Second Edition

CompTIA® CySA+

Guide to Cybersecurity Analyst

MARK CIAMPA, PH.D.

INFORMATION SECURITY

CENGAGE

Australia • Brazil • Canada • Mexico • Singapore • United Kingdom • United States

Second Edition

CompTIA® CySA+

Guide to Cybersecurity Analyst

MARK CIAMPA, PH.D.

INFORMATION SECURITY

CENGAGE

Australia • Brazil • Canada • Mexico • Singapore • United Kingdom • United States

***CompTIA CySA+ Guide to Cybersecurity Analyst*, Second Edition, Mark Ciampa**

SVP, Higher Education & Skills Product: Erin Joyner

VP, Higher Education & Skills Product: Thais Alencar

Product Director: Mark Santee

Product Manager: Danielle Klahr

Product Assistant: Tom Benedetto

Executive Director, Learning Design: Natalie Skadra

Manager, Instructional Design: Erin Doppke

Learning Designer: Natalie Onderdonk

Senior Director, Content Creation: Rebecca von Gillern

Manager, Content Creation: Alexis Ferraro

Senior Content Manager and Content Manager: Anne Orgren and Michele Stulga

Director, Digital Production Services: Krista Kellman

Manager, Digital Services: Laura Ruschman

Digital Delivery Lead: Jim Vaughey

Vice President, Product Marketing: Jason Sakos

Director, Product Marketing: Danaë AprilPortfolio

Marketing Manager: Mackenzie Paine

IP Analyst: Ashley Maynard

IP Project Manager: Nick Barrows

Technical Editor: Danielle Shaw

Developmental Editor: Lisa Ruffolo

Production Service/Composition: SPi

Creative Director: Jack Pendleton

Designer: Erin Griffin

Cover image Source: sollia/Shutterstock.com

Library of Congress Control Number: X X X X X X X X X X

ISBN: 978-0-357-67799-5

Cengage
200 Pier 4 Boulevard
Boston, MA 02210
USA

Cengage is a leading provider of customized learning solutions with employees residing in nearly 40 different countries and sales in more than 125 countries around the world. Find your local representative at **www.cengage.com.**

To learn more about Cengage platforms and services, register or access your online learning solution, or purchase materials for your course, visit **www.cengage.com.**

Printed in the United States of America
Print Number: 01 Print Year: 2021

BRIEF CONTENTS

TABLE OF CONTENTS

PREFACE

CompTIA® CySA+ Guide to Cybersecurity Analysis, 2nd edition, is intended to meet the needs of learners and professionals who are interested in mastering intermediate-level cybersecurity skills and knowledge. It is designed to prepare security analysts, threat intelligence analysts, and incident response handlers who will leverage intelligence and threat detection techniques, analyze and interpret data, identify and address vulnerabilities, suggest preventative measures, and effectively respond to and recover from incidents as they apply to an organization's data, applications, and digital infrastructure. Although there is no designated prerequisite, the *CompTIA® CySA+ Guide to Cybersecurity Analysis* is designed to build upon the CompTIA Security+ certification or equivalent experience. Those seeking to pass CompTIA's CySA+ certification exam will find the course's content, approach, and numerous projects and study questions especially helpful. For more information on CompTIA CySA+ certification, visit CompTIA's website at https://www.comptia.org/.

The course's pedagogical features are designed to provide a truly interactive learning experience and prepare you to face the challenges of cybersecurity. In addition to the information presented in the readings, each module includes the following:

- ***Cybersecurity Today*** opens each module with the details and explanations of a recent real-world cybersecurity event that introduces a topic in the module. This feature provides a real-world context for applying cybersecurity principles and skills.
- ***Grow with Cengage Unlimited!*** boxes throughout each module provide information for reviewing foundational topics and exploring the material presented in more depth.
- ***Two Rights & a Wrong questions*** at the end of every module section help learners with a quick assessment of the main points to ensure a complete understanding of the material.
- ***Multiple case projects*** are included in each module that direct learners into additional research and discussion of key topics of the module.
- ***On the Job case project*** concludes each module with a scenario of a challenging corporate decision that must be made based on the implications of a topic presented in the module.
- ***Knowledge-based assessment questions and hands-on performance-based questions (PBQs)*** that mimic those found on the CompTIA CySA+ certification exam are included in Appendix A. Many of these are presented in a scenario format to put the learner in a "you are there" setting when deciding which tools to use, why they should be used, and how to interpret and analyze the results. In addition, the answers to the Appendix A questions are found in a separate solution file so that learners can compare their knowledge and skills with the answers.

MODULE DESCRIPTIONS

The following list summarizes the topics covered in each module of this course:

Module 1, "Enterprise Threats and Vulnerabilities," looks at threats by exploring different types of attacks. In order for an enterprise to mount a successful defense, it must be aware not only of the attacker's threats but also of its own vulnerabilities. This module covers threats and vulnerabilities associated with technologies other than personal computers and data networks, such as mobile devices, embedded devices, and specialized devices.

Module 2, "Utilizing Threat Data and Intelligence," explores knowing both who the attackers are and how they attack. And because attacks continually evolve, it is also important to take advantage of all available threat intelligence information to know the very latest types of attacks and how to defend against them. This module also explores frameworks and threat research sources along with different modeling methodologies.

Module 3, "Vulnerability Management," focuses on a process known as infrastructure risk visibility and assurance, also called vulnerability management. Its purpose is to be an ongoing examination of the organization's security posture. This module looks at common vulnerabilities, how to configure vulnerability scanning tools, and how to report and remediate scan results.

Module 4, "Cloud Computing and Assessment Tools," introduces cloud computing and its vulnerabilities. It also looks beyond the cloud into vulnerabilities in software, infrastructures, and other assets, and explains the tools that can be used for assessing these vulnerabilities.

Module 5, "Infrastructure Controls," examines how it is necessary to direct influence over attacks through various methods of cybersecurity controls (countermeasures) that organizations implement to prevent, reduce, or counteract security risks. This module explores two broad categories of controls that relate to the infrastructure: infrastructure management controls and configuration controls.

Module 6, "Software and Hardware Assurance Best Practices," explores procedures that have been demonstrated by research and experience to produce optimal results and are used as standards that are suitable for widespread adoption.

Module 7, "Security Monitoring Through Data Analysis," looks at implementing proactive monitoring by using sophisticated data analysis tools. These tools can help detect attacks more quickly and enable defenders to respond promptly.

Module 8, "Security Operations," explores the enhanced automation that is becoming available to security personnel to streamline and speed up security processes. It also looks at a new change in philosophy about threat actors so that proactive security can be applied in seeking out and defending against attackers.

Module 9, "Incident Response Planning and Procedures," discusses how an organization can prepare for a cyber incident. This includes what type of planning is required in order to support meaningful communication, how the critical nature of data can be determined in order to protect it or respond if it is compromised, and what incident response procedures should be used for detection, analysis, containment, eradication, and recovery.

Module 10, "Responding to a Cyber Incident," looks at the steps that are taken in the aftermath of a cyber incident. These steps include identifying indicators of compromise on networks, endpoints, and applications as well as performing digital forensics.

Module 11, "Risk Mitigation," defines risk and explores methods for mitigating risks, especially through using policies, procedures, and frameworks.

Module 12, "Data Protection and Privacy," looks at the controls that organizations can use to protect data. It also discusses the topic of data privacy.

Appendix A contains tools for preparing for the CompTIA CySA+ CS0-002 certification exam. It provides knowledge-based assessment questions and PBQs that are designed to assess the test taker's skills in working with different cybersecurity tools.

Appendix B is a mapping of each CySA+ domain element, the module and section in which it is located, and how that material is covered based on Bloom's taxonomy.

Appendix C contains the answers to the "Two Rights & a Wrong" assessment questions.

FEATURES

To aid you in fully understanding cybersecurity analysis, this material includes many features designed to enhance your learning experience.

Cybersecurity Today. Each module opens with the details and explanation of a recent real-world cybersecurity event. This feature provides a real-world context for applying cybersecurity principles.

Module objectives. Each module lists the concepts to be mastered within that module. This list serves as a quick reference to the module's contents and a useful study aid.

Scenario-based practice questions. Practice questions, many of which are scenario based, help provide more of a real-world setting to help learners assess themselves.

Colorful illustrations, screenshots, tables, and bulleted lists. Numerous full-color diagrams illustrating abstract ideas and screenshots of cybersecurity tools help learners better visualize the concepts of cybersecurity. In addition, the many tables and bulleted lists provide details and comparisons of both practical and theoretical information that can be easily reviewed and referenced in the future.

Notes. Each module's content is supplemented with Note features that provide additional insight and understanding.

Cautions. The Caution features warn you about potential mistakes or problems and explain how to avoid them.

Cengage Unlimited cross-references. For those learners who have a Cengage Unlimited subscription, convenient cross-references to other publications with additional information on relevant concepts invite further study and exploration.

You're Ready prompts. At the end of each module, a "You're Ready" prompt appears that indicates the learner is ready for a specific project.

Key terms. Clickable key terms emphasize the core concepts of cybersecurity.

Module summaries. Each module reading concludes with a summary of the concepts introduced in that module. These summaries revisit the ideas covered in each module.

Two Rights & a Wrong. Each section of every module includes a series of questions that can serve as a quick self-assessment of the material. This helps to ensure a complete understanding of the material.

Case projects. Although it is important to understand the theory behind cybersecurity technology, nothing beats real-world experience. To this end, each module includes several case projects aimed at providing practical implementation experience as well as practice in applying critical thinking skills to the concepts learned throughout the module.

Instructor's Materials

Instructors, please visit cengage.com and sign in to access instructor-specific resources, which include the instructor manual, solutions manual, PowerPoint presentations, syllabus, and figure files.

Instructor manual. The instructor manual that accompanies this course provides additional instructional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional projects.

Solutions manual. Answers to the review questions, scenario-based practice questions, performance-based questions, case projects, and reflection activities are provided.

PowerPoint presentations. This course comes with Microsoft PowerPoint slides for each module. These are included as a teaching aid for classroom presentation, to make available to students on the network for module review, or to be printed for classroom distribution. Instructors, please feel at liberty to add your own slides for additional topics you introduce to the class.

Figure files. All of the figures in the course are reproduced on the Instructor Resource Site. Similar to the PowerPoint presentations, these are included as a teaching aid for classroom presentation, to make available to students for review, or to be printed for classroom distribution.

MINDTAP FOR CYSA+ GUIDE TO CYBERSECURITY ANALYSIS

MindTap is an online learning solution designed to help you master the skills you need in today's workforce. Research shows that employers need critical thinkers, troubleshooters, and creative problem solvers to stay relevant in our fast-paced, technology-driven world. MindTap helps you achieve this with assignments and activities that provide hands-on practice, real-life relevance, and certification test prep. MindTap guides you through assignments that help you master basic knowledge and understanding before moving on to more challenging problems. MindTap activities and assignments are tied to CompTIA CySA+ certification exam objectives. MindTap features include the following:

- ***Live Virtual Machine labs*** allow you to practice, explore, and try different solutions in a safe sandbox environment. Each module provides you with an opportunity to complete an in-depth project hosted in a live virtual machine environment. You implement the skills and knowledge gained in the module through real design and configuration scenarios in a private cloud created with OpenStack.

- The ***Adaptive Test Prep (ATP)*** app is designed to help you quickly review and assess your understanding of key IT concepts. Test yourself multiple times to track your progress and improvement by filtering results by correct answers, by all questions answered, or only by incorrect answers to show where additional study help is needed.
- ***Pre- and Post-Assessments*** emulate the CySA+ certification exam.
- ***Security for Life*** assignments encourage you to stay current with what's happening in the IT field.
- ***Reflection*** activities encourage classroom and online discussion of key issues covered in the modules.

Instructors, MindTap is designed around learning objectives and provides analytics and reporting so you can easily see where the class stands in terms of progress, engagement, and completion rates. Use the content and learning path as is, or pick and choose how your materials will integrate with the learning path. You control what the students see and when they see it. Learn more at https://www.cengage.com/mindtap/.

STATE OF CYBERSECURITY IN INFORMATION TECHNOLOGY

The number of cyberattacks has reached epidemic proportions. According to one report, there are 375 threats per minute, and the total malware in existence now exceeds 1.2 billion instances. New malware targeting mobile devices has increased more than 70 percent annually. Disclosed incidents targeting the United States increased 61 percent in just one quarter. Most users expect that they will be recurring victims of cyberattacks throughout their lifetime.

To defend against these growing numbers of cyberattacks, annual cybersecurity spending by companies and governments worldwide is projected to grow from $146 billion in 2020 to $207 billion by 2024, an increase of almost 30 percent. Yet even though billions of dollars are spent each year on defenses, it appears to be having limited impact on the number of successful attacks.

This imbalance—large amounts of money spent on defenses that still do not stop threat actors—has caused many security professionals to call for a change in thinking about security defenses. Security professionals today must have the knowledge and expertise to analyze data about the different types of attacks. They must also be able to discover any vulnerabilities in the network and devices attached to it, and then strengthen them to resist attacks.

CERTIFICATIONS

To assist current and future security professionals, a security certification is now available to help security workers learn and practice new security skills. This certification is the Computing Technology Industry Association (CompTIA) Cybersecurity Analyst (CySA+). The CySA+ certification is designed for IT security analysts, vulnerability analysts, and threat intelligence analysts. The material covered in this certification helps security professionals apply behavioral analytics to networks in order to improve the overall state of security through providing an enhanced visibility of threats. The CySA+ certification will validate a cybersecurity professional's ability to proactively defend and continuously improve the security of an enterprise by leveraging intelligence and threat detection techniques, analyzing and interpreting data, identifying and addressing vulnerabilities, and recommending preventative measures.

The value of an IT professional who holds a security certification is significant. IT professionals who hold an IT certification earn 3.5 percent more than industry peers who do not have one. Professionals who hold a security certification earn 8.7 percent more than counterparts who do not have a security certification.

Certification provides job applicants with more than just a competitive edge over their noncertified counterparts competing for the same IT positions. Some institutions of higher education grant college credit to students who successfully pass certification exams, moving them further along in their degree programs. For those already employed, achieving a new certification increases job effectiveness, which opens doors for advancement and job security. Certification also gives individuals who are interested in careers in the military the ability to move into higher positions more quickly.

ABOUT THE AUTHOR

Dr. Mark Ciampa is Professor of Information Systems in the Gordon Ford College of Business at Western Kentucky University in Bowling Green, Kentucky. Previously, he was Associate Professor and Director of Academic Computing at Volunteer State Community College in Gallatin, Tennessee, for 20 years. Mark has worked in the IT industry as a computer consultant for businesses, government agencies, and educational institutions. He has published more than 25 articles in peer-reviewed journals and is also the author of over 30 technology textbooks, including *Security+ Guide to Network Security Fundamentals,* 7th Edition; *CWNA Guide to Wireless LANs*, 3rd Edition; *Guide to Wireless Communications, Security Awareness: Applying Practical Security In Your World*, 5th Edition; and *Networking BASICS*. Dr. Ciampa holds a PhD in technology management with a specialization in digital communication systems from Indiana State University, and he has certifications in security and healthcare.

ACKNOWLEDGMENTS

A large team of dedicated professionals all contributed to this project, and I am honored to be part of such an outstanding group of professionals. First, thanks go to Cengage Product Manager Danielle Klahr for providing me the opportunity to work on this project and for her continual support. Thanks also to Cengage Senior Content Manager Anne Orgren, Content Manager Michele Stulga, and Learning Designer Natalie Onderdonk for their valuable input, and to Danielle Shaw for her technical reviews. I would like to give special recognition to developmental editor Lisa Ruffolo. Once again, Lisa provided numerous helpful suggestions, made excellent comments, and continually kept me posted on upcoming deadlines. She expertly managed all the details, both large and small, so that I could stay focused. I also appreciate the significant contributions of the reviewers for this edition: Jeremy Derby, Fayetteville Technical Community College, Fayetteville, NC; Diego Tibaquira, Miami Dade College—Padron, Miami, FL; and Darlene Wood, Fayetteville Technical Community College, Fayetteville, NC. To everyone on the team, I extend my sincere thanks.

Finally, I want to thank my wonderful wife, Susan. Her love, patience, and support were, as always, there from the beginning to end. I could not have done it without her.

Dedication

To Braden, Mia, Abby, Gabe, Cora, Will, and Rowan.

READ THIS BEFORE YOU BEGIN

This book is designed to meet the needs of learners and professionals who want to master intermediate cybersecurity skills. A fundamental knowledge of computers and networks is required, along with a solid understanding of fundamental computer security. Those seeking to pass the CompTIA CySA+ certification exam will find the text's approach and content especially helpful; all CySA+ CS0-002 exam objectives are covered in the text (see Appendix B). The *CompTIA® CySA+ Guide to Cybersecurity Analysis* covers all aspects of network and computer security while satisfying the exam objectives.

The book's pedagogical features are designed to provide a truly interactive learning experience that helps prepare you for the challenges of network and computer security. In addition to the information presented in the text, each module includes one or more virtual lab activities that guide you through implementing practical hardware, software, network, and Internet security configurations step by step. Each module also contains case studies that place you in the role of problem solver, requiring you to apply concepts presented in the module to achieve successful solutions. Additional questions in Appendix A provide even more opportunities to practice using the necessary tools to master cybersecurity analysis.

PART 1

EXTERNAL THREATS AND INTERNAL VULNERABILITIES

What is the first question that should be asked when protecting assets from a cyberattack? That initial question should be, "What external threats could exploit our internal vulnerabilities?" Without this knowledge of attacks and weaknesses, any cybersecurity efforts are doomed to fail. The modules in this first part explore how to identify these threats and vulnerabilities. Module 1 examines the common threats and vulnerabilities of an enterprise. Module 2 explores how to use threat data and intelligence sources to identify emerging threats. This data is then used to help identify vulnerabilities, which is the topic of Module 3. Finally, Module 4 examines cloud computing and tools for assessing vulnerabilities.

MODULE 1
ENTERPRISE THREATS AND VULNERABILITIES

MODULE 2
UTILIZING THREAT DATA AND INTELLIGENCE

MODULE 3
VULNERABILITY MANAGEMENT

MODULE 4
CLOUD COMPUTING AND ASSESSMENT TOOLS

MODULE 1

ENTERPRISE THREATS AND VULNERABILITIES

After completing this module, you should be able to do the following:

1. Identify different types of common attacks
2. Describe the risks associated with mobile devices
3. Explain security issues of embedded and specialized devices

Cybersecurity Today

For the first 100 years of the automobile, wheeled motor vehicles were mechanical devices powered by internal combustion engines (ICE) with gearbox transmissions. Over the last 10 years, however, the car has undergone its most dramatic changes to date. Automobiles have moved from being mechanical devices to predominately electronic ones, providing dramatic increases in fuel economy, safety, and comfort as ICEs are replaced by electric engines with rechargeable batteries. The recent introduction of autonomous vehicles ("self-driving cars") has further revolutionized the automobile industry. It has been said that today's cars are primarily a battery, motor, and computer hardware and software—sometimes without even a driver.

It comes as no surprise that because automobiles rely so heavily on hardware and software that they have been targets of cyberattackers. The first record of car attacks dates back to 2010. By 2015, security researchers had demonstrated how they could remotely control a car from 10 miles away due to a software vulnerability. The researchers changed the air-conditioning settings and the radio, turned off and on the windshield wipers and sprayed wiper fluid on the windshield, and even prevented acceleration on a crowded interstate highway while disabling the brakes so the car ended up in a ditch.

It has been estimated that cyberattackers can take advantage of at least 10 vehicle attack vectors to control or disable a car while it is in motion. Recently, two other attack vectors have been added to the list.

The first additional attack vector is over-the-air (OTA) updates. Much like with today's computer operating systems (OSs), problems with car software can be addressed by patches that are pushed out to millions of cars through wireless transmissions. This saves automakers costly recalls that normally would require the owner to drive to an authorized car dealer for a possibly lengthy repair. It is estimated that by 2022, savings across the industry from OTA updates will reach $35 billion. In addition, OTA updates are not limited to fixing software: they can also address components that are governed by that software. In 2018, a national consumer magazine announced that it would not recommend the Tesla Model 3 due in part to inconsistent braking behavior. One week later, Tesla updated all Model 3 cars through an OTA update that reduced the stopping distance by nearly 20 feet (6 meters).

However, there are issues surrounding OTA updates. Automakers could quietly sidestep regulations requiring public disclosure of defects by silently applying an OTA update. These updates may also incentivize car makers to rush a car to market with poorly tested features, knowing that an OTA update can later solve any issues. There have already been at least

two incidents of car makers pushing out defective OTA updates that rendered safety features, such as rear-view cameras and autopilot features, inoperable.

The more serious issue is that just as automakers can send OTA updates, so, too, can cybercriminals. Unless the wireless updates are sufficiently protected, cybercriminals could send their own malicious instructions to one car or millions of cars. In fact, security researchers have already demonstrated the ability to bypass OTA update security mechanisms designed to prevent this from occurring.

An equally alarming attack vector is the cameras in cars that read road signs. Known as machine vision, this feature is one of the most important features for self-driving cars and cars with a driver relying on an automated piloting system. These vehicles must be able to understand their environment and then react appropriately. The amount of free space between a car with machine vision and the cars ahead and behind must be monitored; solid objects have to be avoided; and all instructions—whether painted on the road itself or posted on signs—must be read, correctly interpreted, and obeyed. It turns out that machine vision, unlike the way humans identify images, can be easily fooled by extraneous markings on a sign that a human would know to dismiss. For example, a small sticker on a road sign would be ignored by someone who knows it is not part of the instructions being conveyed by the sign; a car using machine vision, however, can be tricked by that same sticker.

Security researchers placed small stickers on a stop sign that regular drivers saw but dismissed as the sign looking weathered. However, an autonomous car misread the same stop sign with the sticker as a speed limit sign. In a similar test, a slightly modified right turn sign was mistaken by a car's machine vision as a stop sign. In perhaps the most alarming test, a two-inch piece of black electrical tape was added across the middle of the "3" in the speed limit sign "35 MPH." The car mistook that sign as "85 MPH" and immediately began to accelerate to that speed. (The researchers, for safety's sake, intervened as the car continued to accelerate.)

Researchers have also experimented with injecting frames of an image on digital roadside billboards that are used for advertisements. They found that just displaying a small image of a stop sign for less than half a second—too fast for the human eye to detect—could trick a car's machine vision technology and cause the car to immediately stop. An attacker could hijack an Internet-connected billboard to display these images and cause massive traffic jams or deadly road accidents, all while leaving little if any evidence behind.

The thought of a remote attacker taking control of a 5,800-pound (2,630 kilogram) SUV as it barrels down the road with a helpless driver behind the wheel unable to control it has many security professionals calling for immediate improvements in automobile hardware, software, and connectivity. As one security organization said, "We need to accelerate discussions and awareness of the problems and steer the direction and development of next-generation technologies (puns intended)."

How many cyberattacks have occurred over the last 24 hours? Over the last hour? In the past minute? The number of attacks continues to grow exponentially and has reached unprecedented proportions. According to one report, there are 375 threats per minute. The total malware in existence now exceeds 1.2 billion instances. New malware targeting mobile devices has increased annually more than 70 percent while new macOS malware has increased by 51 percent. Disclosed incidents targeting the United States increased 61 percent, those targeting Great Britain increased 55 percent, and attacks directed at Canada increased 50 percent in just one quarter.[1] Cybercrime will cost the world $10.5 trillion annually by 2025, an increase from $3 trillion in 2015, representing the greatest transfer of economic wealth in human history.[2] And these attacks continue with no end in sight.

To defend against the growing numbers of cyberattacks, enterprises are spending a staggering amount of their budgets on cybersecurity. Annual cybersecurity spending by companies and governments worldwide is projected to grow from $146 billion in 2020 to $207 billion by 2024, an increase of almost 30 percent. In the financial services sector, spending on cyberdefenses equals $3,000 per full-time employee. Microsoft spends $1 billion annually on defenses, while the U.S. government spends $15 billion each year.[3] Yet even though billions of dollars are spent each year on defenses, the number of successful attacks continues to grow.

This imbalance—large amounts of money spent on defenses that still do not stop threat actors—has caused many security professionals to throw up their hands and scream "Enough!" Calls for a change in how cybersecurity is approached and practiced are resonating throughout enterprises of all types and sizes. As one security professional recently said, "It is time for a paradigm shift in the cybersecurity industry."[4]

While attackers have learned to evade traditional signature-based solutions, such as firewalls and antivirus software, a shift to an analytics-based approach is becoming increasingly important for enterprises. To assist future security professionals with this shift, an advanced security certification is now available. This certification is the Computing Technology Industry Association (CompTIA) Cybersecurity Analyst (CySA+). CompTIA CySA+ applies behavioral analytics to networks in order to improve the overall state of security through providing an enhanced visibility of threats. The CySA+ certification will validate a cybersecurity professional's ability to proactively defend and continuously improve the security of an enterprise by leveraging intelligence and threat detection techniques, analyzing and interpreting data, identifying and addressing vulnerabilities, and recommending preventative measures.

This part begins by looking at exploits. The noun "exploit" originally meant an attempt to capture something while on a military expedition. Today the word is often defined as a tool designed to take advantage of a flaw in a computer system, typically for malicious purposes. This definition well encompasses the current challenges of cybersecurity: threat actors are continually seeking to uncover flaws or vulnerabilities in the defenses of an enterprise and then use those to craft a malicious threat.

For an enterprise to mount a successful defense, it must be aware not only of the attacker's threats but also of its own vulnerabilities. To know the external threats without understanding its vulnerabilities is a formula for disaster, just as knowing its flaws but being ignorant of the threats is likewise a recipe for failure. Knowing both external threats and internal vulnerabilities is crucial.

This module looks at the threats by exploring different types of attacks. It also covers threats and vulnerabilities associated with technologies other than personal computers and data networks, such as mobile devices, embedded devices, and specialized devices.

TYPES OF ATTACKS

CERTIFICATION

1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities.

It is important to know the types of attacks that an enterprise faces today. These include attacks using malware, memory vulnerability attacks, web server application attacks, session hijacking, attacks on credentials, exploitation and penetration attacks, and social engineering attacks.

Attacks Using Malware

Malware (*mal*icious soft*ware*) is a "catchall" term for virtually any type of malicious software designed to harm or exploit a device, service, or network. It enters a computer system without the user's knowledge or consent and then performs an unwanted and harmful action. Although the total malware in existence now exceeds 1.2 billion instances, there is still no established standard for classifying the types of malware so that like malware can be grouped together for study.

NOTE 1

Just as there is no standard for classifying malware, there likewise is no standard for naming malware instances. Often malware is simply given a name by the security researcher who first discovered it, which has led to the malware names WannaCry, NotPetya, Cryptolocker, ILOVEYOU, Anna Kournikova, Heartbleed, Stuxnet, and Conficker. The Black Hat security conference annually gives out an award for the most memorable vulnerability name.

However, security professionals have created "container" categories for grouping malware. One such category is malware that attempts to evade detection or helps other malware stay hidden. For example, a *back door* gives access to a computer, program, or service that circumvents any normal security protections. Back doors installed on a computer allow the attacker to return later and bypass security settings. A *logic bomb* is computer code that is typically hidden in a legitimate computer program but lies dormant and evades detection until a specific logical event triggers it.

NOTE 2

The risks of rootkits in OSs are significantly diminished today due to protections built into modern OS software. These protections include preventing unauthorized kernel drivers from loading, stopping modifications to certain kernel areas used by rootkits to hide, and preventing rootkits from modifying the bootloader program.

Another example of malware that aids in evasion techniques is a **rootkit**. A rootkit is malware that can hide its presence and the presence of other malware on the computer. It does this by accessing the lower layers of the OS or even using undocumented functions. This renders the rootkit and any accompanying software undetectable by the OS and common antimalware scanning software designed to seek and find malware.

Memory Vulnerability Attacks

Several attacks are directed at vulnerabilities associated with how a program uses random access memory (RAM) and are often the result of poor techniques (or laziness) by the software developer. Some memory-related attacks attempt to manipulate memory contents. These types of attacks include buffer overflow attacks and integer overflow attacks.

Buffer Overflow

A storage buffer on a computer typically contains the memory location of the software program that was being executed when another function interrupted the process; that is, the storage buffer contains the "return address" where the computer's processor should resume once the new process has finished. Attackers can substitute their own "return address" to point to a different area in the computer's memory that contains their malware code.

A **buffer overflow attack** occurs when a process attempts to store data in RAM beyond the boundaries of a fixed-length storage buffer. This extra data overflows into the adjacent memory locations (a buffer overflow). Because the storage buffer typically contains the "return address," an attacker can overflow the buffer with a new address pointing to the attacker's malware code. A buffer overflow attack is shown in Figure 1-1.

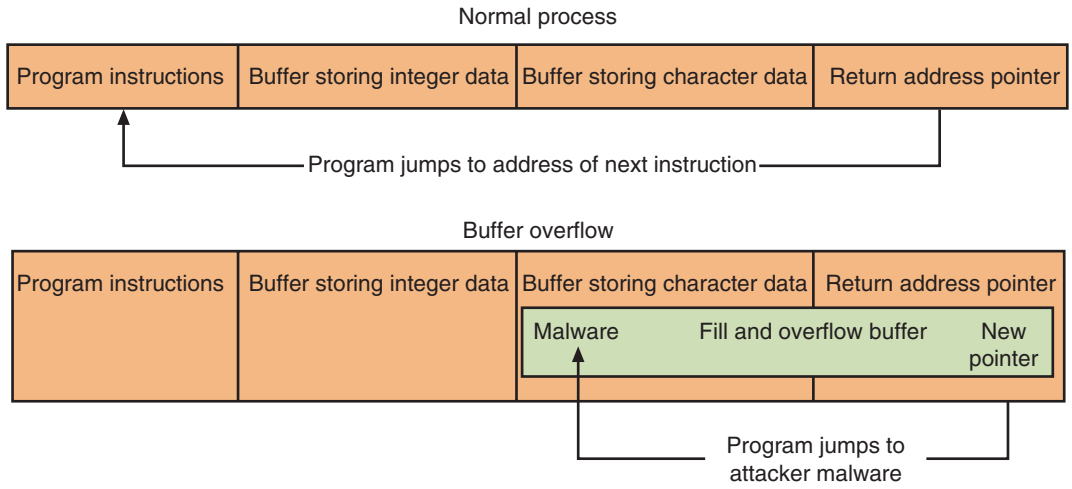


Figure 1-1 Buffer overflow attack

A buffer overflow attack can occur in one of two areas of computer memory. Memory is divided into the following four areas, as shown in Figure 1-2:

- *Data*. This area stores global variables that are separated into initialized and uninitialized variables.
- *Heap*. The heap is dynamic memory for the programmer to allocate as necessary.
- *Stack*. The stack stores local variables that the program uses.
- *Text*. Text stores the code that is being executed.

Each byte of computer memory has a unique address, beginning with zero (low address) to the largest possible address (high address). The *stack* area is near the top of memory with high addresses. Whenever a function is called by the computer program, a portion of stack memory is allocated. When new local variables are declared, more stack memory is automatically allocated. These allocations make the stack grow "down" (from higher memory addresses to

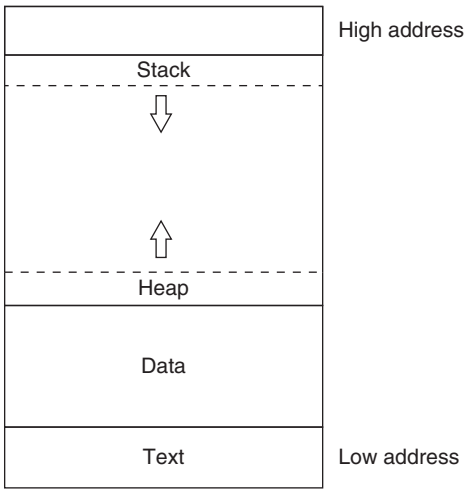


Figure 1-2 Computer memory areas

lower addresses). The *heap* area is allocated explicitly by the program and grows "up" (from lower addresses to higher addresses); it is not deallocated (freed) until the program explicitly mandates it. Because buffers are found in both the stack and heap areas, a buffer overflow attack can occur in either the stack (a *stack overflow*) or the heap (a **heap overflow**).

Integer Overflow

An integer overflow is the condition that occurs when the result of an arithmetic operation—such as addition or multiplication—exceeds the maximum size of the integer type used to store it. When this integer overflow occurs, the interpreted value then wraps around from the maximum value to the minimum value. For example, an eight-bit signed integer has a maximum value of 127 and a minimum value of –128. If the value 127 is stored in a variable and 1 is added to it, the sum exceeds the maximum value for this integer type and wraps around to become –128.

In an **integer overflow attack**, an attacker changes the value of a variable to something outside the range that the programmer had intended by using an integer overflow. This type of attack could be used by an attacker to create a buffer overflow. If an integer overflow could be introduced during the calculations for the length of a buffer when a copy is occurring, it could result in a buffer that is too small to hold the data. A large positive value in a bank transfer could also be wrapped around by an integer overflow attack to become a negative value, which could then reverse the flow of money: instead of adding this amount to the victim's account, it could withdraw that amount and later transfer it to the attacker's account.

NOTE 3

An extreme example of an integer overflow attack would be withdrawing $1 from an account that has a balance of 0, which could cause a new balance of $4,294,967,295!

Web Server Application Attacks

A web server provides services that are implemented as "web applications" through software programs running on the server. A typical web application infrastructure is shown in Figure 1-3. The client's web browser makes a request using the Hypertext Transfer Protocol (HTTP) to a web server, which may be connected to one or more web app servers. These application servers run the specific web apps, which in turn are directly connected to database servers on the internal network. Information from these database servers is retrieved and returned to the web server so that the information can be sent back to the user's web browser. A web application infrastructure is a tempting target for attackers for multiple reasons:

- A successful compromise could impact all web users who access the web server.
- An attack could provide a pathway into the enterprise's network infrastructure.
- The multiple elements in a web application infrastructure provide for a range of vulnerabilities that can be used as different attack vectors.

Two common application attacks are scripting attacks and injection attacks.

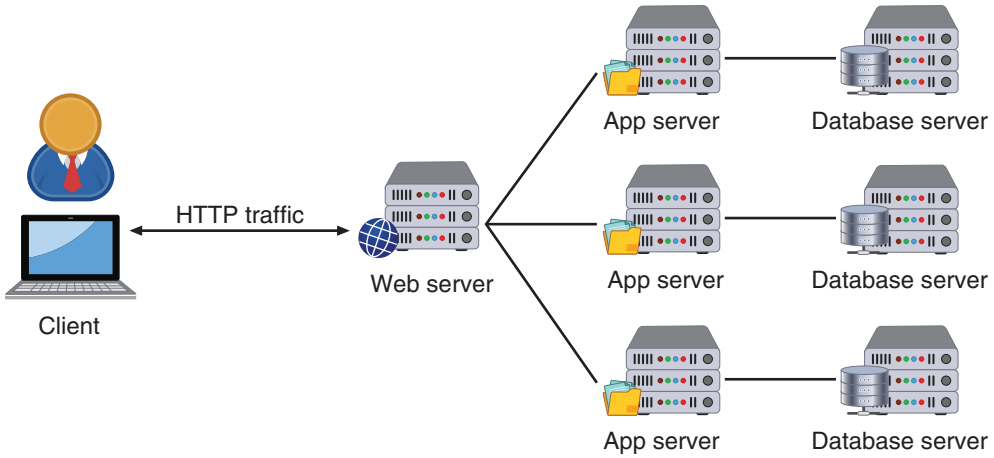


Figure 1-3 Web server application infrastructure

Scripting

Many websites—such as forums or message boards, blogging websites, and social networks—accept user input (visitor comments, web-based collaborations, etc.). The underlying web applications then use the input from users to create dynamic display content. For example, when a user enters CENGAGE into a search box, a webpage could be displayed to the user with the message *You are searching for: CENGAGE*. Or a user could enter a new topic about a recent player trade on a sports web forum that would then be displayed to subsequent users who access that same topic in the forum.

Threat actors can take advantage of this user input and display in a **cross-site scripting (XSS)** attack. The term "cross-site scripting" refers to an attack using scripting that originates on one site (the web server) to impact another site (the user's computer). XSS is essentially a client-side code injection attack using a web application. An attacker attempts to execute malicious scripts in the victim's web browser but not by directly injecting it into the user's web browser. Rather, the attacker inputs that malicious code on a website that accepts user input. The underlying web application that accepts the malicious code then becomes the vehicle to deliver the malicious script to every user's browser when he or she accesses that site. An XSS attack is shown in Figure 1-4.

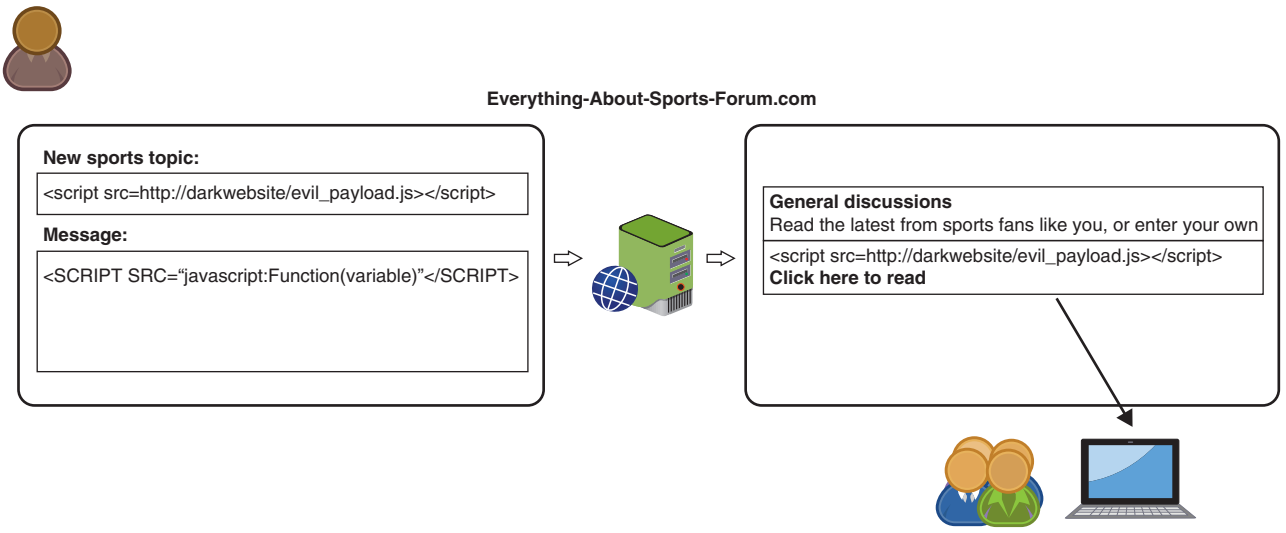


Figure 1-4 XSS attack

CAUTION

Malicious code in an XSS attack can be executed in the user's browser through VBScript, ActiveX, Flash, and even Cascading Style Sheets (CSS). However, it is most commonly executed in JavaScript because JavaScript is fundamental to most browsing experiences. Although web browsers run JavaScript in a tightly controlled environment with limited access to the OS and file system, it still has the potential to be misused by malware.

For a threat actor to launch an XSS attack, the attacker must identify a web application that accepts user input without validating it (called *sanitizing*) and then use that input in a response sent to the user. There are three main types of XSS attacks. These are summarized in Table 1-1.

Table 1-1 Types of XSS attacks

Name	Description	Comments
Reflected XSS	A user enters input into a web application that is then immediately displayed back ("reflected") to initiate the attack.	The simplest form of XSS attack
Persistent XSS	A threat actor enters input into a blog post or forum that is stored ("persistent") and an unsuspecting user later displays it to initiate the attack.	Also called Stored XSS or Second Order XSS
Document Object Model XSS	A web application writes data to the Document Object Model on the web server without proper sanitization and the attacker manipulates this data to include XSS content on the webpage.	The Document Object Model is a convention used to represent and work with objects in an HTML document (and other document types)

A threat actor who controls a script that is executed in the victim's browser through XSS could fully compromise that user. The attacker can do the following:

- Initiate interactions with other application users, including malicious attacks, that appear to originate from the trusted victim.
- Modify any information that the user is able to modify.
- Perform any action within the application that the user can perform.
- View any information that the user is able to view.

Injection

In addition to cross-site scripting attacks on web server applications, attacks called *injections* also introduce new input to exploit a vulnerability. One of the most common injection attacks, called **Structured Query Language (SQL) injection**, inserts statements to manipulate a database server. SQL is a language used to view and manipulate data that is stored in a relational database. SQL injection targets SQL servers by introducing commands into the server, much in the same way that XSS attacks inject malicious commands into a web application. However, with an SQL injection attack, the intent is to retrieve confidential information from the database and not inject malicious code.

An attacker using an SQL injection attack would begin by first entering a fictitious email address on a webpage that included a single quotation mark as part of the data, such as braden.thomas@fakemail.com'. If the message "Email Address Unknown" is displayed, it indicates that user input is being properly filtered and an SQL attack cannot be rendered on the site. However, if the error message "Server Failure" is displayed, it means that the user input is not being filtered and all user input is sent directly to the database. This is because the "Server Failure" message is due to a syntax error created by the additional single quotation mark in the fictitious email address.

Armed with the knowledge that input is sent unfiltered to the database, attackers understand that anything they enter as a username in the web form would be sent to and then processed by the SQL database. Now, instead of entering a username, the attackers would enter valid SQL statements that would be passed directly to the database for processing.

In addition to using SQL to view and manipulate data that is stored in a relational database, other types of databases not using SQL (called *NoSQL databases*) are used. One popular type of NoSQL database manipulates data using the *eXtensible Markup Language (XML)*. Like the markup language Hyper Text Markup Language (HTML) used for webpages, XML is not a processing language but instead is designed to store information. A NoSQL database that uses XML for data manipulation is also subject to an injection attack like SQL injection if the input is not sanitized. This is called an **eXtensible Markup Language (XML) attack**.

Session Hijacking

A *session ID* is a unique value that a web server assigns a specific user for the duration of that user's visit (session). Most servers create complex session IDs by using the date, time of the visit, and other variables such as the device IP address, email, username, user ID, role, privilege level, access rights, language preferences, account ID, current state, last login, session timeouts, and other internal session details. Session IDs are usually at least 128 bits in length and hashed using a secure hash function like SHA-256. A sample session ID is *fa2e76d49a0475910504cb3ab7a1f626d174d2d*. Session IDs can be contained as part of a URL extension, by using "hidden form fields" in which the state is sent to the client as part of the response and returned to the server as part of a form's hidden data, or through cookies.

NOTE 4

Each time a website is visited, a new session ID is assigned and usually remains active as long as the browser is open. In some instances, after several minutes of inactivity, the server may generate a new session ID. Closing the browser terminates the active session ID, and it should not be used again.

Session hijacking occurs when a threat actor takes over a user session. Different methods can be used for hijacking a session. One method involves intercepting the session ID. This can be done through XSS or a **man-in-the-middle (MITM)** attack (sometimes called an on-path attack) in which a communication between two systems is intercepted. In a typical HTTP transaction, a TCP connection is made between the endpoint and the server. Using different techniques, the attacker can divide the original TCP connection into two new connections, one between the client and the attacker and the other between the attacker and the server. The attacker can act as a proxy, being able to read, insert, and modify the information in the intercepted communication. Other methods include tricking the user into clicking a malicious link that contains a prepared session ID that the threat actor knows and can use or attempting to guess the session ID.

Attacks on Credentials

Authentication in information security is the process of ensuring that the person or system seeking access to resources is authentic (not an imposter). Seven recognized elements can be presented to prove this authenticity, since only the real or authentic person would uniquely possess one or more of these elements. These elements that prove authenticity, known as *authentication credentials*, are listed in Table 1-2.

Threat actors use a variety of techniques to attack credentials and gain access to protected systems. Because passwords (something you know) are the most common form of authentication credential, many of these attacks focus on attempting to compromise passwords.

One type of password attack uses "targeted guessing." A **password spraying attack** takes one or a small number of commonly used passwords (*Password1* or *123456*) and then uses this same password when trying to log in to several user accounts. Because this targeted guess is spread across many accounts and is not focused on attempting multiple

Table 1-2 Authentication credentials

Element	Description	Example
Somewhere you are	Restricted location	Restricted military base
Something you are	Unique biological characteristic that cannot be changed	Fingerprint reader
Something you have	Possession of an item that nobody else has	RFID card
Someone you know	Validated by another person	Adriano knows Li
Something you exhibit	Genetically determined characteristic	Red hair
Something you can do	Perform an activity that cannot be exactly copied	Signature
Something you know	Knowledge that nobody else possesses	Keys pressed on a keypad

password variations on a single account, it is much less likely to raise any alarms or lock out the user account from too many failed password attempts. Although password spraying may result in occasional success, it is not considered the optimal means for breaking into accounts.

Another attack takes advantage of the huge number of stolen passwords that have been posted online by threat actors. This treasure trove collection of passwords gives attackers a "head start" in credential attacks. Because users repeat their passwords on multiple accounts, attackers use these passwords in their attacks with a high probability of success. This is known as **credential stuffing**.

NOTE 5

Using stolen password collections as candidate passwords is the foundation of password cracking today, and almost all password cracking software tools accept these stolen "wordlists" as input. Websites host lists of these leaked passwords that attackers can download. One website boasts more than 1.45 *trillion* cracked password hashes.

Grow with Cengage Unlimited!

If you'd like more information about this topic, use your Cengage Unlimited subscription to go to the CompTIA Security+ Guide to Network Security Fundamentals, 7th edition; open Module 12; and read the section titled "Types of Authentication Credentials."

If you don't have a Cengage Unlimited subscription, you can find more information at cengage.com/unlimited.

Exploitation and Penetration Tactics

The goal of a threat actor is to exploit a vulnerability in order to penetrate a system. Generally, threat actors use these tactics for exploitation and penetration:

1. The threat actors first conduct reconnaissance against the systems, looking for vulnerabilities.
2. When a path to a vulnerability is exposed, they gain access to the system through the vulnerability.
3. Once initial access is gained, the threat actors attempt to escalate to more advanced resources that are normally protected from an application or user. This is called **privilege escalation**.
4. With the advanced privileges, they tunnel through the network, looking for additional systems they can access from their elevated position (called *lateral movement*). Threat actors may use a **directory traversal** attack that takes advantage of a vulnerability in a web application or web server software so that a user can move from the root directory to other restricted directories.
5. Threat actors install additional tools on the compromised systems to gain even deeper access to the network. They may also use vulnerabilities to enter commands to execute on a server; this is known as **remote code execution (RCE)**.

6. Threat actors may install a back door that allows them repeated and long-term access to the system in the future. The back doors are not related to the initial vulnerability, so access remains even if the initial vulnerability is corrected.
7. Once the back door is installed, threat actors can continue to probe until they find their ultimate target and perform their intended malicious action—such as stealing research and development (R&D) information, password files, or customer credit card numbers.

CAUTION

The initial system that was compromised—the system through which the attackers first gained entry—most often is not the goal of the attack. Rather, this system only serves as a gateway for entry. Once they are inside the network, the threat actors then pivot or turn to other systems to be compromised, with the goal of reaching the ultimate target. This means they are not defeated if they cannot find a vulnerability on the target; rather, a vulnerability can be used to pivot to the ultimate target.

Social Engineering Attacks

Not all attacks rely on technology vulnerabilities; in fact, some cyberattacks use little if any technology to achieve their goals. *Social engineering* is a means of eliciting information (gathering data) by relying on the weaknesses of individuals. This information elicitation may be the goal of the attack, or the information may then be used for other attacks.

Social engineering **impersonation** (also called identity fraud) is masquerading as a real or fictitious character and then playing out the role of that person on a victim. For example, an attacker could impersonate a help desk support technician who calls the victim, pretends that there is a problem with the network, and asks for a valid username and password to reset the account. Sometimes the goal of the impersonation is to obtain private information, which is known as *pretexting*.

CAUTION

Common roles that are often impersonated include a repairperson, an IT support person, a manager, or a trusted third party. Often attackers will impersonate individuals whose roles are authoritative because victims generally resist saying no to anyone in power. Users should exercise caution when receiving a phone call or email from these types of individuals asking for something suspicious.

Grow with Cengage Unlimited!

If you'd like more information about this topic, use your Cengage Unlimited subscription to go to the CompTIA Security+ Guide to Network Security Fundamentals, 7th edition; open Module 1; and read the section titled "Social Engineering Attacks."

If you don't have a Cengage Unlimited subscription, you can find more information at cengage.com/unlimited.

TWO RIGHTS & A WRONG

1. A rootkit is malware that can hide its presence and the presence of other malware on the computer.
2. The stack is dynamic memory for the programmer to allocate as necessary.
3. A Reflected XSS attack only affects the user who entered data into the website.

See Appendix C for the answer.

THREATS AND VULNERABILITIES OF SPECIALIZED TECHNOLOGY

CERTIFICATION

1.5 Explain the threats and vulnerabilities associated with specialized technology.

The days are long past when threat actors focused only on file servers and desktop computers. Instead, just as individual users and large enterprises have shifted their focus to other technologies, so too have attackers. These technologies include embedded and specialized devices and mobile devices, and they each have specific security issues.

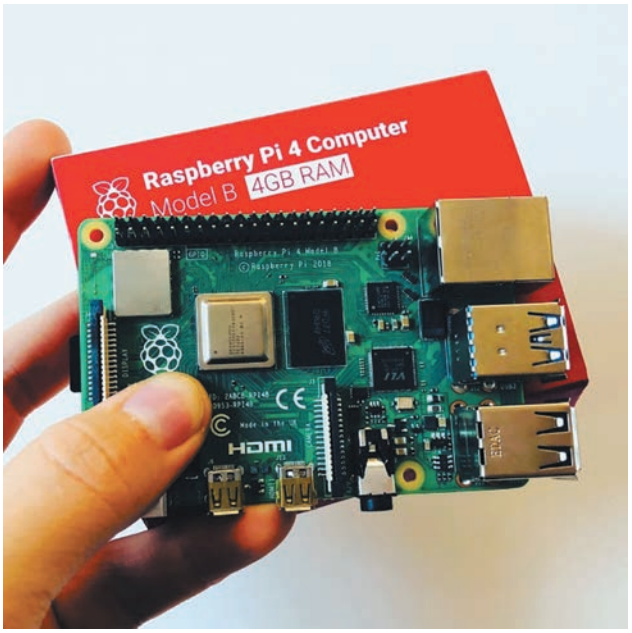
Embedded and Specialized Devices

Not all computing systems are desktop or mobile devices designed for human input. Computing capabilities can be integrated into a variety of different devices. An **embedded system** is computer hardware and software contained within a larger system designed for a specific function. A growing trend is to add these capabilities to devices that have never had computing power before.

Types of Devices

There are several categories of embedded and specialized devices. These include the hardware and software that can be used to create these devices, industrial systems, campus systems, Internet of Things devices, and specialized systems.

Hardware and Software Hardware and software components are available for industrious users to create their own specialized devices. One of the most common hardware components is the Raspberry Pi. This is a low-cost, credit-card-sized computer motherboard, as shown in Figure 1-5. The Raspberry Pi can perform virtually the same tasks that a standard computer device can, such as browsing the Internet, playing high-definition video, creating spreadsheets, and playing games. However, it is most often used to control a specialized device.



Raspberry Pi Foundation

Figure 1-5 Raspberry Pi

NOTE 6

Although both the Raspberry Pi and Arduino can be used to interact with other specialized devices—for example, to control a robot, build a weather station, broadcast an FM radio signal, or build an automatic plant watering device—the Arduino is generally considered a better solution for this type of interaction. It only has a single USB port, a power input, and a set of input/output pins for connections but consumes very little power.

NOTE 7

FPGAs are used in aerospace and defense, medical electronics, digital televisions, consumer electronics, industrial motor control, scientific instruments, cybersecurity systems, and wireless communications. Microsoft is now using FPGAs in its data centers to run Bing search algorithms.

NOTE 8

Modbus TCP/IP must rely on the security capabilities of the local area network for protection.

A device similar to the Raspberry Pi is the Arduino. Unlike the Raspberry Pi, which can function as a complete computer, the Arduino is designed as a controller for other devices: it has an 8-bit microcontroller instead of a 64-bit microprocessor on the Raspberry Pi, a limited amount of RAM, and no OS but can only run programs that were compiled for the Arduino platform, most of which must be written in the C++ programming language.

Although the Raspberry Pi and Arduino are small motherboards, a **field-programmable gate array (FPGA)** is a hardware "chip" or integrated circuit (IC) that can be programmed by the user ("field programmable") to carry out one or more logical operations. (ICs on standard computers as well as on Raspberry Pis and Arduinos cannot be user-programmed.) Specifically, a FPGA is an IC that consists of internal hardware blocks with user-programmable interconnects to customize operations for a specific application. A user can write software that loads onto the FPGA chip and executes functions, and that software can later be replaced or deleted.

An even smaller component than the Raspberry Pi or Arduino is a **system on a chip (SoC)**. An SoC combines all the required electronic circuits of the various computer components on a single IC chip (the Raspberry Pi and Arduino are tiny motherboards that contain ICs, one of which is an SoC). SoCs often use a **real-time operating system (RTOS)** that is a specifically designed OS for an SoC in an embedded or specialized system. Standard computer systems, such as a laptop with a mouse and a keyboard or a tablet with a touch screen, typically receive irregular "bursts" of input data from a user or a network connection. Embedded systems, on the other hand, receive very large amounts of data very quickly, such as for an aircraft preparing to land on a runway at night during a storm. The RTOS is tuned to accommodate very high volumes of data that must be immediately processed for critical decision making.

Industrial Systems **Industrial control systems (ICSs)** manage devices locally or at remote locations by collecting, monitoring, and processing real-time data so that machines can directly control devices such as valves, pumps, and motors without the need for human intervention. Multiple ICSs are managed by a larger **supervisory control and data acquisition (SCADA)** system. SCADA systems are crucial today for industrial organizations. They help to maintain efficiency and provide information on issues to help reduce downtime.

Many SCADA systems use the network communication protocol **Modbus** for transmitting information between devices. Developed in 1979, Modbus originally required a serial port for communication between a single controlling device and up to 247 subservient devices. The controlling device polls each subservient device in a defined sequence, essentially asking each device in turn, "Do you want to transmit?" A subservient device cannot "volunteer" its data but must instead wait until it is polled and approved before transmitting. A later variation to Modbus incorporated the TCP/IP protocol and uses a standard client/server architecture; this variation is called Modbus TCP/IP or Modbus TCP. Although standard Modbus has error-detection capabilities to protect against data corruption, it has no security protections against injected commands or the interception of data.

Campus Systems A "campus" is the grounds and buildings of a school, hospital, business, or similar institution. To decrease the demand on personnel to monitor and manage the many elements that even a single building requires—doors, lighting, HVAC (heating, ventilation, and air conditioning), and fire alarms, just to name a few—modern campuses use **workflow and process automation systems**. These systems interconnect all the various elements so that they can be centrally and automatically monitored and controlled. One common system is a **building automation system** that manages building elements, which often includes a **physical access control** system that can ensure doors are locked and unlocked at specific times for certain individuals.

Internet of Things (IoT) Devices The Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) defines the **Internet of Things (IoT)** as "A global infrastructure for the information society,

enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."[5] More simply, the IoT is connecting any device to the Internet for the purpose of sending and receiving data to be acted upon. Although this definition could encompass laptop computers and tablets, more often IoT refers to devices that heretofore were not considered as computing devices connected to a data network.

IoT devices include wearable technology and multifunctional devices as well as many everyday home automation items such as thermostats, coffee makers, tire sensors, slow cookers, keyless entry systems, washing machines, electric toothbrushes, headphones, and light bulbs, to name just a few. It is estimated that by 2025, there will be more than 25 billion IoT devices, of which more than half will be consumer devices.[6]

Specialized Systems Several types of specialized systems are designed for specific applications. One example is a system that measures the amount of utilities consumed. Traditionally, households have had utilities such as electricity and water measured by an analog meter that records the amount of electricity or water being used. This requires an employee from the utility to visit each home and read from the meter the amount that was consumed for the month so that a bill can be sent to the occupant. These analog meters are being replaced by digital "smart meters." Smart meters have several advantages over analog meters. These are listed in Table 1-3.

Table 1-3 Analog meters vs. smart meters

Action	Analog meter	Smart meter
Meter readings	Employee must visit the dwelling each month to read the meter.	Meter readings are transmitted daily, hourly, or even by the minute to the utility company.
Servicing	Annual servicing is required in order to maintain accuracy.	Battery replacement every 20 years.
Tamper protection	Data must be analyzed over long periods to identify anomalies.	Can alert utility in the event of tampering or theft.
Emergency communication	None available	Transmits "last gasp" notification of a problem to utility company.

The last 20 years have seen a dramatic increase in specialized systems used for transportation. This includes vehicles and drones.

Vehicles. The first automobile specialized systems appeared in mass-production vehicles in the mid-1970s in response to regulations calling for higher fuel economy and emission standards, and they handled basic functions such as engine ignition timing and transmission shifting. By the 1980s, more sophisticated computerized engine-management systems enabled the use of reliable electronic fuel-injection systems, and later active safety systems such as antilock braking and traction and stability control features were added, all controlled by specialized systems.

Initially, these automobile sensors and devices were connected through a complex set of "point-to-point" wiring schemes in which one sensor was directly connected to a monitoring device or to another sensor that required its input (called electronic control units or ECUs). However, it quickly became apparent that there needed to be an improved means for interconnecting the growing number of ECU devices. In 1986, Bosch, a German-based multinational engineering and technology company, introduced the **controller area network (CAN) bus** network for sending and receiving data. CAN essentially consists of two wires, CAN low and CAN high. Data broadcast through CAN from one ECU reaches all other ECUs, which then accept and evaluate the data to determine if it should be received or is unnecessary and can be ignored. A CAN bus is illustrated in Figure 1-6.

Today specialized systems in cars use sonar, radar, and laser emitters to control brakes, steering, and the throttle to perform functions such as blind-spot and pedestrian collision warnings, automated braking, safe distance keeping, and fully automated parking. Some of these specialized embedded systems in cars are shown in Figure 1-7.

NOTE 9

CAN became an international standard in 1993 and data rates up to five megabits per second (Mbit/s) was standardized in 2016. CAN is also used outside of the automotive industry.

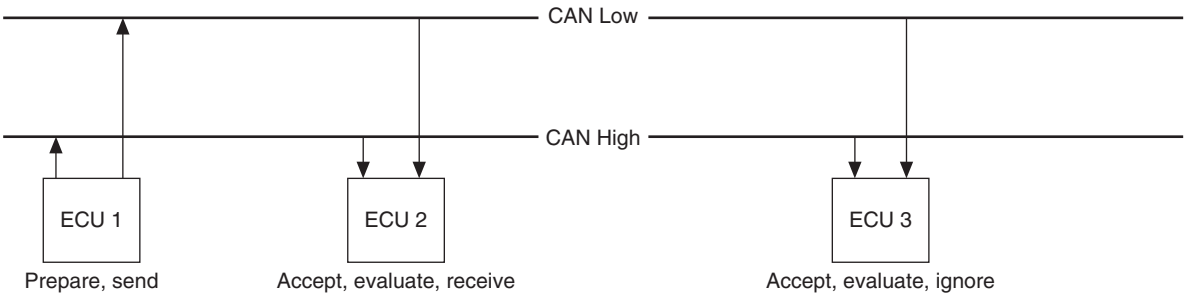


Figure 1-6 CAN bus

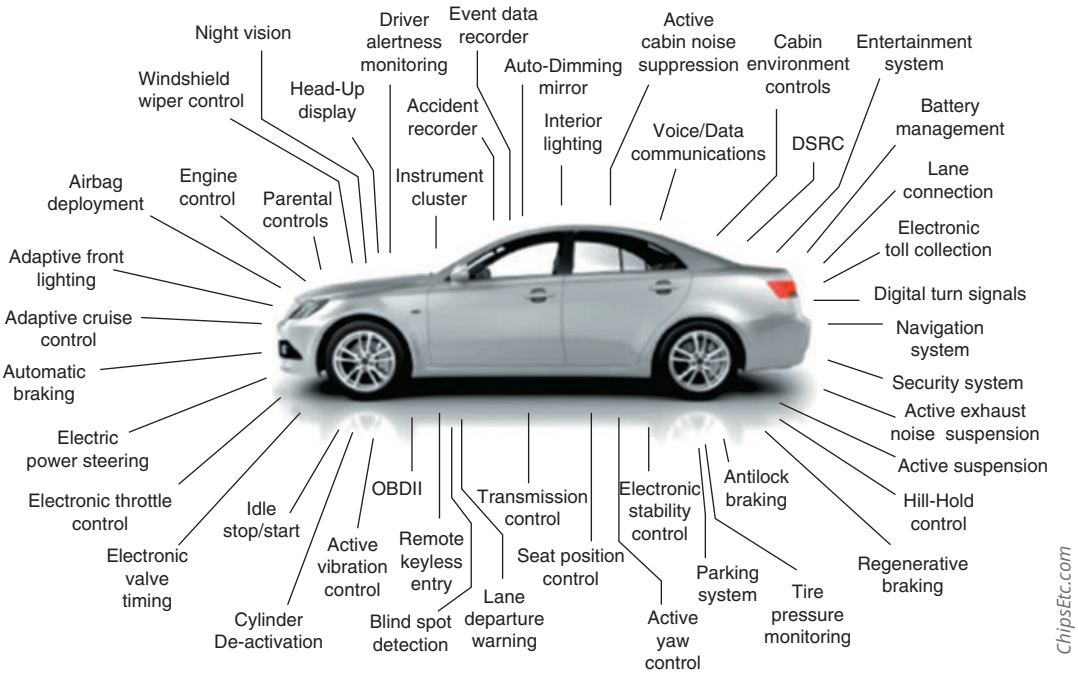


Figure 1-7 Specialized systems in cars

Den Rozhnovsky/Shutterstock.com

Figure 1-8 Drone

Drones. An *unmanned aerial vehicle (UAV)*, better known as a **drone**, is an aircraft without a human pilot on board to control its flight. Drones can be controlled by a remote human operator, usually on the ground, or autonomously by preprogramming the onboard computers. While drones were originally used in military applications, today they have expanded into commercial, scientific, agricultural, and recreational uses. They are commonly used for policing and surveillance, product deliveries, aerial photography, infrastructure inspections, and even drone racing. A drone is seen in Figure 1-8.

NOTE 10

The term drone was first used to refer to unmanned aircraft that were used for target practice by battleships in the 1920s.

Security Issues

Despite the fact that embedded systems and specialized devices are widely used and will continue to grow exponentially, significant security issues surround these systems and devices. The lack of security in embedded systems and specialized devices can result in a wide range of attacks. For example, the vulnerable CAN bus has been a primary target for threat actors in manipulating vehicles.

Several constraints or limitations make security a challenge for these systems and specialized devices. These security constraints are listed in Table 1-4.

Table 1-4 Security constraints for embedded systems and specialized devices

Constraint	Explanation
Power	To prolong battery life, devices and systems are optimized to draw very low levels of power and thus lack the ability to perform strong security measures.
Compute	Due to their size, small devices typically possess low processing capabilities, which restricts complex and comprehensive security measures.
Network	To simplify connecting a device to a network, many device designers support network protocols that lack advanced security features.
Cryptography	Encryption and decryption are resource-intensive tasks that require significant processing and storage capacities that these devices lack.
Inability to patch	Few, if any, devices have been designed with the capacity for being updated to address exposed security vulnerabilities.
Authentication	To keep costs at a minimum, most devices lack authentication features.
Range	Not all devices have long-range capabilities to access remote security updates.
Cost	Most developers are concerned primarily with making products as inexpensive as possible, which means leaving out all security protections.
Implied trust	Many devices are designed without any security features but operate on an "implied trust" basis that assumes all other devices or users can be trusted.
Weak defaults	Usernames ("root," "admin," "support," etc.) and passwords ("admin," "888888," "default," "123456," "54321," and even "password") for accessing devices are often simple and well known.

NOTE 11

In one infamous security incident, a worm named Stuxnet attempted to gain administrative access to other computers through the network to control the SCADA system. It appears that Stuxnet's primary target was nuclear reactors at the Bushehr Nuclear Power Plant. Located in southwestern Iran near the Persian Gulf, Bushehr was a source of tension between Iran and the West (including the United States) because of fear that spent fuel from the reactor could be reprocessed elsewhere in the country to produce weapons-grade plutonium for use in nuclear warheads. Stuxnet was ultimately not successful in its attack.

Over several years, many industry-led initiatives have attempted to address security vulnerabilities in IoT and embedded devices. However, these initiatives were scattered and did not represent a comprehensive solution to the problem. To address security in these devices, governments have begun to propose or enact legislation to require stronger security on embedded systems and specialized devices. The *Internet of Things (IoT) Cybersecurity Improvement Act of 2019* was legislation introduced in the U.S. Senate in 2019. California and Oregon passed state laws addressing IoT security that went into effect in 2020. Both state laws require that connected devices be equipped with "reasonable security features" appropriate for the nature and function of the device and the information the device collects, contains, or transmits. Devices must be designed to protect both the device itself and any information contained within the device from unauthorized access, destruction, use, modification, or disclosure.

Mobile Device Risks

Few technologies can claim a growth rate that equals that of mobile devices. By 2022, 71 percent of the entire global population will be mobile users (5.7 billion). By that same year, mobile data traffic will reach an annual rate of 929.9 exabytes, up from 138.1 exabytes in 2017, and this mobile data traffic will be 113 times that of just 10 years earlier. The gigabyte equivalent of all movies ever made will cross mobile networks every five minutes by 2022.[7]

There is a wide array of mobile devices. These include the following:

- *Tablets*. Tablets are portable computing devices first introduced in 2010. Designed for user convenience, tablets are thinner, lighter, easier to carry, and more intuitive to use than other types of computers. Tablets generally lack a built-in keyboard or mouse. Instead, they rely on a touch screen that users manipulate with touch gestures to provide input.
- *Smartphones*. Smartphones are the most popular mobile devices. The popularity of a smartphone revolves around its OS, which allows it to run apps and access the Internet. Because it has an OS, a smartphone offers a broader range of functionality. Users can install apps to perform tasks for productivity, social networking, music, and so forth, much like a standard computer. Due to its ability to run apps, smartphones are essentially handheld personal computers that can also make phone calls.
- *Portable computers*. As a class, portable computers are devices that closely resemble standard desktop computers. Portable computers have similar hardware (keyboard, hard disk drive, and RAM, for example) and run the same OS (Windows, Apple macOS, or Linux) and applications (such as Microsoft Office and web browsers) as general-purpose desktop computers. The primary difference is that portable computers are smaller, self-contained devices that can easily be transported from one location to another while running on battery power.
- *Wearables*. The most popular wearable technology is a smart watch. A modern smart watch can receive notifications of phone calls and text messages, but it can also be used as a contactless payment system and safety monitor that calls emergency services if the watch detects the user has fallen. Figure 1-9 displays a smart watch.

Source: Alexey Boldin/Shutterstock.com

Figure 1-9 Smart watch

NOTE 12

Another popular type of wearable device is a fitness tracker. Originally designed to monitor and record physical activity, such as counting steps, they likewise have evolved into sophisticated health-monitoring devices. Modern fitness trackers can provide continuous heart rate monitoring, GPS tracking, oxygen consumption, repetition counting (for weight training), and sleep monitoring.

However, several risks are associated with mobile devices. These risks include device vulnerabilities, connection vulnerabilities, and accessing untrusted content.

Mobile Device Vulnerabilities

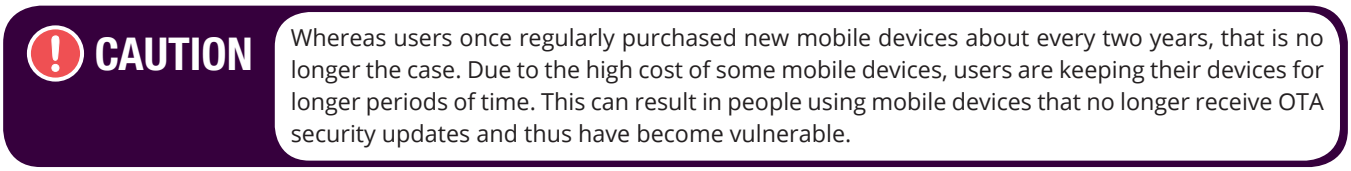
Mobile device vulnerabilities include physical security, limited updates, location tracking, and unauthorized recording.

Physical Security The greatest asset of a mobile device—its portability—is also one of its greatest vulnerabilities. Mobile devices are frequently lost or stolen because, by their very nature, they are designed for use in a wide variety of locations, both public (coffee shops, hotels, and conference centers) and private (employee homes and cars). These locations are outside of the enterprise's normal protected physical perimeter of walls, security guards, and locked doors.

Unless properly protected, any data on a stolen or lost device could be retrieved by a thief. Of greater concern may be that the device itself can serve as an entry point into corporate data. On average, every employee at an organization has access to 17 million files and 1.21 million folders. The average organization has more than half a million sensitive files, and 17 percent of all sensitive files are accessible to each employee.

Limited Updates Currently, there are two dominant OSs for mobile devices. Apple iOS, developed by Apple for its mobile devices, is a closed and proprietary architecture. Google Android is not proprietary but is open for any original equipment manufacturer (OEM) to install or even modify.

Security patches and updates for these two mobile OSs are distributed through firmware over-the-air (OTA) updates. Though these are called "firmware" OTA updates, they include modifying the device's firmware and updating the OS software. Apple commits to providing OTA updates for at least four years after the OS is released. However, OTA updates for Android OSs vary considerably. Mobile hardware devices developed and sold by Google receive Android OTA updates for three years after the device is first released. Other OEMs are required to provide OTAs for at least two years. However, after two years, many OEMs are hesitant to distribute Google updates because it limits their ability to differentiate themselves from competitors if all versions of Android start to look the same through updates. Also, because OEMs want to sell as many devices as possible, they have no financial incentive to update mobile devices that users would then continue to use indefinitely.



Location Tracking Mobile devices with Global Positioning System (GPS) capabilities typically support geolocation, or identifying the geographical location of the device. Location services are used extensively by social media, navigation systems, weather systems, and other mobile-aware applications. However, mobile devices using geolocation are at increased risk of targeted physical attacks. An attacker can determine where users with mobile devices are currently located and use that information to follow them and steal the mobile devices or inflict physical harm. In addition, attackers can craft attacks by compiling a list of people with whom the users associate and the types of activities they perform.

A related risk is GPS tagging (also called geo-tagging), which is adding geographical identification data to media such as digital photos taken on a mobile device. A user who, for example, posts a photo on a social networking site may inadvertently identify a private location to anyone who can access the photo.

Unauthorized Recording Video cameras ("webcams") and microphones on mobile devices have been a frequent target of attackers. By infecting a device with malware, a threat actor can secretly spy on an unsuspecting victim and record conversations or videos.

Connection Vulnerabilities

Vulnerabilities in mobile device connections can also be exploited by threat actors. These vulnerabilities are summarized in Table 1-5.

Accessing Untrusted Content

Normally, users cannot download and install unapproved apps on their iOS or Android device. This is because users must access the Apple App Store or Google Play Store (or other Android store) to download an app to install on a mobile device; in fact, Apple devices can only download from the App store. However, users can circumvent the

Table 1-5 Connection vulnerabilities

Name	Description	Vulnerability
Tethering	A mobile device with an active Internet connection can be used to share that connection with other mobile devices through Bluetooth or Wi-Fi.	An unsecured mobile device may infect other tethered mobile devices or the corporate network.
USB On-the-Go (OTG)	An OTG mobile device with a USB connection can function as either a host (to which other devices may be connected such as a USB flash drive) for external media access or as a peripheral (such as a mass storage device) to another host.	Connecting a malicious flash drive that is infected with malware to a mobile device could result in an infection, just as using a device as a peripheral while connected to an infected computer could allow malware to be sent to the device.
Malicious USB cable	A USB cable could be embedded with a Wi-Fi controller that can receive commands from a nearby device to send malicious commands to the connected mobile device.	The device will recognize the cable as a human interface device (similar to a mouse or keyboard) giving the attacker enough permissions to exploit the system.
Hotspots	A hotspot is a location where users can access the Internet with a wireless signal.	Because public hotspots are beyond the control of the organization, attackers can eavesdrop on the data transmissions and view sensitive information.

installed built-in limitations on their smartphone (called *jailbreaking* on Apple iOS devices or *rooting* on Android devices) to download from an unofficial third-party app store (called *sideloading*) or even write their own custom firmware to run on their device. Because these apps have not been vetted, they may contain security vulnerabilities or even malicious code.

CAUTION Jailbreaking and rooting give access to the underlying OS and file system of the mobile device with full permissions. For example, a jailbreak on an Apple iPhone will give users access to a UNIX shell that has root privileges, essentially allowing the user to do anything on the device.

Jailbreaking and rooting are not the same as carrier unlocking. Originally, almost all cell phones were connected ("locked") to a specific wireless carrier so that neither the phone nor the phone number could be transferred to another carrier. This restriction was enforced by a 2012 decision from the Library of Congress that cell phone unlocking was a violation of the Digital Millennium Copyright Act. However, in 2015, the Unlocking Consumer Choice and Wireless Competition Act, which approved carrier unlocking, was passed.

Another way untrusted content can invade mobile devices is through short message service (SMS), which are text messages of a maximum of 160 characters, or multimedia messaging service (MMS); which provides for pictures, video, or audio to be included in text messages; or rich communication services (RCS), which can convert a texting app into a live chat platform and supports pictures, videos, location, stickers, and emojis. Threat actors can send SMS messages that contain links to untrusted content or send a specially crafted MMS or RCS video that can introduce malware into the device.

Grow with Cengage Unlimited!

If you'd like more information about this topic, use your Cengage Unlimited subscription to go to the CompTIA Security+ Guide to Network Security Fundamentals, 7th edition; open Module 5; and read the section titled "Securing Mobile Devices."

If you don't have a Cengage Unlimited subscription, you can find more information at cengage.com/unlimited.

TWO RIGHTS & A WRONG

1. A field-programmable gate array (FPGA) is an integrated circuit (IC) that can be programmed by the user to carry out one or more logical operations.
2. A CAN bus is a network in a vehicle used for sending and receiving data.
3. Both Apple iOS and Google Android provide OTA updates for at least four years after the OS is released.

See Appendix C for the answer.

VM LAB You're now ready to complete the live, virtual machine labs for this module. The labs can be found in the Apply It folder in each MindTap module.

MODULE SUMMARY

- Malware, or malicious software, refers to any type of malicious software that is designed to harm or exploit a device, service, or network. It enters a computer system without the user's knowledge or consent and then performs an unwanted and harmful action. An example of malware that aids in evasion techniques is a rootkit, which is malware that can hide its presence and the presence of other malware on the computer. It does this by accessing the lower layers of the OS or even using undocumented functions.
- Several attacks are directed at vulnerabilities associated with how a program uses RAM. A storage buffer on a computer typically contains the memory location of the software program that was being executed when another function interrupted the process and is the "return address" where the computer's processor should resume once the new process has finished. A buffer overflow attack occurs when a process attempts to store data in RAM beyond the boundaries of a fixed-length storage buffer and overflows the buffer with a new address pointing to the attacker's malware code. A buffer overflow attack can occur in one of two areas of computer memory—either the stack or the heap. An integer overflow is the condition that occurs when the result of an arithmetic operation exceeds the maximum size of the integer type used to store it.
- A web server provides services that are implemented as "web applications" through software programs running on the server. A web application infrastructure is a tempting target for attackers. Many websites accept user input, and then underlying web applications use the input to create dynamic display content. Threat actors can take advantage of this user input and display in a cross-site scripting (XSS) attack. The term cross-site scripting refers to an attack using scripting that originates on one site (the web server) to impact another site (the user's computer). There are three main types of XSS attacks: Reflected XSS, Persistent XSS, and Document Object Model XSS. In addition to cross-site scripting attacks on web server applications, attacks called injections also introduce new input to exploit a vulnerability.
- One of the most common injection attacks, called Structured Query Language (SQL) injection, inserts statements to manipulate a database server. A NoSQL database that uses eXtensible Markup Language (XML) for data manipulation is also subject to an injection attack like SQL injection if the input is not sanitized. This is called an eXtensible Markup Language (XML) attack.
- A session ID is a unique value that a web server assigns a specific user for the duration of that user's visit (session). Session hijacking occurs when a threat actor takes over a user session. Different methods can be used for hijacking a session. One method involves intercepting the session ID. This can be done through XSS or a man-in-the-middle (MITM) attack in which a communication between two systems is intercepted.
- Threat actors use a variety of techniques to attack credentials and gain access to protected systems. Because passwords are the most common form of authentication credential, many of these attacks focus on attempting to compromise passwords. A password spraying attack uses one or a small number of commonly used passwords (Password1 or 123456) and then uses this same password when trying to log in to several different

user accounts. Another attack takes advantage of the very large number of stolen passwords that have been posted online by threat actors. Because users repeat their passwords on multiple accounts, attackers use these passwords in their attacks with a high probability of success. This is known as credential stuffing.

- Once initial access is gained into a system, threat actors attempt to escalate to more advanced resources that are normally protected from an application or user. This is called privilege escalation. Threat actors may use a directory traversal attack that takes advantage of a vulnerability in a web application or web server software so that a user can move from the root directory to other restricted directories. Threat actors install additional tools on the compromised systems to gain even deeper access to the network. They may also use vulnerabilities to enter commands to execute on a server known as remote code execution (RCE).
- Not all attacks rely on technology vulnerabilities; in fact, some cyberattacks use little if any technology to achieve their goals. Social engineering is a means of eliciting information (gathering data) by relying on the weaknesses of individuals. Social engineering impersonation is masquerading as a real or fictitious character and then playing out the role of that person on a victim.
- An embedded system is computer hardware and software contained within a larger system that is designed for a specific function. A growing trend is to add these capabilities to devices that have never had computing power before. Hardware and software components are available for industrious users to create their own specialized device. One of the most common hardware components is the Raspberry Pi. This is a low-cost, credit-card-sized computer motherboard. A device similar to the Raspberry Pi is the Arduino. Although the Raspberry Pi and Arduino are small motherboards, a field-programmable gate array (FPGA) is a hardware "chip" or integrated circuit (IC) that can be programmed by the user to carry out one or more logical operations. A system on a chip (SoC) combines all the required electronic circuits of the various computer components on a single IC chip. SoCs often use a real-time operating system (RTOS) that is a specifically designed OS for an SoC in an embedded or specialized system.
- Industrial control systems (ICSs) control devices locally or at remote locations by collecting, monitoring, and processing real-time data so that machines can directly control devices such as valves, pumps, and motors without the need for human intervention. Multiple ICSs are managed by a larger supervisory control and data acquisition (SCADA) system. Many SCADA systems use the network communication protocol Modbus for transmitting information between devices. Although standard Modbus has error-detection capabilities to protect against data corruption, it has no security protections against injected commands or the interception of data.
- A campus is the grounds and buildings of a school, hospital, business, or similar institution. In order to decrease the demand on personnel to monitor and manage the many elements of buildings on campus, modern campuses utilize workflow and process automation systems. These systems interconnect all the various elements so that they can be centrally and automatically monitored and controlled. One common system is a building automation system that manages building elements, which often includes a physical access control system that can ensure doors are locked and unlocked at specific times for certain individuals.
- The Internet of Things (IoT) is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies. The IoT is connecting any device to the Internet for the purpose of sending and receiving data to be acted upon. IoT usually refers to devices that heretofore were not considered as computing devices connected to a data network.
- Several types of specialized systems are designed for specific applications. Automobiles have evolved into sophisticated systems with numerous sensors and electronic control units (ECUs). The controller area network (CAN) bus network is used for sending and receiving data in a vehicle. Data broadcast through CAN from one ECU reaches all other ECUs, which then accept and evaluate the data to determine if it should be received or is unnecessary and can be ignored. An unmanned aerial vehicle (UAV), or a drone, is an aircraft without a human pilot on board to control its flight. Drones can be controlled by a remote human operator, usually on the ground, or autonomously by preprogramming the onboard computers.
- Although embedded systems and specialized devices are widely used and will continue to grow exponentially, significant security issues surround these systems and devices. The lack of security in embedded systems and specialized devices can result in a wide range of attacks. Several constraints or limitations make security a challenge for these systems and specialized devices.

- Several risks are associated with mobile devices. The greatest asset of a mobile device—its portability—is also one of its greatest vulnerabilities. Mobile devices are frequently lost or stolen because, by their very nature, they are designed for use in a wide variety of locations outside of the enterprise's normal protected physical perimeter of walls, security guards, and locked doors. Unless properly protected, any data on a stolen or lost device could be retrieved by a thief.
- Security patches and updates for two mobile OSs are distributed through firmware over-the-air (OTA) updates. Apple commits to providing OTA updates for at least four years after the OS is released. However, OTA updates for Android OSs vary considerably from two to three years. Also, because OEMs want to sell as many devices as possible, they have no financial incentive to update mobile devices that users would then continue to use indefinitely.
- Mobile devices with Global Positioning System (GPS) capabilities typically support geolocation, which is identifying the geographical location of the device. Mobile devices using geolocation are at increased risk of targeted physical attacks. An attacker can determine where users with mobile devices are currently located and use that information to follow them and steal the mobile devices or inflict physical harm. Video cameras ("webcams") and microphones on mobile devices have been a frequent target of attackers. By infecting a device with malware, a threat actor can secretly spy on an unsuspecting victim and record conversations or videos. Vulnerabilities in mobile device connections can also be exploited by threat actors.
- Normally users cannot download and install unapproved apps on their iOS or Android device. This is because users must access the Apple App Store or Google Play Store (or other Android store) to download an app to install on a mobile device; in fact, Apple devices can only download from the App store. However, users can circumvent the installed built-in limitations on their smartphone (called jailbreaking on Apple iOS devices or rooting on Android devices) to download from an unofficial third-party app store (called sideloading) or even write their own custom firmware to run on their device. Because these apps have not been vetted, they may contain security vulnerabilities or even malicious code.

Key Terms

buffer overflow attack
building automation system
controller area network (CAN) bus
credential stuffing
cross-site scripting (XSS)
directory traversal
Document Object Model XSS
drone
embedded system
eXtensible Markup Language (XML) attack
field-programmable gate array (FPGA)
heap overflow
impersonation
industrial control system (ICS)
integer overflow attack
Internet of Things (IoT)
man-in-the-middle (MITM)
Modbus
password spraying attack
Persistent XSS
physical access control
privilege escalation
real-time operating system (RTOS)
Reflected XSS
remote code execution (RCE)
rootkit
session hijacking
Structured Query Language (SQL) injection
supervisory control and data acquisition (SCADA)
system on a chip (SoC)
workflow and process automation systems

Review Questions

1. Which of the following is FALSE about rootkits?
   a. A rootkit is malware that can hide the presence of other malware.
   b. Rootkits continue to be used extensively, and their usage has not diminished.
   c. Rootkits can be used to hide their own presence.
   d. Rootkits cannot be detected by either an OS or common antimalware scanning software.
2. What is the goal of a buffer overflow attack?
   a. To change the address in the buffer to the attacker's malware code
   b. To cause the computer to function erratically
   c. To steal data stored in RAM
   d. To link to an existing rootkit

3. Which area of computer memory is dynamic memory for the programmer to allocate as necessary?
   a. Text
   b. Stack
   c. Heap
   d. Data

4. Jan is explaining to his colleague the reasons why a web application infrastructure is a tempting target for attackers. Which of the following is NOT a reason Jan would give?
   a. A successful compromise could impact all web users who access the web server.
   b. An attack could provide a pathway into the enterprise's network infrastructure.
   c. An attack on a web application infrastructure is considered the easiest attack to create.
   d. The multiple elements in a web application infrastructure provide for a range of vulnerabilities that can be used as different attack vectors.

5. Which of the following is FALSE about a cross-site scripting (XSS) attack?
   a. The underlying web application that accepts the malicious code becomes the vehicle to deliver the malicious script to every user's browser when he or she accesses that site.
   b. An attacker attempts to execute malicious scripts in the victim's web browser by directly injecting it into the user's web browser.
   c. XSS is essentially a client-side code injection attack using a web application.
   d. The term cross-site scripting refers to an attack using scripting that originates on one site (the web server) to impact another site (the user's computer).

6. Ricardo is reviewing the different types of XSS attacks. Which attack only impacts the user who entered the text on the website?
   a. Reflected XSS
   b. Persistent XSS
   c. Document Object Model XSS
   d. Universal XSS

7. What is the goal of an SQL injection attack?
   a. To corrupt data in the database
   b. To manipulate a NoSQL database
   c. To extract data from a database
   d. To inject malware that will infect the web browsers of subsequent users

8. Bette is researching how a session hijacking attack could occur. Which of the following would she NOT find as a means for the attack to occur?
   a. MITM
   b. XSS
   c. Guessing the session ID
   d. MVFL

9. Which of the following is FALSE about a password spraying attack?
   a. It takes one or a small number of commonly used passwords in attempts to break into an account.
   b. Because it is spread across many different accounts, it is much less likely to raise any alarms.
   c. It is considered as the optimal means for breaking into accounts.
   d. It is a type of targeted guessing.

10. Why is credential stuffing effective?
    a. Because users repeat their passwords on multiple accounts
    b. Because it can circumvent all known password security protections
    c. Because it is the fastest known password cracking attack
    d. Because it is the oldest and most reliable attack on passwords

11. What is the goal of a directory traversal attack?
    a. It has no goal other than to silently look through files stored on a file server.
    b. Its goal is to move from the root directory to other restricted directories.
    c. Its goal is to identify a vulnerability in a server or endpoint so that access can be gained into a network.
    d. Its goal is to pivot to another server.

12. What is pretexting?
    a. Sending text messages to selected victims
    b. Obtaining private information
    c. Preparing to enter a network through a RCE vulnerability
    d. Moving laterally before entering a vulnerable endpoint

13. Which type of OS is found on an embedded system?
    a. RSTS
    b. SoC
    c. RTOS
    d. XRXS

14. Aiko has been asked by her friend if she should download and install an app that allows her to circumvent the built-in limitations on her Android smartphone. What is this called?
    a. Jailbreaking
    b. Side-caring
    c. Rooting
    d. Pivoting

15. Aiya wants a new notebook computer. She has asked a technician about a model that has USB OTG. Which of the following would the technician NOT tell Aiya about USB OTG?
    a. A device connected via USB OTG can function as a peripheral for external media access.
    b. A device connected via USB OTG can function as a host.
    c. Connecting a mobile device to an infected computer using USB OTG could allow malware to be sent to that device.
    d. USB OTG is only available for connecting Android devices to a subnotebook.

16. The organization for which Cho works has just purchased a manufacturing plant that has many machines using Modbus. Cho has been asked to research Modbus. Which of the following will Cho NOT find regarding Modbus?
    a. Many SCADA systems use Modbus.
    b. The original version of Modbus used serial ports.
    c. A later variation to Modbus incorporated the TCP/IP protocol.
    d. Modbus is robust security.

17. What is the network used in vehicles for communications?
    a. CAN
    b. ECU
    c. EDU
    d. M-BUS

18. Which of the following is NOT a security constraint for embedded systems and specialized devices?
    a. Power
    b. Compute
    c. Cost
    d. Patches

19. Which of the following is the greatest asset but also a security vulnerability of a mobile device?
    a. Low cost
    b. Portability
    c. Cameras
    d. Small screen

20. What is geo-tagging?
    a. Restricting where an app functions based on its location.
    b. Adding geographical identification data to media.
    c. Tracking a victim who is wearing a GPS-enabled wearable device.
    d. Using the GPS feature of a smartphone.

Case Projects

Case Project 1-1: Rootkits

Research how rootkits can evade detection from an OS or antimalware software. What techniques does it use to hide itself? How can it hide other malware? Besides hiding malware on a hard drive, where are other locations that rootkits can hide malware? Write a one-page paper on your research.

Case Project 1-2: Heap Overflow

Research heap overflows. How do they work? How can they be prevented? How common is this type of attack? Write a one-page paper on your research. Include a drawing of how RAM looks before and after a heap overflow attack.

Case Project 1-3: Document Object Model XSS

Search the Internet for information on Document Object Model XSS. What is a Document Object Model (DOM)? Where are DOMs found? How do threat attacks attempt to compromise them? How can they be used in an XSS attack? What is the defense against them? Write a one-page paper on your research.

Case Project 1-4: Real-Time Operating System (RTOS)

What features are found in a real-time operating system? How is it specifically designed for an SoC? What are its advantages? What are its disadvantages? Compare the features of three RTOSs, and create a table listing each along with its features. Write a one-page paper on your research.

Case Project 1-5: On the Job

Suppose you work for a company that has just hired a new senior vice president. After reviewing the budgets of all departments, the new VP went on record saying that the amount of money spent on cybersecurity is too large in proportion to the size of the company. She recommends an immediate 23 percent reduction in the cybersecurity budget. She has decided on this amount after informal conversations with other companies that have about the same number of employees. However, these other companies perform completely different functions: one company is in manufacturing while the other is a service organization, neither of which is the same as your company. The new VP says she will retract her recommendation if someone can prove that there have been no significant attacks due to the money spent on cyber defenses and not just because your company is unattractive to threat actors. Create a one-page memo to the senior vice president that explains your views on cybersecurity spending.

References

1. "McAfee Labs Threats Report," Jul. 2020, accessed Nov. 3, 2020, www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-july-2020.pdf.
2. "Cybercrime to Cost the World $10.5 Trillion Annually by 2025," *Cybersecurity Ventures*, accessed Dec. 30, 2020, www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-The-World-10-5-Trillion-Annually-By-2025.html#:~:text=18%2C%202020%20(GLOBE%20NEWSWIRE),%243%20trillion%20USD%20in%202015.
3. Crawley, Kim, "Cybersecurity Budgets Explained: How Much Do Companies Spend on Cybersecurity?" *AT&T* Cybersecurity, May 5, 2020, accessed Nov. 3, 2020, https://cybersecurity.att.com/blogs/security-essentials/how-to-justify-your-cybersecurity-budget.
4. Moynahan, Matthew, "How Not to Waste a Trillion Dollars on Cybersecurity," *Forbes*, Nov. 9, 2018, accessed Apr. 21, 2019, www.forbes.com/sites/forbestechcouncil/2018/11/09/how-not-to-waste-a-trillion-dollars-on-cybersecurity/#75f16ed0df9a.
5. "Overview of the Internet of Things, Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks—Next Generation Networks—Frameworks and Functional Architecture Models," Jun. 2012, Retrieved May 18, 2017, www.itu.int/rec/T-REC-Y.2060-201206-I.
6. "Forecast Number of IoT Connected Objects Worldwide from 2018 to 2025, by Type," Statista, retrieved May 28, 2020, www.statista.com/statistics/976079/number-of-iot-connected-objects-worldwide-by-type/.
7. "VNI Mobile Forecast Highlights Tool," Cisco, accessed Nov. 6, 2020, www.cisco.com/c/m/en_us/solutions/service-provider/forecast-highlights-mobile.html.

MODULE 2

UTILIZING THREAT DATA AND INTELLIGENCE

After completing this module, you should be able to do the following:

1. Identify different threat actors
2. Describe threat intelligence sources
3. Define frameworks and research sources
4. Explain modeling methodologies

Cybersecurity Today

Cybercrime is universally seen as relentless, undiminished, and unlikely to stop because it is just too easy and rewarding. One reason is that the chances of being caught and punished are almost negligible. Cybercriminals who operate in foreign nations can attack users and governments around the world with impunity because they know that their own government agencies reject any attempts to cooperate with law enforcement agencies in the victim's country and openly laugh at any attempts to extradite these criminals for prosecution. Often foreign governments take this approach to show open contempt against another nation or because the government itself is funding and supporting these attacks.

Another reason for unrestrained global cybercrime is that there has been a lack of a united global effort against it. A single nation in which the victims reside ("victim nation") must attempt to negotiate with the "attacking nation" for justice. Most attacking nations simply ignore these pleas, as they face few repercussions. If the victim nation breaks off diplomatic relations with the attacking nation or stops exporting its goods to them, the attacking nation will simply turn to another nation to import those same goods. This lack of unity among nations against cybercrime is one of the recognized reasons why cybercrime runs unabated.

However, two watershed events in recent years may have finally turned the tide against international attackers hiding behind foreign attacking nations. First, foreign governments, most notably Russia, have been identified as meddling in the democratic election processes of other nations. The United States, the Netherlands, Ukraine, and France have all been victims of foreign cyberattacks and operations to affect political campaigns, candidates, and open political discourse. Using sophisticated social media efforts as well as more traditional cybersecurity attacks on voter rolls and state electoral systems, these incidents have been designed as a concerted campaign to undermine democracy and weaken trust in the democratic process and institutions. These attacks have been directed at perceived opponents and other foreign governments to move support toward candidates who are more sympathetic to Russian interests.

The second watershed event was cyberattacks used to disrupt healthcare organizations fighting the COVID-19 pandemic. Security researchers have detected cyberattacks in Canada, France, India, South Korea, and the United States targeting prominent pharmaceutical companies and vaccine researchers directly involved in creating vaccines and treatments.

Threat actors have also attacked individual hospitals, the hospital system in Paris, the computer systems of Spain's hospitals, hospitals in Thailand, medical clinics in Texas, a healthcare agency in Illinois, and even international bodies such as the World Health Organization (WHO). These attacks are alleged to be the efforts of a group known as Strontium, an actor originating from Russia, and two actors—Zinc and Cerium—from North Korea.

These two watershed events have galvanized countries to take a unified stand against foreign nation-state actors. Knowing that many nations banding together can have much more influence than a single victim nation, several international efforts have recently been initiated as multi-stakeholder coalitions involving countries around the world to actively combat the attacks.

In 2019, the United Nations established a Group of Governmental Experts (GGE) on advancing responsible state behavior in cyberspace for cybersecurity. In 2020, three major efforts were begun. More than 65 healthcare-related organizations joined the Paris Call for Trust and Security in Cyberspace. These include pharmaceutical organizations working on vaccines, hospitals, and government health institutes. The Paris Call remains the largest multi-stakeholder coalition addressing these issues, and its first principle is the prevention of malicious cyber activities that threaten indiscriminate or systemic harm to people and critical infrastructures. In May 2020, a group of 36 of the world's most prominent international law experts, in what has become known as the Oxford Process, issued a statement making it clear that international law protects medical facilities at all times. In August of the same year, the Oxford Process issued a second statement emphasizing that organizations that research, manufacture, and distribute COVID-19 vaccines are also protected. Finally, the CyberPeace Institute and International Committee of the Red Cross led an effort by 40 international leaders calling on governments to stop the attacks on healthcare.

While the overall impact of these initiatives remains to be seen, one thing is clear. For the first time, nations from around the world are banding together to address cybersecurity threats in new ways.

There are no major sporting events today in which two teams playing for the championship do not know in advance who their opponent is. This is because enabling both teams to know their opponent in advance gives them time to study the strengths and weaknesses of the opposition and then craft a plan that leads to victory.

Likewise, in the competition known as cybersecurity, it is important to know both who the attackers are and how they attack. Because attacks continually evolve, it is also important to take advantage of all available threat intelligence information to know the very latest types of attacks and how to defend against them. With that information at hand, security can become more effective and efficient.

In this module, you will explore using threat data and intelligence. First, you will examine today's threat actors and their threats. You will then look at threat data and intelligence. Next, you will explore frameworks and threat research sources and, finally, study different modeling methodologies.

THREAT ACTORS AND THEIR THREATS

CERTIFICATION

1.1 Explain the importance of threat data and intelligence.

"Know your enemy" is an oft-quoted statement, with applications ranging from military to sports. Knowing the cybersecurity attackers and their attacks is likewise important in creating a strong cyberdefense.

NOTE 1

The famous Chinese military strategist Sun Tzu said more than 1,500 years ago in *The Art of War*, "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

Who Are the Threat Actors?

In cybersecurity, a **threat actor** is a term used to describe individuals or entities who are responsible for cyber incidents against enterprises, governments, and users. The generic term *attacker* is also commonly used, as is *malicious actor.* In the past, the generic term *hacker* referred to a person who used advanced computer skills to attack computers. Yet because that title often carried with it a negative connotation, it was qualified in an attempt to distinguish between different types of hackers. The different types of hackers are summarized in Table 2-1.

Table 2-1 Types of hackers

Hacker type	Description
Black hat hackers	Threat actors who violate computer security for personal gain (such as to steal credit card numbers) or to inflict malicious damage (corrupt a hard drive)
White hat hackers	Also known as ethical attackers, they attempt to probe a system (with an organization's permission) for weaknesses and then privately provide that information back to the organization
Gray hat hackers	Attackers who attempt to break into a computer system without the organization's permission (an illegal activity) but not for their own advantage; instead, they publicly disclose the attack to shame the organization into taking action

However, these broad categories of hackers did not accurately reflect the differences among threat actors. The attributes, or characteristic features, of today's different groups of threat actors can vary widely. While some groups have a high level of capability and a massive network of resources, others are "lone wolves" who know how to acquire easy-to-use software like the one shown in Figure 2-1 to perform high-level attacks or know

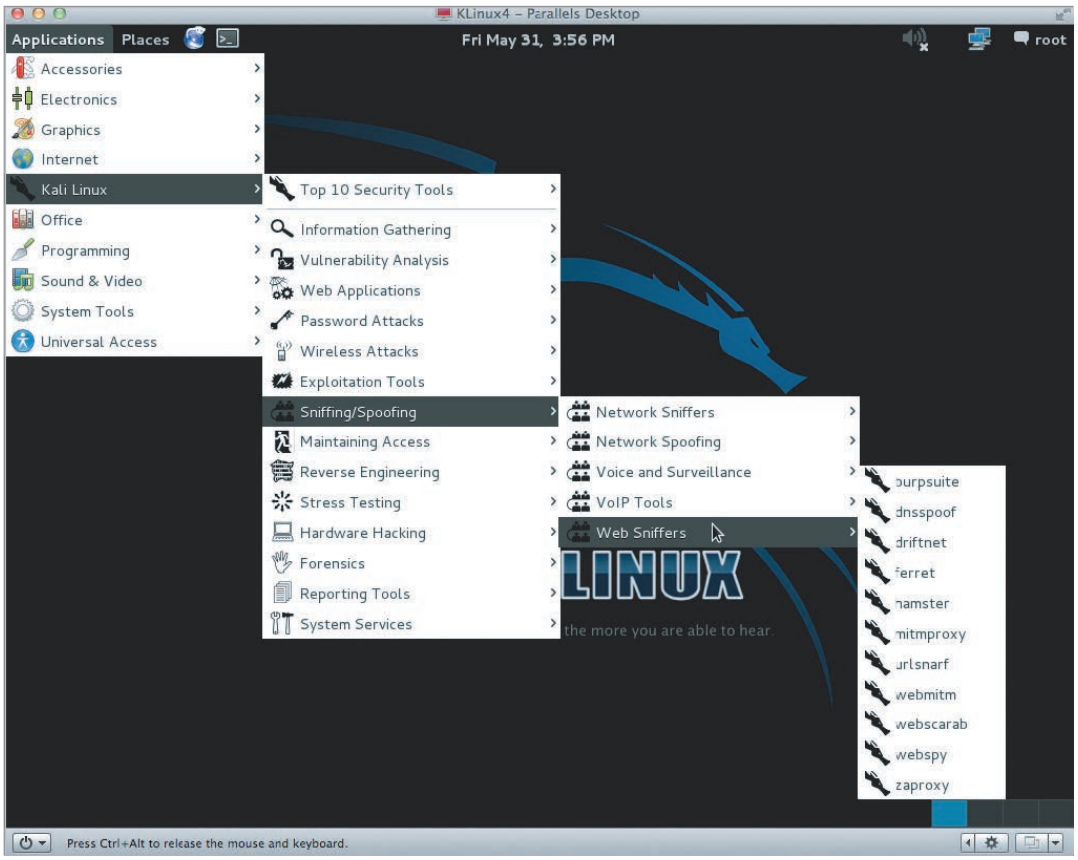


Figure 2-1 Easy-to-use attack software

where to purchase **commodity malware**, which is malware sold by other threat actors that can be customized for specific attacks. Whereas some threat actors work within the enterprise (internal), others are strictly from outside the organization (external). Finally, the intent or motivation—that is, the "why" behind the attacks—can vary widely.

Despite these differences, one element is common to all threat actors: they pose a serious threat to security. Threat actors who may not be as well educated in cyberattacks or may lack the "deep pockets" of funding sources nevertheless are a real threat. Many attackers have even modeled their work after modern economic theories, such as finding the optimum "price point" in which victims will pay a ransom. Some enterprising attackers who sell their commodity malware to other attackers now design these attack tools as a suite that receive regular updates and enhancements. It is a serious mistake to underestimate *any* modern threat actors.

Today threat actors are classified into distinct categories that address their capabilities, resources, and motivations. These include hactivists, nation-state actors, insider threats, and others.

Hactivists

A group that is strongly motivated by ideology (for the sake of their principles or beliefs) is **hactivists** (a combination of the words *hack* and *activism*). Most hactivists do not explicitly call themselves "hacktivists," but the term is commonly used by security researchers and journalists to distinguish them from other types of threat actors.

In the past, the types of attacks by hactivists usually involved defacing websites. They did so as a means of making a political statement (one hactivist group changed the website of the U.S. Department of Justice to read *Department of Injustice*) or performing retaliation (hactivists have disabled a bank's website because that bank stopped accepting online payments deposited into accounts belonging to groups supported by hactivists).

However, today most hactivists work through disinformation campaigns by spreading fake news and supporting conspiracy theories. As an example, hactivists were active during the coronavirus disease (COVID-19) pandemic of 2020. One large group of what were considered far-right neo-Nazi hactivists embarked on a months-long disinformation campaign designed to weaponize the pandemic by questioning scientific evidence and research. In another instance, thousands of breached email addresses and passwords from U.S. and global health organizations—including the U.S. National Institutes of Health, Centers for Disease Control and Prevention, and the WHO—were distributed on social media by these groups (called *doxing*). The intent was to encourage others to use this information to harass and distract the health organizations.

Nation-State Actors

Governments are increasingly employing their own state-sponsored attackers for launching cyberattacks against their foes. They are known as **nation-state actors**. Their foes may be foreign governments or even their own citizens that the government considers hostile or threatening. A growing number of attacks from state actors are directed toward businesses in foreign countries with the goal of causing financial harm or damage to the enterprise's reputation.

Many security researchers believe that nation-state actors might be the deadliest of any threat actors. When money motivates a threat actor, but the target's defenses are too strong, the attacker simply moves onto another promising target with less effective defenses. With nation-state actors, however, the target is very specific, and the attackers keep working until they are successful. These state-sponsored attackers are highly skilled and have enough government resources to breach almost any security defense.

Insiders

Another serious threat to an enterprise comes from its own employees, contractors, and business partners, called *insiders*, who pose an **insider threat** of manipulating data from the position of a trusted employee. The threats that come from insiders can be either intentional or unintentional.

Intentional Insiders There are several reasons that insiders may intentionally steal or alter data that belongs to their organization. A healthcare worker, for example, who is disgruntled about being passed over for a promotion, might illegally gather health records on celebrities and sell them to the media. A securities trader who loses billions of dollars on bad stock bets could use knowledge of the bank's computer security system to conceal the losses through fake transactions. These attacks by intentional insiders are harder to recognize than other types of attacks because they come from within the enterprise, while defensive tools are usually focused on outside attackers.

Intentional insider attacks can be costlier than attacks from the outside. Six out of ten enterprises reported being a victim of at least one insider attack during 2019. The focus of these insiders were intellectual property (IP) theft (43 percent), sabotage (41 percent), and espionage (32 percent).[1] Because most IP thefts occur within 30 days of an employee resigning, it is thought that these insiders believe that either the IP belongs to them instead of the enterprise or that they were not properly compensated for their work behind the IP. In recent years, government insiders have stolen large volumes of sensitive information and then published it to alert its citizens of clandestine governmental actions.

Unintentional Insiders Attacks are often the result of unintentional insiders. Although they may not have malicious intent, due to their action (or inaction), unintentional insiders can unwittingly cause harm (or increase the probability of serious future harm) to the organization's resources and assets. The reasons range from carelessness, too much multitasking, and low situational awareness. Consider the following actual events:

- HSBC, one of the largest banking and financial services institutions in the world, had to apologize in 2017 after an insider employee unintentionally emailed personal information about its customers to various account holders. The personal information contained names, email addresses, countries of residence, the name of the customers' relationship manager, and HSBC customer identification numbers. This error follows earlier incidents by HSBC of sending the details of 1,917 pension scheme members—including addresses, dates of birth, and national insurance numbers—and sending the details of 180,000 policyholders.
- Wells Fargo, when subpoenaed by an attorney for information related to a lawsuit, should have sent a few emails and selected documents. However, an insider unintentionally sent 1.4 gigabytes of confidential information about 50,000 of the bank's wealthiest clients. The information included customers' names and Social Security numbers along with financial details such as the size of their investment portfolios and the fees the bank charged them.

NOTE 2

The response by Wells Fargo to this incident was, "This was the unfortunate result of an unintentional human error involving a spreadsheet."

Data supports evidence of the harm that is caused by unintentional insiders. Almost two out of every three organizations found that a careless employee or contractor was the root cause of most insider incidents. Misdelivery, or sending sensitive information to a recipient who is not authorized to receive it, is the fourth most frequent action that results in data breaches across all businesses and was the cause of 35 percent of all data breaches in 2019.[2]

NOTE 3

Insider carelessness often involves the employee not considering the consequences of an action. For example, more than half of all employees admit to allowing a friend or family member to use employee-issued technology equipment while at home, which could expose access to highly sensitive data such as the organization's proprietary information or private customer data.

Other Threat Actors

In addition, there are other categories of threat actors. These are summarized in Table 2-2.

Table 2-2 Descriptions of other threat actors

Threat actor	Description	Explanation
Competitors	Launch attack against an opponent's system to steal classified information.	Competitors may steal new product research or a list of current customers to gain a competitive advantage.
Brokers	Sell their knowledge of a weakness to other attackers or governments.	Individuals who uncover weaknesses do not report it to the software vendor but instead sell them to the highest bidder, who is willing to pay a high price for the unknown weaknesses.
Cyberterrorists	Attack a nation's network and computer infrastructure to cause disruption and panic among citizens.	Targets may include a small group of computers or networks that can affect the largest number of users, such as the computers that control the electrical power grid of a state or region.
Organized crime	Moving from traditional criminal activities to more rewarding and less risky online attacks.	Organized criminal syndicates are usually run by a small number of experienced online criminal networks who do not commit crimes themselves but act as entrepreneurs.
Shadow IT	Employees become frustrated with the slow pace of acquiring technology, so they purchase and install their own equipment or resources in violation of company policies.	Installing personal equipment, unauthorized software, or using external cloud resources can create a weakness or expose sensitive corporate data.

Classifying Threats

At a U.S. Department of Defense (DoD) news briefing in 2002, the Secretary of Defense Donald Rumsfeld was asked a question regarding the lack of evidence linking a foreign government with the supply of weapons of mass destruction to terrorist groups. Secretary Rumsfeld responded:

> *Reports that say that something hasn't happened are always interesting to me, because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say, we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones.*[3]

Secretary Rumsfeld's statement is considered the first time the general public was exposed to the concept of *known knowns*, *known unknowns*, and *unknown unknowns*. However, national security and intelligence professionals had for several years used a similar approach based on an analysis technique created in the mid-1950s. This technique was developed to help individuals understand their relationship with others and themselves. The technique is called the *Johari window* and is shown in Figure 2-2.

NOTE 4

At the time that Secretary Rumsfeld made his comments, he was criticized because some individuals felt that the comments did not make sense and were an unnecessarily complex way of explaining the issues around security intelligence. However, as time passed, his observation was considered insightful.

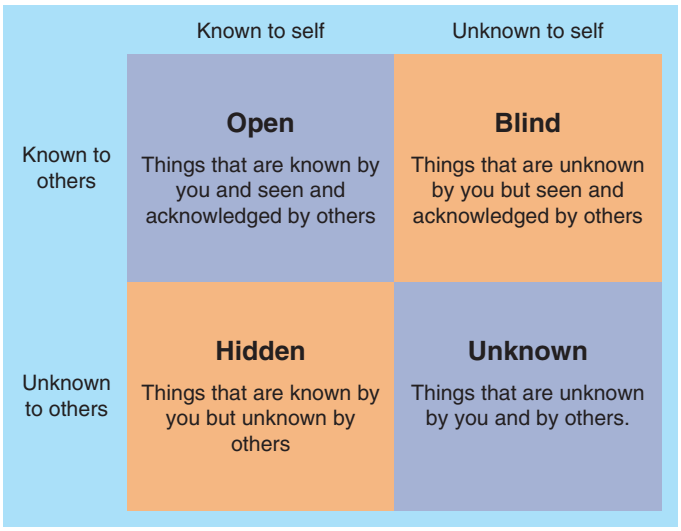


Figure 2-2 Johari window

Today cybersecurity professionals have adopted the Johari window as one means of classifying cybersecurity threats, particularly **known threats vs. unknown threats**, or classifying threats by comparing the knowledge of the threat actor to security personnel. Figure 2-3 applies the Johari window to these cybersecurity threats.

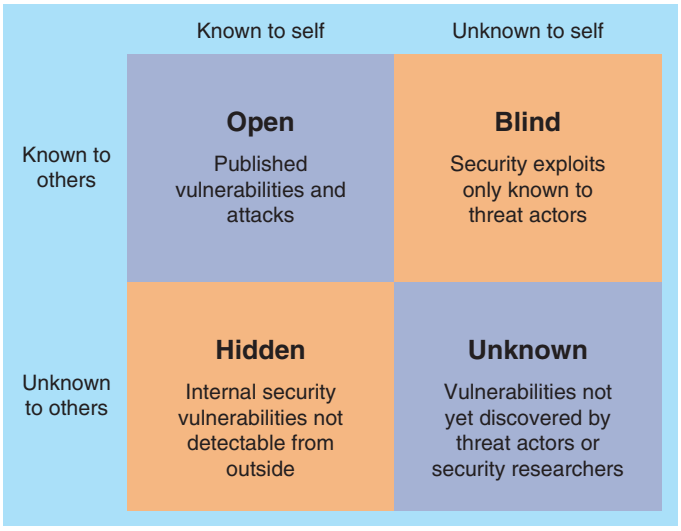


Figure 2-3 Johari window cybersecurity threats

The four categories of these threats are as follows:

- *Known knowns*. These are threats that both threat actors and security personnel are aware of, such as a virus that has been active for several years. The defense against these threats is established technologies and devices such as antivirus solutions and firewalls.
- *Known unknowns*. Known unknowns refer to vulnerabilities that the organization is aware of in their systems but outside threat actors have not discovered. A defense against these are actions taken by the organization to address the vulnerability.

- *Unknown knowns*. These are threats that are known to threat actors but not to security professionals. Often called **zero-day attacks**, these are unknown vulnerabilities and give victims no time (*zero days*) to prepare or defend against the attacks. There is no defense strategy against unknown knowns.
- *Unknown unknowns*. Unknown unknowns are security threats that currently are hidden from both threat actors as well as security professionals. There is no indication when—or if—they will be found. Like unknown knowns, there is no specific defense against these.

NOTE 5

Although the Johari window is a common means of classifying threats, there are others as well.

A particularly ominous threat that has emerged in recent years must also be classified. Nation-state actors are known for being well-resourced and highly trained attackers. They often are involved in multiyear intrusion campaigns targeting very sensitive economic, proprietary, or national security information. These threat actors have created a new class of attacks called **advanced persistent threats (APTs)**. They use innovative attack tools (*advanced*), and once a system is infected, they silently extract data over an extended period of time (*persistent*). APTs are most commonly associated with nation-state actors.

TWO RIGHTS & A WRONG

1. Hactivists are responsible for the class of attacks called advanced persistent threats.
2. Hactivists are strongly motivated by ideology.
3. Brokers sell their knowledge of a weakness to other attackers or a government.

See Appendix C for the answer.

THREAT DATA AND INTELLIGENCE

CERTIFICATION

1.1 Explain the importance of threat data and intelligence.

1.2 Given a scenario, utilize threat intelligence to support organizational security.

Threat data and intelligence has become a vital source today for organizations attempting to defend against emerging attacks. Using threat data and intelligence involves understanding what constitutes threat data and intelligence, knowing the intelligence cycle, and understanding the categories and sources of threat intelligence.

What Is Threat Data and Intelligence?

At one time, organizations were reluctant to share information about attacks on their networks and endpoints, often because they were concerned about "bad publicity" that might arise from the disclosure. Not sharing details about threats (**threat data and intelligence**) only crippled cybersecurity defenses. Organizations had data and intelligence on threats that affected only that organization, which resulted in a limited volume of details. In addition, they could not address emerging or zero-day attacks.

Today, however, that is no longer the case. Organizations are pooling their experiences and knowledge gained about the latest attacks with the broader security community. Sharing this type of information has become an important aid to help other organizations shore up their defenses.

An example of the type of information that is shared is the evidence of an attack. Most organizations monitor their networking environment to determine what normally occurs. This data is then used to create a database of *key risk indicators (KRIs)*. A KRI is a metric of the upper and lower bounds of specific indicators of normal network activity. These indicators may include the total network logs per second, the number of failed remote logins, network bandwidth, and outbound email traffic. When a KRI exceeds its normal bounds, it could be (but is not always) evidence of an **indicator of compromise (IoC)**. An IoC shows that a malicious activity is occurring but is still in the early stages of an attack.

Making IoC information available to others can prove to be of high value, as it may indicate a common attack that other organizations may also be experiencing or will soon experience. This information aids others in their predictive analysis or discovering an attack before it occurs.

NOTE 6

Like radar that shows the enemy approaching, predictive analysis helps determine when and where attacks may occur.

In addition to identifying an imminent attack by sharing IoCs, threat intelligence sharing can also aid in other areas such as **incident response** (handling a cyberattack or data breach), **vulnerability management** (identifying and addressing security vulnerabilities), **risk management** (controlling threats to assets), **security engineering** (building systems to resist attacks), and **detection and monitoring** (uncovering and managing vulnerabilities).

The Intelligence Cycle

What is the difference between *data, information,* and *knowledge*? Although these terms are often used synonymously, they vary significantly. Table 2-3 provides definitions and examples that illustrate the differences between these terms.

Table 2-3 Differences between data, information, and knowledge

Element	Definition	Example
Data	Discrete, objective facts	141, 700, A, 701, B
Information	Organized data that has been processed so it has meaning and value	Course 141-700 is offered in the A-Term
Knowledge	Expert skills and experience applied to information in order to make informed decisions	Enrollment in CIS 141/700 A-Term has increased over CIS 141/701 in the B-Term

NOTE 7

Another element that could be added is *wisdom*, which may be defined as administering knowledge.

When a cyber incident occurs, the data about it can be captured, such as the type of attack, the target, the time of day it occurred, and the IP address of the source. However, the data is only discrete facts and, in this form, has limited value. The data needs to be "processed" to become useful information. The process through which raw cybersecurity data becomes useful threat intelligence information can be illustrated by the **intelligence cycle**, also called the *threat intelligence lifecycle*. Figure 2-4 illustrates an intelligence cycle. This cycle is considered a multi-step cyclical process: more than one step is involved, and the process continues to cycle with no endpoint.

CAUTION A multitude of intelligence cycles relate to cybersecurity, each with any number of steps using different terminology. The intelligence cycle presented here is the core of most intelligence cycles.

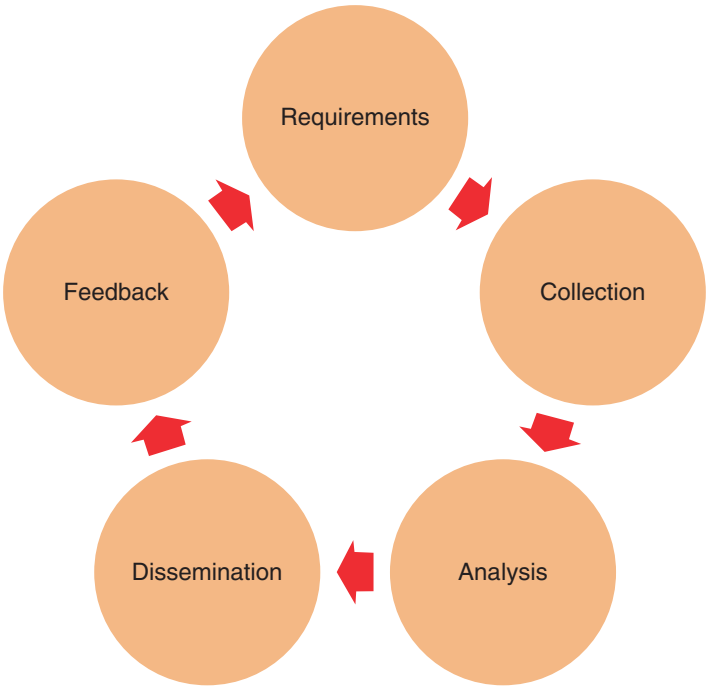


Figure 2-4 Intelligence cycle

The steps of the intelligence cycle are as follows:

- *Requirements*. The **requirements** phase of the intelligence cycle sets the high-level goals for the threat intelligence program. This involves determining the information assets and business processes that need to be protected, the potential impacts of losing those assets or interrupting those processes, and the priorities of what order to provide protection. This phase helps determine the types of threat intelligence that are needed to protect assets and respond to threats. For example, if a goal is to understand likely threat actors, this could be framed as a question such as, "Which actors on underground forums are actively soliciting data concerning our organization?"
- *Collection*. **Collection** is the process of gathering information to address the most important intelligence requirements. Numerous sources provide this threat information. An organization can gather log information and metadata from internal networks and security devices by conducting targeted interviews with knowledgeable security sources, scanning security news and blogs, harvesting information from user forums, scraping attacker data posted on public sites (called "pastes"), and even infiltrating threat actor closed sources. An increasing number of organizations are subscribing to threat data feeds from industry organizations and cybersecurity vendors for threat intelligence.
- *Analysis*. The data gathered at the collection stage typically will be a combination of finished information (such as intelligence reports from cybersecurity experts and vendors) along with raw data (like malware signatures or pasted leaked credentials). This data must be processed into a format usable by the organization in the **analysis** phase. Different collection methods often require different means of processing. For example, an analysis may involve extracting IP addresses from a security vendor's report or extracting indicators from an email before enriching them with other information.
- *Dissemination*. The results of the analysis phase will drive decisions about how this information should be acted upon and distributed to where it needs to go (**dissemination**). Typical decisions involve whether to investigate a potential threat, what actions to take immediately to stop an attack (such as communicating with endpoint protection tools for automated blocking), how to strengthen security controls, or how much investment in additional security resources may be needed. These decisions then drive how the threat intelligence is disseminated.

NOTE 8

Most organizations have multiple security-related teams that need threat intelligence. The process of dissemination should be determined in advance by asking the teams how best to provide the information to them. There are several questions that could be asked: What threat intelligence do you need? How can external information support your activities? How should the intelligence be presented to make it easily understandable and actionable for you? How often should we provide updates and other information? Through what media should the intelligence be disseminated?

- *Feedback*. The final phase is **feedback** regarding how effective the threat intelligence was. Feedback can be viewed as answering the basic question, "What did we do right, and what did we do wrong?" The answers then become input back into the requirements phase to improve the overall intelligence cycle.

Categories of Threat Intelligence Sources

There are two broad categories of threat intelligence sources. These are open source and closed source intelligence.

Open Source Intelligence

Threat intelligence that is freely available, often called **open source intelligence (OSINT)**, has become a vital resource. The most basic level of OSINT typically consists of public lists of threat indicators that anyone can download. This type of threat intelligence, sometimes called "abuse feeds" and "blacklists," is curated by one or more security professionals as a service (or sometimes just as a hobby) to the larger security community. Users of these public lists are also encouraged to upload their own malware samples to be analyzed.

A more formalized level of OSINT sharing is conducted through trusted communities where official membership is required and the members exchange their own threat information. This information is often collected and then disseminated through public information sharing centers. A typical sharing center is the U.S. Department of Homeland Security (DHS) Cyber Information Sharing and Collaboration Program (CISCP). The CISCP "enables actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure sectors." With the DHS serving as the coordinator, the CISCP enables its members (called "partners") to not only share threat and vulnerability information but also take advantage of the DHS's cyber resources. Some of the CISCP services include the following:

- *Analyst-to-analyst technical exchanges*. Partners can share and receive information on the tactics used by threat actors and emerging trends.
- *CISCP analytical products*. A portal can be accessed through which partners can receive analysis of products and threats.
- *Cross-industry orchestration*. Partners can share lessons learned and their expertise with peers across common sectors.
- *Digital malware analysis*. Suspected malware can be submitted to be analyzed and then generate malware analysis reports to mitigate threats and attack vectors.

NOTE 9

The CISCP program is free to join and use. Those interested must agree to a Cyber Information Sharing and Collaboration Agreement (CISCA), which enables DHS and its partners to exchange anonymized information. Once partners sign the agreement, DHS coordinates an on-boarding session to customize how DHS and the organization can exchange information.

The final level of OSINT is composed of similar organizations that share information that may be unique to their specific industry. These include the areas of healthcare, financial services, aviation, government, and critical infrastructure. The organizations that share OSINT are called **information sharing and analysis communities**.