CYBERSECURITY

DUANE C. WILSON

THE MIT PRESS ESSENTIAL KNOWLEDGE SERIES

The MIT Press would like to thank the anonymous peer reviewers who provided comments on drafts of this book. The generous work of academic experts is essential for establishing the authority and quality of our publications. We acknowledge with gratitude the contributions of these otherwise uncredited readers.

This book was set in Chaparral Pro by New Best-set Typesetters Ltd.

Library of Congress Cataloging-in-Publication Data

Names: Wilson, Duane, author.
Title: Cyber security / Duane Wilson.
Description: Cambridge, Massachusetts : The MIT Press, [2021] | Series: The MIT Press essential knowledge series | Includes bibliographical references and index.
Identifiers: LCCN 2020033978 | ISBN 9780262542548 (paperback)
Subjects: LCSH: Computer security. | Internet—Security measures. | Computer networks—Security measures. | Data protection.
Classification: LCC QA76.9.A25 W554 2021 | DDC 005.8—dc23
LC record available at https://lccn.loc.gov/2020033978

10 9 8 7 6 5 4 3 2 1

CONTENTS

SERIES FOREWORD

The MIT Press Essential Knowledge series offers accessible, concise, beautifully produced pocket-size books on topics of current interest. Written by leading thinkers, the books in this series deliver expert overviews of subjects that range from the cultural and the historical to the scientific and the technical.

In today's era of instant information gratification, we have ready access to opinions, rationalizations, and superficial descriptions. Much harder to come by is the foundational knowledge that informs a principled understanding of the world. Essential Knowledge books fill that need. Synthesizing specialized subject matter for nonspecialists and engaging critical topics through fundamentals, each of these compact volumes offers readers a point of access to complex ideas.

1

CYBERSECURITY ORIGINS

Internet security has become an enormous challenge. Almost everything we see, touch, or use is connected to the internet, including cell phones, wearable devices, home appliances, and even semiautonomous vehicles. The internet is a portal for businesses, governments, and other institutions, providing remote access to trade secrets, medical records, and financial data. And such is the paradox of connectivity: the more connected our computer systems, the more exposed they are to cyberattacks—attempts to steal data, corrupt software, disrupt operations, and even physically damage hardware and networked infrastructures.

The field of cybersecurity exists to meet the challenge of understanding and protecting against such attacks. In this book, I will present the risks associated with internet use, modern methods to defend it, and general principles for safer internet use. These principles, which have been developed over the years by cybersecurity experts, tend to be disseminated to and implemented by businesses, governments, and other organizations for which the stakes are understandably high.

A network, however, is typically only as strong as its weakest link. A cyberattack on an organization often proceeds from a successful attack against just one individual. And if that person has not been trained to identify the key indicators of a cyberattack, they may unwittingly open the back door, or front door, to an intruder. This book aims to arm the reader with the knowledge needed for the front line of the cyberbattle.

The origins of cybersecurity can be traced back to World War II. At that time, cipher machines were used for cryptography—the act of sharing secrets using codes. A cipher machine is a device that is used to keep communications private through encryption—the process of making a message private. These machines were rudimentary but frequently effective methods of secure communication during wartime. During World War II, the primary cipher machine used by Nazi Germany was called Enigma (see figure 1) and the ones used by the Japanese troops were code-named Purple. Both machines had a similar operational protocol:

1. An operator—the sender—at a command post would be given a message to encrypt.

2. The sender would type the message on the machine.

Network [ARPANET], the precursor to the modern internet.) Creeper was an experimental self-duplicating program that was designed to demonstrate mobile transmittal of computer applications. It moved between computers connected to the ARPANET (the first version of the internet) and using BBN's TENEX operating system (OS), infected both computers and printers, displaying the message "I'M THE CREEPER: CATCH ME IF YOU CAN."[2]

In 1982, Richard Skrenta, a curious fifteen year old, wrote the code for Elk Cloner, the first computer virus known to be spread "in the wild," meaning outside a closed network or research environment. The virus was installed on floppy diskettes that stored the Apple II OS. When a computer was booted from an infected disk, the virus would copy itself to any uninfected floppy disk it could access—at that time, most computers had dual disk drives, and OS disks were often used to boot up multiple computers. On every fiftieth infected computer, the virus would display the following text (shown here in the groovy style of the 1980s):

> **Elk Cloner: The program with a personality**
>
> It will get on all your disks
>
> It will infiltrate your chips
>
> Yes it's Cloner!

It will stick to you like glue

It will modify ram too

Send in the Cloner![3]

These two cases illustrate how software applications—if they are able to spread uncontrollably—can be irritating and intrusive at best, even if they weren't meant to be harmful. Yet the Morris worm created in 1988 was deliberately written with malicious intent and arguably led to the cybersecurity field as we know it today. Robert Tappan Morris, then a graduate student at Cornell University, launched his worm surreptitiously from a computer based at MIT that was connected to the then-nascent internet. What made the Morris worm malicious was that it created far more copies of itself than Morris intended, which drained the infected computer's resources—this is now known as a denial-of-service attack. Such attacks impact a computer system's *availability*, the second fundamental cybersecurity goal. Estimates at the time claimed that the worm infected more than ten thousand computers and cost the government hundreds of thousands to millions of dollars to decontaminate the stalled computers. Morris was tried and convicted in a federal court.

So why was the internet's design so insecure? Have there been improvements over the years to address some of its inherent vulnerabilities? To answer these questions, we must briefly understand one of its core features—*packet switching*. In 1961, MIT PhD computer science student Leonard Kleinrock published a theoretical paper on packet switching, an alternative method to purely electronic signals for sharing data between connected computer systems. A packet consists of a header and payload; the header tells the network's hardware where and how to deliver the payload, the contents of the message. The concept was later adopted in the early plans for ARPANET by MIT-trained electrical engineer Lawrence (Larry) G. Roberts, who was then working for the Defense Advanced Research Projects Agency.

Kleinrock would later obtain a professorship at the University of California in Los Angeles; his lab was selected as the first node for the nascent ARPANET. As more computers were added to ARPANET, computer scientists focused on software to govern the shuttling of data across the network. An early example is the host-to-host protocol, which outlined the rules by which information is exchanged: the message (or packet) format, delivery time, file type, and other such variables. Today, consumers assume that their internet-connected devices have built-in cybersecurity measures, however that was not a concern for the internet pioneers. Somehow they did not anticipate the diversity and intensity of the cyberattacks that now plague the internet.

The Morris worm attack could have been prevented. Estimates are that it shut down roughly 10 percent of all the computers connected to the internet at the time; that's essentially a cyberpandemic! That worm proliferated largely because the early internet had a flat structure rather than a hierarchical one. Today, the internet is essentially made up of public and private networks separated by *firewalls*—cybersecurity protocols that monitor and control the flow of traffic into and out of private networks (i.e., an organization's local network). A simple firewall would have stopped the Morris worm in its tracks. The internet is now more secure, but it is also more threatened. In the subsequent chapters, I will explore both the threats and modern cyberdefenses. Additionally, I will show how cybersecurity is practically implemented on the internet, and discuss how the field is likely to change with new and forthcoming technologies, such as blockchain technology or quantum cryptography.

2

FOUNDATIONS

In the early 1960s, people saw the great potential of transmitting and sharing information across different systems, with a focus on the scientific and military fields. The theory of packet switching, which forms the basis of the modern-day internet, emerged after MIT's J. C. R. Licklider proposed the first global network of computers in 1962. Along with early technological innovations came the need to secure sensitive data, software, and applications, giving birth to cybersecurity. Further underscoring the importance of cybersecurity is the explosion of internet (or World Wide Web [WWW]) users, who jumped from one billion in 2005 to more than four billion in 2019.[1] And that's only 53 percent of the world's (still growing) population!

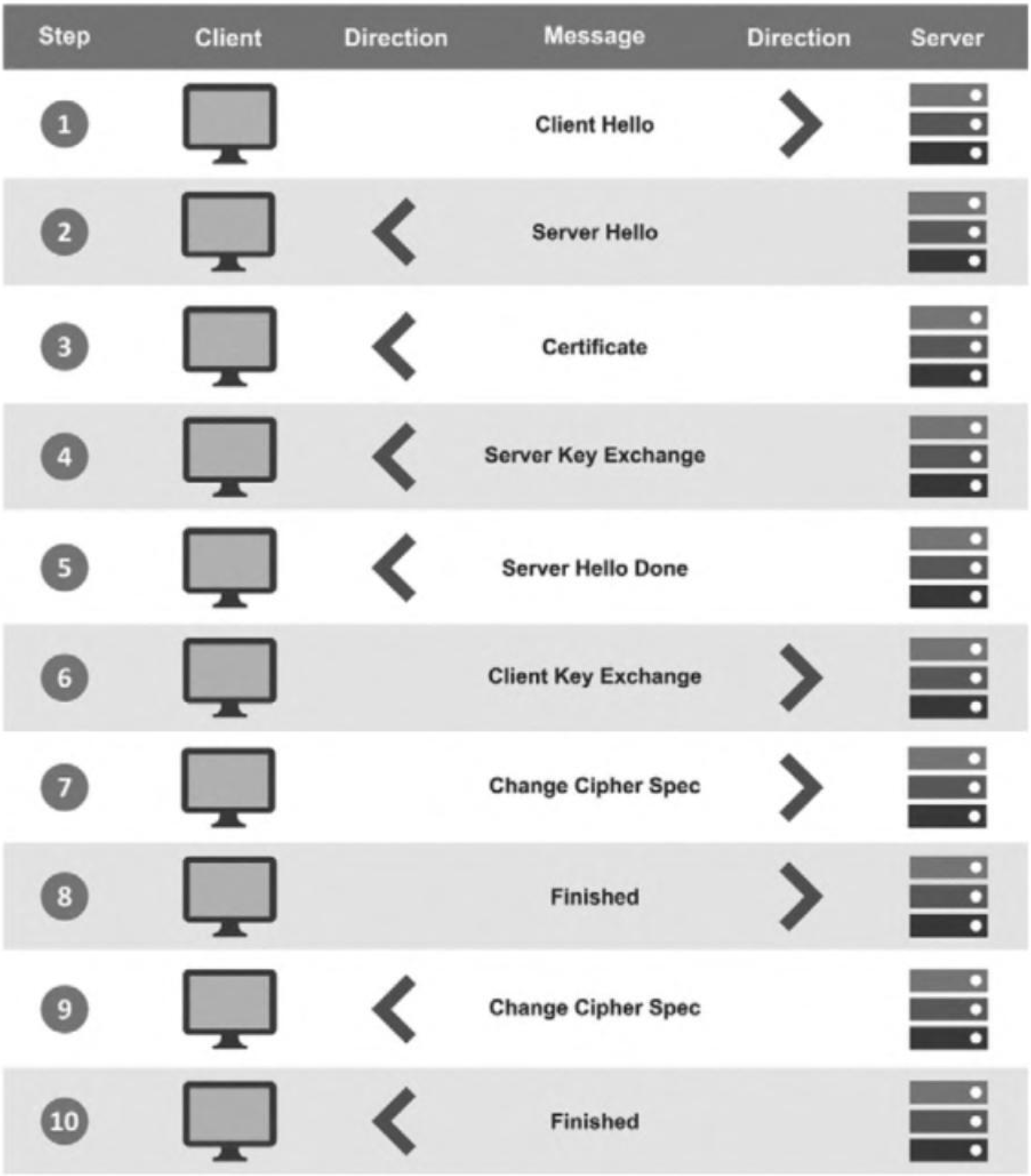
The WWW is responsible for the interaction between humans via technological mediums. The terms *WWW* and the use of encryption. Described further in the next chapter, encryption is a fundamental part of cryptography that allows for data to be translated into a form that is illegible to those without authorized access. Encryption requires a secret key that is known only to the parties that possess it. Decryption is the opposite of encryption and is known as the process of converting the encrypted data back to its original form. In the digital world, encryption and decryption are accomplished at varying levels of sophistication, but at a high level, they are essentially the same as using a key to lock and unlock our house or car.

There are two forms of encryption: symmetric and asymmetric. Symmetric encryption uses the same key to both encrypt and decrypt data. Asymmetric encryption uses a key that is publicly available to encrypt (public key) and a key that is kept private to decrypt (private key). Symmetric key encryption is much faster than asymmetric key encryption, so it is the preferred choice for encrypting or decrypting data. The asymmetric key can be used to encrypt the symmetric key to protect it from being stolen. The combination of symmetric and asymmetric key encryption is effective for protecting a variety of online transactions. Indeed, it forms the basis for the blockchain and other technologies that have given rise to cryptocurrencies.

The standard technology for keeping an internet connection secure while safeguarding sensitive data being

sent between the client and web server is the Secure Sockets Layer (SSL). Someone who purchases a domain name is typically given the option of purchasing an SSL certificate, which works like a digital wallet containing information that identifies its owner and the metadata about that owner. An SSL certificate prevents criminals from reading and modifying any information being transferred between websites, including potential personal details. When a website is secured by an SSL certificate, the website address, or URL, will show up as a Hypertext Transfer Protocol Secure (HTTPS), and not just HTTP. A recent update to the SSL is Transport Layer Security (TLS), which allows users to view the details of the certificate, including the issuing authority and corporate name of the website owner.

Both SSL and TLS enable us to talk to other users or computer systems online in a secure manner – through the establishment of a secure communications channel. They are generally used interchangeably, and you will often see them denoted as SSL/TLS in writing. SSL/TLS uses both asymmetric and symmetric key encryption to accomplish the goal of secure data transmission. At a high level, the steps used behind the scenes for SSL/TLS are those depicted in figure 2. In summary, a client (a networked computer) and the server (the host of resources that the client needs to access) contact one another, the SSL/TLS certificate is presented, the client authenticates it, they



Step	Client	Direction	Message	Direction	Server
1	🖥		Client Hello	>	🗄
2	🖥	<	Server Hello		🗄
3	🖥	<	Certificate		🗄
4	🖥	<	Server Key Exchange		🗄
5	🖥	<	Server Hello Done		🗄
6	🖥		Client Key Exchange	>	🗄
7	🖥		Change Cipher Spec	>	🗄
8	🖥		Finished	>	🗄
9	🖥	<	Change Cipher Spec		🗄
10	🖥	<	Finished		🗄

Figure 2 SSL/TLS encrypted session establishment.

exchange a list of supported cipher suites and agree on one, and then key exchange occurs.[3]

Blockchain Security

Encryption is also a fundamental process for cryptocurrencies, which have become a mainstream topic. The underpinning of cryptocurrencies like Bitcoin is called a blockchain—a distributed database containing records, or transactions, stored simultaneously on multiple computers. Cryptocurrencies are based on several cryptographic foundations—to include encryption. The unique characteristic that makes the blockchain interesting is its ability to verify various types of transactions without needing a centralized authority. The encryption of blockchain data is necessary to preserve a user's privacy and confidentiality. Each time a transaction is made, a record of it is stored on the blockchain. Similar to the SSL/TLS handshake protocol described above, a key aspect of privacy in blockchains is the use of private and public keys. Blockchain systems use asymmetric/public key cryptography to secure transactions between users.[4] With their growth in popularity, blockchain systems are one of the primary uses of cryptography today. Given the massive interest, an increasing number of blockchain-based start-up companies have sprung up, and investment in them has grown transformation that produces an irreversible representation of the item that was hashed. In other words, data is transformed using a cryptographic key and function that results in a string of characters that represents that file, application, password, or system contents. This same operation can be performed before the file, application, password, or system contents are accessed. This verifies that the integrity of the item has not changed since its last known "trusted" state. Referring back to the house analogy, let's say you notice that your safe has been tampered with; you may still have an integrity issue regardless of the results of the "house scan" for system integrity.

Three of the top examples of integrity principles being used today are *passwords*, application *verification*, and *tripwire*. Passwords are still the most widely used form of authentication in conjunction with some form of a username. To maintain their integrity and confidentiality, passwords are not stored in their native form. Once you create a password, it will be hashed, *salted*, and then stored. Adding the salt to hashing provides another level of security for password integrity. A salt is essentially a one-time random stream of characters that is changed every time the password is updated. The application automatically updates the salt, without requiring interaction by the user or system owner. The best modern-day example of a salt is the completely automated public Turing test to tell computers and humans apart (captcha). Each time