Cybersecurity Myths and Misconceptions

Cybersecurity Myths and Misconceptions

Avoiding the Hazards and Pitfalls that Derail Us

Eugene H. Spafford, Leigh Metcalf, and
Josiah Dykstra

Illustrations by Pattie Spafford

Addison-Wesley

Boston • Columbus • New York • San Francisco • Amsterdam • Cape Town
Dubai • London • Madrid • Milan • Munich • Paris • Montreal • Toronto • Delhi • Mexico City
São Paulo • Sydney • Hong Kong • Seoul • Singapore • Taipei • Tokyo

The authors and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Visit us on the Web: informit.com/aw

Library of Congress Control Number: 2022951313

ISBN-13: 978-0-13-792923-8
ISBN-10: 0-13-792923-4

ScoutAutomatedPrintCode

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where:

- Everyone has an equitable and lifelong opportunity to succeed through learning.
- Our educational products and services are inclusive and represent the rich diversity of learners.
- Our educational content accurately reflects the histories and experiences of the learners we serve.
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview).

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

- Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

Contents at a Glance

Part I General Issues

Part II Human Issues

Part III Contextual Issues

Part IV Data Issues

Foreword

When Gene ("Spaf") Spafford asked me to write a foreword to this book, I asked to see some of it first. First, I read the Table of Contents and was much taken and amused by the droll way in which the authors introduced the myths that mythguide us. Then I thought they should revise the title to *Cybersecurity Mythconceptions*. The introduction is wonderfully clear and plain spoken, with a certain self-deprecating and disarming style that helps readers accept the possibility that they may have been taken in by myths and mythunderstandings (OK, that can get old, I guess, but it is so tempting!).

All kidding aside this is an important book. Cybersecurity is often all about decisions and choices we make as to which software we use, which practices we adopt, and which safety beliefs we hold dear. The clarity with which the authors explain how we might be misled (see, I stifled my addiction to puns) aids in making the book so effective. As they uncover each myth about cybersecurity, they allow us to feel superior—"How ironic that some people believe this dumb idea!" You are made to feel as if you would never fall for this, and somehow this makes each case all the more memorable.

This is a style reminiscent of C.S. Lewis's famous *The Screwtape Letters*, in which a senior satanic tempter teaches his young protégé, Wormwood, about the ways in which humans can be steered away from goodness and rationalize their behavior to justify it. Safe networking is a serious matter. The Internet and the more general "cyberspace" of all programmable objects can be hazardous not only owing to deliberate, malicious behavior, but also because of mistakes programmers, network operators, and others make.

I have long believed that accountability and agency are key to safety in online, cyber-environments. It must be possible to identify bad actors and hold them accountable. That will require both the ability to penetrate the veil of pseudonymity and international cooperation because cyberspace, like the Internet, crosses international boundaries in the normal course of operation. Agency is vital. Participants in cyberspace must have the tools necessary for protection, including legal structures and agreements to track down those engaged in harmful or criminal behavior.

Among the most powerful of defensive tools is critical thinking. This book is all about understanding how to think more critically about risks in cyberspace. This takes work. It's not a free lunch. Bad actors prey upon our frailties as humans. Sadly, that includes our natural inclination to help those in need. So many scams exploit these and other positive social feelings. This book provides us with the ability to see through these ruses. It also arms us with safer practices such as two-factor or multifactor authentication, use of cryptography, backup, and redundancy. There are many ways in which things can go wrong in the complex cyberspaces of the 21st century. A combination of personal, business, and governmental practices is needed to defend against risks. As is often the case, forewarned is forearmed.

Read the book, laugh at the right places, and put your learning to work. You won't regret it.

—Vint Cerf, Internet Pioneer, August 2022

Introduction

Imagine a hypothetical company, GoodLife Bank. GoodLife is a mid-size regional bank with 12 brick-and-mortar branches, online services, and 325 employees. Terry, the Chief Information Security Officer (CISO), wants to implement user activity monitoring for bank employees. The Chief Executive Officer (CEO), Pat, balks at the proposal. "Our people are fine. They have never stolen money from us before, and we have never had this monitoring. We will be fine. That's a waste of money," Pat says.

As another hypothetical, imagine a government organization, the Department of Redundant Information Department (DRID), part of the Agency for Propagating Bureaucracy (APB). At a staff meeting, the new Chief Information Officer (CIO) asks the DRID department head, Chris, what they have as security beyond the Federal Information Security Management Act (FISMA) minimums. Chris replies, "We do not need anything else—we do not have anything anyone would want to steal. Plus, no one would want to steal whatever we have." (You can see why he is a valued employee at DRID.)

Both CISOs, Chris and Terry, have fallen for myths about cybersecurity. Throughout this book, we'll return to these fictitious (but representative) organizations and personnel. They represent common views and approaches that we hope to illustrate.

There is a lot to know to be successful in the profession and application of cybersecurity. Knowledge is passed along in many forms, including formal education and experiential learning. Defending a computer from digital threats requires insights into how the hardware and software work, how defenses can block some threats and not others, and how to recognize when something is incorrect. One potentially dangerous pitfall is perpetuating traditional practices or beliefs as truth without evidence. While cybersecurity is an evolving discipline, we still hear the refrain "that's the way it's done" when we question an approach. The human brain naturally resists change, so it will take effort to overcome old myths.

Many aspects of culture are passed down as proverbs and stories. History and traditions are core to the human story; however, those who relay wisdom about how we're supposed to act do not necessarily supply practical or reliable advice. Folk wisdom and folklore are sometimes used merely to justify what we already do or believe rather than as informed guidelines for action.

Why do you wear a hat when you go outside in the cold? Did someone tell you that you lose 90% of your body heat from your head and you do not want to catch a cold? Motivating, perhaps. Correct? Hardly.[1]

[1] You lose body heat through anything uncovered. You would freeze faster, utterly naked, except for a hat, than if you were bundled up with a bare scalp. And being physically cold is not what gets you sick anyway. "Wear a coat, or you will catch a cold" is more folk wisdom that predates the medical knowledge that viruses cause colds, not cold weather. See, for instance, www.nytimes.com/2004/10/26/health/the-claim-you-lose-most-of-your-body-heat-through-your-head.html

Some myths are stickier than others. That is, some are more pervasive and persistent, thus making them difficult to change. In Chapter 8, for example, we will talk about whether “the user is the weakest link.” Lots of people hold that view, but it is misleading.

We want cybersecurity to be effective, informed, and reasonable. In our experience, we have seen people make errors and suboptimal choices because they are influenced by bias or misunderstanding. In a few cases, people know the hazards and plow on anyway. There is also an important distinction between being uninformed and being misinformed. The primary goal of this book is not to teach technology concepts for the first time, though that is a desirable side effect. Instead, we will focus on areas where people *think* they are informed.

There’s considerable confusion about good security practices, but there seems to be some agreement on bad security practices, such as reusing passwords. Those “bad” practices might not be uniformly poor but depend on other parameters and conditions. Many of the bad practices sound logical, especially to people new to the field of cybersecurity, and that means they get adopted and repeated despite not being correct. For instance, why is the user not the weakest link? We hope that this book helps you to think more clearly about cybersecurity.

Our goal is to tackle decades of accumulated folk wisdom head-on. We want our readers to make better decisions grounded in reality. No matter how cybersecurity folk wisdom started or how it’s still being spread, we assume that people have good intentions and are not deliberately trying to misinform.[2] Myths are not lies or intentional falsehoods. Myths are stories that embody a belief regarding some fact or phenomenon. Our goal is to set things straight where persistent pitfalls exist.

We also want to address some of people’s innate biases when confronting complicated or new situations. We all have some heuristics we employ to make decisions, and we have biases about the outcomes. Many of those are suitable for everyday situations; however, computing is complex, and some adversaries do not behave according to our typical mental models. Understanding where the biases might (mis)lead our decision-making is valuable.

The goal of this book is not to blame or accuse anyone of wrongdoing! We know that not everyone falls for every pitfall. You might even be shocked that there are people who believe a particular myth on our list. Some of the concepts we discuss might have even been (mostly) true once upon a time, but the field continually advances, and circumstances change. Too many people think that cybersecurity is only about technology, but it is about more than that. As an illustration, many computer science degree programs do not include required courses in psychology despite the important role that people have in cybersecurity.

You might have never been exposed to the logical fallacies and cognitive biases described in this book. When you hear myths in your everyday encounters, do not belittle anyone. Instead, consider our

[2] Except those in marketing, perhaps. Clark Stanley knew exactly the fraud of his snake oil.

suggestions to help explain another view. We present this book with humility. We have been wrong before, and we will be wrong again.[3] We all learned new things writing this book!

Let's be clear that not everything we came to understand long ago about cybersecurity was a false belief or idea. For part of the 1990s, SSL/TLS was considered unnecessary and unimportant. This was not a myth: it was the reality of the time for many enterprises. Eventually, it became desirable and indispensable.

Cybersecurity Myths of the Past

A few decades ago, a common myth was that antivirus (AV) companies created and released malware so people would need their products. You can see the popular appeal of believing that a company manufactures artificial demand and its solution, but this is no more than a conspiracy theory. (It was also part of the plot of a science fiction novel, *When HARLIE Was One*, by David Gerrold, written in 1972.)

We do not hear this myth often anymore. Why not? It seems to be one that faded away on its own. Today, most people recognize that antivirus software is necessary for good cybersecurity. There is evidence of criminals, vandals, and nation-states creating malware, but no evidence suggesting that antivirus companies are doing so. . . or ever did.

How might this myth have been dispelled earlier, even in the 1990s during its height?

- **Looking for evidence or studies to support the myth would be the first step.** Some people did investigate. No evidence was found. Those findings did not make the myth completely disappear, but they did chip away at the claim's veracity. Looking for data is a common technique we suggest for other myths in this book.
- **Another technique is to consider alternative explanations and motivations, then apply Occam's Razor: give priority to the most straightforward and least-complicated explanation.** For antivirus companies to be writing viruses, they would have to swear all their employees to secrecy because it would destroy their business if the truth leaked. Also, they would occasionally have to miss viruses (or set them loose internally) so as not to appear to have too much insider information. Moreover, they would need to employ actors to attend conferences and post online about writing "their" viruses. Is that simpler and more likely than having rogue authors unaffiliated with the companies?

This book is about myth-busting, but there will never be a world free of myths. This is because humans tend to create myths to help explain our experiences. In particular, we have evolved to process information quickly, and when we cannot immediately explain something, we formulate an answer.

[3] Well, at least two of the three of us may be.

Myths will likely become more common and more challenging to correct going forward. People have access to a growing wealth of information, including misinformation. We have seen the spread of ludicrous and sometimes destructive myths, including some about contrails, vaccines, and space beings infiltrating governments. For many people, it's increasingly challenging to determine what is authentic and credible. This is why we all need the skills to spot myths as soon as they emerge and the techniques to help correct them, whether in cybersecurity or elsewhere.

Who Is This Book For?

This book is primarily for cybersecurity professionals and amateurs, including students, designers, developers, analysts, and decision-makers. Existing infosec professionals gain by improving cybersecurity when myths are dispelled. Those new to the field will better understand folk wisdom in context and preempt mistakes. For experienced practitioners, it will shed new light on techniques and approaches they might apply and advise how they can avoid inadvertently falling into traps that undermine good cybersecurity. It also suggests how more experienced practitioners might help mentor others.

If you are not in the field of cybersecurity, this book might still be for you. Cyber defense is relevant for everyone who relies on technology. That undoubtedly includes you. In particular, decision-makers and business leaders also need an accurate understanding of cybersecurity: They often accept or manage risk, a key element of what we describe throughout the book.

We do not presume that our readers have particular titles, experiences, or deep technical knowledge in specific areas, only that they are discerning, open-minded, and are somewhat familiar with the topic area. We provide references throughout the book and a list of further reading at the end of each chapter that, we believe, might be helpful if a reader needs more information than we provide. Two characteristics of a professional are lifelong learning and the willingness to challenge current beliefs upon receipt of new information; unlike in the political arena, it is usually *positive* when someone evolves their viewpoint![4]

The three co-authors—who work in academia, industry, and government—have all studied and written about cybersecurity and computer science. Science can update, validate, and dispel cybersecurity myths by using standardized methods and producing valid evidence. Engineering can use science to create more robust, reliable artifacts. The authors have, combined, close to a century of experience in everything from cybersecurity design and research to incident response to forensics and beyond. We work in science and engineering. Throughout our careers, we have seen people in cybersecurity repeatedly make avoidable mistakes resulting from myths and misconceptions. Our intent with this book is to educate students and practitioners; we believe it is the first book to consolidate this information in one place.

[4] Cf. https://doi.org/10.1016/j.tics.2022.02.004

The Myth and Legend of Hackers

Astute readers will notice that we are deliberate when using the term *hackers* in this book about cybersecurity. Despite its origins as a label for a skilled technology enthusiast, an unfortunate negative connotation has overloaded this term. Because we support the positive meaning of hacker, we use **adversary** or **attacker** to describe those persons with malicious purposes. We might use the phrase "malicious cyber actor," a term of art that arose in U.S. government publications around 2011. We also use the term "bad guy" as a term to mean a generic malicious cyber actor; this use is not intended to imply gender, and neither is "good guy."

Hacker is not the only negative connotation in cybersecurity. As we will see in our discussions of several upcoming myths, the term *user* is used with disrespect and contempt in too many discussions. We encourage people to be sensitive to this issue, seek other terms, or be clear in their usage.

The Origin of Myths

Before we explore and dispel any myths, it will be helpful to understand their origins and why they are so persistent. One reason is that technology and threats change, but education is slow to catch up. Unless people take continuing education seriously, it's easy to fall behind when old truths become modern myths. All too often, when workloads are high and things are moving quickly, education is given a lower priority.

Myths and misconceptions exist, to varying degrees, among all groups. No person or organization is immune, even cybersecurity experts. Here are three examples:

- In a 2017 Pew Research Center 13-question survey of American adults about cybersecurity topics, most could correctly answer only two of them. Only 54% were able to identify examples of phishing attacks.[5]
- In interviews with 25 students who had taken at least one course in cybersecurity, researchers identified four common themes: over-generalizations, conflated concepts, biases, and incorrect assumptions. For example, "Many students over-generalize and form misconceptions by assuming that encryption achieves additional properties beyond confidentiality: preventing manipulation, protecting against theft, and ensuring availability." The researchers attributed these errors to inexperience in the field of cybersecurity.[6]
- A study of 20 non-experts and cybersecurity staff at a university revealed cybersecurity misconceptions among both staff and employees. For example, "Some employees believed that links were more dangerous than attachments as clicking them automatically compromised the computer, while others argued that attachments were harmless if you did not allow them to install."[7]

[5] www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/

[6] https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1030&context=jcerp

[7] www.usenix.org/system/files/conference/soups2018/soups2018-nicholson.pdf

Are Myths Different From Superstitions?

A book about myths and misconceptions might make you wonder about their relationship with superstitions.

Superstitions have permeated every facet of human existence for all of recorded history, from sports to weather to medicine. Perhaps you have a lucky pair of socks or avoid the numbers 13 or 666. Maybe you believe in jinxes or curses. These are, in formal terms, examples of magical thinking.

Digital life is not immune from magical thinking. Today we might have a ritual to close all the background apps on our phone or reboot the computer to “optimize their performance.”[a] According to Matthew Hutson, author of *The 7 Laws of Magical Thinking: How Irrational Beliefs Keep Us Happy, Healthy, and Sane*, magical thinking helps us make sense of an irrational world and gives us comfort, agency, and control. We will return to this topic of magical thinking in Chapter 3.

Myth and superstition are different. A myth is an incorrect fact or incorrect explanation of observation, while superstition is a belief based on the supernatural. It is a myth that goldfish have a 3-second memory. It is a superstition that knocking on wood wards off bad luck. To give a computing-related example, many kids in the 1980s believed that blowing on game cartridges would fix technical problems because dust might be causing issues. Removing the cartridge, blowing on it, and reinserting it often fixed the problem: a poor initial mechanical connection. The explanation that it was dust was a myth. If they believed the cartridge was infested with a poltergeist, removed it and performed an exorcism, then reinserted it, that would be superstition. Either way, the act of removal and reinsertion would fix the problem and reinforce the belief.

This book focuses on myths, not superstition. If you think sticking crystals to your laptop and deploying firewall rules based on your horoscope will keep your system safe, then this book is not for you; however, we advise you to have good backups and insurance.

Some readers might be thinking, “Wait, what about religion?” We are not going to opine on that in any way. We will observe that we have yet to see any peer-reviewed, replicable studies confirming that prayers affect downtime from security incidents. Furthermore, if you believe your computer center is being attacked by demons, this book will not help you—burn some sage and hire an exorcist but do not be surprised if neither helps!

[a] For more peculiar technology behaviors, see Nova, Nicholas, Miyake, Katherine, Chiu, Walton, and Kwon, Nancy, *Curious Rituals: Gestural Interaction in the Digital Everyday* (2012); https://curiousrituals.files.wordpress.com/2012/09/curiousritualsbook.pdf

Overarching Themes

We have written this book based on our experience, studies, and conversations with peers. A few fundamental ideas underlie all of what we have written, and we would like you to consider them as organizing principles for your work in the field.

First, cybersecurity is not merely about protecting computers and networks. Cybersecurity is about protecting the technology and data that underpin society. Computing is not an independent area of academic study—it is a field of technology that enables and supports modern life. Computing is used to run banks, utility systems, commerce, schools, law enforcement agencies, medical care, entertainment, and more. Lives depend on the correct functioning of systems. Our ability to interact in civil society would disappear if computing stopped working, often in sudden and unexpected ways. Thus, when we talk about defeating attacks on computing or protecting computing, it is more than computers and networks: It is fundamentally about protecting society and civilized life.

Second, cybersecurity involves computers; however, cybersecurity is primarily about humans. People program computers. People design and build computers. People buy computers and deploy them. And yes, people abuse computers. We should not lose sight of the fact that computers are tools used by people, intended for people, and built by people. Addressing cybersecurity issues requires focusing on humans and human actions.

Third, sometimes computers malfunction. It is also the case that sometimes people make mistakes. Usually, computers malfunction because of errors or oversights by the humans who designed or run them; computer hardware has become increasingly reliable. We should not attempt to excuse the bad behavior of a computer system by blaming the computer, as in "The computer decided" or "The computer made a mistake." The issues are usually the fault of whoever wrote the software, entered the data, or operated the system. The same is true of systems using Artificial Intelligence (AI) and Machine Learning (ML)—the problem is how those systems were trained and who decided to depend on their output. In every case, it is people who bear the responsibility. When a car runs a traffic light, we can almost always assign responsibility to the driver, not the vehicle or the light.

Last, as you can gather from these themes, we see cybersecurity as human-centric. Our goal with this book (and much of our professional work) is to help people understand how to use computing better and more safely. We are not interested in assigning blame, but rather in identifying ways for people to improve the technology and processes. We believe cybersecurity experts should be viewed as enablers of good practice, as allies and educators—not as authoritarian arbiters of arcane rules who mete out punishment for transgressions.

One way to look at the human-centric fundamentals is to realize there is a misconception, often amplified by anthropomorphic terms, that computers somehow "think." Computers do not think—people do. As you read through the book, we hope you identify other cases where biases and misconceptions tilt toward blaming computers instead of people.

Roadmap for This Book

This book is divided into four parts—general issues, human issues, contextual issues, and data issues—where we present more than 175 myths, biases, and misconceptions. The chapters are organized and tied together by themes that group similar myths. The chapters can be read independently or back-to-back. The section titles within the chapters identify specific myths or themes. In each section, we explain a myth or misconception, give some examples of it in practice, and discuss how to avoid it. Some chapters are technical, such as those on vulnerabilities, malware, and forensics. Others describe how cybersecurity is influenced by our thinking and decision-making, such as the chapters on logical fallacies and communication.

The material we present contains only a few technology-specific security suggestions—most of the items we present go to people's perceptions, decisions, and actions. This is because, as we noted, most cybersecurity problems are caused by people.[8] Many books discuss how to architect and operate technological solutions, although those are usually about applying patches (often imperfectly) to the underlying problems. Our book is intended to help you make progress against some of those root causes.

Cybersecurity, and computing in general, are rife with acronyms. We have endeavored to expand every acronym we use the first time; however, we also realize that an unfamiliar acronym might no longer be remembered once you have read a few chapters. Thus, we provide a table of acronyms at the end of the book, so if you encounter one that is unfamiliar, you can find an expansion of the term. If that is still a mystery, we recommend using your favorite search engine to get some additional background information—but (of course) be careful which links you follow!

Also, at the end, we have provided a set of short explanations of some of the concepts and terms used in the text. Thus, if you are unfamiliar with (for example) a firewall or the `log4j` vulnerability, you can read a short explanation in the appendix. We will warn you that these explanations are not intended to be tutorials! The appendix is solely intended to help the reader understand the material enough to grasp the basic ideas. Thus, if you run across a term you do not immediately recognize, look for it in the appendix. We do not promise it will be there, but it might be.

At the end of almost every chapter, we have provided some references for further exploration: books, academic papers, reports, and standards documents. These lists are not intended to be exhaustive, so if we have missed some that you think are particularly important, let us know at <mail:myth-misconception@googlegroups.com>, and if there are subsequent editions of this book, we will consider them for addition. Our intent is to provide you with some helpful starting points for further exploration. As we note in Chapter 1, cybersecurity is a journey, not a destination!

The chapters are interspersed with original hand-drawn illustrations that offer a lighthearted view of various myths. These images showcase the essence of some of the myths, and we believe they will entertain as much as they explain. We hope that you find them a whimsical addition to the writing.

[8] https://techxplore.com/news/2022-06-cyberattacks-human-error.html

Disclaimer

The views expressed in this book are those of the authors alone. Reference to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the United States Government, the Department of Defense, or any other organization with which the authors may be affiliated.

Register your copy of *Cybersecurity Myths and Misconceptions* on the InformIT site for convenient access to updates and/or corrections as they become available. To start the registration process, go to informit.com/register and log in or create an account. Enter the product ISBN (9780137929238) and click Submit. Look on the Registered Products tab for an Access Bonus Content link next to this product, and follow that link to access any available bonus materials. If you would like to be notified of exclusive offers on new editions and updates, please check the box to receive email from us.

Acknowledgments

Though this book is based on many decades of first-hand experience, it is more complete and richer because of others' ideas, questions, and insights. We thank our many friends and colleagues who engaged in valuable conversations and contributed ideas of myths and misconceptions over the years. Thanks, in particular, to Mikhail Atallah, Becky Bace, Jon Biggs, Matt Bishop, Bob Courtney, Earl Crane, Will Dorman, Matthew Dunlop, Simson Garfinkel, Jeffrey Havrilla, Allen Householder, David Isacoff, Brent Laminack, Amir Manteghi, Gary McGraw, William Hugh Murray, Peter Neumann, Ken Olthoff, Brad Pittack, Damien Riehl, and Deana Shick.

Special thanks to the people who reviewed draft materials and provided valuable suggestions and feedback: Matt Bishop, Tom Longstaff, Kathryn Renae Metcalf, Wendy Nather, Megan Nyre-Yu, Thomas Schreck, Winn Schwartau, and Elizabeth K. Spafford; Andrew Grosso and Mark Rasch provided insightful comments on the law chapter. Additional thanks to Vint Cerf for writing the foreword to this book.

We are grateful to the entire team at Pearson, who expertly helped in this endeavor. Our thanks to copyeditor Jill E. Hobbs who made, sure, we; didn't—use: incorrectpunctuation and globs of wrongly letter thingies, er, words. Our executive editor was James Manly and our development editor was Chris Cleveland; both patiently navigated working with the three authors and the illustrator, even when it required doing something in a new or creative way.

About the Authors

Eugene H. Spafford is one of the most senior academics in the field of cybersecurity. During his 40-plus years in computing—including 35 years as a faculty member at Purdue University, where he founded CERIAS, the Center for Education and Research in Information Assurance and Security—Spaf (as he is widely known) has worked on issues in privacy, public policy, law enforcement, intelligence, software engineering, education, social networks, operating systems, and cybersecurity. He has developed fundamental technologies in intrusion detection, incident response, firewalls, integrity management, and forensic investigation.

Dr. Spafford is a Fellow of the American Academy of Arts and Sciences (AAA&S), the Association for the Advancement of Science (AAAS), the ACM, the IEEE, and the (ISC)2; a Distinguished Fellow of the ISSA; and a member of the Cyber Security Hall of Fame—the only person to ever hold all these distinctions. In 2012, he was named as one of Purdue's inaugural Morrill Professors—the university's highest award for the combination of scholarship, teaching, and service. In 2016, he received the State of Indiana's highest civilian honor by being named a Sagamore of the Wabash.

More information may be found at https://ceri.as/spaf-bio.

Leigh Metcalf is a Senior Network Security Research Analyst at the Carnegie Mellon University Software Engineering Institute's cybersecurity (CERT) division. CERT is composed of a diverse group of researchers, software engineers, and security analysts who are developing cutting-edge information and training to improve the practice of cybersecurity. Before joining CERT, Leigh spent more than 10 years in industry working as a systems engineer, architect, and security specialist.

Dr. Metcalf has presented research at numerous conferences. She is the co-author (with William Casey) of the book *Cybersecurity and Applied Mathematics* (Syngress, 2016) as well as the co-author (with Jonathan Spring) of the book *Using Science in Cybersecurity* (World Scientific, 2021). She is also the Co-Editor-in-Chief (with Arun Lakhotia) of the ACM journal *Digital Threats: Research and Practice* (DTRAP).

Josiah Dykstra is a seasoned cybersecurity practitioner, researcher, author, and speaker. He is a senior leader in the Cybersecurity Collaboration Center at the National Security Agency (NSA) and the owner of Designer Security, LLC. Dr. Dykstra holds a Ph.D. in computer science and previously served as a cyber operator and researcher. He is interested in cybersecurity science, especially where humans intersect with technology. He has studied stress in hacking, action bias in incident response, and the economics of knowing when sharing threat intelligence is more work than it is worth.

Dr. Dykstra is a frequent author and speaker, including Black Hat and RSA Conference. He received the CyberCorps® Scholarship for Service (SFS) fellowship and is one of six people in the SFS Hall of Fame. In 2017, he received the Presidential Early Career Award for Scientists and Engineers (PECASE) from then President Barack Obama. Dr. Dykstra is a Fellow of the American Academy of

Forensic Sciences and a Distinguished Member of the Association for Computing Machinery (ACM). He is the author of numerous research papers and the book *Essential Cybersecurity Science* (O'Reilly Media, 2016).

More information may be found at https://josiahdykstra.com.

Pattie Spafford is a freelance artist, writer, and equestrienne. She holds a Ph.D. in art education. This Dr. Spafford has over 25 years of experience in K–12, college education, and community and museum art programs. Her current major research project integrates geography, art, and horses. Pattie maintains an active studio practice with bead embroidery and ink drawing as her preferred media.

Pattie's programs have received awards from national, state, and local arts agencies throughout her career, including the National Endowment for the Arts, the Louisiana Board of Regents, a NAHRO National Award of Merit, and the Louisiana Art Education Association Art Educator of the Year.

Chapter 1

From *Cybersecurity Myths and Misconceptions: Avoiding the Hazards and Pitfalls that Derail Us*, by Eugene H. Spafford, Leigh Metcalf, and Josiah Dykstra (ISBN-13: 978-0-13-792923-8) Copyright © 2023 Pearson Education, Inc. All rights reserved.

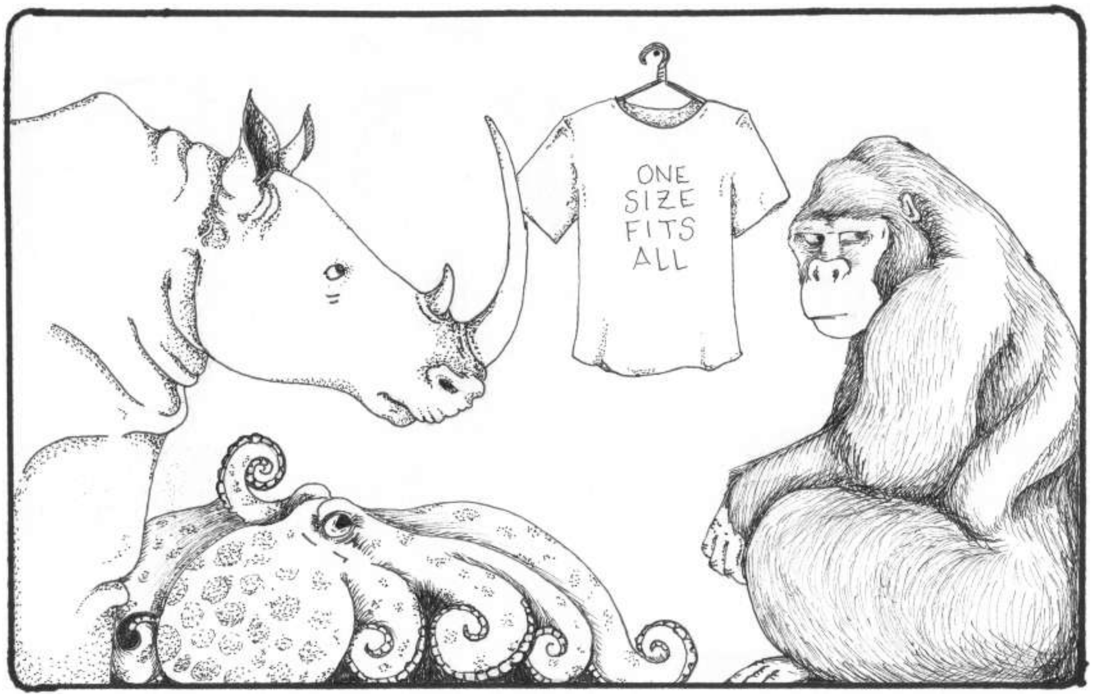


FIGURE 1.1 Security must fit a myriad of users and situations.

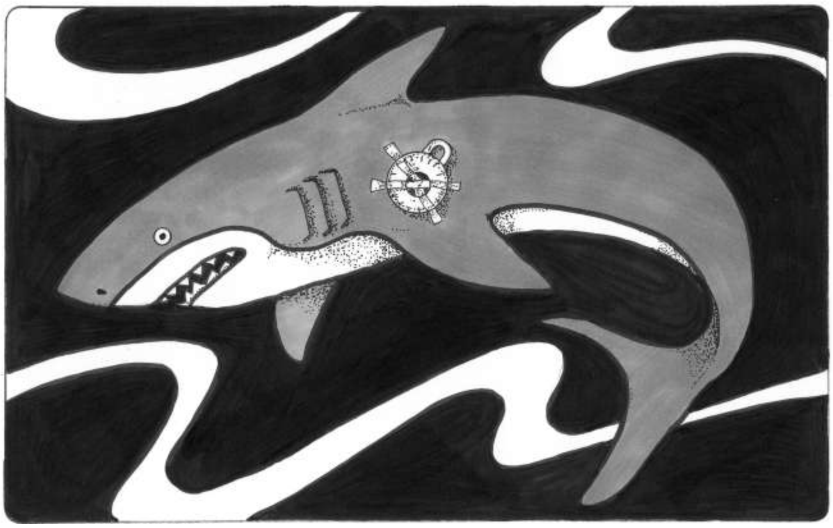


FIGURE 1.2 A lock icon does not necessarily mean there is no risk.

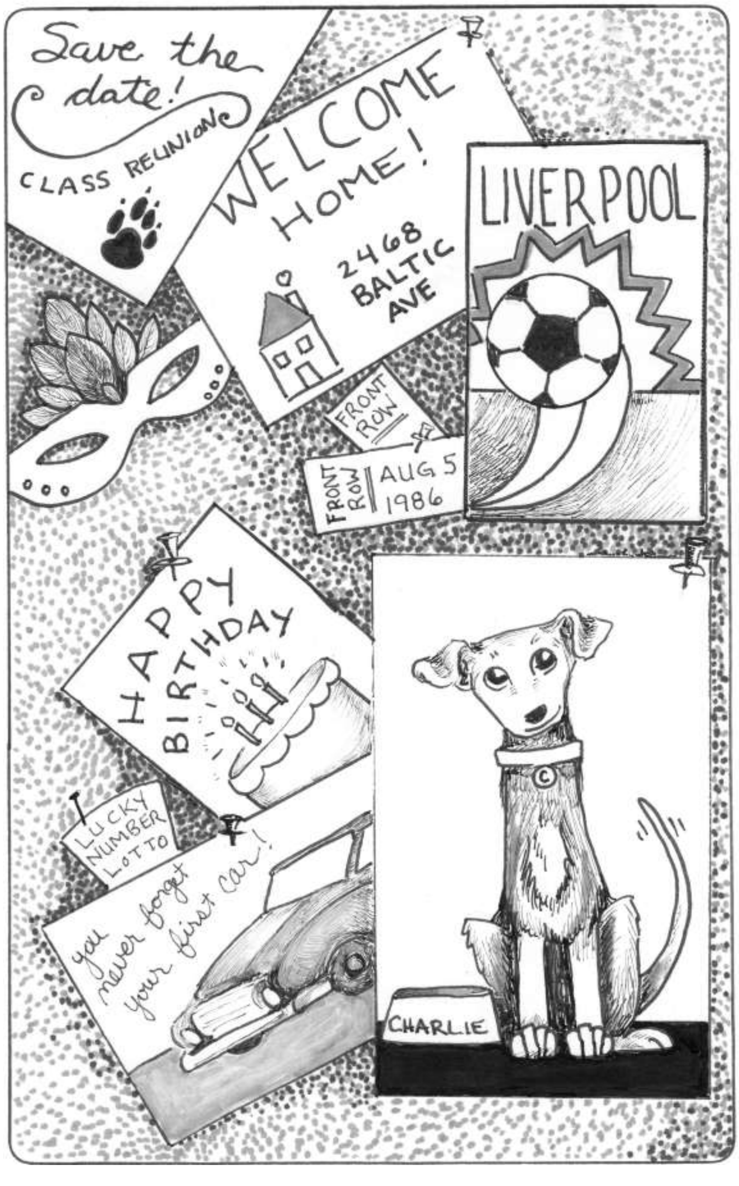


FIGURE 1.3 Strong passwords are difficult to generate and remember

Chapter 2

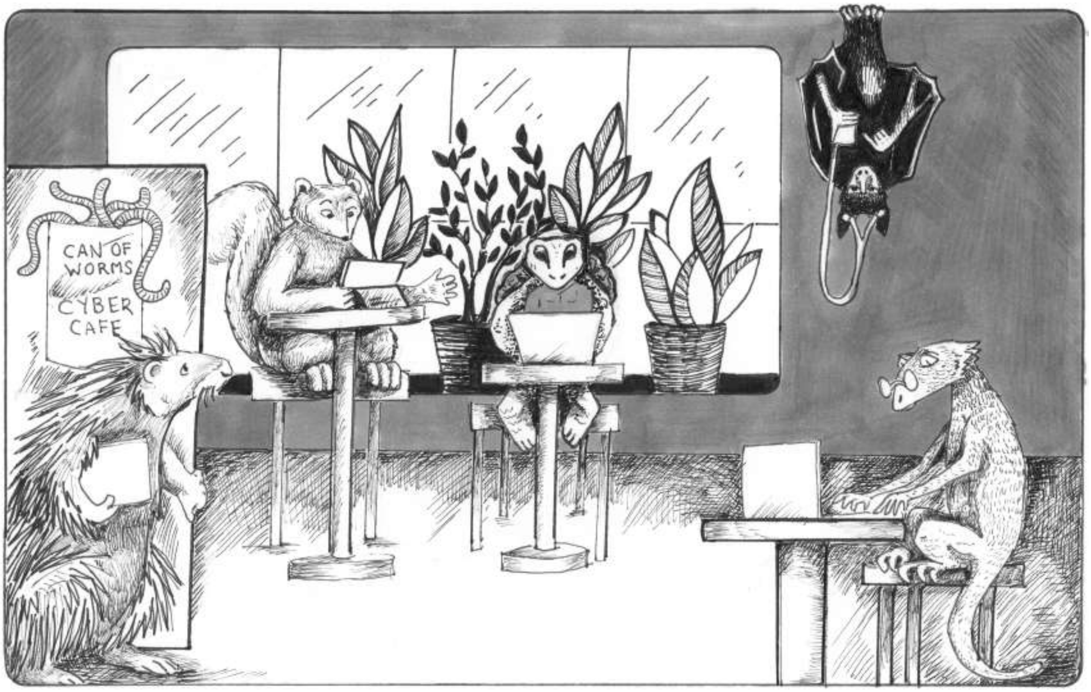


FIGURE 2.1 Modern networks are dynamic.

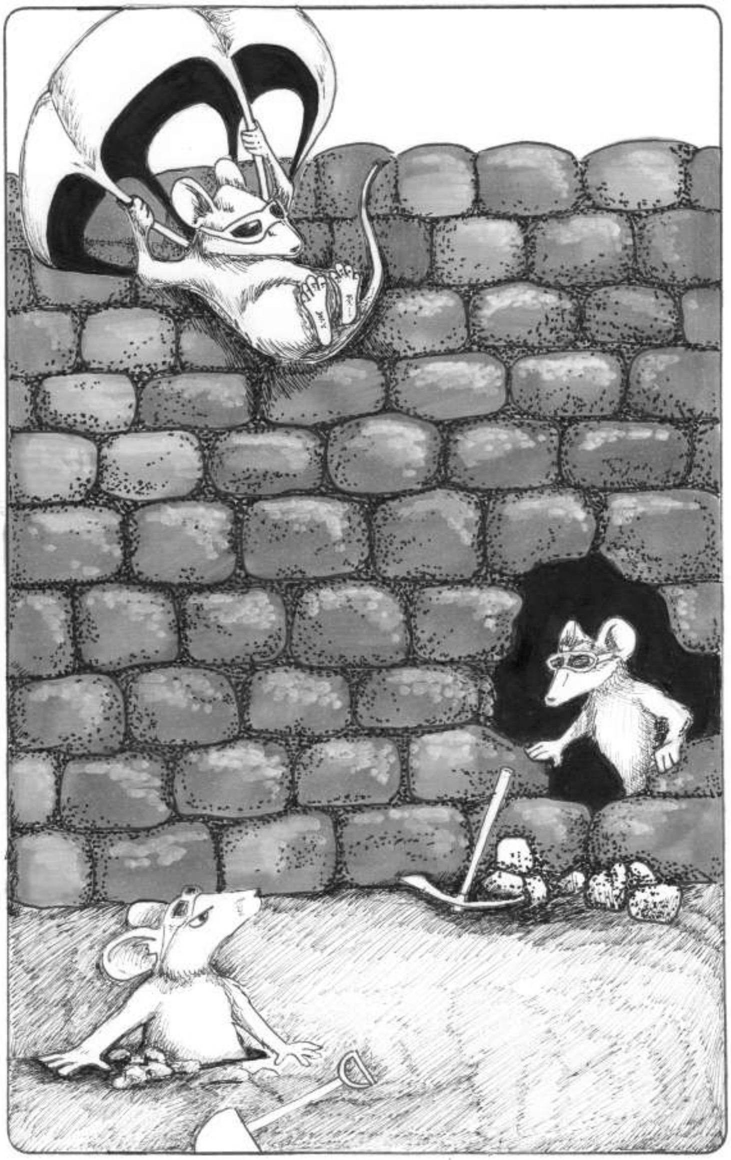


FIGURE 2.2 Breaching the firewall.

From *Cybersecurity Myths and Misconceptions: Avoiding the Hazards and Pitfalls that Derail Us*, by Eugene H. Spafford, Leigh Metcalf, and Josiah Dykstra (ISBN-13: 978-0-13-792923-8) Copyright © 2023 Pearson Education, Inc. All rights reserved.

Chapter 3

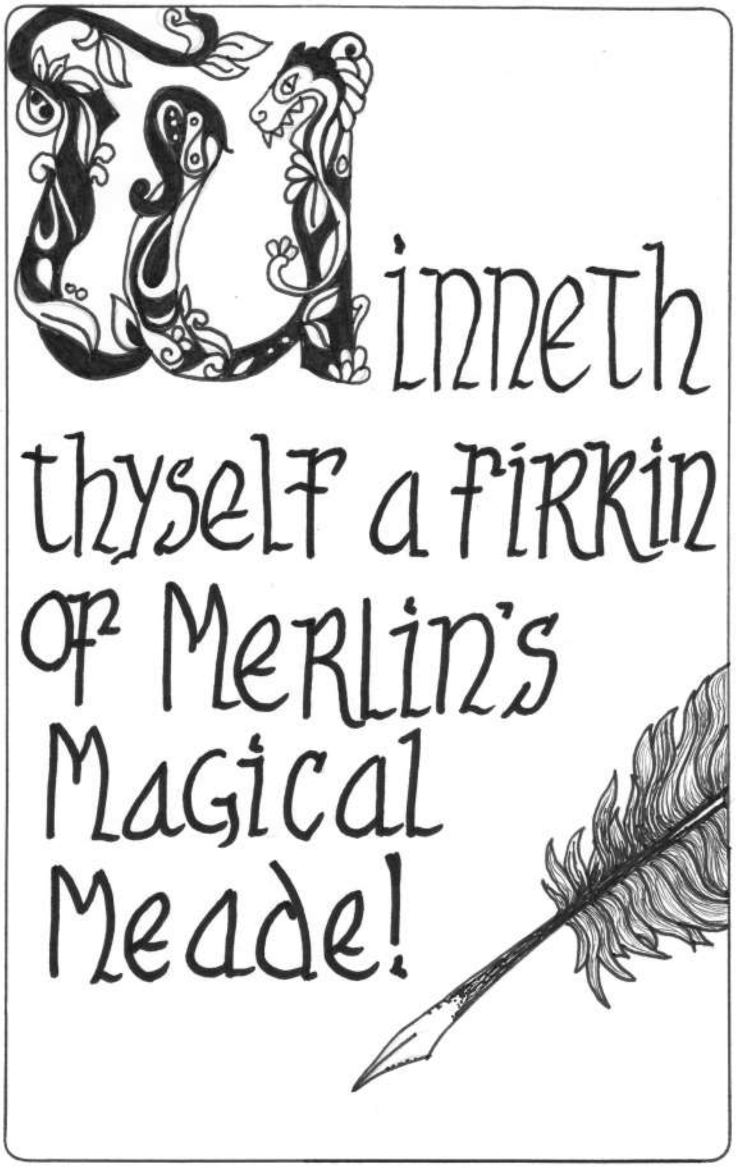


FIGURE 3.1 What phishing could have looked like during the Renaissance.

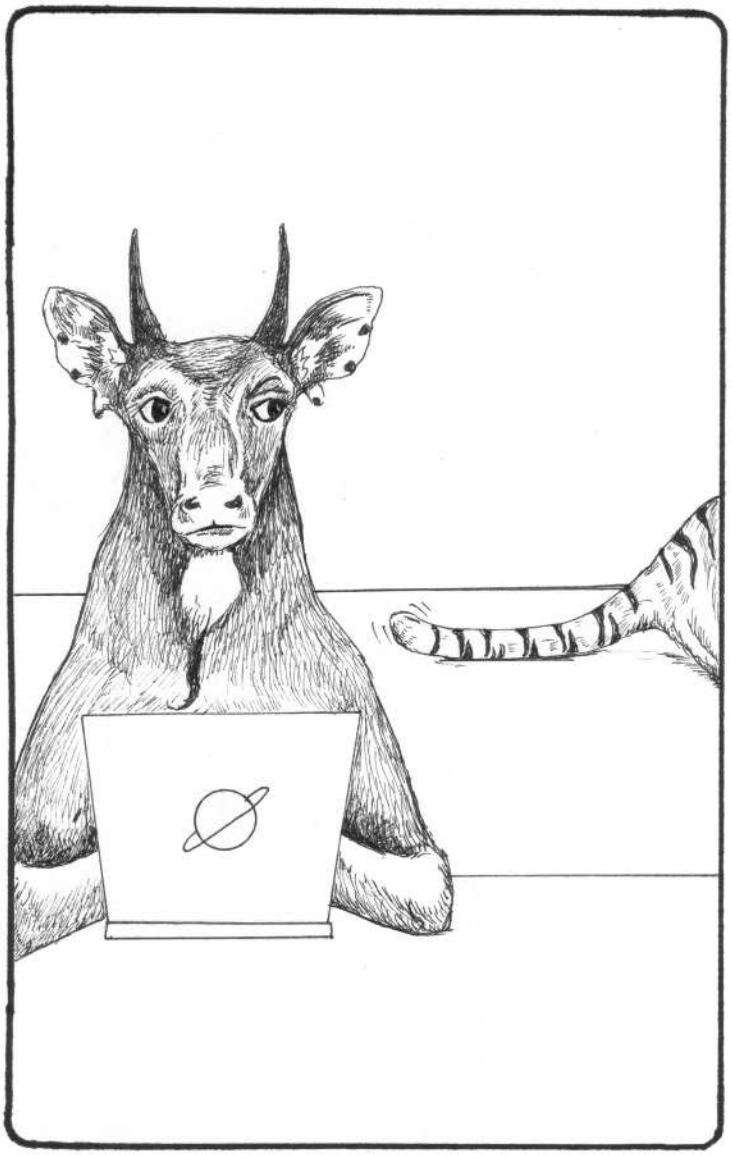


FIGURE 3.2 Blaming the user while the threat is still in the room.

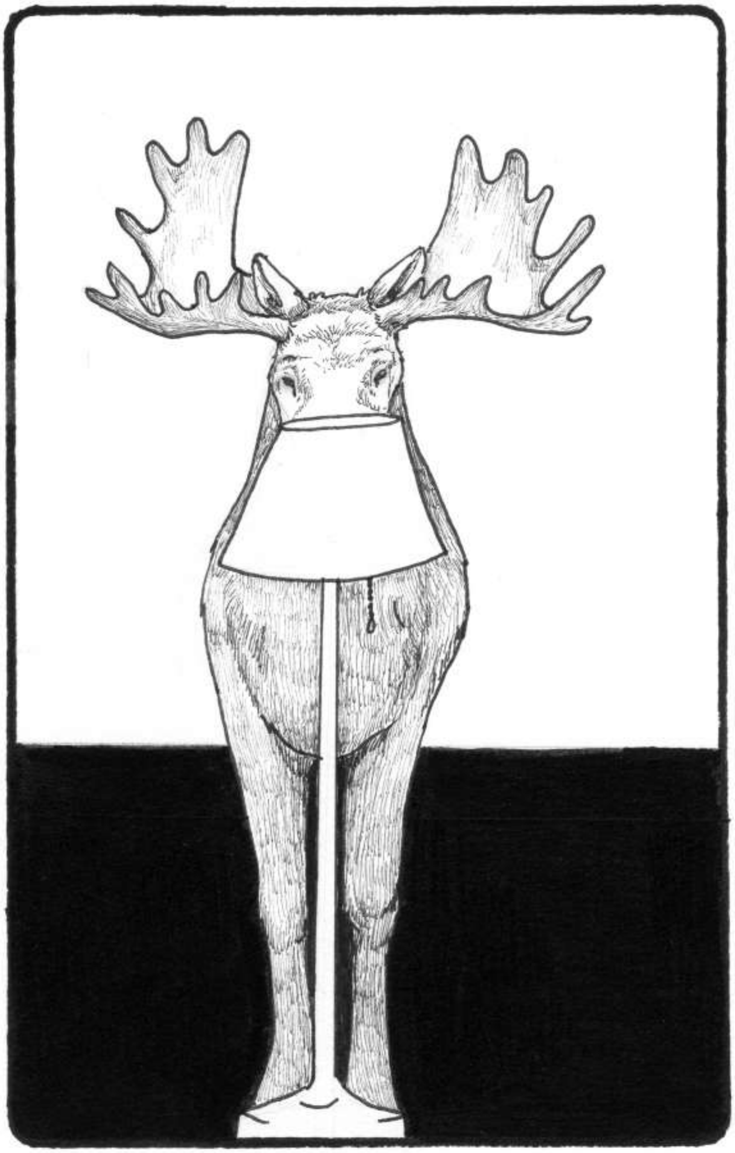


FIGURE 3.3 Security through obscurity is like believing a moose behind the floor lamp will never be found!

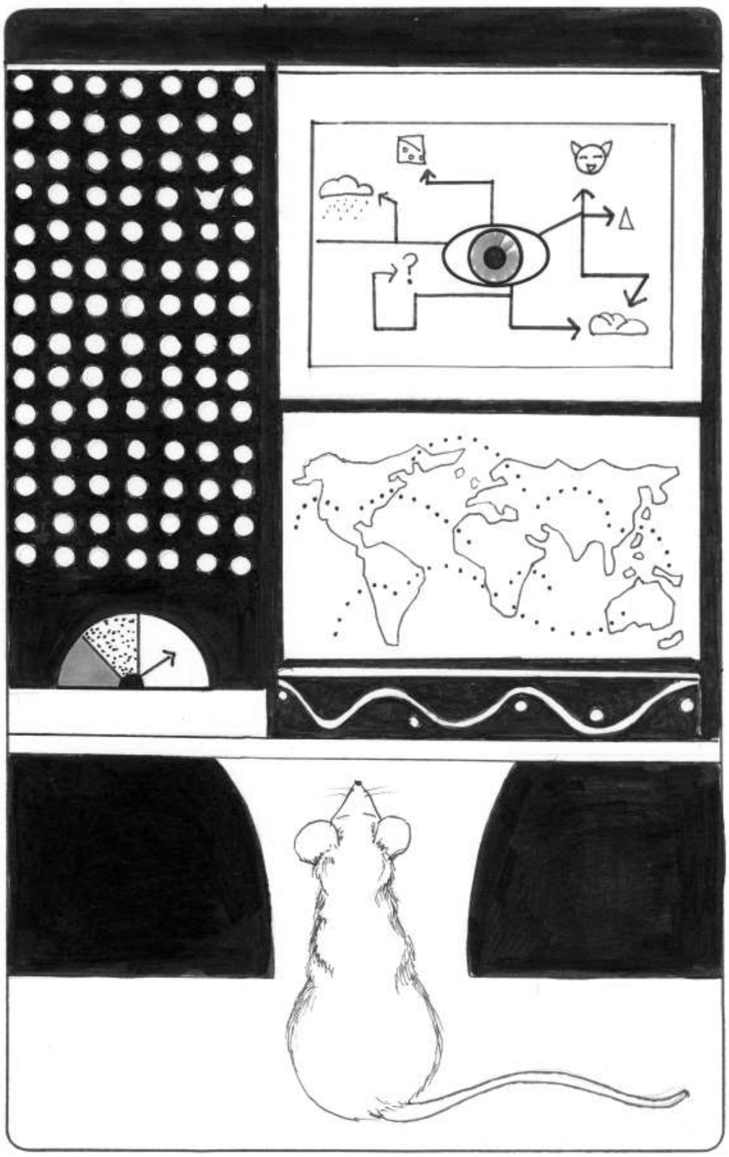


FIGURE 3.4 Blinkenlights! The illusion of visibility and control.

FIGURE 3.5 The magic of five 9's is also an illusion in cybersecurity.

Chapter 4

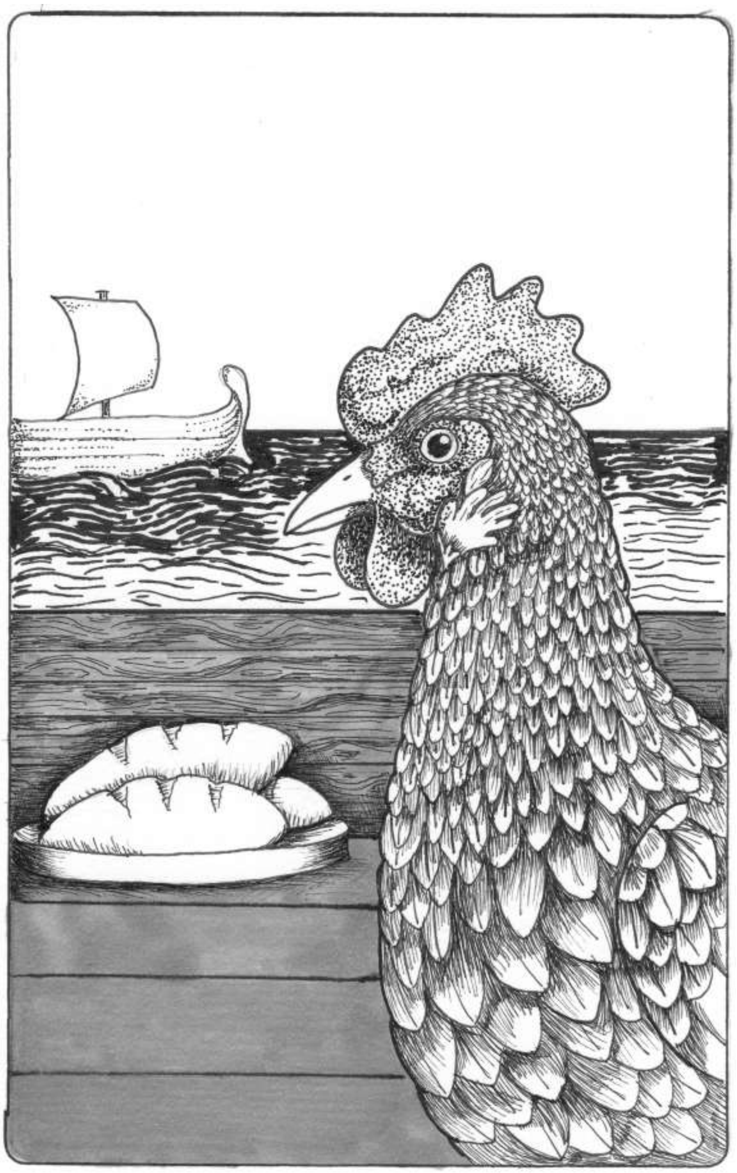


FIGURE 4.1 Killing chickens will not cause the battle to go better.

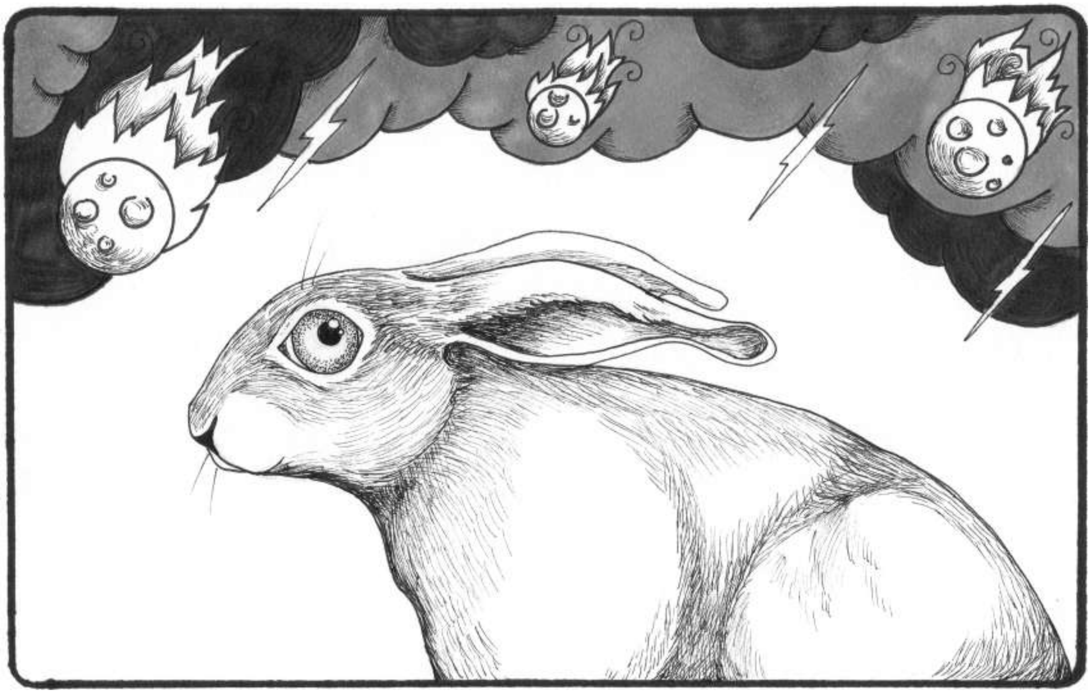


FIGURE 4.2 There are threats everywhere, and the sky is falling!

FIGURE 4.3 "Hold my beer!" said Australia to those who thought all swans were white.

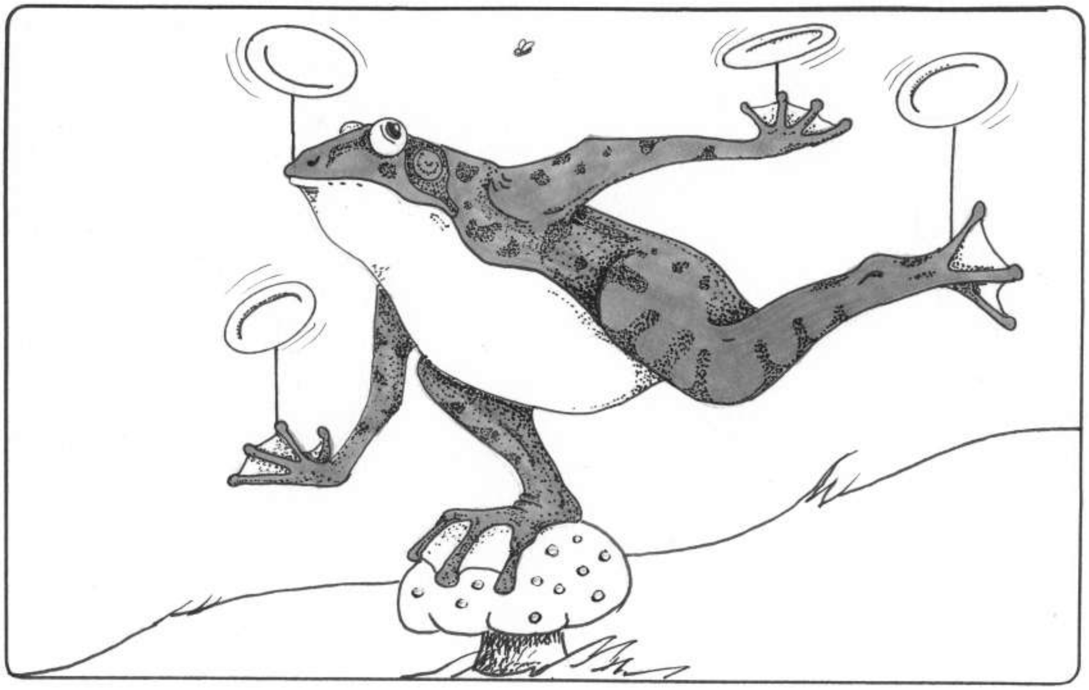


FIGURE 4.4 Trying to keep balancing the things that might be better to let go.

Date	User	Host	Login Status	Source Address
5/1/2022, 7:01:30 AM	user01	vm01	Failure	203.0.113.6
5/1/2022, 7:01:31 AM	user01	vm01	Failure	203.0.113.6
5/1/2022, 7:01:32 AM	user01	vm01	Failure	203.0.113.6
5/1/2022, 7:01:33 AM	user01	vm01	Failure	203.0.113.6
5/1/2022, 7:01:34 AM	user01	vm01	Failure	203.0.113.6
5/1/2022, 7:01:35 AM	user01	vm01	Failure	203.0.113.6
5/1/2022, 7:01:36 AM	user01	vm01	Failure	203.0.113.6
5/1/2022, 7:01:37 AM	user01	vm01	Failure	203.0.113.6
5/1/2022, 7:01:38 AM	user01	vm01	Success	203.0.113.6

TABLE 4.1 Sample login logs showing correlation.

Chapter 5

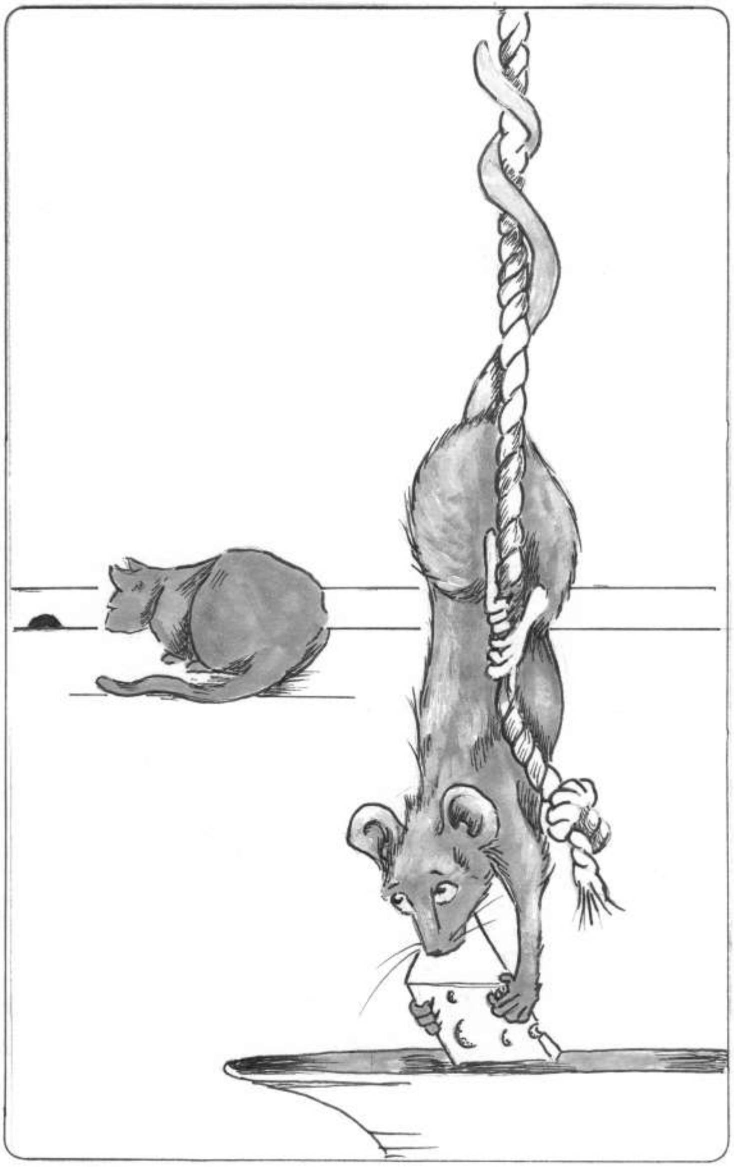
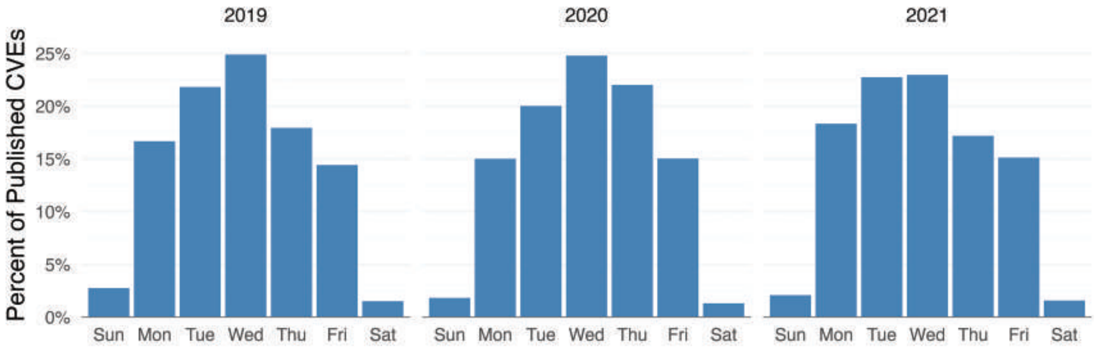


FIGURE 5.1 Thinking the mouse must be in the last place it was seen.



Source: Mitre CVE List, retrieved 2022-07-15

Chapter 6

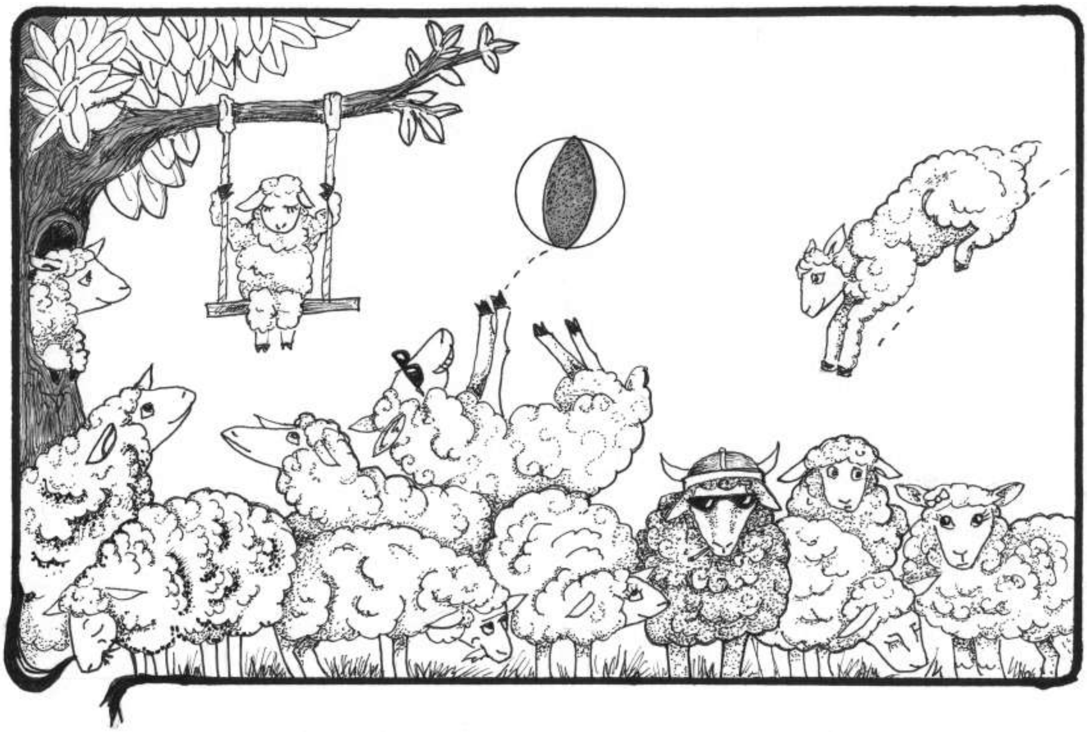


FIGURE 6.1 Tragedy of the Commons.

Chapter 7

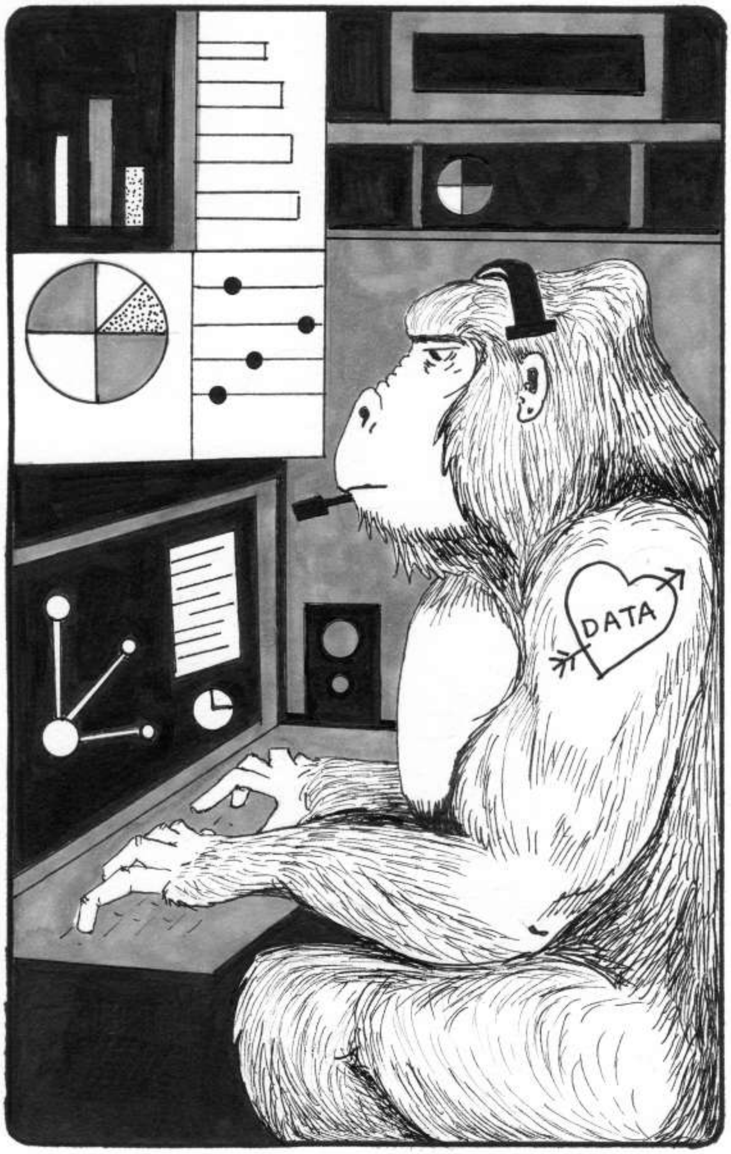


FIGURE 7.1 We can solve all problems with data. Moar data!

Chapter 8

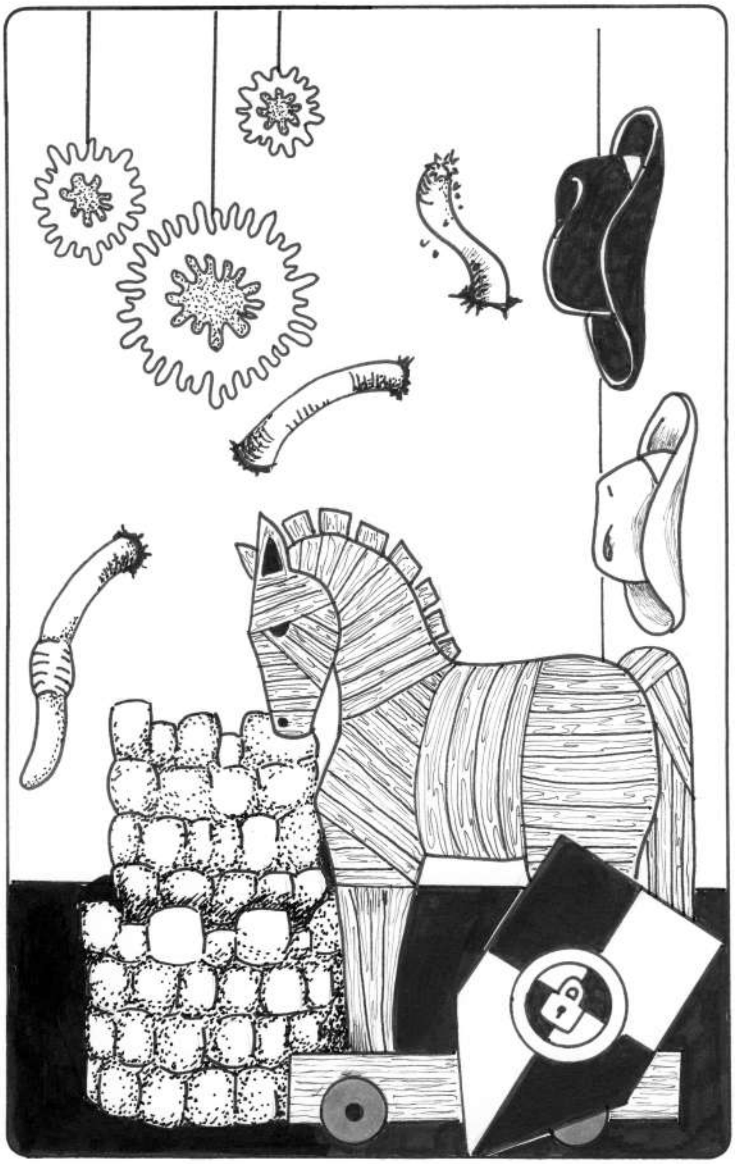


FIGURE 8.1 The attic of cyber analogies.

FIGURE 8.2 Users making bad choices.

From *Cybersecurity Myths and Misconceptions: Avoiding the Hazards and Pitfalls that Derail Us*, by Eugene H. Spafford, Leigh Metcalf, and Josiah Dykstra (ISBN-13: 978-0-13-792923-8) Copyright © 2023 Pearson Education, Inc. All rights reserved.

FIGURE 8.3 A new view of cyber hygiene.

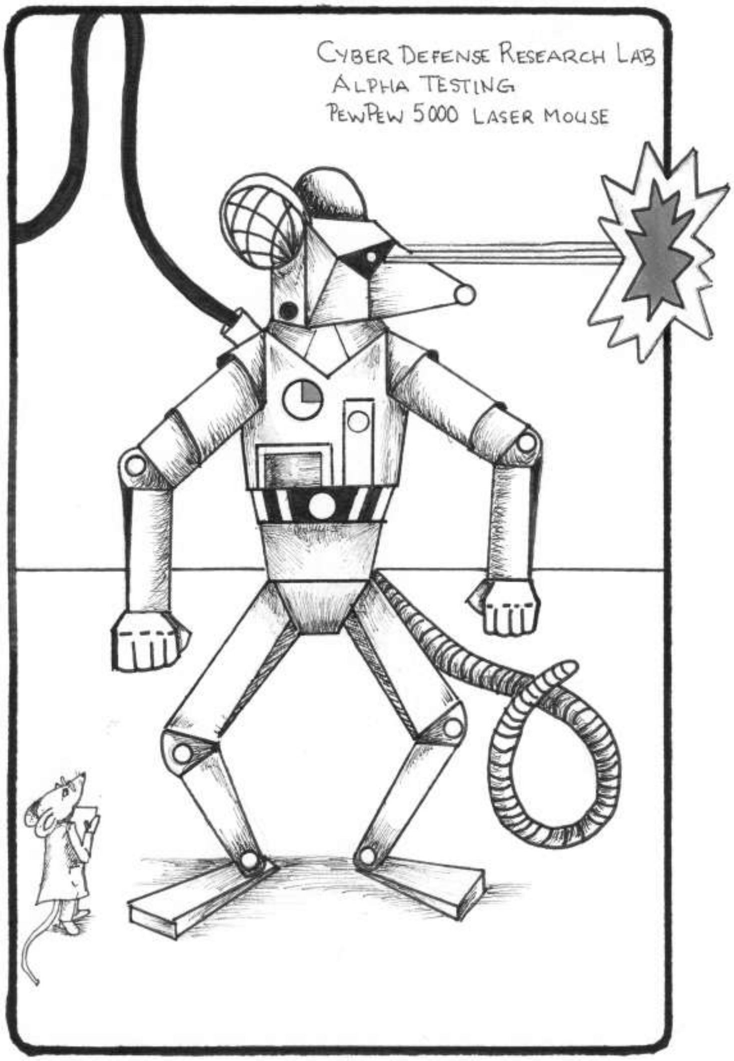


FIGURE 8.4 Pew pew!

Analogy	Positives	Negatives
Keys	Something we must have to unlock/decrypt a message.	In public-key cryptography, different keys are used to lock and unlock.
Firewall	Can stop dangerous network traffic.	*Allows* some things to pass through by design.
Blast radius	Can give a sense of the scope of the damage, including some second-order effects.	The impact of an attack does not always correspond to physical space limitations. Not a blast!
DMZ	A subnetwork more open to public access than the fortified internal area.	Both sides (network owner and Internet) do not mutually agree to no conflict.
Castle	Fortified, layered security helps protect people and their valuables	No longer a rigid boundary around networks and data.
The weakest chain link	Security (i.e., a chain) relies on many variables and can be broken if one component (i.e., a link) is compromised. Everything is dependent on the least-strong element.	End users are not the only people in cyber. Systems should compensate for humans who will make poor decisions.
Virus	Term is commonly used and conveys the concept of contamination and spread.	No built-in, self-enhancing immune system. The human immune system recognizes new threats and auto-responds.
Files	A collection of data arranged in a meaningful order.	Many identical copies. Need not be stored in one piece/place.

TABLE 8.1 Summary of pros and cons of analogies used in cybersecurity.

Chapter 9

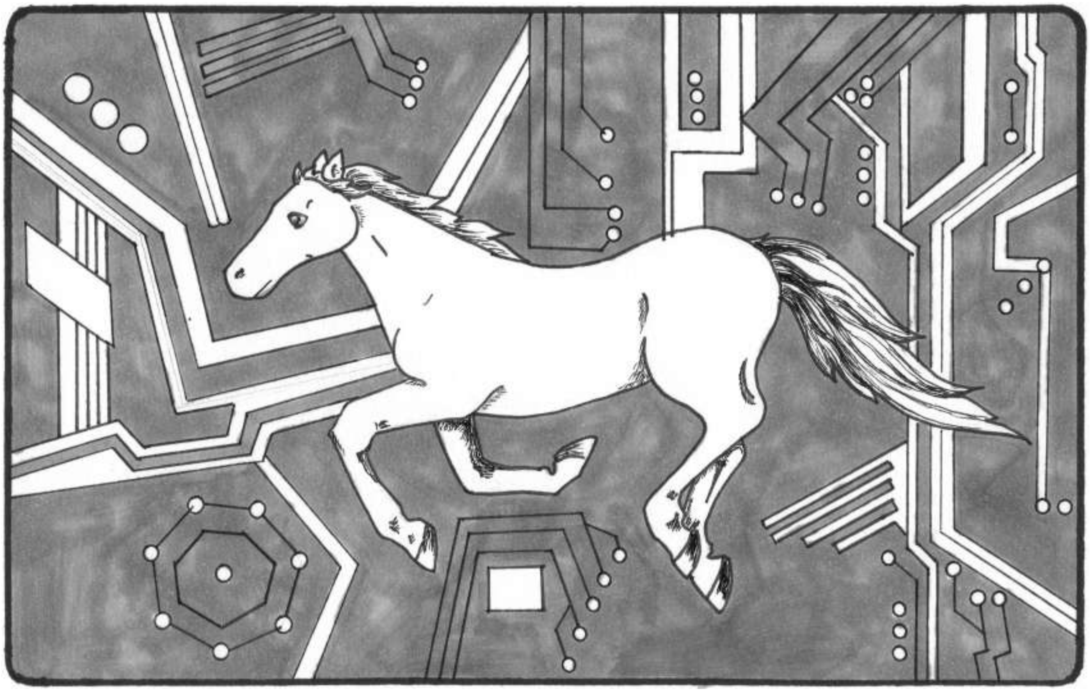


FIGURE 9.1 The Law of the Horse.

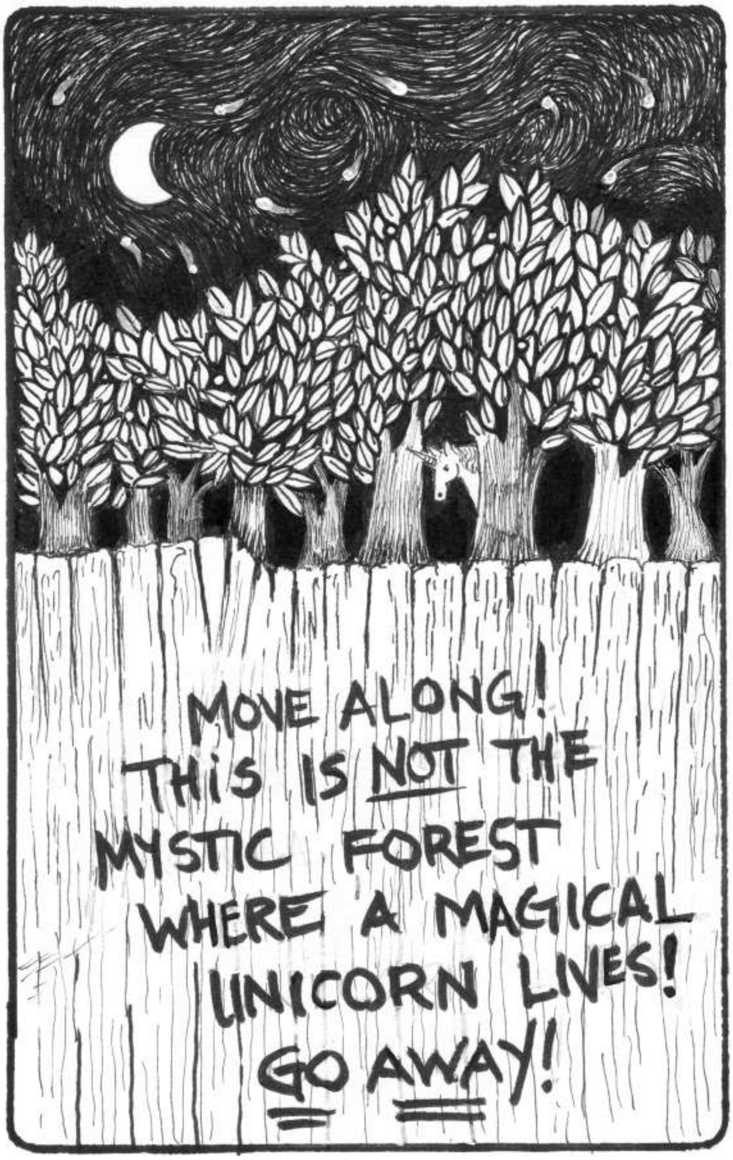


FIGURE 9.2 The Streisand Effect.

Chapter 10

FIGURE 10.1 Carefree honey badger swimming in data.

FIGURE 10.2 Tools do not dictate creation or destruction.

Chapter 11

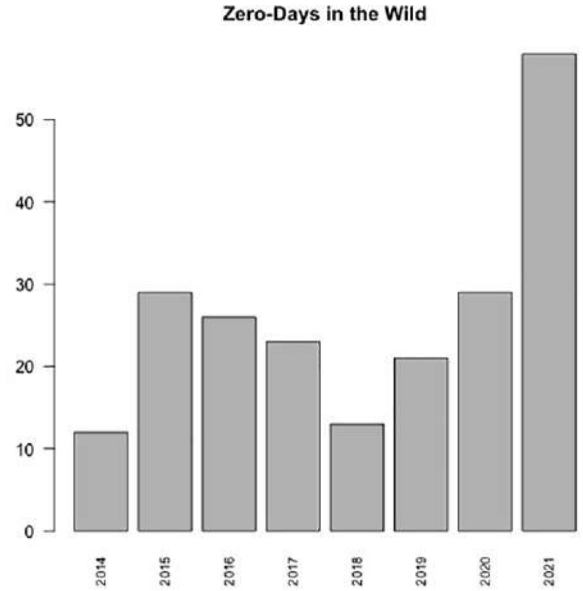


FIGURE 11.1 Google Project Zero: zero-days in the wild.

FIGURE 11.2 Worry about likely risks.

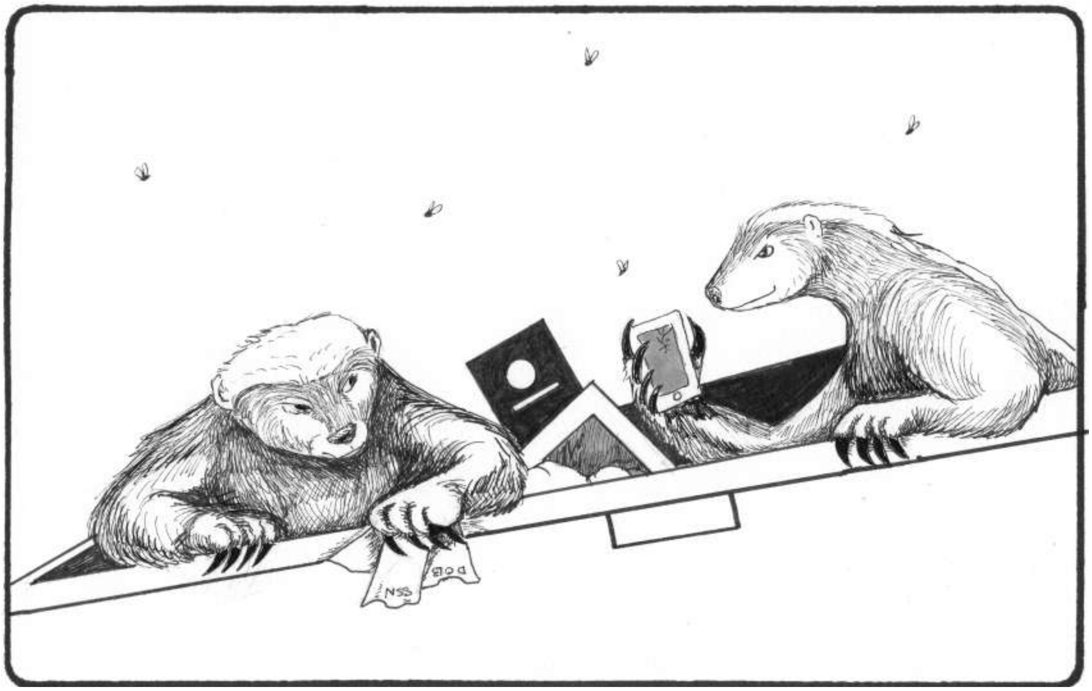


FIGURE 11.3 Dumpster diving.

FIGURE 11.4 Kill-Bit battle.

From *Cybersecurity Myths and Misconceptions: Avoiding the Hazards and Pitfalls that Derail Us*, by Eugene H. Spafford, Leigh Metcalf, and Josiah Dykstra (ISBN-13: 978-0-13-792923-8) Copyright © 2023 Pearson Education, Inc. All rights reserved.

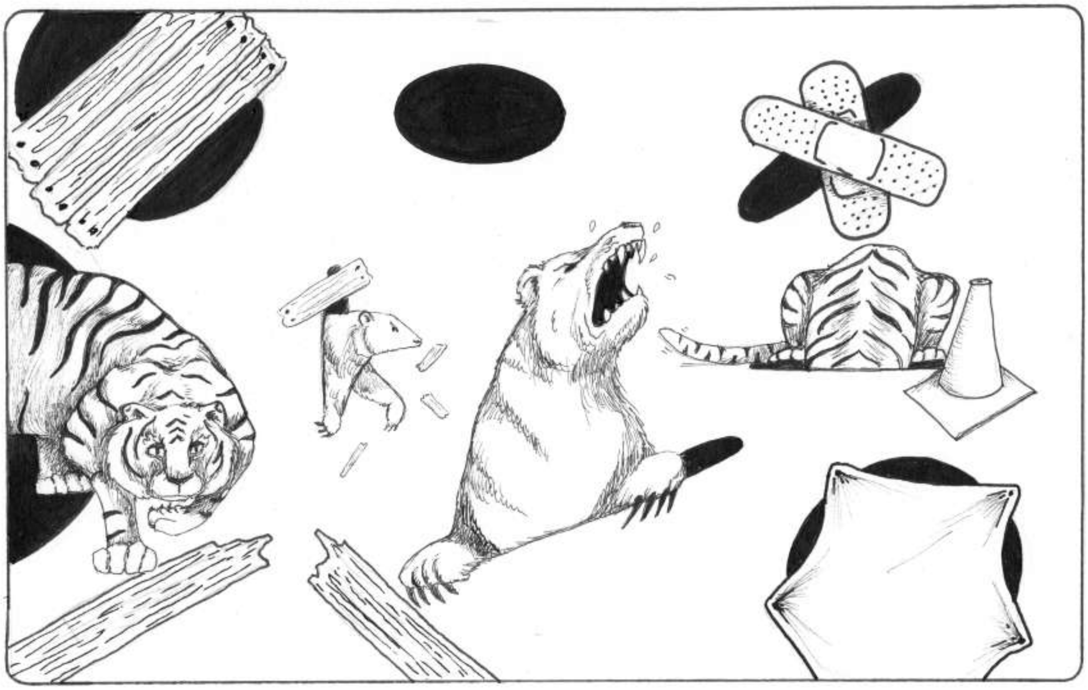


FIGURE 11.5 Tigers and grizzlies and patches, oh my.

Chapter 12

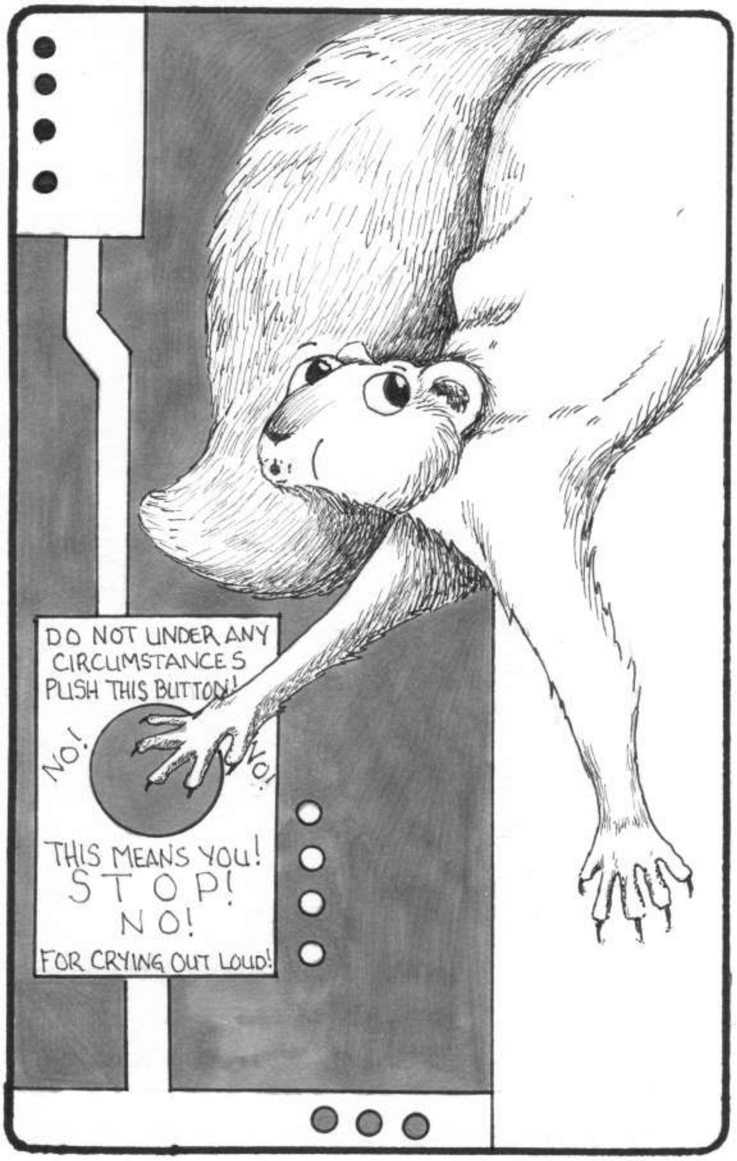


FIGURE 12.1 What does this button do?

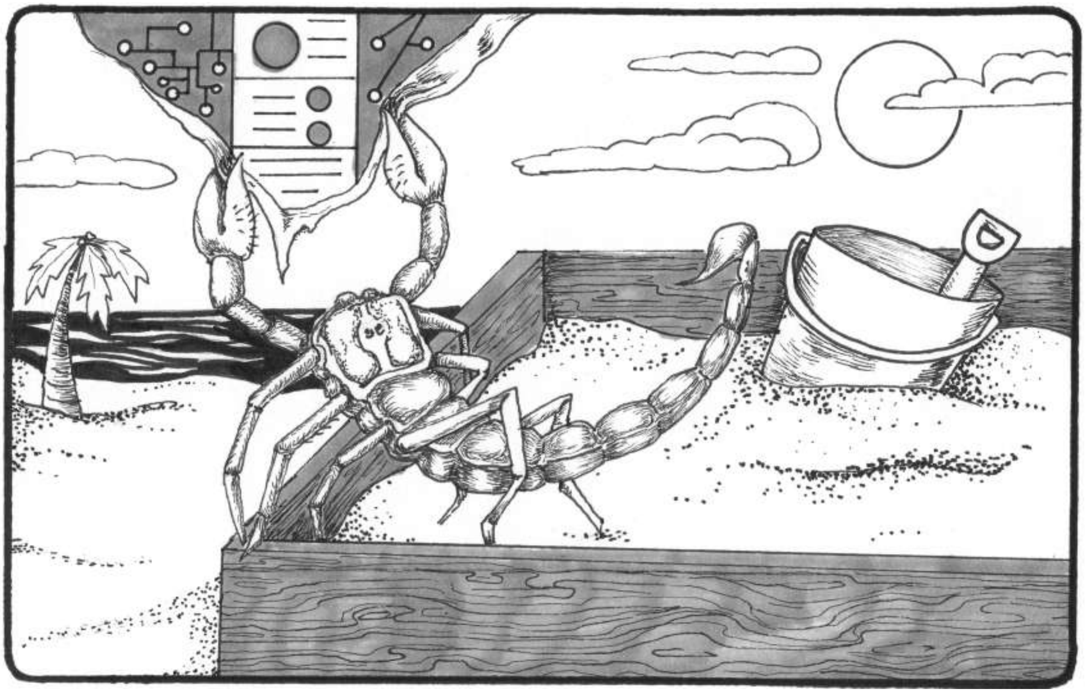


FIGURE 12.2 Escaping the sandbox.

Chapter 13

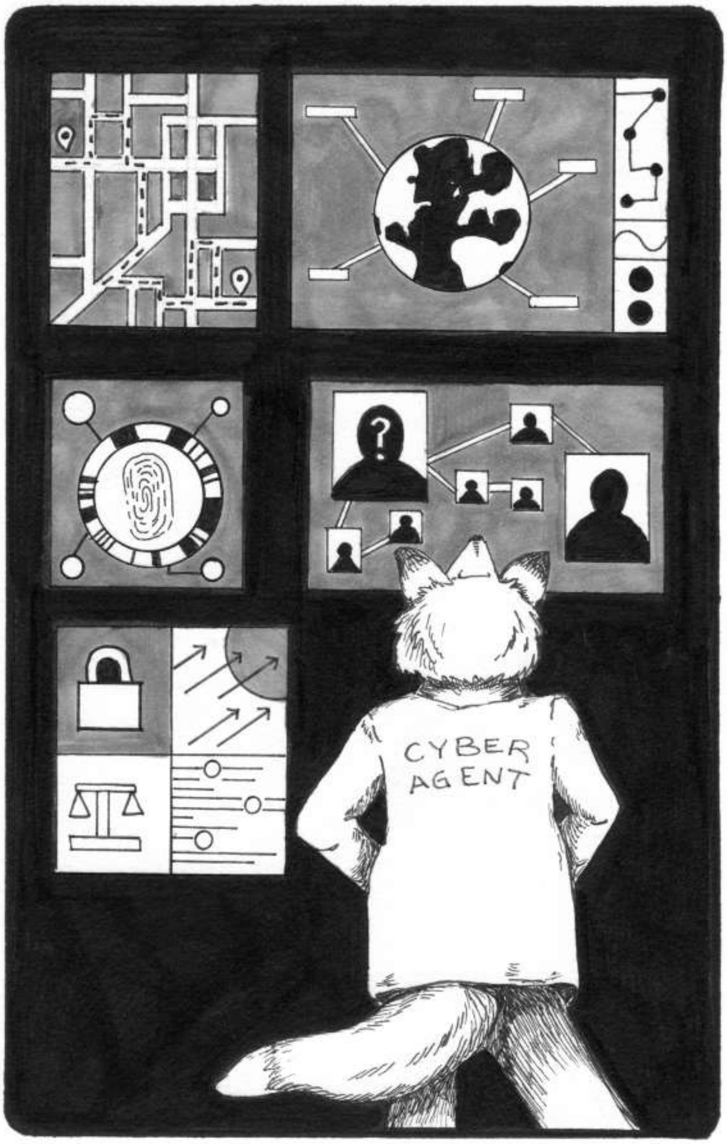
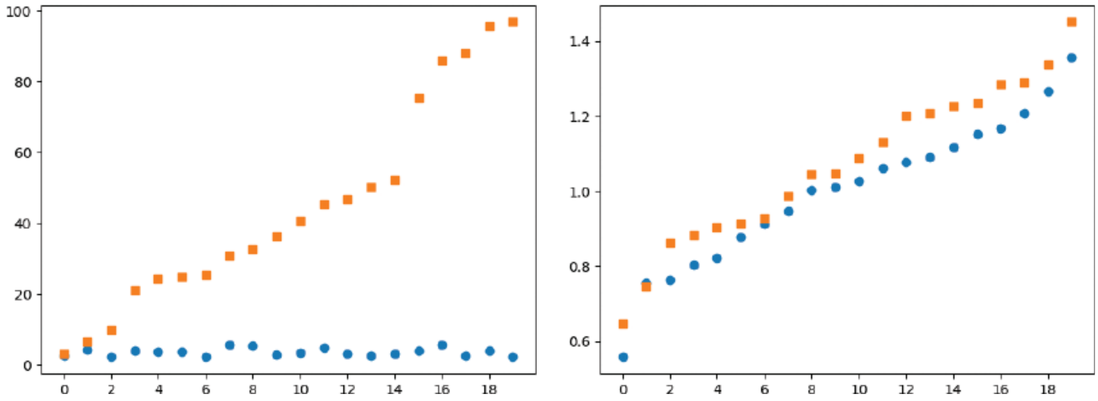


FIGURE 13.1 Many believe the unrealistic portrayal of cyber as shown on TV.

Chapter 14



(a) No correlation

(b) Correlated data

FIGURE 14.1 Correlation examples.

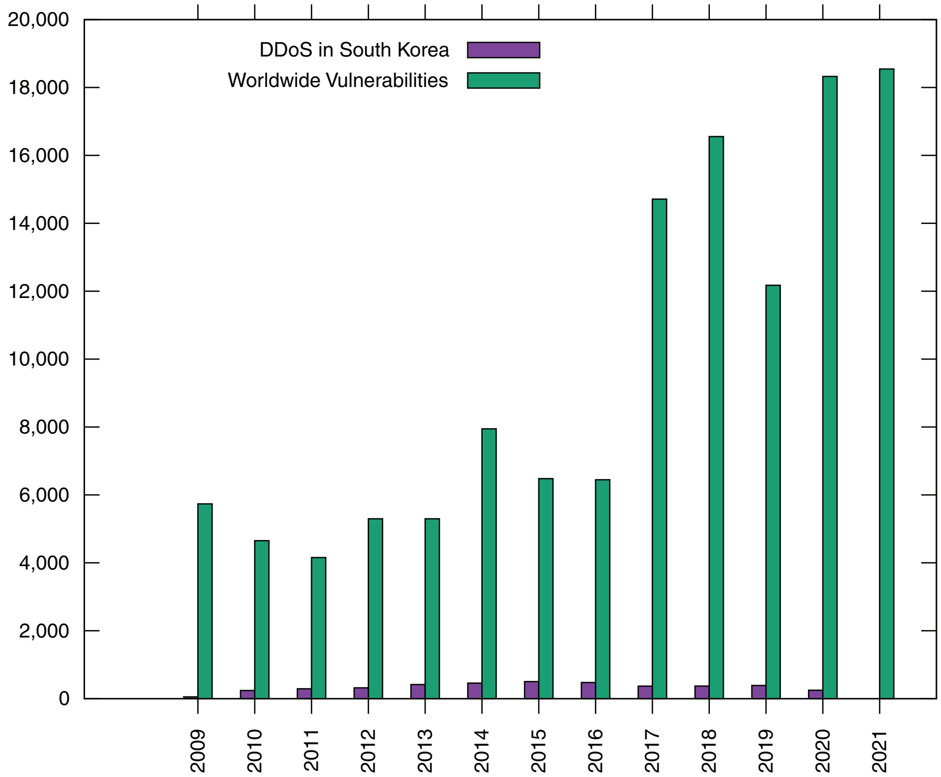


FIGURE 14.2 DDoS in South Korea compared to the number of vulnerabilities worldwide.

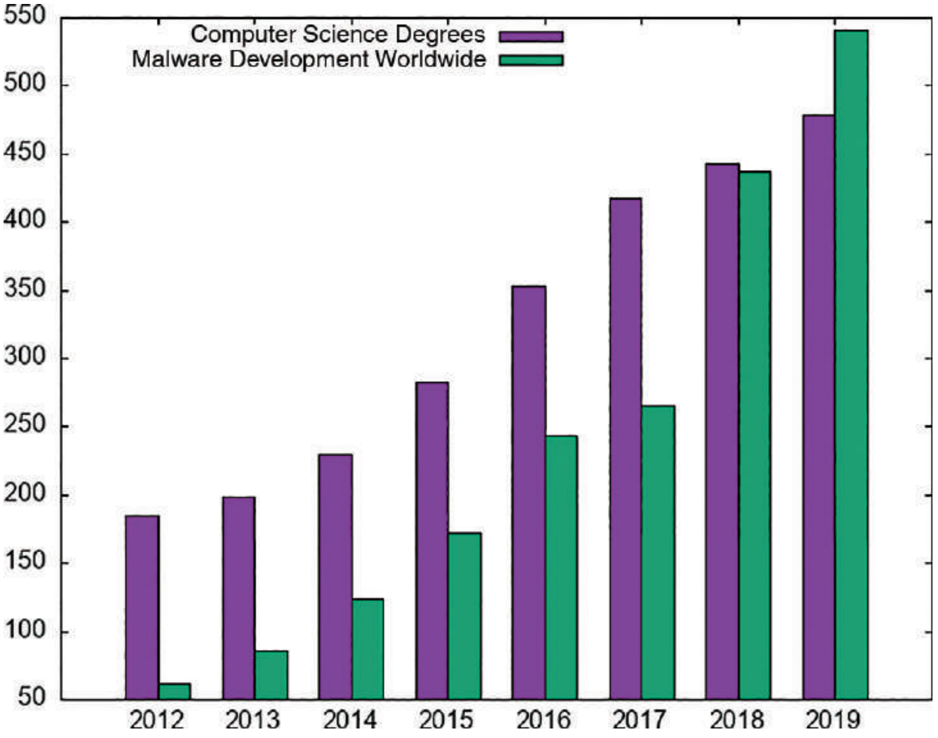
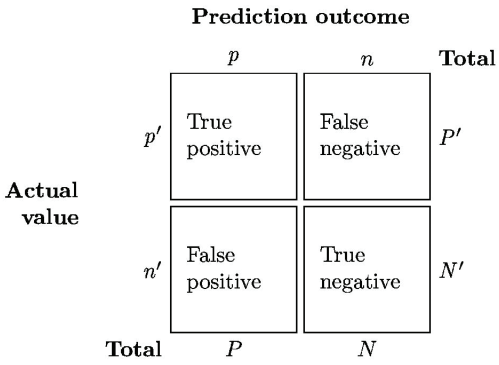
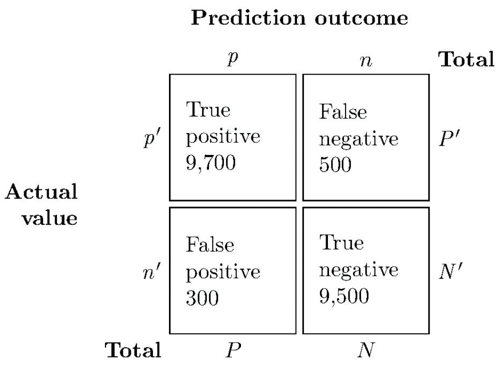


FIGURE 14.3 Malware developed worldwide and computer science degrees.



		Prediction outcome		
		p	n	Total
Actual value	p'	True positive	False negative	P'
	n'	False positive	True negative	N'
	Total	P	N	

FIGURE 14.4 A confusion matrix.



		Prediction outcome		
		p	n	Total
Actual value	p'	True positive 9,700	False negative 500	P'
	n'	False positive 300	True negative 9,500	N'
	Total	P	N	

FIGURE 14.5 A confusion matrix in use.

FIGURE 14.6 Gathering random groceries.

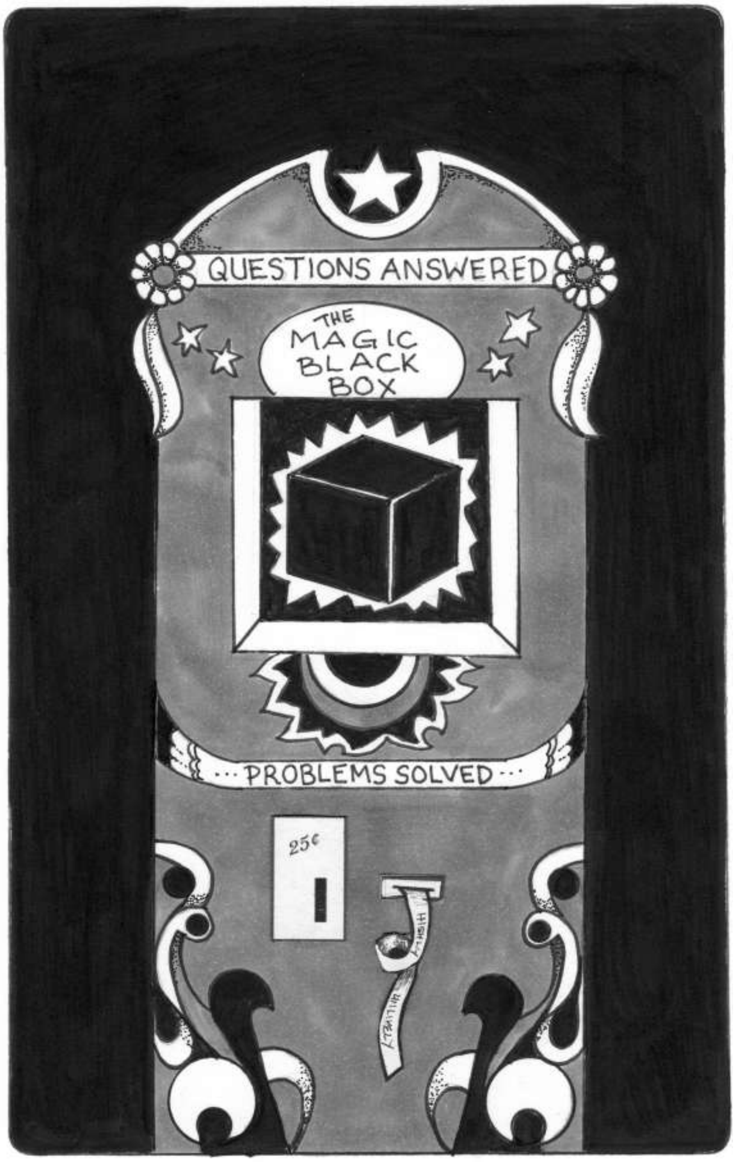
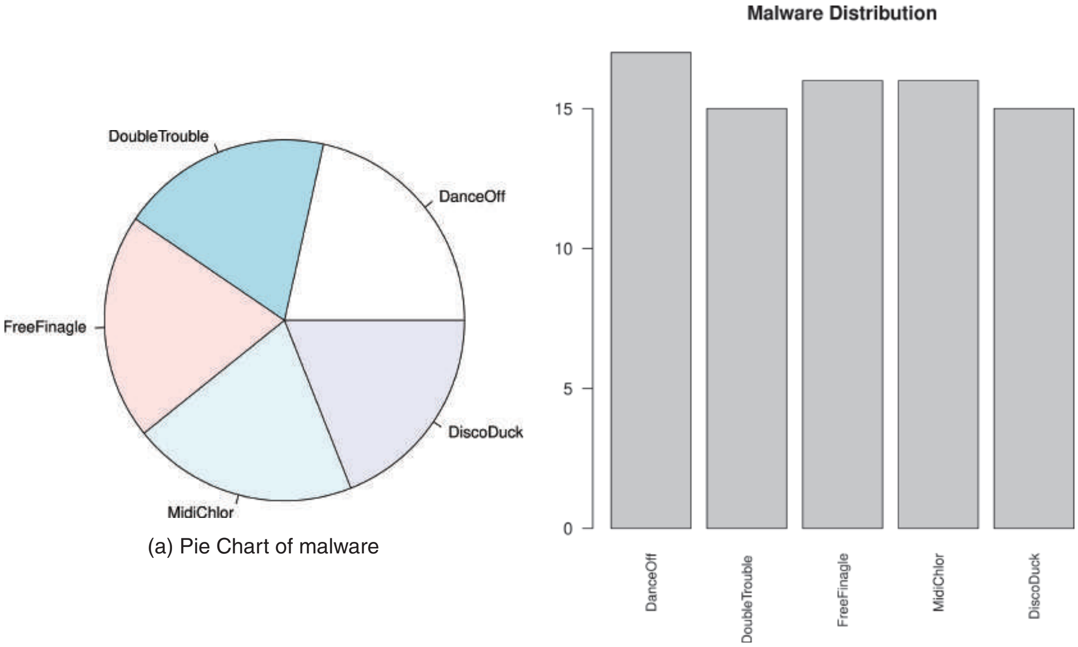


FIGURE 14.7 Magic black box.

From *Cybersecurity Myths and Misconceptions: Avoiding the Hazards and Pitfalls that Derail Us*, by Eugene H. Spafford, Leigh Metcalf, and Josiah Dykstra (ISBN-13: 978-0-13-792923-8) Copyright © 2023 Pearson Education, Inc. All rights reserved.

Chapter 15

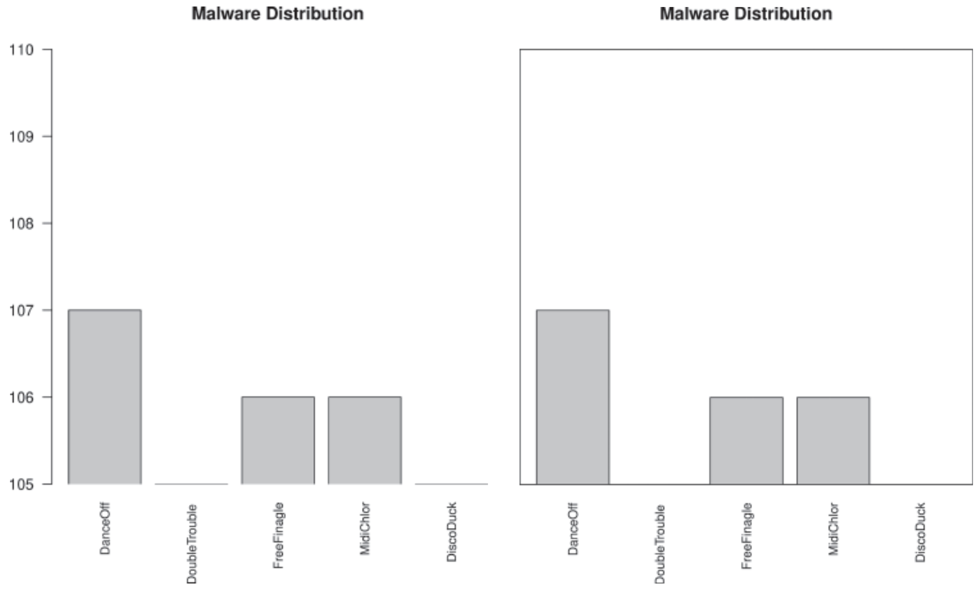


(a) Pie Chart of malware

(b) Bar plot of malware

FIGURE 15.1 Same malware data visualized as a pie chart and bar plot.

FIGURE 15.2 The right use for pie charts.



(a) A not as useful malware bar plot

(b) A really not as useful malware bar plot

FIGURE 15.3 Two bad bar plots

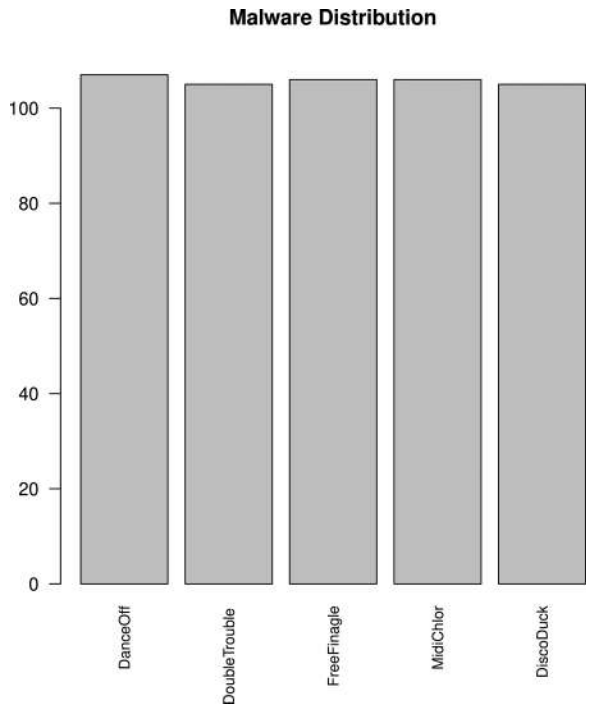


FIGURE 15.4 A well-designed bar plot.

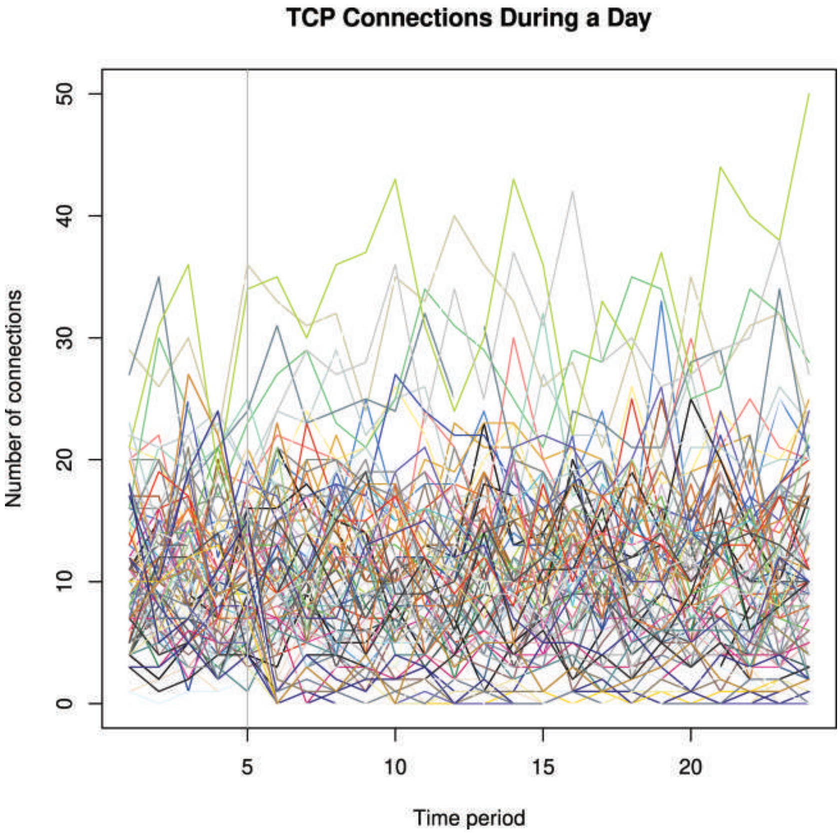


FIGURE 15.5 A figure that has lost the plot.

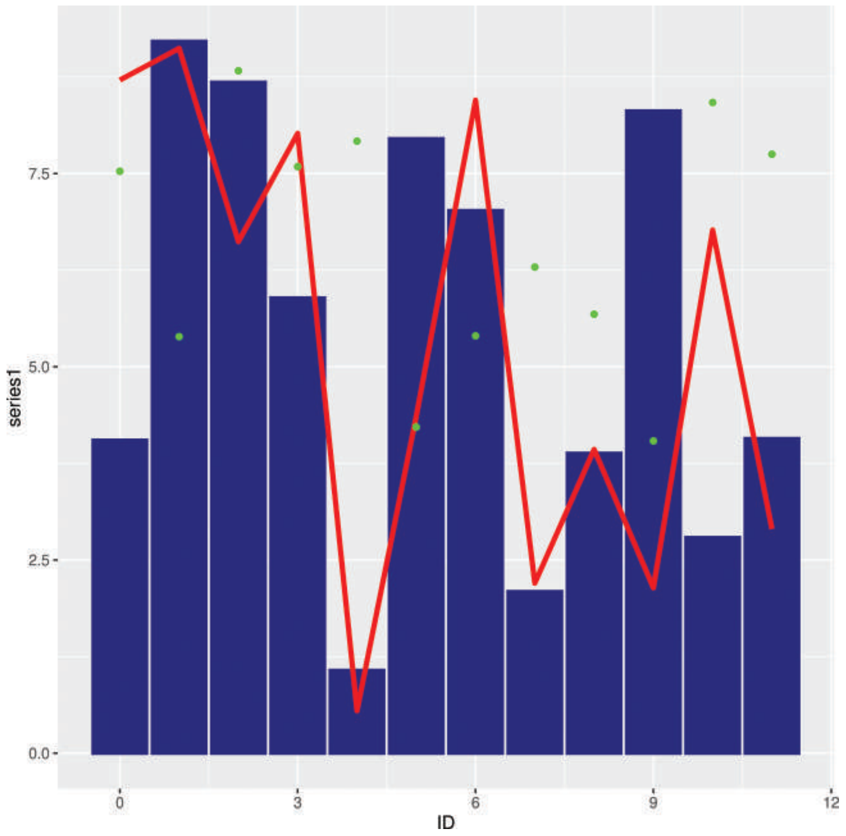


FIGURE 15.6 The plot thickens, and entirely too much.

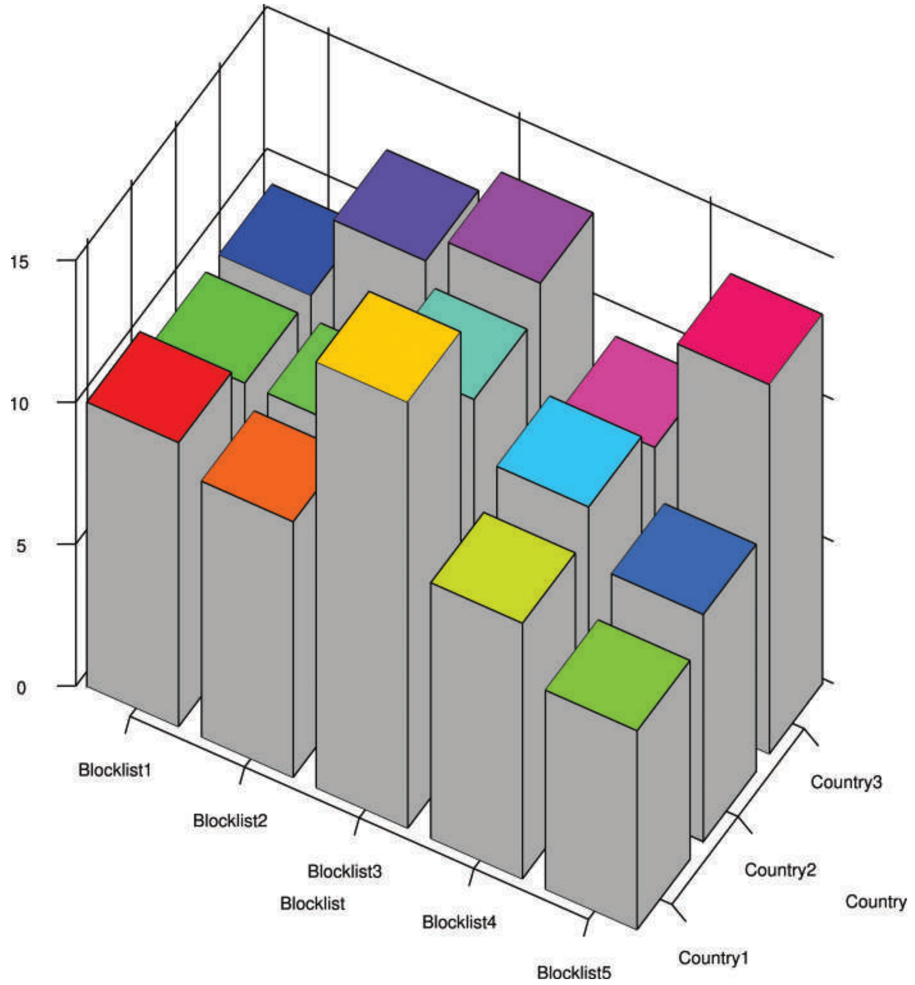


FIGURE 15.7 Three-dimensional bar plot.

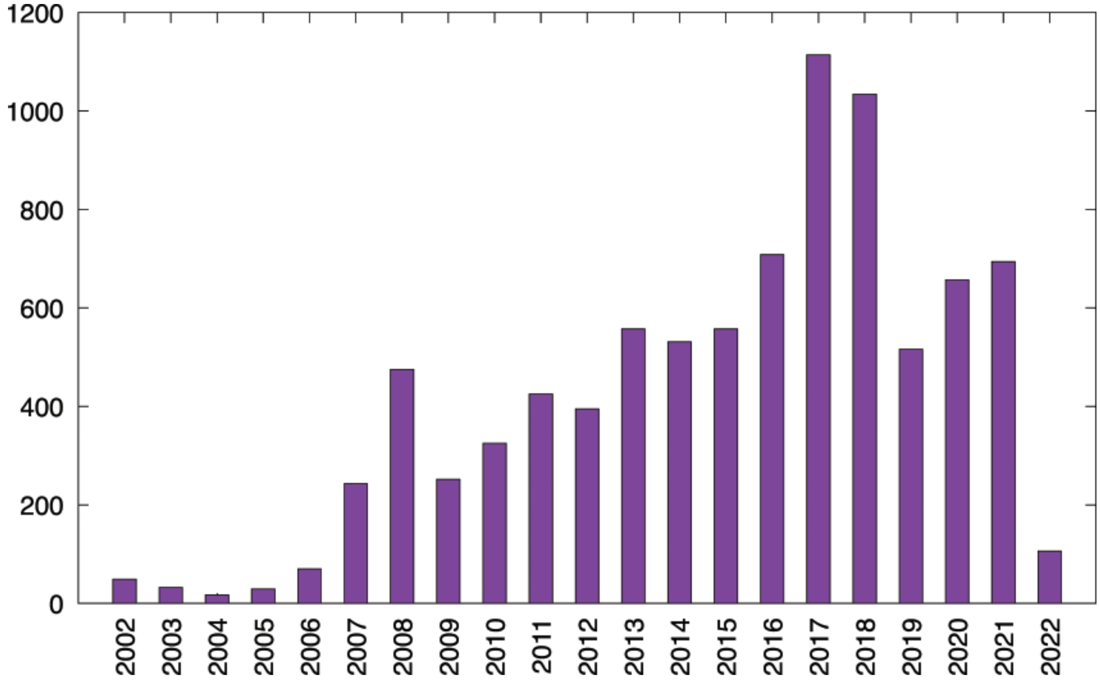


FIGURE 15.8 CWE-20 by Year.

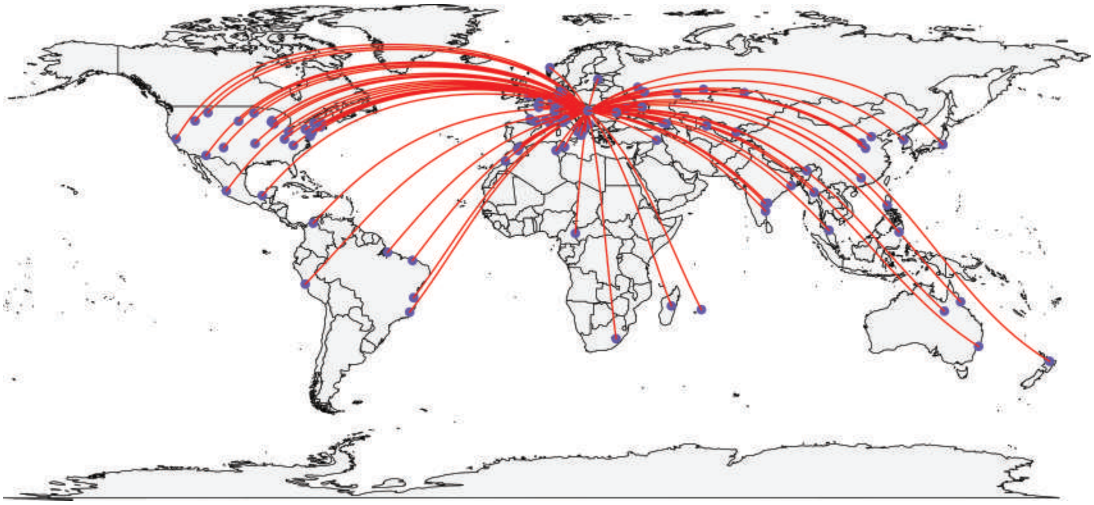


FIGURE 15.9 Geographic Botnet Behavior.

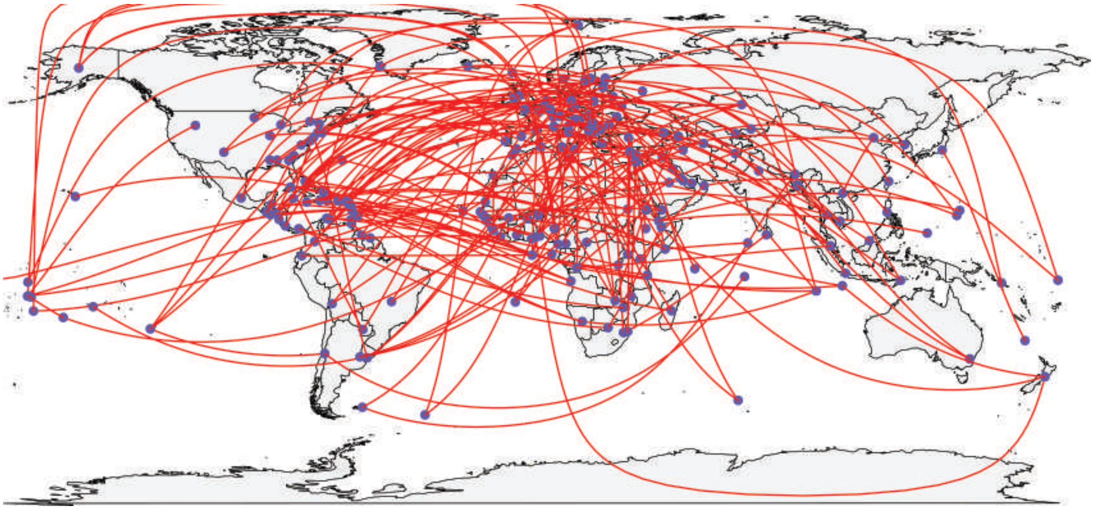


FIGURE 15.10 Geographic P2P Botnet Behavior.

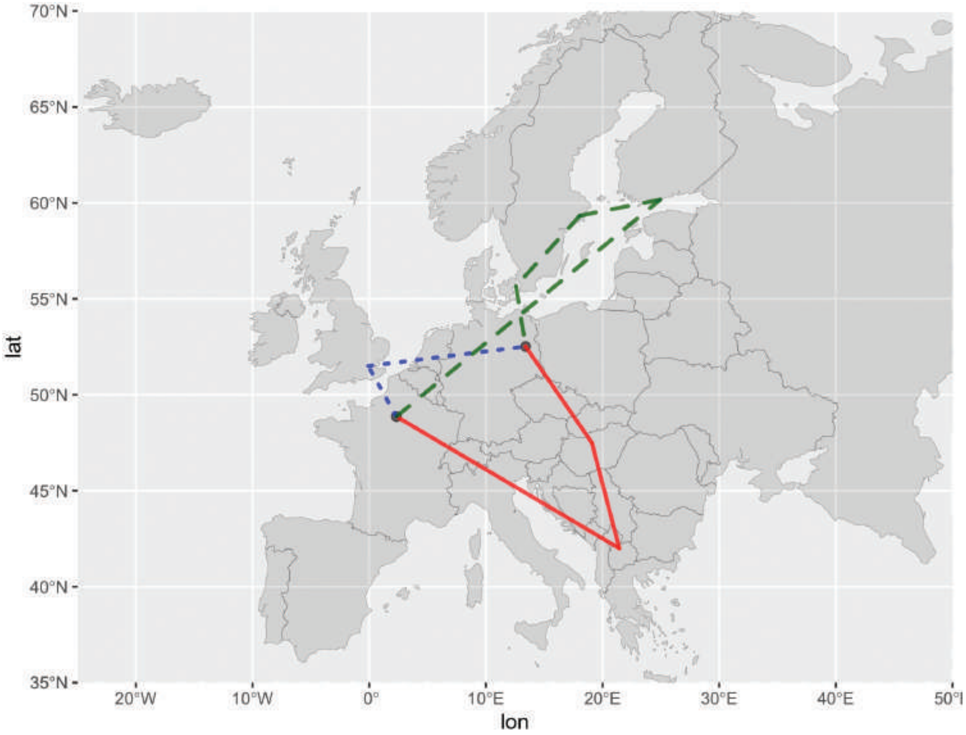
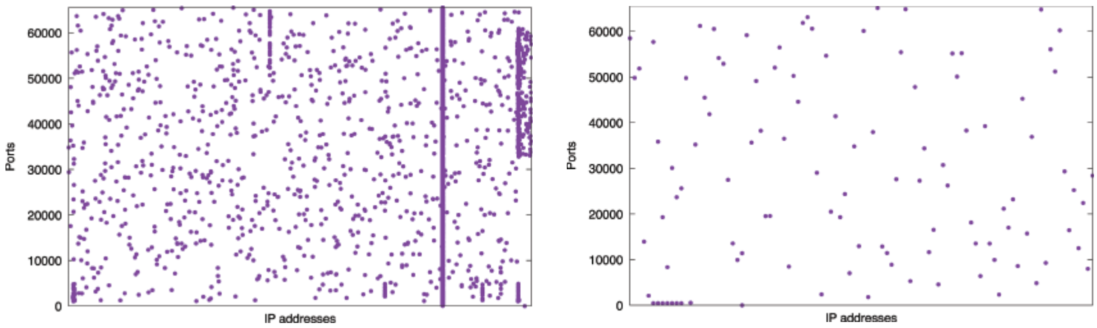


FIGURE 15.11 Example of BGP Routes.



(a) An hour of IPs and ports.

(b) A snapshot of IPs and ports.

FIGURE 15.12 Two illustrations of IPs and ports.

Chapter 16

FIGURE 16.1 Feed the documentation beast

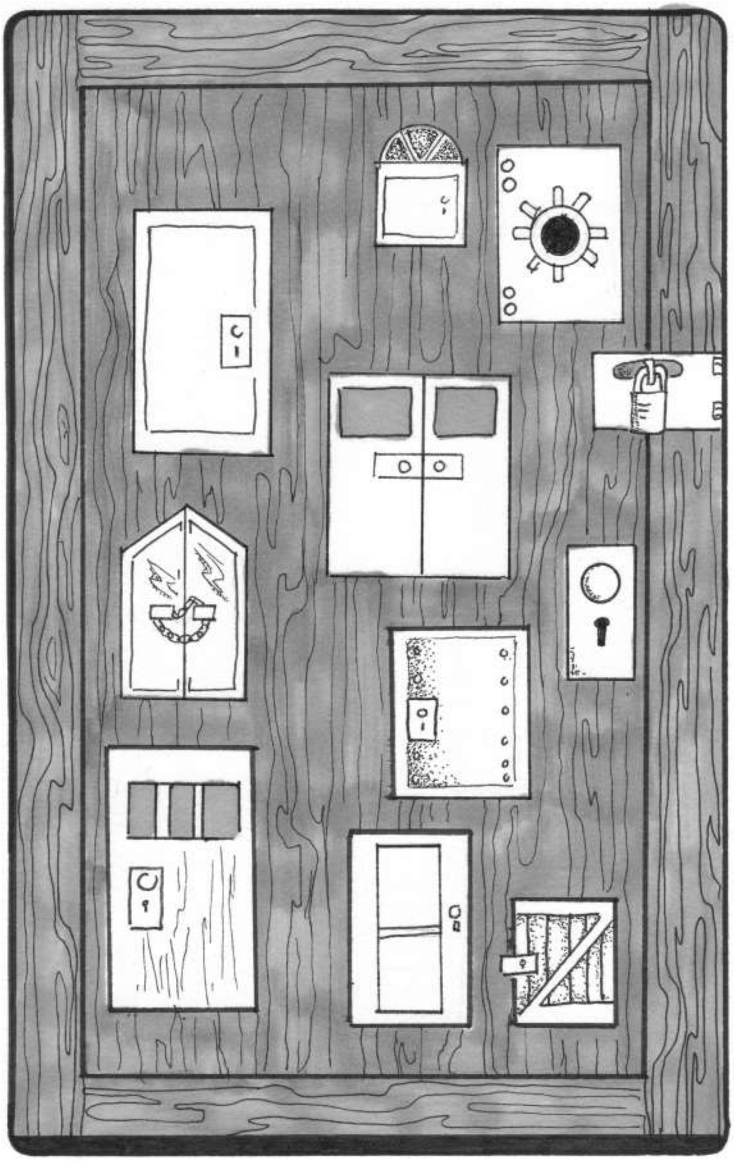


FIGURE 16.2 Overly complicated security.

Appendix

Short Background Explanations

This appendix contains short descriptions of items mentioned throughout the text. These are intended to provide some context for readers who might not be familiar with these items. These descriptions should **not** be taken as definitive or fully detailed! Some of them have details omitted that we do not see as necessary to understand their use in the book. We recommend consulting good textbooks, tutorials, and reliable news sources if you want more details on any of these topics.

Advanced Persistent Threat (APT)

APT as a term refers to organized penetration activity. It is often activity by a nation-state espionage group or organized criminal gang; as we have noted elsewhere, a criminal group might be working for a government so the attack involves both. APT attacks are usually stealthy, long-lived, and intended for data exfiltration. APT attacks are generally targeted at high-value organizations. A person is highly unlikely to have an APT incident on their home computer—unless they are an employee or contractor for a major company or government agency. APTs tend to use stealthy methods such as spear phishing, attacks on zero-day vulnerabilities, or supply chain insertion. Thereafter, the attackers may alter commands and configurations to provide persistent access.

Cloud Computing

A cloud is a collection of computers and storage, either private or commercial (public). Clients might use the resources in the cloud from other clients. The basic idea behind the cloud is that the resources can be flexibly allocated and deallocated as clients need without requiring the individual clients to have a built-up reserve that they might not be using all the time.

Cloud services might provide virtual storage, computers, or desktops. They might also supply software services on demand. The common names for these are Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Desktop as a Service (DaaS). Several vendors provide these services on a per-use or subscription basis.

See also "Færie Dust Can Make Old Ideas Magically Revolutionary" in Chapter 1.

Cross-Site Scripting

Cross-Site Scripting, also known as XSS, is a vulnerability that allows attackers to inject their own script into a website. It occurs when the website allows the user to input text but doesn't validate or clean it. It's considered one of the most common JavaScript vulnerabilities—though it isn't really a problem with JavaScript, but rather with how the website uses it.[1]

Rather than entering simple text, the attacker will enter bits of code. If there's no validation, the web server may execute the code.

Cybersecurity and Infrastructure Security Agency (CISA)

CISA[2] is a U.S. federal agency that was put into place in 2018 with the Cybersecurity and Infrastructure Security Agency Act of 2018. It replaced the National Protection and Programs Directorate (NPPD) as the department handling cybersecurity for the Department of Homeland Security (DHS). The mission of CISA is:

> We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

CISA has two defined roles. It is the operational lead for the `.gov` domain. That is, this agency is the lead for federal non-DoD cybersecurity issues. It also acts as the national coordinator for critical infrastructure security.

Firewall

In building construction, a *firewall* is designed to prevent fire from spreading. Of course, the best-case scenario is that there is no fire. If you happen to get unlucky and a fire starts, the firewall will stop it

[1] https://owasp.org/www-community/attacks/xss/

[2] www.cisa.gov/

from spreading beyond the firewall, at least for some time. The firewall does not attempt to determine whether it's a good fire or a bad fire; it simply stops everything right there. In cybersecurity, a firewall is either a dedicated device or software that lets you decide there is good traffic and bad traffic and allows you to let the good traffic in but keep the bad traffic out.

Before firewalls, it wasn't easy to keep people from accessing your system. If you had a web server, anyone could access it by default. If someone decided to flood your server with requests, you had to deal with it until they got bored. The firewall changed that.

At the most basic level, firewalls look at IP addresses, domains, ports, and protocols for filtering and blocking. Some firewalls will look into packets for specific contents and patterns. Generally, firewalls operate on traffic in real time. Firewalls are often located at the perimeters of networks. Firewall devices might also handle other duties, such as intrusion detection, routing, VPN management, and traffic shaping.

A firewall is a good first line of defense, but it should not be your only defense. There are ways to get past one, some unexpected and others on purpose, such as through email. You want people to email you, but an email is also often an infection vector.

Honeypots

Honey draws flies and wasps.[3] If you wish to distract the nuisance insects from more valuable items and perhaps trap them for study, a pot of sticky honey will serve the purpose. Similarly, if you want to decoy attackers and maybe study their tools and methods, you would deploy a honeypot system: a system that appears authentic and tempting to the attacker, but is instrumented and monitored.

Honeypots are but one example of deception and decoys. Others include fake documents and fake credentials, which are called honeytokens.

Internet Worm and the WANK Worm

One of the oldest worms distributed on the Internet, the Internet worm, also known as the Morris worm, took the computing world by storm on November 2, 1988.[4] It took advantage of several vulnerabilities, including one in the sendmail program, a common program used to send email at the time. The worm's author allegedly wrote it to see if he could, and it caused havoc for days.[5]

[3] And Winnie-the-Pooh, but we assume Pooh is benign.

[4] Spafford, Eugene H., "The Internet Worm Program: An Analysis." ACM SIGCOMM Computer Communication Review; Vol. 19, No. 1 (1989): 57.

[5] See the section"Because You Can, You Should" in Chapter 1, "What Is Cybersecurity?" for more discussion.

The worm resulted in the first felony conviction under the CFAA[6] and led DARPA to fund the CERT/CC at Carnegie Mellon University.[7] CERT/CC was created to be a central point to manage network emergencies, as no such agency existed at the time.[8]

The WANK worm of 1989 was an attempt to cause havoc by locking people out of their systems, threatening to delete files, and making monitors display a message that included the phrase "Worms Against Nuclear Killers," presumably the origin of the name. It started at NASA, but it did not stay there, as often happens with worms.[9] It spread from NASA to the U.S. Department of Energy, and then to CERN in Switzerland and RIKEN in Japan. The guess from some is that the worm's creators were attempting to cause havoc before the launch of the Galileo spacecraft, which had a small amount of plutonium on board to power a fuel cell. The worm authors failed in that goal, and the spacecraft launched on time. While some people think that the reason for creating the worm was the spacecraft, others believe it was to cause trouble. One of the investigators of the incident surmised the authors were playing with the word "wank," which is British slang.[10]

The worm was eventually traced to two Australian men, which led to the first major Australian trial for computer crimes.[11] One of the men helped the authorities when he called *The New York Times* to brag about writing the code. The result was a lot of time and money cleaning it up, while the men were sentenced to community service for the crime.

The Morris and WANK worms highlighted how vulnerable networks of systems were and underscored that cybersecurity needed a higher priority. The Internet, in particular, was built on trust, and some people are constantly seeking ways to abuse that trust for their advantage or amusement.

Intrusion Detection System (IDS)

An IDS has a simple job. It's there to detect intrusions; thus, it's great that it has such a relevant name. A host-based IDS monitors activity on a computer to identify questionable activity.

A Network Intrusion Detection System monitors traffic and looks for suspicious traffic patterns. It does not know what suspicious traffic is: It has to be programmed to recognize it. For example, the `log4j` vulnerability was exploited remotely through web traffic, and we know what that web traffic should contain. That means we can set up a rule on the IDS to look for any web requests that contain characters matching a `log4j` exploit.

[6] www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

[7] DARPA was prompted to do this by William Scherlis of Carnegie Mellon.

[8] www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/DARPA/20-F-1335_Final_Production_CERT_CC_1988.pdf

[9] www.realclearscience.com/blog/2019/01/12/when_nasa_got_wanked.html

[10] https://web.archive.org/web/20080227132540/www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf

[11] No record is available to determine if one of the men said, "Hold my beer," before writing said code.

In general, an IDS does not do anything with the traffic other than creating an alert, which should be investigated, and possibly blocking the traffic. Some of these systems can be coupled with other tools to change firewall rules, alter network traffic, and more.

`log4j` Vulnerability

Application developers love logging systems. These systems can help them find and fix problems if they know what happened. For a web server, we want to know who accessed which page, when, and how.[12] The more information available, the easier it is to debug. Otherwise, for web applications, we are effectively debugging in the dark with our hands under a blanket and the screen brightness set to 0.

The Apache Software Foundation develops `log4j` to manage logging in applications.[13] This would be a short description if that is all `log4j` did. Instead, Apache gave this software more functionality. It logs messages and can also be programmed to be smart about the messages it gets. Unfortunately, it turns out that attackers could take advantage of this feature, thus sparking multiple CVEs and a lot of work from security researchers. The vulnerability was exploited for cryptojacking and installing backdoors.[14] The first report of the U.S. Cyber Safety Review Board was on the `log4j` vulnerability.[15]

Orange Book/Trusted Computer System Evaluation Criteria (TCSEC)

The TCSEC, colloquially known as the Orange Book,[16] was a set of standards issued by the National Computer Security Center (NCSC) of the NSA that defined how to assess the trust level of specific computer systems.[17] It described six levels, from Minimal Protection (which meant the target failed the assessment) to Verified Protection, which included formal verification of code.

The original version, released in 1983, was considered the first significant methodology for security evaluation. It had several problems, not the least of which was keeping up with changing software and practices. It was also focused on the operating system and building it to be trustworthy when protecting confidentiality, which was soon not the only threat.[18]

[12] Web logs do not necessarily record "why" someone accessed a particular webpage.

[13] https://logging.apache.org/`log4j`/2.x/

[14] www.zdnet.com/article/log4shell-exploited-to-infect-vmware-horizon-servers-with-backdoors-crypto-miners/

[15] www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf.

[16] Called that because the printed version of the book had an orange cover.

[17] https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf

[18] www.cs.clemson.edu/course/cpsc420/material/Evaluation/TCSEC.pdf and Lipner, Steven B., "The Birth and Death of the Orange Book," *IEEE Annals of the History of Computing*, Vol. 37, No. 2 (2015): 19–31.

Phishing

Fishing is the attempt to catch a fish by dangling an attractive bait on a hook. Phishing is attempting to enter a system by dangling an attractive bait in an email.

In this kind of attack, an email appears to be from a reputable source and directs the recipient to accomplish a task. The request is often presented with some urgency to encourage action before careful consideration. The phish might ask the reader to log into a portal, enter a credit card number, or generally do something that seems reasonable and rational yet gives up their information. Other phishing attacks might seek to induce the recipient to click on an attached document or link that will result in a flaw in the current system being exercised, such as infection with malware.

Phishing is popular with malicious actors because it works. In 2020, there were over 240,000 complaints about phishing.[19] There were undoubtedly many more incidents that were not reported (or detected). The AntiPhishing Working Group (APWG) reported over a million phishing attempts in the first quarter of 2022, representing a significant increase.[20]

In spearphishing, the phish is carefully tailored and targeted directly at someone rather than being sprayed across many recipients. In SMS phishing, the phish comes through SMS messaging rather than emails; this kind of attack is sometimes referred to as "smishing" (and unsolicited advertising is sometimes referred to as "SPIM," corresponding to email SPAM).

Spearphishing of high-value targets (e.g., the CEO) is sometimes referred to in the literature as "whaling."

Rowhammer Attack

If you take a hammer to a row of glass and repeatedly hit it, sooner or later, that glass will break. *Rowhammer* (or *Row hammer*) is an attack that applied the same idea to memory chips. Dynamic Random Access Memory (DRAM) is kept in a grid of memory, so Rowhammer rapidly and repeatedly accesses one row of the grid in an attempt to build up an electric charge[21] that will modify or delete data in other rows of the memory grid.[22] The goal is to flip some bits to either disclose information or alter information flow.

[19] www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[20] https://apwg.org/trendsreports/

[21] Roughly akin to rubbing socks on a carpet to build up a static charge.

[22] https://arstechnica.com/information-technology/2015/03/cutting-edge-hack-gives-super-user-status-by-exploiting-dram-weakness/

SolarWinds Incident

SolarWinds[23] is a software development house specializing in network and systems management software. Its software is widely used by organizations from government to industry and everything in between. One of its products is the Orion platform, which manages IT environments. It's an all-in-one solution to control everything, from the infrastructure in the environment to the applications in use.

Unfortunately, in 2020 the company was the victim of an attack.[24] The attackers used that access to upload updates to the company's portal that contained Trojans. When customers downloaded and installed these altered updates,[25] havoc erupted. The customers of SolarWinds, if they installed updates, were now victims of the same attackers. CISA announced, with other government agencies, that it appeared a Russian group was behind the attack.

This incident involved a *software supply chain attack*. You (if you were a victim of this) were not attacked directly, but your supplier was. In these attacks, you would have done nothing wrong to become the victim—the attacker discovered that it was easier to attack your supplier and then use that route to attack you.

Virtual Private Network (VPN)

A VPN is software that creates an encrypted "tunnel" between two points. It acts as if it was a dedicated network link over which traffic flows. An eavesdropper cannot read the encrypted traffic. A VPN connection might also provide protected connectivity to a trusted DNS server to prevent spoofing attacks on the client endpoint.

Remote workers often use VPNs to have a remote machine "inside" the network of their employer. In these cases, the VPN terminates inside the enterprise's firewall, and the clients act as remote, semi-tethered clients. VPNs are also often used to circumvent content controls (e.g., censorship) imposed by political entities and organizations.

WannaCry

WannaCry was a ransomware attack in May 2017. The ransomware attacked Windows systems and held the data on the systems until a bitcoin ransom was paid. It spread from system to system and demanded at least $300 from the victims, eventually increasing that demand to $600.[26] The interesting thing about WannaCry was the built-in kill switch. The ransomware looked for a domain, and if

[23] www.solarwinds.com/

[24] www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html

[25] You trust your software provider's website, right?

[26] www.techtarget.com/searchsecurity/definition/WannaCry-ransomware

the domain didn’t exist, then the ransomware happily encrypted the victim’s drive. If it did exist, then the ransomware wouldn’t spread any further. A researcher, Marcus Hutchins, discovered that the malware was looking for the nonexistent domain and registered it to see what would happen. As luck would have it, that activated the kill switch, and the ransomware stopped spreading.

It was estimated that the ransomware caused $4 billion in damage.[27]

Zero Trust

Zero trust is not a product or a protocol; instead, it’s an attitude and an architecture.[28] It’s a way of looking at the problems of design and implementation of security to include the idea that no one should be trusted and everyone must be verified. Systems are treated as if they were already breached. All activity is suspect until proven otherwise. Traditionally, users would authenticate themselves once, and everything would assume that the associated activity was still that user. Zero trust removes that assumption, minimizing where trust credentials may be used.

See also “Færie Dust Can Make Old Ideas Magically Revolutionary” in Chapter 1, “What Is Cybersecurity?”

[27] https://securityintelligence.com/articles/what-has-changed-since-wannacry-ransomware-attack/

[28] www.darkreading.com/perimeter/forrester-pushes-zero-trust-model-for-security

Acronyms

ABET Accreditation Board for Engineering and Technology

ACM Association for Computing Machinery

AI Artificial Intelligence

AML Adversarial Machine Learning

ANSI American National Standards Institute

APT Advanced Persistent Threat

APWG Anti-Phishing Working Group

AS Autonomous System

ASLR Address space layout randomization

AV Antivirus

AWS Amazon Web Services

BGP Border Gateway Protocol

CDT Center for Democracy and Technology

CEO Chief Executive Officer

CFAA U.S. Computer Fraud and Abuse Act of 1986

CIA Central Intelligence Agency

CIO Chief Information Officer

CISA Cybersecurity and Infrastructure Security Agency

CISO Chief Information Security Officer

CME Common Malware Enumeration

CMM Capability Maturity Model

CMS Content Management System

CNA CVE Numbering Authority

CTI Cyber Threat Intelligence

CVD Coordinated Vulnerability Disclosure

CVE Common Vulnerability Enumeration

CVSS Common Vulnerability Scoring System

CWE Common Weakness Enumeration

DaaS Desktop as a Service

DB Database

DDoS Distributed Denial of Service

DEP Data Execution Prevention

DFIR Digital Forensics and Incident Response

DHS Department of Homeland Security

DMCA Digital Millennium Copyright Act

DMZ Demilitarized Zone

DNS Domain Name System

DoS Denial of Service

DPRK Democratic People's Republic of Korea—North Korea

DRAM Dynamic Random Access Memory

EAR Export Administration Regulations

ECPA Electronic Communications Privacy Act

EDR Endpoint Detection and Response

EFF Electronic Frontier Foundation

EKG Electrocardiogram

EPIC Electronic Privacy Information Center

EPSS Exploit Prediction Scoring System

FACR Foreign Assets Control Regulations

FBI Federal Bureau of Investigation

FedRAMP U.S. Federal Risk and Authorization Management Program

FEMA Federal Emergency Management Agency

FFRDC Federally Funded Research and Development Center

FIRST Forum of Incident Response and Security Teams

FISMA Federal Information Security Management Act

FUD Fear, Uncertainty, and Doubt

GDPR General Data Protection Regulation

GUI Graphical User Interface

HIPAA Health Insurance Portability and Accountability Act

HR Human Resources

HTTPS Hypertext Transfer Protocol Secure

IaaS Infrastructure as a Service

IANA Internet Assigned Numbers Authority

IAU International Astronomical Union

ICS Industrial Control Systems

IDS Intrusion Detection System

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IMAP Internet Message Access Protocol

IoE Internet of Everything

IoT Internet of Things

IP Internet Protocol

IRB Institutional Review Board

ISO International Organization for Standardization

ISP Internet Service Provider

ISSA Information Systems Security Association

ITAR International Traffic in Arms Regulations

LOAC Law of Armed Conflict

MAC Media Access Control

MFA Multifactor Authentication

ML Machine Learning

NAT Network Address Translation

NATO North Atlantic Treaty Organization

NCSC National Computer Security Center

NFC Near-Field Communication

NFT Non-fungible Token

NICE National Initiative for Cybersecurity Education

NIST National Institute of Standards and Technology

NPPD National Protection and Programs Directorate

NSA National Security Agency

OPSEC Operational Security

OS Operating System

OSI Open Systems Interconnection

OSS Open Source Software

PaaS Platform as a Service

PCI DSS Payment Card Industry Data Security Standard

P2P Peer-to-Peer

PHI Protected Health Information

PII Personally Identifiable Information

POP Post Office Protocol

RAT Remote Access Trojan

RCE Remote Code Execution

RFC Request for Comments

ROP Return-Oriented Programming

SaaS Software as a Service

SBOM Software Bill of Materials

SCADA Supervisory Control And Data Acquisition

SHA Secure Hash Algorithm

SLA Service Level Agreement

SLO Service Level Objective

SMTP Simple Mail Transfer Protocol

SOC Security Operations Center

SSL Secure Socket Layer

TCP Transmission Control Protocol

TCSEC Trusted Computer System Evaluation Criteria

TLS Transport Layer Security

TOR The Onion Router

TPM Trusted Platform Module

TTP Tactics, Techniques, and Procedures

UDP User Datagram Protocol

UFO Unidentified Flying Object

VEP Vulnerabilities Equity Process

VPN Virtual Private Network

WWW World-Wide Web

XDR Extended Detection and Response