DATABASE AND APPLICATION SECURITY

A PRACTITIONER'S GUIDE

R. SARMA DANTURTHI

FREE SAMPLE CHAPTER

Database and Application Security

A Practitioner's Guide

R. Sarma Danturthi

Addison-Wesley

Figure Credits

Figures 02.01a-b, 03.02, 03.03a-b, 05.01, 05.02, 06.01 – 06.05, 07.07, 07.08, 07.11, 07.15, 08.01, 08.02, 09.03, 10.03, 11.02, 11.05, 11.09 – 11.13, 12.02, 16.02 – 16.05: Microsoft Corporation

Figures 04.02, 05.03, 07.09: Oracle Corporation

Figure 07.10c: The Department of Defense

Figure 09.02: National Institute of Standards and Technology

Figure 11.06: PayPal Holdings, Inc

Figure 11.07 & 11.08: The Apache Software Foundation

Figure 12.03: OWASP Foundation, Inc.

Figure 13.03: The United States Navy

Figure 14.01 & 14.02: The ZAP Dev Team

Figure 14.03 & 14.04: PortSwigger Ltd

Figures 14.05-14.07: Aircrack-ng

Figure 14.08 & 14.15: United States Department of Defense

Figure 14.16: Office of the Director of National Intelligence

Figure 14.17: SLEUTH KIT LABS

Figure 15.01a-b: Okta, Inc.

Figure 15.02: DigitalOcean, LLC.

Figure 15.03: Apple Inc

Cover image: Thapana Onphalai / Shutterstock

Visit us on the Web: informit.com/aw

Library of Congress Control Number: 2024931425

Hoboken, NJ

ISBN-13: 978-0-13-807373-2

ISBN-10: 0-13-807373-2

$PrintCode

Editor-in-Chief
Mark Taub

Director, ITP Product Management
Brett Bartow

Executive Editor
James Manly

Production Manager
Sandra Schroeder

Development Editor
Ellie C. Bru

Production Editor
Mary Roth

Copy Editor
The Wordsmithery LLC

Technical Editor(s)
Brock Pearson

Team Coordinator
Tammi Barnett

Cover Designer
Chuti Prasertsith

Composition
codeMantra

Proofreader
Donna E. Mulder

Indexer
Erika Millen

Dedication

This book is offered jointly into the divine hands of Swami Satyananda Saraswati and Swami Sivananda Saraswati.

Contents at a Glance

Part I. Security Fundamentals

Chapter 1: The Basics of Cybersecurity: In this chapter, the reader is introduced to security fundamentals of CIA-DAD and the authentication fundamentals IAAA. After giving details of hardware, software, and physical security, the roles of users are discussed. A detailed example of security in an organization is then presented to the reader.

Chapter 2: Security Details: This chapter discusses details of encryption, compression, indexing, and archiving. It goes into depth about encryption algorithms, PKI, email security, and non-repudiation. Current and new algorithms are touched on briefly in this chapter as well.

Chapter 3: Goals of Security: The "who is who" in security, RACI matrix, and the goals of security are discussed in this chapter. Events and incidents are also discussed along with risks and breaches. This chapter also stresses the importance of logs and reengineering a project while keeping security as a top priority.

Part II. Database Security—The Back End

Chapter 4: Database Security Introduction: ACID and BASE databases are discussed with examples in this chapter. DDL and DML are shown separately after defining DIT and DAR. Structural and functional security issues in DBs are discussed as well, and a plan for procedural security is put forward for consideration.

Chapter 5: Access Control of Data: Access control with MAC, DAC, RBAC, and RuBAC with roles and privileges is discussed in this chapter. Hashing and checksum examples and how they can be applied to DB are discussed. This chapter also covers monitoring DB with triggers and data protection with various database objects such as views.

Chapter 6: Data Refresh, Backup, and Restore: Data refresh, import, export, backup, and restore methods are shown in this chapter. Readers will learn how the backups and restores should be kept and tested regularly, in addition to daily/weekly/monthly tracking.

Chapter 7: Host Security: A host is a location (such as a Linux server) that keeps the DB and applications. Taking care of host security is important too as the DB is hosted on the server. This chapter shows how to create cron jobs or scheduled jobs on servers and provides numerous examples.

Chapter 8: Proactive Monitoring: Proactive monitoring helps prevent incidents and helps an organization to be fully prepared. Proactive monitoring can be done with logs, triggers, and more. Log file generation and reading are discussed to keep the reader up to date about what to expect.

Chapter 9: Risks, Monitoring, and Encryption: Risks can be mitigated, transferred, or accepted. But before choosing what to do with a risk, the risk needs to be measured. Risk monitoring is discussed in this chapter, along with DB monitoring, encrypting a DB, and generating automated alerts.

Part III. Application Security—The Front End

Chapter 10: Application Security Fundamentals: Application security starts with good coding fundamentals and following an acceptable coding standard. Cohesion and coupling are discussed, and practical examples show server- and client-side security and checking. Change management is introduced in this chapter to help explain why unauthorized changes to code and DB are not allowed and must follow an approved change management process.

Chapter 11: The Unseen Back End: This chapter discusses stored procedures in the back-end DB and how SQL code can be stored on the DB to run queries rather than creating plaintext queries on the front end then passing them to the DB. Stored procedures offer better security and can be easily embedded into many high-level programming languages.

Chapter 12: Securing Software—In-House and Vendor: Requirements to test in-house-developed software and vendor software are different and each should be tested separately to avoid any vulnerabilities. This chapter discusses the SAST tools available and what the tests show. It also shows why patching and software updates are required and should be done as soon as they are released.

Part IV. Security Administration

Chapter 13: Security Administration: The "need to know" and "least privilege" along with clearances given to subjects are discussed in this chapter. Change management is touched on once more to show how the systems all work in tandem to allow only authorized changes. Legal liabilities are discussed in detail as well the benefits of being proactive in maintaining security.

Chapter 14: Follow a Proven Path for Security: A proven path for achieving security in the DB and application is to conduct around-the-clock monitoring after implementing security controls. Proven path includes testing regularly with various tools and conducting audits. Operational security is discussed in this chapter.

Chapter 15: Mobile Devices and Application Security: Mobile devices pose a new threat as they are now widespread and used everywhere. Wi-Fi security, user privacy, and cryptography's role in these devices are discussed in this chapter along with sandboxing and the NIST's directions for mobile devices.

Chapter 16: Corporate Security in Practice: This chapter discusses each aspect of corporate security in detail—physical, software, hardware, and others. It covers how new employees are onboarded and an existing employee can renew their credentials. Attacks and losses are explained, as well as how an organization can recover from an attack. This chapter covers "lessons learned" and how to document the details after an incident materializes.

Contents

Foreword

The computer industry has exploded in a way nobody probably imagined. Along with that explosion came hackers, who utilize the same technology to steal information and cause immeasurable harm. Initially, hackers used viruses to create havoc, either for fun or financial damages. Now, they use innovative methods such as ransomware to lock systems and demand money in huge sums. We are at a point where we do not know what comes next in terms of these exploitations. All we can do is to check our risks, mitigate them to our best possible effort, and do continuous monitoring. By keeping our eyes open for the new threats, we can be better prepared. As you will read in this book, there is no single foolproof method to securing an application of a database. The method to secure these has been, and should always be, a multi-pronged defense method. This is known as defense in depth—employing various possible actions that can detect or even stop an attack.

For this reason, security must start from step zero and should remain a high priority throughout the life cycle of a software or database. In this book, database and application security are discussed in a practical way. Change management, running STIG tests, audits, and creating lessons learned documents are all very important in creating a suitable and secure posture for an IT organization. Each branch of IT, be it networking, operating system, coding, designing etc., has to worry about the security of IT to create a good security posture for the application, DB, or the organization at large. When resources are available, it is also important to isolate DB and application servers.

In the end, security is everyone's responsibility and cannot be achieved by one person. For this reason, we often hear the phrase, "If you see something, say something." Bystanders, or those who think "it is not my job to report," are essentially responsible if they ignore a threat after seeing one. Insider threats are equally dangerous, if not more so, because a disgruntled insider may have more "inside information" that they can pass to others and exploit.

The methods discussed in this book to achieve a good security posture in an organization are only what are known to this day. In other words, this is the research we know now and are currently implementing. We must evolve with a continuous learning curve and implement new methods as hackers and attackers come up with newer techniques to exploit. These methods will continue to get more complex since servers can host more than a simple database and one application. Migration to the cloud is catching up to us too and anything that is transferred to a cloud platform is always considered to be at risk. Mobile devices such as smart phones and tablets will further evolve and all we can do is go with the flow and adapt to new technologies, new threats, and new challenges.

Cybersecurity is both a very challenging and very fun field to work in. The ultimate law to excel in this field remains to be this—keep your eyes open, learn continuously, adapt, and grow with the field. Whether you are an application developer, DB coder, DB administrator, or system administrator, this book will help you achieve a strong security posture in your organization. But remember that cybersecurity is a security posture that can only be achieved by working with everyone around you. The first line of defense in security is YOU.

Godspeed in learning the details of cybersecurity!

Introduction

After working in the IT field for over 20 years, the idea to put into words what I have learned took shape. I started creating my own lists of "to do's" while developing a DB or an application. These to-do lists started to become large and routine processes due to developments in the IT field. Certifications such as Sec+, CISSP, and ITIL have become mandatory requirements in various organizations for developers, DB, and system administrators. After working with various people who implemented security religiously and those who ignored the security part with equal vigor, I felt it was time to put my to-do lists into the form of a book.

The result is the book you have in your hands. Since security details need to be mentioned before they are implemented, the first section goes over the fundamentals of cybersecurity. As you will read in this book, security is never a one-person job. Therefore, after discussing DB security and application security, I added a fourth section on security administration to give details of corporate security in action. All aspects of security are discussed in the last section to give the reader an idea of how cybersecurity aligns with corporate security, IT security, and physical security.

Who Should Read This Book?

This book is for IT professionals who want to learn how to secure their DB or their applications with a multi-pronged stature. System administrators can use this book in securing their hosts, creating firewall rules, and hardening the IIS side of hosting an application. The book might be helpful in learning security of software and DBs and may help with Sec+ and CISSP certifications.

The book should be used at every stage of the software or DB development process to create a strong cybersecurity posture. It also helps in learning the fundamentals for an aspiring student in IT and cybersecurity. The book touches on both Oracle and SQL Server software. Any programming language security can be achieved with applications by incorporating the methods discussed in this book. Students can learn about change management and its process before they enter a corporate environment. Parts of the book also discuss steps for taking care of mobile devices and BYOD at an office. This book could also be used for a general audience to understand the attacks that exist in DB and applications and learn how to prevent those attacks.

How This Book Is Organized

It is recommended that this book be read cover-to-cover to learn about various routes of cybersecurity for DBs and applications that are hosted on Linux or Windows servers.

The book is divided into four sections:

Part I. Security Fundamentals

Part II. Database Security—The Back End

Part III. Application Security—The Front End

Part IV. Security Administration

Parts II and III discuss the security details for DB and applications. Since security cannot be achieved by one single person, Part IV discusses the security administration with the change management process. Various administrative functions—creating roles, granting privileges, and the related paperwork—are included in Part IV. Most of the references are from NIST and organizations such as Microsoft and Oracle. The examples given for Linux were run on the open-source free Linux and express editions of the software from Microsoft, Oracle, and others such as OWASP, Autopsy, etc.

At the end of each chapter, there are chapter-specific questions and answers to those questions to test the readers' understanding. It is recommended that the readers get an account with a cloud provider such as Google or Microsoft Azure (free trial and then very cheap for using on a monthly basis) to create a virtual machine to install free software (SQL Developer, SQL Server Express Edition, etc.) and test the scripts given in this book for hands-on experience.

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets [ ] indicate optional elements.
- Braces { } indicate a required choice.
- Braces within brackets [{ }] indicate a required choice within an optional element.

Acknowledgments

I'd like to give special recognition to Mr. James Manly at Pearson for providing me the opportunity to put my ideas into writing. When I was working with him on cybersecurity testing questions, we had a casual discussion about the idea of a book where I mentioned that many coding professionals either do not know or just ignore the security aspect in databases and application coding. He encouraged me to put up a synopsis and gave me ample time to write, edit, and bug him at will about the book, the writing topics, and the style. We have developed a great relationship over the past four years and the credit entirely belongs to him.

In my professional life, there are countless individuals who willingly taught me their knowledge, shared their expertise, and allowed me to scale their shoulders to look beyond what I knew. All my current and past employers have been incredibly supportive and gave me opportunity to learn the idea of a "solution-oriented" approach. It would be impossible to repay them with anything in return. As much as I want to thank the people I wanted emulate, it is the group of people, who taught me how *not* to behave, that needs my special thanks. Again, I thank both these groups of people. You made my days, weeks, months, and life a classy one without comparison.

A big "thank you" goes out to the production team that worked tirelessly on this book: Eleanor Bru, Cindy Teeters, Jayaprakash P., Mary Roth, Donna Mulder, and Charlotte Kughen. They have been incredibly professional and a pleasure to work with. I couldn't have asked for a better team than the one at Pearson.

About the Author

Dr. R. Sarma Danturthi holds a PhD in Engineering from the University of Memphis (Memphis, TN) and works for the US Department of Defense. He has several years of experience with IT security, coding, databases, and project management. He holds Sec+, CISSP, and PMP certifications. He has also taught undergraduate and graduate-level courses in Engineering and Information Technology at Marquette University and Gallaudet University as an adjunct professor. He has been a subject matter expert in editing/reviewing IT security books for Pearson, CompTIA, and ISC2 and created test questions for CISSP, CISA, CISM, and CEH certifications. He has published several peer-reviewed papers in engineering, project management's PMI's knowledge shelf. He is the author of *70 Tips and Tricks for Mastering the CISSP Exam* (APress, 2020).

Chapter 1

Basics of Cybersecurity

Cybersecurity

The earliest computers, such as the ZX-Spectrum or the original Apple computer designed by Steve Jobs and his colleagues, didn't require login information or user credentials. Anyone could just switch on the machine, open a word processing application, type, and print. Most of those standalone machines did not even connect to a network. At that time, the only thing people wanted was a machine that could print a document and play a few funny games.

The languages used were simple, too—BASIC, C, and so on. Some systems used mostly by government organizations had huge machines called mainframes that ran languages such as FORTRAN and COBOL. A few database programs, such as DBase III and DBase IV, existed. For a desktop computer user who wanted nothing more than a word processing program for documents and a couple of games, all these extra language features did not exist, were neither required nor known.

If you asked most people about computer security in those days, the only answer you would get was about the physical security of the machine in the office or home. Personally identifiable information (PII) such as Social Security Number (SSN) and date of birth did exist in some files, but nobody gave a second thought to losing that information or otherwise finding that it had been compromised. Universities even printed the SSNs on students' primary ID cards. Once in a while, a smart aleck stole credit card numbers in postal mail and used them, but the instances of extensive fraud—like what we have now—were rare.

Then came the era of Windows, Windows NT, and networking. The number of computing machines and the desktop machines exploded. Thanks to the ever-changing and improving technologies, the mainframes that occupied several thousand square feet of physical space slowly gave way to smaller units. As the explosion continued, hackers and attackers have found new ways to steal and smarter ways to dupe users to compromise

a single system, a segment of a network, or even a complete network. To counter these attacks or hacking attempts, corporations have started reinventing their systems, reconfiguring software, and updating the login procedures for single computers and networks.

Along the way, new words like *phishing* and *whaling* have been introduced to identify the fraud. Even as governments and computing corporations were busy inventing new antifraud protection and technologies, hackers were getting smarter, too, and they used the same new technologies to invent worse methods to hack and steal. In the early days of Windows, Bill Gates even invited hackers to attend a meeting to share their methods in the hope that Microsoft could design software to avoid those attacks. At one point, people predicted that hacking attempts would end by a particular year, but so far, nothing has stopped hackers. They continue to come up with innovative ways to breach security. New hacking techniques, such as ransomware attacks, continue to be developed and make us wonder when, or even if, these attacks will end.

Although you may be happy with your systems and software with their increasing speeds and evolving technologies, you should never forget that someone is always watching what you do—even if the system is in your bedroom and not physically accessible to anyone. Shopping, checking for an address, finding out where to order a pizza, and almost everything else is online and uses the Internet. The cable that connects your computer to your Internet Service Provider (ISP) is not even required any longer because of the availability of Wi-Fi networks. We now also have more threats than before because most people carry phones and mobile devices such as tablets.

Before we delve deep into attacks, countermeasures, and cybersecurity, let's first talk about a few important terms in cybersecurity. In this chapter, we touch on the basics of cybersecurity: the terms, fundamentals of guarding the data, what to guard, how successful we can become in guarding, and how we can independently decide if the guards we deploy to counter the threats are really successful.

CIA-DAD

Before 1998, the United States Air Force came up with the concept of confidentiality in computing. After several iterations, they introduced a refined model of CIA-DAD to adequately cover topics of current day cybersecurity. But with the cyberattacks becoming increasingly numerous, we needed a set of rules for good security practice in the computer industry. Thus, the first Parkerian Model of six factors, or Hexad, was developed in 1998. The general consensus is that these are the rules for now but they'll continue to evolve as attackers and hacking attempts evolve. We can minimize the risk but may never really eliminate cyberattacks or the risks associated with hacking attempts.

Let's turn our attention to security fundamentals and the elements of the CIA-DAD triad (Figure 1-1).

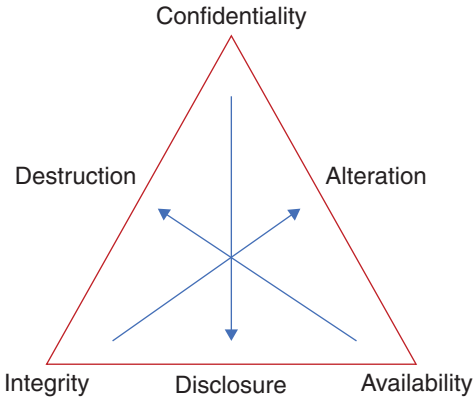

Figure 1-1 *CIA-DAD Triad*

Confidentiality

According to NIST, confidentiality is "preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information."

This term dictates that the data, service, or information is provided in a secure way. It does not mean that the information or data is provided to everyone who requests it. The information is provided to those who need it or who have a "need to know." Once such a person requests information or data, their credentials are verified. After credentials are confirmed as currently valid, the data or information is given to the person. For confidentiality to happen, the user must sign a document known as a non-disclosure agreement (NDA), as well as any other documents an organization requires.

The opposite of confidentiality is *disclosure*, which means the data or information is disclosed to everyone without the need to check their credentials. Once information or data falls into the wrong hands, anything can happen, including problems associated with lawsuits and a flurry of financial troubles.

Integrity

Integrity demands that the service is providing the data or files in the original format without any modifications. When modified, the information can become useless or sometimes even harmful. For example, imagine your blood test or other medical test data is available from a lab to your physician. If one or two numbers have changed in the report sent to the physician, the results are inaccurate, which can cause alarm to the patient. Therefore, data transmission—electronic or otherwise—must be correct, accurate, and unchanged. As with confidentiality, the information or data is provided to "need to know" persons. Integrity of electronic transmissions is achieved by adding a hash to files and providing additional metadata.

The opposite of integrity is *alteration* or changed/corrupted data.

Availability

Usually, service providers such as cloud providers or Internet service providers offer some promise for their services, such as whether the service can be provided 24x7x365 or is more limited during some periods like holidays. Availability demands that during the mutually agreed times, data is available without delay. Some information is available at any time of day (hospital service, medical data, websites selling products, and so one), but other information is provided only during office hours (for example, medical billing and auto repairs). Some information is also available via self-service, which means a person can go to the data or information source (online or offline) and use proper credentials to obtain information at any time. For this type of service, it is assumed that the service provider keeps their website active all the time. Amazon.com shopping and Netflix streaming are examples.

The opposite of availability is *destruction* or that the information is not available when requested.

Note that when any one of the three factors is maintained, the other two factors come into play as well. When a service is available, the information is provided confidentially to those who have a need to know, and the provided data is unchanged and is in the original required or requested format.

I-A-A-A

Another important concept in the cybersecurity field is identification, authentication, authorization, and auditing/accounting (IAAA). These words have a lot of significance because if security is weak on a network, anyone can log into the system and hack the data from the files. Identifying a person who has a "need to know" and letting that identified person confirm who they are before giving them access to the files or data are important processes. Earlier technologies allowed anonymous logins and file transfer protocols (FTP), and they were misused greatly to hack important data files, passwords, and such. Then came IAAA, which is described in detail in the following sections.

Identification

Identification refers to finding out who is the person trying to log in to a server or system. Does the person physically exist or is it an anonymous user or an automated program trying to log in with a stolen username and password?

Identification in an organization can usually be done with a corporate ID card or some other credential issued to users after verifying proper government-issued documentation, such as a driver's license, passport, or SSN, and establishing an NDA policy between the issuer and the user. Several other types of physical identification can be issued, such as an access card with a chip or simple picture ID. In the past, identification cards used to have the user's PII, such as SSN, printed on them, but with the increase in cyberattacks based on PII, SSNs are now replaced by random-number employee IDs.

This kind of physical identification falls into the class of *what an employee/user has*.

Authentication

If an employee/user is able to demonstrate with proper identification who they are, next is the step of *verifying or validating that user* to make sure the user indeed exists and the presented identity belongs to that user. This can be done by a human guard stationed at the entrance to the facility or asking the user to supply a personal identification number (PIN) or some other form of proof. Access cards usually require a code of at least four digits to be entered. The code is matched with the issued card to confirm the user's identify and allow the user to log in. In some cases, a second form of authentication is used or required for better protection. A system with this additional step is known as multifactor authentication (MFA). One example is sending a text message with a one-time password/PIN (OTP) to the user's registered phone number. The OTP is valid only for a few minutes and cannot be reused. Any mismatch between the number sent and the number entered results in a refusal to confirm the identity of the user. To prevent damage to the system, the user is disallowed or the account is locked after a few unsuccessful attempts.

This kind of authentication falls into the class of *what the user knows*—a PIN or another number that confirms the user's identity.

Authorization

Once the user has provided proper identity and it has been confirmed and authenticated, a user is allowed to successfully go into a facility physically or log in to a system or network. Now it's a question of what the authenticated user should be allowed to view, read, or write. Or what access should a logged-in user be allowed?

The access allowed to a logged-in user with proper identity and authentication is known as authorization. Authorization depends on what the user really needs to know for their day-to-day work. Simply because a user has a proper identity and has provided proof for authentication, they are not necessarily permitted full access to everything. In other words, users are given access according to the rules of least privilege, which means a user has the access required for their work—nothing less and nothing more. It also means a user may not have administrative privileges to enter a server room physically or go to a system registry to modify settings or install a new program.

Authorization can be given uniformly to all users or at branch/department level as required. Any special authorizations need paperwork completed, background checks done, and signatures taken.

After access is granted, users who log in or enter an area can do what they like—though we expect the users to do what they are only authorized to do per organizational policies. For example, a user who is allowed access to a facility can go to the printer area and collect printed material that does not belong to them or log in to any computer that is not allotted to them in their workspace. Thus, there remains another step to find out what the properly identified, authenticated, and authorized person is actually doing—which is discussed in the following section.

Auditing or Accounting

Tracking what a user does with their given permissions is known as auditing or accounting. Accounting and auditing are done by examining the log files or recorded actions of the user. In a physical building, the recording can be done by a video surveillance camera or the software that records entry and exit times.

Note that the auditing by a third-party person who is not affiliated with the organization is preferred to auditing by a user who works for the organization. By hiring a third-party auditor, any favoritism or partiality can be easily avoided.

Regular reviewing of logs and physical access records demonstrates how a user is correctly using their authorizations and not "moving" vertically or horizontally crossing their given boundaries. When auditing or accounting raises any red flags, the authorizations of users need to be readjusted, and employees are warned of their encroachments into security. Likewise, the organizational permissions or conditions that allowed the user to cross their boundaries—for example, drive or file permissions that allow anyone to read or write—are adjusted not to allow the users to access the files or data.

Defense in Depth

Defense in depth is the term used for employing defense or security for protecting information with multiple controls all the way from the top level to the very bottom level to make sure that the data or information remains safe. The National Institute of Standards and Technology (NIST) defines *defense in depth* as "The application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering heterogeneous security technologies, methods or controls in the common attack vectors to ensure that attacks missed by one technology, method or controls are caught by another."

Defense in depth tells users that security needs to be employed at every level so that if security at one level fails, it may be able to catch the intruders at another level. In the corporate world, defense in depth is employed by various means. Physical controls or videos monitor users' entrance and exits, computer log files record the users' login times and actions, programs prevent users from installing unnecessary software, antivirus programs prevent installing or copying of virus files, email programs require identification and verification via public key infrastructure (PKI), and the data or server rooms require users to have an additional access card that is issued with further security clearance. Governmental departments used to give a security clearance by checking the users' activities once a year or so, but as of the beginning of 2020, security clearance is a daily process of tracking users' activities on the Internet in general and on social media websites such as Facebook, Snapchat, and TikTok. Thus, defense in depth works in tandem with a continuous process of tracking a user. Security has no end point or phase because hackers and intruders continue to invent new methods to compromise security as the technology provides newer machines, facilities, and equipment.

Hardware and Software Security

The first line in defense of cybersecurity is always the user (or YOU). Hardware and software come next. Although the two things work independently, they are indispensable to each other.

Hardware security has two parts: individual system security and wired or wireless network security. Individual system security depends on the type of processor, the programs used, and the basic core safety of the operating system that runs with the processor. Known vulnerabilities of a processor, memory chips, and even the additional drive or disks attached to a system are all causes of worry in terms of security. Systems we use at home are connected to our ISP's network either via Wi-Fi or a wired connection. Wi-Fi requires a router and modem, which need to be secure with good passwords to limit or prevent any hacking attempts. Loose and easily guessed or default passwords are a cause for concern. The protocols (WPA, WEP, TKIP, and so on) we use for setting up the Wi-Fi router need to be looked at closely. Likewise, a lack of a firewall on these hardware devices can also make it easy for a hacker to break our individual networks.

Networked systems have their own problems with open ports, default passwords, switches, hubs, the router, balancers, and so on. If the organization maintains its own web servers, how secure are they? How secure are their server and ports? Are there some ports open, or do they allow anonymous logins? If the organization is expecting a large traffic flow on their web server, can their single server manage the traffic or would it need a load balancer to control the traffic? Usually a trusted computing base (TCB) is established with a standard setup for all users. This baseline setup decides which programs are given to the users by default (for example, Word, Excel, Outlook) and which are not. TCB usually consists of fully vetted end-user machines, application servers, web servers, database servers and clients, and so on.

Software security has two distinct problems: bugs arising from bad code are either syntactic or semantic errors and problems from attacks such as SQL injection, bad software design, and memory leaks. Poor coding with errors, weak cohesion and strong coupling between modules, not scanning the software, not testing the software for bugs, and regression errors are also causes of concern in software security. Logic bombs introduced purposefully by disgruntled employees are hard to find, but code reviews can clear those errors.

In general, software security must be included right from the design stage all the way to the very end of deployment in the software development life cycle. If the organization is developing software in-house, how good is the development team with security? Or if the organization is purchasing the software off the shelf, is the third-party software good enough? Is it tested to withstand a vulnerability-based attack? Does the third-party software get regular updates, known as patches and service packs, to fix any vulnerabilities? These factors need to be taken into account to avoid any hacks. A security reference monitor, part of the operating system, usually allows for logins and access between users and systems and the associated log files for auditing.

A generic developmental cycle in software has three different machines or environments known as development, test, and production servers. A programmer writing code or checking a new third-party software to be purchased is only allowed do these things on the developmental machine and servers. Once development is complete, the code in executable form is transferred to a test machine, where an independent tester takes the lead to check functional requirements of the program. Once development and testing have passed, a code review might be conducted to remove any logic bombs or some possibly visible semantic errors in code. At this point, additional security tests for vulnerabilities are performed. Only after these successful phases is the program deployed on the production server.

Firewalls, Access Controls, and Access Control Lists

Firewalls and access control lists (ACL) are either software or hardware. Firewalls have rules that can be set up, edited, or changed depending on the requirements. While blocking traffic, ACLs allow some traffic based on a routing table or some other rule. A default firewall rule that allows all traffic should always be at the bottom of a rules list after filtering out most of the traffic with various other rules. However, you have to make sure the rules are set up rather than assuming that they are already set up. Setting up rules alone would not complete the security of a system or software. The gist is to check the firewall logs on a daily basis to find any activity or noise that is trying to cause any trouble.

ACLs are a set of inbound and outbound rules defined for controlling network traffic to grant or deny access to certain digital environments such as files and networks. ACLs use this set of rules to filter traffic or limit user access.

ACLs are mainly two types: filesystem ACL and networking ACL. Filesystem ACL limits access privileges to files and/or directories, and they work at the operating system level to tell which users can access the system and files and what they can do with those files (read/write/execute). Networking ACLs work on the computer network that contains routers, switches, and other equipment, and they decide which type of traffic can flow on the network and which activity is denied (implicitly or explicitly). In either type of ACL , a log is created when a user tries to access the resources. The log is helpful for the system administrator to check what is happening on the organizational files and network resources.

An organization dealing with various products can also implement an ACL in their offices for physical access. Physical access is decided by the clearance levels required to access an asset (“the need to know”). For example, even the most experienced programmer who worked for 10 years in an organization may not need to enter the data room where the physical machines are stored for data storage. Likewise, most employees don’t need to access a plenum space in an office, prohibited areas, print servers, or the fire/water safety controllers or the HVAC room. These factors of who can access what is usually decided by the company, with least privilege and need-to-know rules depending on the policies set by the company’s data custodians and its CEO.

Physical Security

Next comes the importance of physical security. Does an organization allow all people to come and go freely into the building? For example, university buildings allow anyone to enter and exit during office hours. There were several reports of panhandlers entering a university building during office hours to steal food and lightweight equipment. In those cases, security wasn't very tight.

Physical buildings also need security from physical attacks by road traffic, which can be handled by installing barriers, placing guards at the entrance, and so on. Contractors or people claiming to be contractors can be a threat when they drive into the office facility in a large truck loaded with explosives, as happened in the bombing of Oklahoma City's Alfred P. Murrah Federal Building in 1995. Video surveillance cameras, recorders, and rotating gates or doors help slow the traffic and avoid piggybacking. Advanced controls with biomedical equipment also provide extra security. Data rooms with automatically locking doors and emergency lights on power failures are important to consider.

If an organization has an office in a state like California where there is a greater threat of earthquakes, floods, and heavy rains, proper physical guards need to be in place to ensure safety of the personnel, assets, data, other equipment, and the office building itself. The design of physical security needs to anticipate even things that may happen without warning, such as pandemics like the spread of COVID-19, because using VPN for virtual offices or teleworking will be the norm sooner or later. In these cases, proper digital or physical signatures are necessary for better safety of both the employees and the organization.

Users are a primary contributor to the downfall of security. It doesn't matter how much cybersecurity is implemented by an organization and how smart the programs employed are if the users aren't vigilant. This is the basic reason why the first line of defense is always YOU.

It is important that you keep your eyes open at all times to make sure you know what is happening around you and report any suspicious activity. This is known as "if you see something, say something" rule. When an organization employs a person and gives access to that person, they assume that employee is honest and will follow the mutually agreed upon rules. The organization also assumes that the employees follow the rules they read and sign in the NDA. Employees, contractors, and vendors entering the facility have to apply due diligence and not allow piggybacking and misuse of resources and assets.

Everyone has a role to play in security, although the CEO, chief security officer, and information and protection security officers often get the blame when something goes wrong. However, each of us is an equal stakeholder, and we need to practice, advise, and learn every day about unexpected attacks and contribute to help the organization. We should remember that objects/assets (what) have permissions (how), and the users (who) have rights (how). These terms mean we design a secure environment for how assets/objects use permissions or how the objects and assets are used and what rights a user has when accessing a resource—IT or otherwise.

No matter how hard a corporation tries to help with security, users have a limited memory and can only remember a few things on a permanent basis. Therefore, it is very important to train employees regularly about security, including active shooters, terrorist attacks, natural disasters, and fire drills. Training helps people remember what they've learned when an attack actually happens. Training also should be enforced with strict rules, and it is important to remove both computer and building access from employees who do not follow the policies of training and retraining.

Practical Example of a Server Security in an Organization

Let's consider an example of how corporate security is set up. Tables 1-1 through 1-5 illustrate how we can set up layers of security to achieve defense in depth. Each layer has an extensive framework of rules and regulations that must be followed. Though each layer is cohesive and acts independently, all units in a corporation work with each other with a common goal of a highly secure environment because security is everyone's responsibility. Note that this is a simplified example and can expand and shrink depending on the size of the corporation, needed security, the location of the site, and many other factors—both locally and on a larger scale.

Table 1-1 *Physical Security Aspects in an Organization*

Item	Why Is It Important?	Remediation
Gate and door entries	Avoids forced entries and piggybacking, helps block unwanted intruders.	Implement access cards with a PIN, station a guard to check manually.
Server rooms	Protection of servers, data, and personnel.	Implement additional card access, closed doors at all times.
Lock and key for files or records	Corporate data protection, theft of PII.	Use locks and keys and advise users to always lock unused cupboards or overhead storage bins.
Computers, printers, phone, or fax	Equipment is expensive and valuable for daily work, and it isn't easy to replace.	Buy insurance for equipment, locks and keys with a chain, electronic lock protection.
Fire and smoke	Danger for all working people, suffocation, hardware parts can be damaged from change in humidity levels.	Install alarms, avoid storing flammable and unapproved items in office.
Lighting inside	Bad lighting can cause physical eye problems for employees and may encourage theft.	Install adequate lighting, automatic lighting that turns on and off when people enter and exit premises.

Item	Why Is It Important?	Remediation
Inventory and storerooms	Missing or stolen equipment can be a problem. Bad log records cannot trace inventory—who is borrowing what from the inventory and where the equipment is used and to whom it is allotted.	Use closed-circuit cameras, video and audio recordings, up-to-date logs/records of equipment being checked in and checked out with proper signatures of customers.
Door locks/blind spot mirrors	Dangers of being locked in or out or having secure doors unlocked due to power failures, shootings, and other dangers to human lives.	Make sure the correct type of doors are installed. Regularly check mirror and video camera (pan/zoom) alignments.
First aid kits and emergency supplies	Not being installed, or regularly checked, or not restocked results in danger to human lives.	Check regularly, update with portable pacemakers. Educate employees how to use them.
Alternate sites	If not up to date, disaster recovery is difficult. Data can be lost. Can result in financial burden.	Keep data up to date on all alternate sites. Check regularly with a tabletop or live exercise.
Other physical assets	These help run the business smoothly.	

Table 1-2 *Software Security Aspects in an Organization*

Item	Why Is It Important?	Remediation
Software copies, if any (repositories)	Lost copies are hard to restore. Can fail an independent audit. Loss of copyrights and possible duplication.	Install software repositories, update and maintain copies by version regularly. Save hard disks or USB drives with software copies. Label drives correctly.
Removable media	Loss can cause data loss and financial penalties, jail time, and other repercussions.	Protect data in transit and at rest. Maintain a secure safe and bank for removable media.
Firewalls	Weak or default rules can allow viruses and malware to get in.	Update/create firewall rules, update software, watch the logs daily.
Development/test copies	Loss can destroy basic software design idea, requirements, testing rules, and results.	Maintain separate repositories by version, check repositories for safety regularly.

Item	Why Is It Important?	Remediation
Production copy	Loss can result in financial doom and piracy. Hard to recover and involves lawsuits and lengthy legal processes.	Maintain separate repositories by version, check repositories for safety regularly. Patent or copyright the software as required.
Antivirus	Not installing up-to-date protection and new patches leaves software vulnerable against new viruses and attacks.	Choose good antivirus software, update regularly with patches, watch logs daily.
Log files	Loss of log files or not maintaining time synchronization can result in attacks being ignored.	Create code to send email to system administrators when there is any log file change. Track daily.
VPN, networking software	For teleworking and remote personnel, VPN should be up to date with enough connections and security to prevent risk loss/theft of data.	Update the software. Install patches. Invest in a good software package with signed contracts.
Trusted baseline image	Users install unnecessary software, exposing more vulnerabilities. Trusted baseline image allows least privilege uniformly across all machines.	Create the baseline after all tests are complete. Update accordingly but keep checking individual machines randomly and warn users about excess privileges.
Data and other PII files	Loss of data can derail a corporation with a flurry of problems from law enforcement, government, and lawyers.	Maintain due diligence and due care; keep security up to date, watch data in transit, at rest, and in use. Take all precautions as required per local and federal laws.
Other software assets	Vendor supplied, in-house software is hard to replace and may need more spending.	Keep vendor contracts up to date. Maintain all assets per regulations and expect the unexpected to happen and be ready.

Table 1-3 *Hardware Security Aspects in an Organization*

Item	Why Is It Important?	Remediation
Laptops and desktops	Loss, degradation, replacement, and updates are expensive, time-consuming, and need several hours of labor/contracts.	Keep equipment locked with physical locks and keys. Obtain and maintain up-to-date signed agreements from users for accepting the equipment.
Cables, bricks, and chargers	Loss can result in a minor financial burden. These also often need replacement due to heavy use.	Be ready with additional inventory for replacement, for non-functioning or burned out units.

Item	Why Is It Important?	Remediation
Access card or other readers	Unauthorized access can result in various issues like tampering with email and files. Access should be only for permitted and approved users who sign NDAs. Card readers and associated software must be up to date.	Lock systems when not used with access cards or passwords/PINs.
Printers or plotters	Important papers can be stolen. Printers/plotters/supplies are at a risk for damage/theft.	Allow printer access with access card or login only. Use chains and locks for expensive printers/plotters and supplies.
Special phones	Video phones and VOIP are hard to set up, are expensive, and have messages stored in memory. People with disabilities may use special phones that are very expensive.	Install good versions; maintain and update software required regularly. People with disabilities may need extra care of their communication equipment.
Office supplies	Though sometimes cheap, some are expensive, such as the plotter supplies, ink, and cartridges.	Track with logs who is using what and check logs regularly of the needed and depleted supplies.
Servers (DB, network, and so on)	By far, these are the most expensive to replace or buy new. They also need special software.	Invest in a separate team that works on these machines and their security.
Routers, modems, and so on	These network components are the bread and butter of the network.	Should regularly be checked and updated. Logs should be read daily for any possible trouble and malware attacks. Passwords should be enforced and maintained with strict corporate password policies.
Other hardware assets	Hardware will continue to evolve and need investment to keep pace with the future.	Update as required, but do take care of data on older hard disks and other devices and follow corporate policy for data protection, preservation, and destruction.

Table 1-4 *Network Security Aspects in an Organization*

Item	Why Is It Important?	Remediation
LAN/WAN	Broken network inhibits data flow and causes financial losses, data loss, and innumerable other related issues.	Invest in good networking infrastructure and topology and update regularly.
Antivirus	Not installing up-to-date antivirus protection and new patches does not protect against methods of attack. This software is different from normal antivirus software installed on each machine.	Choose good antivirus software, update regularly with patches, watch logs daily.
Firewalls	Network firewalls, routing tables, and other safety features need to be updated regularly to avoid loss or theft of data.	Implement firewall rules, update regularly, and watch the logs.
Other network security	Networks will continue to evolve and need investment to keep pace with the future (fiber optics, new topologies and networks, and so on).	Update as required and follow corporate policy for data protection, preservation, and destruction.

Table 1-5 *Environmental Security Aspects in an Organization*

Item	Why Is It Important?	Remediation
Barriers all around the building	Vehicles can ram into a building or crash, either accidentally or intentionally.	Barriers protect the building from severe damage. Orange or red paint warns users to stay away and not to park around these items.
Surroundings	Dark, empty, dimly lit surroundings are a cause for concern for attacks, theft, and shootings.	Install light fixtures (solar powered, auto shut off) around the building. Alarms should be available to be activated in case of dangers. Regularly check the alarms and make sure they work through all seasons of the year.
Roads to the building	Clear and drivable roads without potholes or thick plant and tree growth on either side. No long and winding roads.	Visibility should be clear with straight roads without hindrances. Regularly check and re-surface.
Video surveillance	Serves as evidence or proof in a court of law. Can record very important information without human interaction.	Adjust pan and zoom of the camera, examine the recordings daily. Update broken lenses, dysfunctional cameras (due to weather or otherwise).

Item	Why Is It Important?	Remediation
Fire extinguishers	Help control fires and save human lives and equipment.	Should be examined, updated, or replaced per local fire department laws—usually once every six months or year. Work with the local codes and regulations to update.
Water sprinklers for fire	All rooms must have functional sprinklers to save human lives and buildings in case of fire.	Test these regularly, replace dysfunctional units and update.
Natural disasters	These are unexpected and unavoidable but risk and damage can be minimized with proper plans.	Buy insurance for these events; establish a chain of command to make sure all human lives are safe.
Unexpected attacks	Terrorist or pandemic attacks cannot be expected ahead.	Be prepared for active shooters and terrorist attacks. Train employees regularly.
Physical safety	Human life is irreplaceable and the first priority. Ensuring physical safety reduces financial burden on the corporation.	Establish a chain of command; train and retrain users regularly, conduct tabletop exercises to make sure all human life is protected.
Parking lot/signs/fences	Fences, signs, and lot numbering help users find their vehicles; they also discourage intruders from entering the premises and otherwise help with safety.	Posted signs and warnings should be stern and clear. Fences and borders should be checked regularly and damages fixed.
Other environmental	Rules can change from time to time and from county to county or state to state.	Discuss with local municipalities and counties/districts to see what is required to ensure safety.

In this book, we only discuss the database and software security in detail, but it is important to know that factors such as those listed in the preceding tables contribute to security for software and databases because a single lapse can directly affect databases or software regardless of whether they are small or big or developed in-house or acquired off the shelf. Remember, security is the responsibility of *everyone*. Failing to educate and train can be the fault of a corporation, but the fault rests equally on each person if they fail to report anything suspicious. As we previously stated, the rule in security is, "if you see something, say something." Sometimes following simple rules can make a lot of difference in our lives.

Summary

Cybersecurity is everyone's responsibility and has the basics of confidentiality, integrity, and availability. Secure access to assets is defined with the process of identification, authentication, and authorization. Once access is given to a user, they are audited for their accountability in their day-to-day work. Several layers of security are put in place in an organization with various controls to achieve defense in depth. Defense in depth helps in such a way that if one or more controls fail, another control can possibly detect a breach or threat.

Security considerations for hardware and software are different. Physical security of the hardware and software assets is important too. Access control decides who can access what assets in an organization. Access controls can be for files on an operating system, inbound and outbound traffic on a network, or physical access to buildings and assets. The roles of users are important too because a corporation decides what role each user is given and access can be dependent on that given role. In this chapter, we also demonstrated various aspects of security in an organization.

Chapter 1 Questions

1. What are the three factors of a security triad? What are their opposite factors?
2. If a company has lost all its data from repositories and cannot find backup copies, what factor or security triad does the company violate?
3. If an approved and authorized user requests a file and finds that the contents of the file have been modified, what security factor have the changes in the file violated?
4. Who is the best person to do accounting or auditing in a corporation?
5. Why is authentication required when a user can scan their identity card to enter a secure building?
6. What is the importance of logs in IT and cybersecurity?
7. When natural disasters are unavoidable, why should a corporation worry about them?
8. How should a corporation implement physical fire safety for its buildings?
9. Do corporations really save development, test, and production copies of software?
10. Who is ultimately responsible for security in an IT organization?

Answers to Chapter 1 Questions

1. Confidentiality, integrity, and availability (CIA). The opposite factors of the security triad are disclosure, alteration, and destruction (DAD).
2. Availability. Because all the data is destroyed, the company cannot supply information or data to legitimate users.
3. The integrity factor is violated because the file contents were modified.
4. A third-party independent, certified, and licensed auditor is the best person to conduct an audit. Such a person can ensure that the audit is frank and devoid of favoritism.
5. Authentication helps double-check the person as the genuine person who was issued the identity card. Usually this involves the user remembering a PIN or code to enter and a way to prove that the person who entered the PIN is indeed the person who was issued the access card.
6. Logs and log files provide entries and details of intruders, attacks, and the time of entry and exit. Examining logs daily can demonstrate details of who is entering with authorization and who is an intruder. Firewall, database, and network logs also show any entries to demonstrate excessive logins, denial of service, or attacks coming from external IPs.
7. It is true that natural disasters cannot be avoided but the first priority of any disaster is to save human life. Establishing a chain of command, training and retraining employees regularly regarding how to handle natural disasters, and contacting employees when a disaster strikes to make sure of their safety are all very important.
8. Fire safety can be achieved by installing extinguishers and a sprinkling system but you must also consult local fire departments to determine their codes and laws. The fire department can advise the best possible solutions to be implemented.
9. Yes, corporations really save their development, test, and production software copies separately on code repositories by version and subversion numbers. All are well documented in each environment.
10. Corporate cybersecurity is the responsibility of everyone, although CEO and security officers are the owners and custodians who take care of implementing the policies and rules. This is the main reason why corporate security follows the rule of "if you see something, say something."

This page intentionally left blank

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y-Z