internet numbers", RFC 1020, DOI 10.17487/RFC1020, 2024

Rekhter, Moskowitz, Karrenberg, de Groot, Lear, 1996: Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, 1996

Aesop, 1867: Aesops (1867), "The Flies and the Honeypot". Aesop's Fables (Lit2Go Edition). Retrieved February 01, 2025, from <https://etc.usf.edu/lit2go/35/aesops-fables/391/the-flies-and-the-honeypot/>,

Triggs, 2024: Triggs, Robert, What is AOSP? Everything you need to know, 2024

Westin, 1973: Allan F. Westin, Databanks in a Free Society, 1973

Index

319.....	11	Bluetooth Security.....	241
A2DP.....	171	Bluetooth Special Interest Group.....	170
Accelerated Graphics Port.....	22	Border Gateway Protocol.....	130
Accounts.....	201, 289	Brown out.....	277
Ad-blocking.....	302	Bug bounty.....	214
Address Resolution Protocol.....	22, 129	Bugs.....	43, 213
Advanced Audio Distribution.....	171	Burp Suite.....	54
Advanced Video Remote Control.....	171	Cache memory.....	61
AGP.....	22	Cain & Abel.....	54
AI.....	304	CAT3.....	80
Aircrack.....	53	CAT5.....	79
AirDrop.....	176, 244	CAT5/5e/6.....	23
AirPlay.....	176, 244	CD.....	23, 226
AM.....	22, 156	Cellular data.....	241
Amplitude modulation.....	22, 156	Cellular network.....	241
Android.....	48, 58, 232	Cellular Networks.....	165, 283
Android Open Source Project.....	22, 252	Central processing unit.....	60
Anti-malware.....	224	CGI.....	23
Antivirus.....	22	Chromebooks.....	58
AOSP.....	22, 252	CIDR.....	23
AP Isolation.....	241	Classless Inter-Domain Routing.....	23
API.....	22	Cloud Services.....	113
Apple.....	58, 95, 101	Coaxial.....	75
Application Programming Interface.....	22	Common Gateway Interface.....	23
Application proxy.....	151	Compact Disc.....	23, 226
Applications.....	218	Composite Video.....	75
ARP.....	22, 129	Computers.....	89
Artificial Intelligence.....	304	Conduit.....	238
Audio Interface.....	67, 77	Confidentiality.....	242
Authenticated scan.....	250	Containers.....	111
Authentication.....	201, 241	Cookies.....	289
Authorization.....	242	CPE.....	23
AV.....	22	CPU.....	60
AVRCP.....	171	Customer Premise Equipment.....	23
Backup Plans.....	200	Cyber attack.....	41
Backup Power.....	278	Data Backups.....	194
Backups.....	194	Data Leak.....	256
BGP.....	130	DDR.....	24
Billboards.....	283	Dedicated Graphics Processing Unit.....	24
Blu-ray disc.....	226	Dedicated video card.....	66
Bluebugging.....	243	Default Gateway.....	138, 266
BlueJacking.....	242	Defense-in-depth.....	190
BlueSmacking.....	242	Denial of Service.....	52, 242, 256
Bluesnarfing.....	243	DGPU.....	24, 66
Bluetooth.....	22, 79, 169, 241	DHCP.....	24, 137, 144, 269
Bluetooth profiles.....	171	DHCP.....	151

Differential backup.....	194	Graceful Shutdowns.....	278
Digital Video Disc.....	25, 226	Graphics Card.....	66
Digital Visual Interface.....	74	Graphics Processing Unit.....	26
DisplayPort.....	24, 69, 73	Hands-free.....	171
DisplayPort Ethernet Channel.....	24	Hard Disk Drive.....	63
Distributed Denial of Service.....	52	Hardware.....	45, 58
DNS.....	24, 137, 151, 275	HDD.....	63
Domain Name System.....	151	HDMI.....	26, 69
DPEC.....	24	HDMI Ethernet Channel.....	26, 73
Driver.....	25	HDMI.....	73
Dual Data Rate.....	24	Headset.....	171
DVD.....	25, 226	HEC.....	26, 73
DVI.....	74	HFP.....	171
Dynamic Host Control Protocol....	24, 137	High Definition Multimedia Interface	26
Dynamic routing.....	130	Home and Small Business Network Architecture.....	260
Electrical surge.....	277	Home Automation.....	178
Email.....	42	Home Automation Security.....	245
Enclaves.....	260	Honey Pot.....	251
Encrypted communication.....	183	Host.....	229
Endian.....	265	Host isolation.....	240
Equipment Protection.....	277	HSP.....	171
Ericsson.....	170	IBM.....	170
ESATA.....	72	IDE.....	65
Ethernet.....	25	IDS.....	247
Ethernet Switch.....	128	IDS/IPS.....	27
Ettercap.....	54	IEEE 1394.....	68
Exploit.....	215	IEEE 802.11.....	155
F-Droid.....	252	IEEE 802.15.1-2002.....	170
Faraday cage.....	283, 301	IEEE 802.15.1-2005.....	170
Fault tolerance.....	111	IEEE1394.....	84
Firewall.....	25, 265	IGPU.....	27, 66
Firewall rules.....	266	Image Backups.....	199
Firewalls.....	130	Incremental backup.....	194
Firewire.....	68, 84	Industrial, Scientific and Medical...28	
Flash memory.....	226	Industry Standard Architecture.27, 65	
Floppy diskettes.....	226	Installed Software.....	43
FM.....	26, 156	Integrated Drive Electronics.....	65
FOSS.....	26, 217	Integrated graphics card.....	66
Free and open source software. .	26, 217	Integrated Graphics Processing unit27	
Frequency modulation.....	26, 156	Integrated video.....	66
Full backup.....	194	Intel.....	170
Gaming servers.....	270	Internet.....	286
GDPR.....	296	Internet Browsing.....	42
General Data Protection Regulation	295	Internet of Things.....	27
GNU Linux.....	26	Internet Protocol Address.....	27
Google Play Store.....	253	Internet Service Provider.....27, 122	
Google Services.....	252	Internet-of-Things Devices.....	48
GPU.....	26	Intrusion Detection and Prevention Systems.....	247

Intrusion Detection System.....	27	Mint.....	91
Intrusion Prevention System.....	27	Mobile Code.....	218
IOS.....	27, 231	Mobile Device.....	30
IoT.....	27, 245	Mobile Devices.....	48, 102, 252, 301
IoT Devices.....	104	Modem.....	30
IP Address.....	27, 130	Monitor.....	88
IP Addressing.....	130	Motherboard.....	59
iPadOS.....	231	MSATA.....	71
Ipconfig.....	159	Multi-core processing.....	60
IPFire.....	265	Multi-factor authentication.....	14, 29
IPS.....	247	Nameservers.....	275
IPv4.....	122, 130	NAND.....	30
IPv6.....	148	NAS.....	201
ISA.....	27, 65	NAT.....	30, 147
ISM.....	23, 28, 169	Near Field Communication.....	31
ISO/IEC 18092:2013.....	31, 177	Netstat.....	222
ISP.....	27, 122, 144	Network address translation.....	147
Java.....	110	Network Attached Storage.....	201
Jazz drives.....	226	Network Firewall.....	232
John the Ripper.....	54	Network Security.....	232
Kali Linux.....	54	Next hop router.....	138
KB/MB/GB/TB.....	28	NextCloud.....	31
LAN.....	28	NFC.....	31, 79, 245
Lightning.....	85	NIKTO.....	55
Linux.....	58, 91, 99, 232	Nmap.....	55, 222
Local Area Network.....	28	Nokia.....	170
Local group policy.....	228	Non-ionizing electromagnetic radiation.....	166
Logical Port.....	28	Non-volatile Memory Express.....	69
Logical ports.....	218	NVMe.....	31, 69
Lsof.....	223	OBEX.....	243
M.2.....	69	Object exchange.....	243
MAC.....	129	OEM.....	31, 45
MAC Address.....	28	Open Systems Interconnect.....	121
MAC address filtering.....	241	Operating System.....	31
MacOS.....	28, 101, 231	Operating Systems.....	89
Maltego.....	54	OPNSense.....	265
Malware.....	28, 46, 255	Optical discs.....	226
Masquerading (see NAT).....	29	Opting Out.....	300
Media Access Control.....	28, 129	Original Equipment Manufacturer.....	31
Media servers.....	270	OS.....	31
Mesh network.....	165	OSI.....	130
Message Integrity.....	242	OSI Model.....	31, 124
Metasploit.....	54	OWASP ZED.....	55
MFA.....	14, 29	Package managers.....	216
MFA, and Passkeys.....	201	Pairing mode.....	172
Micro-HDMI.....	73	Pairing/Bonding.....	242
Microsoft Windows.....	29, 98	Parallel Advanced Technology Attachment.....	65
Mini-DisplayPort.....	73	Passkeys.....	213
Mini-HDMI.....	69, 73	Passwords.....	201
Mini-PCIe.....	70		
Mini-SATA.....	71		

PATA.....	65	Ransomware.....	33, 42, 46, 213, 255
Patching.....	44	RCA.....	75
Patching plan.....	217	Redundancy.....	111
Payload.....	250	Redundant Array of Inexpensive Disks	33, 201
PBAB.....	171	Registry key.....	228
PC.....	32, 57, 91	Remote Access VPN.....	183
PCI.....	32	Remote Hosting.....	274
PCIe.....	32, 67, 70	Repositories.....	108
Penetration Testing.....	250	Reverse proxy.....	38, 151
People Make Games.....	292	RF.....	34, 155
Peripheral Component Interface.....	32	RFID.....	34, 176, 245
Peripheral Component Interface Express.....	32	RIP.....	130
Persistent Remote Access.....	256	RJ-11 Connector.....	80
Personal cloud servers.....	270	RJ-45 Connector.....	79
Personal Information Protection and Electronic Documents Act.....	295	Roblox.....	292
Personal Privacy.....	284	Robux.....	292
Personal Video Recorder.....	33	ROM.....	104
PfSense.....	265	Root.....	104
Phishing.....	32, 42, 50	Router.....	34
Phone Book Access.....	171	Routers.....	125, 130
Pi-hole.....	32	Routing Information Protocol.....	130
Pinhole,.....	267	Rubber Ducky.....	228
PIPEDA.....	296	S-Video.....	75
Plain-old-telephone-system.....	33	Sandbox.....	215, 229
Play Store.....	253	Sandboxie-Plus.....	229
Pod slurping.....	227	Sandboxing.....	229
Port Forwarding.....	32	SAS.....	65
Portable media.....	106, 225	SATA.....	65, 70
Ports.....	218	SCSI.....	65
PoS.....	33	SDK.....	34
Post Quantum Cryptography.....	33	Security Information and Event Monitoring.....	35
POTS.....	33, 152	Security Information and Event Monitoring Systems.....	249
Powershell.....	46	Security researchers.....	214
PQC.....	33	Segmentation.....	232
Processor.....	60	Self-hosted Services and Applications	270
PS/2.....	87	Self-hosting.....	270
Public IP address.....	144	Serial Advanced Technology Attachment.....	65
Puppy Linux.....	91	Serial Attached SCSI.....	65
PVR.....	33	Serial Interface.....	80
Quantum computers.....	286, 304	Service Set Identifier.....	35, 160
Quantum Computing.....	304	Services.....	218
Radio communication.....	165	Session Initiation Protocol.....	35
Radio frequency.....	34	Shodan.....	55
Radio Frequency Identification. .	34, 176	Sideloading.....	34
RAID.....	33, 201	SIEM.....	35
RAM.....	33, 62	SIEMs.....	249
RAM dumping.....	227		
Random Access Memory.....	33, 62		

SIG.....	170	USB-C.....	69
Single-board computer.....	265	UTM.....	36, 248
SIP.....	35	VB.....	46
Site-to-site VPN.....	183	VGA.....	37, 75
Small Computer System Interface. .	65	Vice set identifier.....	160
Smishing.....	35, 50	Video card.....	66
Smoothwall.....	265	Video Graphics Array.....	37, 75
Sn1per.....	55	Virtual Machine.....	37
Snapchat.....	292	Virtual Machines.....	108
Snowydrive,.....	227	Virtual Memory.....	62
Social Engineering.....	51, 227	Virtual Private Network. .	38, 146, 183
Social Media.....	291	Virtual Private Networks.....	287
Socket.....	35	Virtual Private Server.....	38
Software bugs.....	43	Virus.....	37
Software development kit.....	34	Vishing.....	37, 50
Sogu Campaign.....	227	Visual Basic.....	46
Solid State Disk.....	35	VM.....	37
Solid State Drive.....	64	Voice over Internet Protocol. .	37, 123
Sophos UTM.....	265	VoIP.....	37, 123
Sound Card.....	67	VPN.....	38, 146, 183, 287
Spear-phishing.....	35, 42, 50	VPN service provider.....	183, 287
Spoof.....	241	VPS.....	38, 275
SSD.....	35, 64	Vulnerabilities.....	43
SSID.....	35, 160, 240	Vulnerability.....	214
Standard Builds.....	200	Vulnerability assessment.....	249
Static Route.....	35, 130, 138	Vulnerability Scanners.....	249
Static Routing.....	141	WAF.....	38, 151
Stuxnet.....	226	WAN.....	38, 269
Subnet mask.....	131	WAP.....	38
Surge suppressing power bar.....	277	Web Application Firewall.	38, 151
Switch.....	36	Web servers.....	270
Switchblade.....	226	WEP.....	39, 160
Terminal.....	36	Wide Area Network.....	38
THC Hydra.....	55	WiFi.....	39, 79, 155, 269, 282
The Social Dilemma.....	291	WiFi Access Point.....	38
Third-party cookies.....	290	WiFi mesh network.....	165
Thunderbolt.....	68, 86	WiFi Protected Access 2.....	39
TLS.....	36	WiFi Protected Access 3.....	39
Toshiba.....	170	WiFi Protected Access,.....	39
Ubuntu.....	36, 91	Windows.....	58, 98, 231
Unauthenticated scan.....	250	Windows Defender.....	225
Unified Threat Management...36,	248	Windows Management	
Uninterruptible power supply. 36,	277	Instrumentation,.....	250
Universal Serial Bus.....	81	Windows PC.....	59
Unlock.....	104	Windows Remote Management. .	250
UPS.....	36, 277	Wired Equivalent Privacy.....	39
USB.....	68, 81	Wireless Personal Area Network. .	23,
USB 3.0.....	69	31, 40	
USB device overflow.....	226	Wireless Personal Area Networks. .	169
USB drives.....	226	Wireshark.....	56
USB Hacksaw.....	226	Wordpress.....	276

WPA.....	39, 160, 239, 241	Zero Trust Architecture.....	40
WPA2.....	39, 160, 241	Zero-day.....	215
WPA3.....	39	Zigbee.....	40, 178, 245
WPA3.....	241	Zip drives.....	226
WPAN.....	23, 40, 169	ZTA.....	40
Z-Wave.....	40, 178, 245		57, 64, 71, 73 ff., 80, 83, 85 ff.
Zero Trust.....	40		