

Dear student

There are significant efforts behind the completion of this book, in the process of its preparation, review, and development, and there are funds spent to print it and deliver it to you, to support your learning and your scientific and moral advancement, so, try to be faithful to this effort, appreciating it by preserving your book.



وزارة التعليم
Ministry of Education
2026 - 1448

Name: School:

Deposit number: **1446/19517**
ISBN: **978-603-514-067-6**

Cybersecurity

Third year - Secondary stage - Pathways System

1448 - 2026 Edition

المملكة العربية السعودية

رؤية
2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

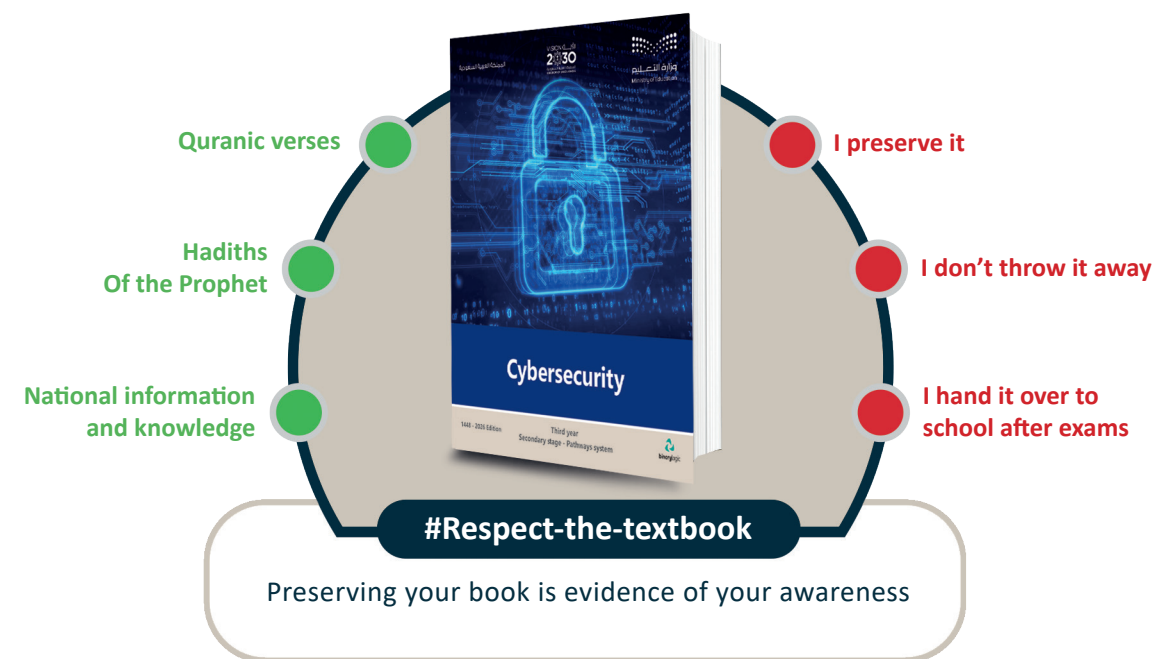
وزارة التعليم
Ministry of Education

Cybersecurity

1448 - 2026 Edition

Third year
Secondary stage - Pathways system





قررت وزارة التعليم تدريس
هذا الكتاب وطبعه على نفقتها



المملكة العربية السعودية

Cybersecurity

Secondary stage - Pathways system

Third year



Publisher: Tatweer Company for Educational Services

Published under a special agreement between Binary Logic SA and Tatweer Education Services Company (Contract No. 0003/2022) for use only in the Kingdom of Saudi Arabia

Copyright © 2026 Binary Logic SA

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without permission in writing from the publishers.

Please note: This book contains links to websites that are not maintained by Binary Logic. Although we make every effort to ensure these links are accurate, up-to-date and appropriate, Binary Logic cannot take responsibility for the content of any external websites.

Trademark notice: Product or corporate names mentioned herein may be trademarks or registered trademarks and are used only for identification and explanation without intent to infringe. Binary Logic disclaims any affiliation, sponsorship, or endorsement by the respective trademark owners. Windows is a registered trademark of Microsoft Corporation. "Python" and the Python logos are registered trademarks of Python Software Foundation. Wireshark is a registered trademark of Wireshark Foundation. DB Browser for SQLite is a registered trademark of DB Browser for SQLite. Google Chrome is a registered trademark of Alphabet Inc.

The above companies or organizations do not sponsor, authorize, or endorse this book.

The publisher has made every effort to trace all copyright holders, but if they have inadvertently overlooked any they will be pleased to make the necessary arrangements at the first opportunity.



©National Curriculum Center, 2025

National Curriculum Center

Cybersecurity. / National Curriculum Center .-

Riyadh, 2025

141p.; 210*25.5cm

L.D. no.: 1446/19517

ISBN: 978-603-514-067-6

Copyright reserved to the Ministry of Education

www.moe.gov.sa

Enrichment and support materials on the “iEN Ethraia Platform”



ien.edu.sa

Dear students, parents and anyone interested in education, we welcome your communication to improve our textbooks. Your suggestions are our top priorities.



fb.ien.edu.sa



Introduction:

The progress and development of countries is measured by the ability to invest in education, and the extent to which their educational system responds to the requirements and changes of the generations. In the interest of the Ministry of Education sustaining the development of its educational systems, and in response to the vision of the Kingdom of Saudi Arabia 2030, the Ministry of education has taken the initiative to adopt the “Secondary Education Pathways” system to bring about an effective and comprehensive change in high school.

The secondary education pathways system provides a distinguished and modern educational model for high school in the Kingdom of Saudi Arabia, which efficiently contributes to:

- Strengthening the values of belonging to our homeland “the Kingdom of Saudi Arabia” and loyalty to its wise leadership “may God protect him” based on a pure belief supported by the tolerant teachings of Islam.
- Strengthening the values of citizenship by focusing on them in school subjects and activities, in line with the demands of sustainable development, and the development plans in the Kingdom of Saudi Arabia that emphasize the consolidation of both values and identity, based on the teachings of Islam and its moderation.
- Qualifying students in line with future specializations in universities or the required jobs; ensuring the consistency of education outputs with the labor market requirements.
- Enabling students to pursue education in their preferred path at early stages, according to their interests and abilities.
- Enabling students to join specific scientific and administrative disciplines related to the labor market and future jobs.
- Participation of students in an enjoyable and encouraging learning environment in school based on a constructive philosophy and applied practices within an active learning environment.
- Delivering students through an integrated educational journey from the primary level to the end of the high school level and facilitating their transition process to post-general education.
- Providing students with technical and personal skills that help them deal with life and respond to the requirements of their level.
- Expanding opportunities for graduate students through various options in addition to universities, such as: obtaining professional certificates, joining applied faculties, and earning job diplomas.

The pathways system consists of nine semesters that are taught over three years, including a common first year in which students receive lessons in various scientific and humanities fields, followed by two specialized years, in which students study a general path and four specialized paths consistent with their interests and abilities, which are: the Rightful path, Business Administration path, Computer Science and Engineering path, Health and Life path, which makes this system the best for students in terms of:

- The existence of new study subjects that match the requirements of the Fourth Industrial Revolution and development plans, and the Kingdom’s Vision 2030, which aims to develop higher-order thinking, problem-solving, and research skills.
- Elective field programs that are consistent with the needs of the labor market and students’ interests, as they enable students to join a specific elective field according to a specific job skill.
- Scale as it ensures the achievement of students’ efficiency and effectiveness, and helps them identify their tendencies and interests, and reveal their strengths, which enhances their chances of success in the future.
- Volunteer work designed specifically for students in line with the philosophy of activities in schools, and is one of the graduation requirements; which helps to promote human values, and build society (its development and cohesion).

- Bridging which enables students to move from one path to another according to specific mechanisms.
- Proficiency classes through which skills are developed and the achievement level improved, by providing enrichment and remedial mastery classes.
- The options of integrated learning and distance learning, which are built in the paths system based on flexibility, convenience, interaction and effectiveness.
- The graduation project that helps students integrate theoretical experiences with applied practices.
- Professional and skill certificates granted to students after completing specific tasks, and certain tests compatible with specialized organizations.

Accordingly, the computer science and engineering path as one of the updated paths at the secondary level contributes to achieving best practices by investing in human capital, and transforming the student into a participating and productive individual for science and knowledge, while providing him with the skills and experience necessary to complete his studies in fields that meet his interests and abilities, or to join the labor market.

Cybersecurity is one of the main subjects in the Computer Science and Engineering Pathway, presented in a single comprehensive book. This book aims to provide an understanding of the concepts and technologies associated with Cybersecurity, specifically focusing on cyber threats and mitigation strategies. The course introduces students to the importance of Cybersecurity in various industries, such as finance, healthcare, and government. It covers the fundamentals of Cybersecurity, including risk assessment, software and network security, and incident response. The book also provides practical exercises to reinforce students' understanding of the concept of cryptography. The book emphasizes the importance of user awareness, proactive threat detection, and the use of digital tools in protecting individuals and organizations.

The Cybersecurity book is characterized by modern engagement methods, which make students learn and interact with it through the various exercises and activities they provide. This book also emphasizes important aspects of Cybersecurity education and learning, which are:

- The connection between the content and real-life cyber threats.
- Diversity of ways to display engaging content.
- Highlights the role of the learner in the teaching and learning processes.
- Attention to the contents' structure and coherence.
- The skill of employing appropriate techniques in different situations.
- The ability to employ various methods in evaluating students in proportion to their differences.

To be on pace with global developments in this field, the Cybersecurity book will provide the teacher with an integrated set of diverse educational materials that take into account the individual differences between students, in addition to educational software and websites, which provide students with the opportunity to employ modern technologies and practice-based communication. This solidifies its role in the teaching and learning process.

As we present this book to our dear students, we hope it will capture their interest, meet their requirements, and make learning this material more enjoyable and useful.

God grants success



Contents

1. Fundamentals of Cybersecurity 8

Lesson 1	Introduction to Cybersecurity.....	9
	Exercises.....	16
Lesson 2	Cybersecurity Risks and Vulnerabilities	20
	Exercises.....	30
Lesson 3	Cybersecurity Threats and Controls.....	34
	Exercises.....	44
Project		48

2. Cybersecurity Protection and Response 50

Lesson 1	Hardware, Software and Operating System Security	51
	Exercises.....	63
Lesson 2	Network and Web Security.....	66
	Exercises.....	82
Lesson 3	Digital Forensics and Incident Response	86
	Exercises.....	98
Project		100

3. Advanced Topics in Cybersecurity 102

Lesson 1	Cybersecurity Regulations and Laws	103
	Exercises.....	108
Lesson 2	Cryptography in Cybersecurity	112
	Exercises.....	126
Lesson 3	Cybersecurity in Emerging Technologies.....	130
	Exercises.....	137
Project		140



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



1. Fundamentals of Cybersecurity

In this unit, you will learn about the fundamental concepts of cybersecurity, its history and role in the modern world, the main risks and vulnerabilities that are present in technological systems, and what the defense and response strategies to mitigate and combat them are. Finally, you will learn about data protection in cybersecurity, how access control can be implemented to secure information systems, and the role of ethical hacking in protecting organizations and companies.

Learning Objectives

In this unit, you will learn to:

- > Describe the field of cybersecurity and its history.
- > List the key principles of cybersecurity.
- > Analyze the main job roles in cybersecurity.
- > Illustrate how Saudi Arabia has become an emerging leader in cybersecurity.
- > Examine the various categories of malware.
- > Explain how cyberattacks work.
- > Evaluate different strategies for risk identification, mitigation, and management.
- > Outline how access control techniques help protect information systems.
- > Explain the role of ethical hacking in the field of cybersecurity.



Lesson 1

Introduction to Cybersecurity

Link to digital lesson



www.ien.edu.sa

What is Cybersecurity?

Cybersecurity is a field that has become increasingly important in recent years as technology has become more integrated into our daily lives. With the rise of the Internet and the proliferation of computers and mobile devices, cybersecurity has become essential for protecting our sensitive information and ensuring that our online activities are safe and secure. The field of cybersecurity encompasses a range of practices and techniques designed to protect against cyber threats and attacks.



The National Cybersecurity Authority (NCA) in KSA was established by a royal decree as the national authority and reference on cybersecurity. The NCA mandate gives the following definition for cybersecurity:

Cybersecurity is the protection of networks, IT systems, operational technologies systems and their components of hardware and software, their services and the data they contain from any penetration, disruption, modification, access, use or unauthorized exploitation. The concept of cybersecurity also includes information security and digital security.

One of the key challenges in cybersecurity is the constantly evolving nature of cyber threats. The cybersecurity field is constantly moving, so professionals need to continuously update their security measures. Cybersecurity involves various domains, such as data security, network security, cryptography, and cyber risk management.

The interdisciplinary nature of cybersecurity makes it a challenging and exciting field to work in, with many opportunities for learning and career advancement.

Protecting data and information is essential, and cybersecurity measures are necessary to safeguard against cyberattacks. Personal data, financial information, and intellectual property are all at risk, and the consequences for individuals of a successful cyberattack can be severe. One significant consequence of a cyberattack is financial loss. A successful attack can result in the theft of money or valuable assets.

For businesses, the financial consequences of a cyberattack can be even more severe, with potential losses in millions

Cybersecurity Threats

Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, or modification of information, or denial of service.

Cybersecurity Attacks

A cybersecurity attack is an action by an adversary to damage, disrupt, or gain unauthorized access to a computer system, network, or data.

of dollars. A cyberattack can also result in reputational damage, which can be challenging to recover from. Consumers and clients may lose trust in a business that has suffered a cyberattack. Cyberattacks can also result in legal liabilities. Businesses may be held responsible for damages if sensitive data is compromised. In some cases, cyberattacks can even threaten national security. Governments and military organizations are at risk of cyberattacks that can disrupt critical infrastructure or steal sensitive data. A successful attack can result in the loss of state secrets or military strategies, which can have severe consequences. Cybersecurity is essential for individuals as well. With the rise of online banking and e-commerce, personal financial information is at risk of theft. Personal data such as PII (Personal Identifiable Information), addresses, and phone numbers can also be stolen and used for identity theft. Cybersecurity measures such as strong passwords and two-factor authentication can help protect individuals from these threats.

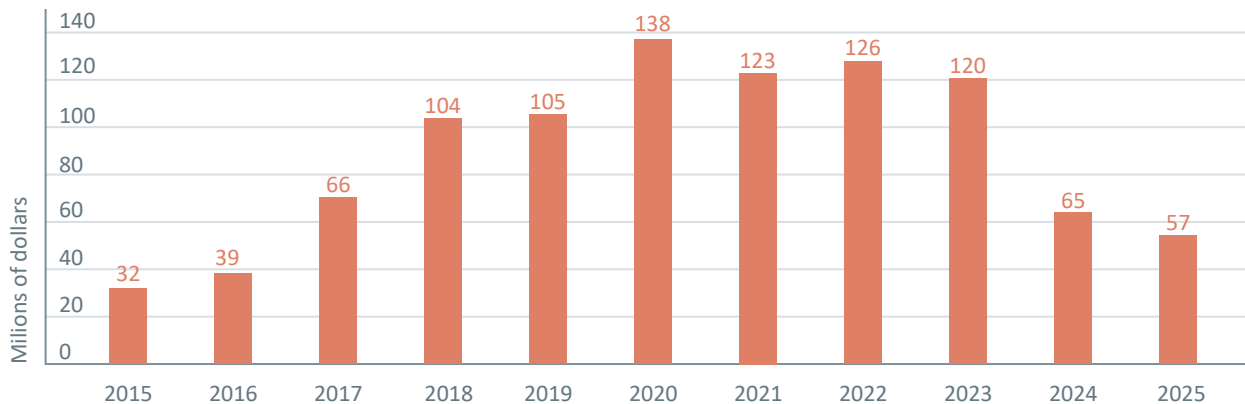


Figure 1.1: Cyberattack Incidents with \$1M+ in reported losses in the last decade, measured in millions of dollars, provided by the Center for Strategic & International Studies (CSIS)

History of Cybersecurity

Cybersecurity history can be traced back to the 1970s, when computing networks were developed. In 1986, computer viruses emerged, causing damage to data and systems. To fight cyberattacks, firewalls and encryption were developed. Firewalls control traffic, and encryption protects data and information. Despite new defenses, cybercriminals still find ways to bypass them.

The 21st century has seen a significant increase in large-scale cyberattacks, with governments, corporations, and individuals at risk. Some of the most high-profile cyberattacks include the 2017 Equifax data breach, which exposed the personal data of over 140 million people, and the 2020 SolarWinds attack, which affected numerous U.S. government agencies and private companies. Some of the biggest data breaches in history are illustrated in figure 1.2. As technology advances and becomes more integrated into our lives, the need for cybersecurity will only continue to grow.

In recent years, there has been a push for greater cybersecurity awareness and education. Governments and organizations have developed cybersecurity frameworks and guidelines to help individuals and businesses protect themselves from cyber threats. Cybersecurity professionals are in high demand, with many job opportunities. As cyberattacks become more sophisticated, the need for skilled professionals who can defend against them will only continue to grow.



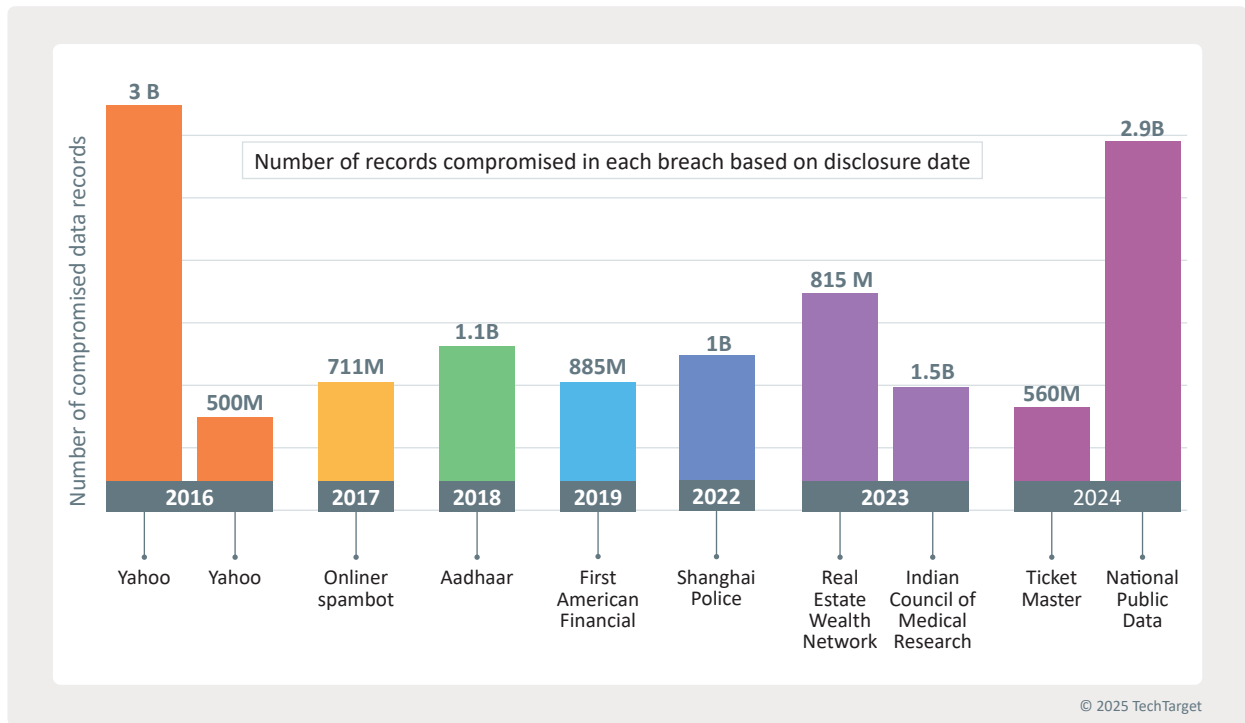


Figure 1.2: 10 of the biggest data breaches in history based on TechTarget research

Key Principles of Cybersecurity

The protection of computer systems, networks, and data from unauthorized access and malicious activities is of utmost importance. To establish a strong and effective security framework, it is essential to adhere to key principles of cybersecurity. Understanding and implementing these principles is vital for safeguarding sensitive information, ensuring data accuracy, and maintaining uninterrupted access to critical resources. These key principles are presented below:

Confidentiality, Integrity, and Availability (The CIA Triad)

The CIA triad is a widely used model for designing and implementing cybersecurity policies and practices.

The acronym stands for Confidentiality, Integrity, and Availability, which are the three main goals of protecting information and systems from unauthorized access, modification, or disruption.

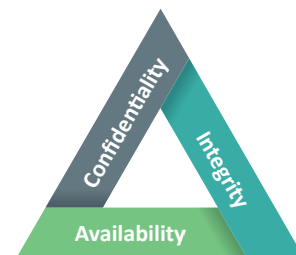


Figure 1.3: The CIA Triad

Confidentiality refers to preserving authorized restrictions on information access. No one can access data that does not belong to them. Confidentiality can be maintained through various methods, such as encryption, access controls, and data masking. However, it's crucial to be aware that confidentiality can face potential threats, such as a phishing attacks, where attackers impersonate legitimate entities to trick individuals into revealing sensitive information.

Integrity refers to the assurance that data is accurate and has not been tampered with. Data integrity is essential for maintaining trust in information systems. Without data integrity, users cannot be confident of the accuracy of the information they receive. Measures such as encryption and digital signatures can help ensure data integrity. An example of a threat is the interception of communications between two parties. An attacker could infiltrate an unsecured Wi-Fi network and manipulate the data packets being transmitted, modifying the content without the knowledge of the sender or recipient.

Digital Signature

A digital signature is a type of electronic signature that uses mathematical algorithms to verify the authenticity and integrity of a message, document or transaction.

Availability refers to the guarantee that information is accessible when needed. Availability is essential for ensuring that systems and services are available to users at all times. Redundancy, backups, and disaster recovery planning can help ensure availability. Denial-of-service attacks are a common way attackers attempt to compromise availability by flooding a network with large quantities of traffic that cause operations to stop.

Job Roles in Cybersecurity

The field of cybersecurity offers a wide range of job opportunities for individuals with varying backgrounds and skill sets. From technical roles such as cybersecurity analysts and penetration testers to managerial roles such as Chief Information Security Officer (CISO), there are a variety of job roles available in cybersecurity to suit different interests and career goals. In addition to technical and managerial roles, there are also roles in cybersecurity policy and governance, such as cybersecurity consultants and cybersecurity compliance officers. As the demand for cybersecurity professionals continues to grow, so does the diversity of job roles and career paths in this field. There are both local and global cybersecurity specialist shortages and it is one of the required future jobs. Below are the main job roles in cybersecurity as presented by the Saudi Cybersecurity Workforce Framework (SCyWF).

The SCyWF Taxonomy

	Job Categories	Specialty Area	Job Roles
	Cybersecurity Architecture, Research and Development (CARD)	Cybersecurity Architecture (CA)	• Cybersecurity Architect • Secure Cloud Specialist
		Cybersecurity Research and Development (CRD)	• Systems Security Development Specialist • Cybersecurity Developer • Secure Software Assessor • Cybersecurity Researcher • Cybersecurity Data Science Specialist • Cybersecurity Artificial Intelligence Specialist



	Job Categories	Specialty Area	Job Roles
	Leadership and Workforce Development (LWD)	Leadership (L)	• Chief Information Security Officer/Director • Cybersecurity Manager • Cybersecurity Advisor
		Workforce Development (WD)	• Cybersecurity Human Capital Manager • Cybersecurity Instructional Curriculum Developer • Cybersecurity Instructor
	Governance, Risk, Compliance and Laws (GRCL)	Governance, Risk and Compliance (GRC)	• Cybersecurity Risk Officer • Cybersecurity Compliance Officer • Cybersecurity Policy Officer • Security Controls Assessor • Cybersecurity Auditor
		Laws and Data Protection (LDP)	• Cybersecurity Legal Specialist • Privacy/Data Protection Officer
	Protection and Defense (PD)	Defense (D)	• Cybersecurity Defense Analyst • Cybersecurity Infrastructure Specialist • Cybersecurity Specialist
		Protection (P)	• Cryptography Specialist • Identity and Access Management Specialist • Systems Security Analyst
		Vulnerability Assessment (VA)	• Vulnerability Assessment Specialist • Penetration Tester / Red Team Specialist
		Incident Response (IR)	• Cybersecurity Incident Responder • Digital Forensics Specialist • Cybercrime Investigator • Malware Reverse Engineering Specialist
		Threat Management (TM)	• Threat Intelligence Analyst • Threat Hunter

	Job Categories	Specialty Area	Job Roles
	Industrial Control Systems and Operational Technologies (ICS/OT)	Industrial Control Systems and Operational Technologies (ICS/OT)	• ICS/OT Cybersecurity Architect • ICS/OT Cybersecurity Infrastructure Specialist • ICS/OT Cybersecurity Defense Analyst • ICS/OT Cybersecurity Risk Officer • ICS/OT Cybersecurity Incident Responder

Cybersecurity in Saudi Arabia

The Kingdom of Saudi Arabia has emerged as a global leader in cybersecurity, securing the top spot on the Global Cybersecurity Index (GCI). GCI is a trusted reference that measures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue. As cybersecurity has a broad field of application cutting across many industries and various sectors, each country's level of development or engagement is assessed along five pillars – (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Development, and (v) Cooperation – and then aggregated into an overall score. Saudi Arabia also is ranked second in the World Competitiveness Yearbook (WCY) for 2023 published by the Switzerland-based International Institute for Management Development (IMD).



National Cybersecurity Authority

The National Cybersecurity Authority (NCA) is the national authority for cybersecurity affairs in the Kingdom of Saudi Arabia. It aims to protect the Kingdom's vital interests, including national security, sensitive infrastructure, priority sectors, and government services and activities.



الاتحاد السعودي للأمن
السيبراني والبرمجة والدرونز
SAUDI FEDERATION FOR CYBERSECURITY,
PROGRAMMING & DRONES

SAFCSP

The SAFCSP is a national institution that aims to empower the local workforce and enhance their capabilities in the fields of Cybersecurity, Software Development, Drones and Advanced Technologies based on international best practices.

Cybersecurity Career Initiatives in Saudi Arabia

Saudi Arabia has been taking significant steps to address the need for cybersecurity jobs and expertise in the country. The following are the initiatives in Saudi Arabia:



وزارة التعليم

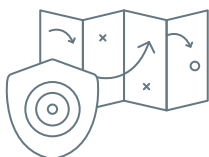
Ministry of Education

2026 - 1448



Education and Training

The Saudi government has invested heavily in cybersecurity education and training programs to develop local talent. Several universities and institutes in Saudi Arabia offer degree programs and certifications in cybersecurity, and the government has also launched training initiatives to upskill current IT professionals in cybersecurity. Examples include NCA Cybersecurity Academy programs that have many tracks and aim to develop and build national capabilities in the field of cybersecurity and localize cybersecurity training content. Also, SAFCSF provides cybersecurity training camps and competitions. NCA released the Saudi Cybersecurity Higher Education Framework (SCyber_Edu) to ensure the quality of cybersecurity higher education in Saudi Arabia. The framework aims to set the minimum requirements for higher education programs in cybersecurity and to ensure the alignment of their learning outcomes with the national needs of the cybersecurity workforce.



Cybersecurity Strategy

Saudi Arabia has developed a comprehensive national cybersecurity strategy that outlines the country's vision and goals for cybersecurity. The strategy includes plans to develop cybersecurity talent within the country, as well as measures to protect critical infrastructure and enhance international cooperation on cybersecurity.



Industry Partnerships

The Saudi government has also been working closely with private sector companies to address the need for cybersecurity expertise. For example, the government has partnered with international companies to provide training and development programs for cybersecurity professionals.



Cybersecurity Sector Development

Saudi Arabia has many initiatives for accelerating the development and growth of the cybersecurity sector in the Kingdom and building its capacity. These initiatives include the national program CyberIC, which is an umbrella of many initiatives such as the National Cyber Drills, Cybersecurity training initiatives targeting various categories the society, the cybersecurity challenges to encourage innovation and entrepreneurship in the field, and the cybersecurity accelerator, which stimulates the local industry system in cybersecurity and links emerging companies in cybersecurity technologies with investors.



Exercises

1

Read the sentences and tick ✓ True or False.	True	False
1. Firewalls and encryption were developed to combat increasing cyberattacks.	☐	☐
2. Government agencies are one of the main targets of cyberattacks.	☐	☐
3. All cybercrimes have the same level of severity and consequences.	☐	☐
4. Confidentiality, integrity, and authentication make up the CIA triad.	☐	☐
5. The SAFCSF is a national institution that aims to train local talent in AI.	☐	☐
6. Integrity refers to the assurance that data is accurate and has not been tampered with.	☐	☐
7. Encryption, access controls, and data masking are methods used to maintain data confidentiality.	☐	☐
8. Confidentiality ensures that data is accurate and has not been tampered with.	☐	☐
9. A CISO is an executive overseeing an organization's cybersecurity program.	☐	☐
10. Chief Information Security Director is a job role in cybersecurity.	☐	☐



4

5



6

7



Lesson 2

Cybersecurity Risks and Vulnerabilities

Link to digital lesson



www.ien.edu.sa

Introduction to Risks And Vulnerabilities

Cybersecurity vulnerabilities are weaknesses in computer systems, networks, and devices that cybercriminals can exploit to carry out malicious activities. Cybersecurity vulnerabilities can result from software bugs, misconfigured systems, and human error.

The consequences of cybersecurity attacks can be severe, including data theft, financial loss, and reputational damage. Therefore, individuals and organizations must be aware of potential cybersecurity threats, identify the existing vulnerabilities and determine the potential risks and implement robust cybersecurity measures to protect those systems.

Cyberattacks are malicious activities by cybercriminals to exploit vulnerabilities in computer systems, networks, and devices. Cyberattacks come in different forms and can be classified into various categories based on the techniques used by the attacker to compromise a system. Various types of actors can be responsible for cybersecurity threats and cyberattacks. They can be broadly categorized based on their capabilities, resources, methods, and motivations. Table 1.1 illustrates some of the types.

Cybersecurity Assets

Cybersecurity assets are anything of value, to an individual, organization, or country that could be negatively impacted by a malicious cyberattack.

Cybersecurity Vulnerabilities

Cybersecurity vulnerabilities are weaknesses in a computer system, network, or application that can be exploited by malicious actors in order to cause damage or gain unauthorized access to sensitive data.

Cybersecurity Risks

Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of data (or control systems) and reflect the potential adverse impacts to organizational operations and assets, individuals, other organizations, and the nation.

Table 1.1: Types of cyberattack actors

Type	Description
Nation-State Actors	These are sophisticated groups, often part of a government's military or intelligence service, that carry out cyberattacks to gain a strategic advantage, conduct espionage, disrupt critical infrastructure, or spread disinformation. Their motivations can be political, economic, or military.



وزارة التعليم

Ministry of Education

2026 - 1448

Type	Description
Organized Crime Groups	These are professional criminals who execute cyberattacks for monetary gain. They often employ tactics such as ransomware, identity theft, credit card fraud, and other types of cybercrime. Their primary motivation is financial.
Hacktivists	Hacktivists are individuals or groups that use hacking to promote a political or social cause. They often engage in activities such as defacing websites or conducting denial-of-service attacks to gain attention for their cause. Their motivation is often ideological or political.
Insider Threats	These are individuals within an organization who have legitimate access but use it maliciously or irresponsibly. They might be motivated by a variety of reasons such as financial gain, revenge, or coercion.
Script Kiddies	This term refers to amateur hackers who use existing hacking tools and scripts to carry out attacks without much technical expertise. They might do it for fun, to gain notoriety, or to challenge themselves.
Competitors	These could be companies that engage in corporate espionage to gain a competitive advantage. They might be looking for trade secrets, unannounced products or strategies, or sensitive information that can be used to their advantage.

The most common type of cyberattack is done by implanting malware, which is a program designed to harm a computer system or network. Different types of malware include viruses, worms, trojans, and ransomware. Malware types can be differentiated based on their propagation mechanism and payload. For the propagation mechanism, malware can spread using various techniques such as user-initiated, email-based, web-based, network-based, and portable media-based. Malware payloads are code that deliver their malicious intent. Payload types include data or file encryption, stealing credentials or confidential information, remote access, or malicious functioning of a system.

Viruses

A virus is a piece of code that attaches itself to another program or file and executes when that program or file is run. A virus can corrupt or delete data, modify system settings, or spread to other files or devices. One famous example is the CIH or Chernobyl virus. The CIH virus is a malicious computer virus that was released in 1998. The virus could disable the computer system and cause information to be lost. The virus was contained, but because of its destructive potential, the incident resulted in greater security measures for Windows operating systems. Another example is a boot sector virus designed to infect your computer's boot sector, which is the area of your computer's hard drive containing the code needed for the computer to start up. Boot sector viruses can render your computer unusable or cause it to crash. They typically spread to other computers through infected USB drives or by downloading infected software from the Internet.

Worms

Worms are similar to viruses but do not need to attach themselves to other programs or files to replicate. Instead, they spread rapidly across networks, consuming system resources and causing damage. One example of a worm is the Mydoom worm, which caused significant damage to computer systems worldwide in 2004.

Trojans

A trojan is malware that disguises itself as a legitimate or useful program but performs malicious actions in the background. A trojan can create backdoors for remote access, steal personal information, download other malware, or display unwanted ads. For example, the Zeus trojan was a banking trojan that targeted Windows users and stole their online banking credentials, credit card numbers, and other sensitive data.

Ransomware

Ransomware is malware that locks or encrypts the user's files or device and demands payment for their restoration. Ransomware can also threaten to delete or expose the user's data if the ransom is not paid within a certain time limit. Ransomware can be spread through email attachments, phishing links, or network vulnerabilities. For example, the WannaCry ransomware was a worm that exploited a Windows vulnerability and infected hundreds of thousands of computers in 2017. The ransomware encrypted the user's files and displayed a message demanding an amount of Bitcoin for their decryption. The ransomware also had a kill switch to stop its spread if a certain domain name was registered.

Adware

Adware is malware that displays unwanted advertisements on the user's device or browser. Adware can also collect information about the user's browsing habits and preferences to deliver targeted ads. Adware can be annoying and intrusive but is not necessarily harmful. However, some adware can install other malware or expose users to malicious websites. Adware can be installed either with the user's consent (as part of free software) or without it (through phishing links or drive-by downloads). For example, the Gator adware offered to save passwords and fill out forms for users but also displayed pop-up ads and collected personal information. The adware was bundled with other free software and required users to accept its installation terms and conditions.

Spyware

Spyware is malware that monitors and collects information about the user's online activity, browsing history, keystrokes, personal data, or system configuration. Spyware can also change browser settings, redirect web pages, or display pop-up advertisements (ads). Spyware can be installed without the user's consent or knowledge through bundled software, phishing links, or drive-by downloads. For example, the CoolWebSearch spyware was a browser hijacker that redirected users to unwanted websites and displayed pop-up ads. The spyware also changed browser settings and installed additional malware. Another example is the Keylogger spyware, which recorded every user's keystroke and sent it to a remote server. The spyware could capture passwords, credit card numbers, chat messages, and sensitive information.

Types of Cyberattacks

In addition to attacks caused by malware, many other types of cyberattacks can be used to compromise computer systems, networks, and devices. Below are presented some of the most common types of cyberattacks.



Social Engineering Attacks

Social engineering is a form of manipulation used by attackers to exploit human weaknesses and acquire sensitive information in order to gain unauthorized access to physical or computer systems. Attackers attempt to trick users into revealing sensitive information, such as passwords, credit card numbers, or other personal information. These attacks often come in emails or messages that appear to be from a legitimate source, such as a bank or a popular social media site. The messages typically contain a link that leads to a fake website designed to look like a legitimate site, where the user is prompted to enter their information. The following are the main types of social engineering attacks:

Phishing:

Attempts to trick victims into clicking on fraudulent links sent via email.

Smishing:

Similar to phishing, except it comes as text message (SMS) on messaging apps. A smishing text usually contains a fraudulent link.

Vishing:

In this type of attack, cybercriminals call potential victims, pretending to be a legitimate company or person, to request personal information from a victim.

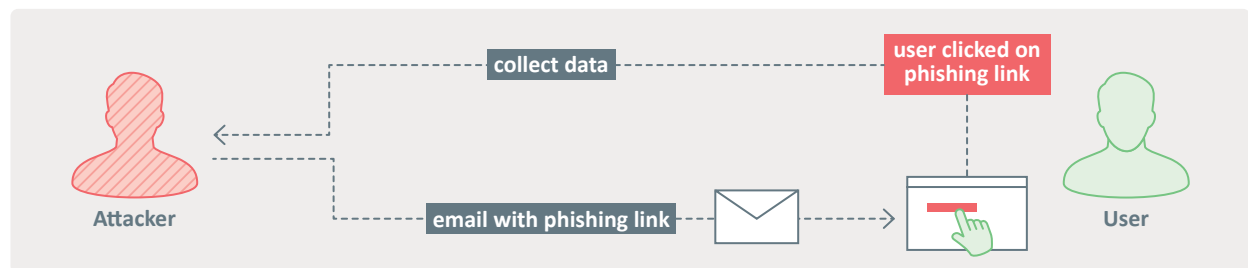


Figure 1.6: Example of a social engineering phishing attack

The screenshot shows a phishing email from ACT BANK. The email has a dark header with a warning icon and the text "Your account is on hold." The main body of the email says "Please update your payment details" and "Hi Dear,". It then states: "We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details." Below this is a red button that says "UPDATE ACCOUNT NOW". At the bottom, it says "Need help? We're here if you need it. Visit the [Help Centre](#) or [contact us](#) now." Three callouts point to specific parts of the email:

- The email says your account is on hold because of a billing problem.** (Points to the header warning)
- The email has a generic greeting.** (Points to "Hi Dear,")
- The email invites you to click on a link to update your payment details.** (Points to the "UPDATE ACCOUNT NOW" button)

Figure 1.7: Illegitimate link example

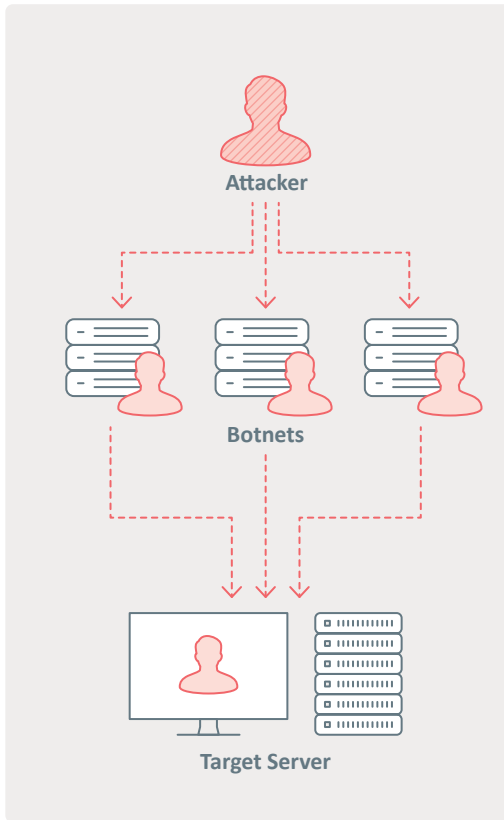


Figure 1.9: Example of a DDoS botnet attack

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks

DoS and DDoS attacks are cyberattacks that flood a network or server with traffic to overwhelm it, making it difficult or impossible for legitimate users to access the service, which is an attack on availability. In a DoS attack, a single computer or device is used to flood the network, while in a DDoS attack, multiple devices are coordinated to attack the network simultaneously. These attacks can be carried out using a variety of techniques, such as sending large volumes of requests to a server or flooding the network with traffic from multiple sources. DoS and DDoS attacks can have serious consequences, such as shutting down critical services or disrupting business operations.

Organizations can protect themselves against these attacks by implementing firewalls and intrusion detection systems (IDSs) and using content distribution networks (CDNs) to distribute traffic across multiple servers.

In 2020, the COVID-19 pandemic led to a surge in DDoS attacks against healthcare organizations. Attackers targeted hospitals and healthcare providers, causing disruptions to critical services. Some large-scale attacks have been known to generate traffic in the order of terabits per second (Tbps), overwhelming targeted systems.

Man-in-the-Middle (MitM) Attacks

MitM attacks are cyberattacks where an attacker intercepts communications between two parties to eavesdrop or manipulate the conversation. This can be done by inserting themselves between the two parties and relaying messages back and forth, allowing the attacker to read or alter the messages. MitM attacks can be carried out using various techniques, such as packet sniffing or IP spoofing, which forge false network information.

These attacks can have serious consequences, such as the theft of sensitive information or the manipulation of financial transactions. Users can protect themselves against MitM attacks by using encryption technologies, such as HTTPS & VPN, and being cautious when using public Wi-Fi networks. In 2020, a MitM attack occurred when attackers used a vulnerability in Zoom's encryption to intercept and eavesdrop on video calls. The attackers were able to gain unauthorized access to sensitive information, such as business plans and financial data.

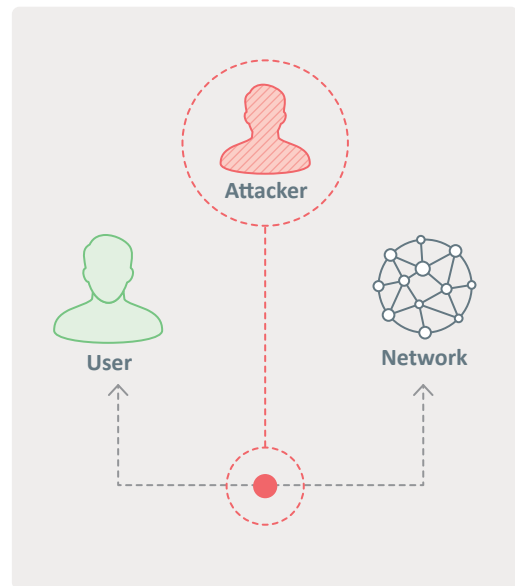


Figure 1.8: Example of a MitM attack



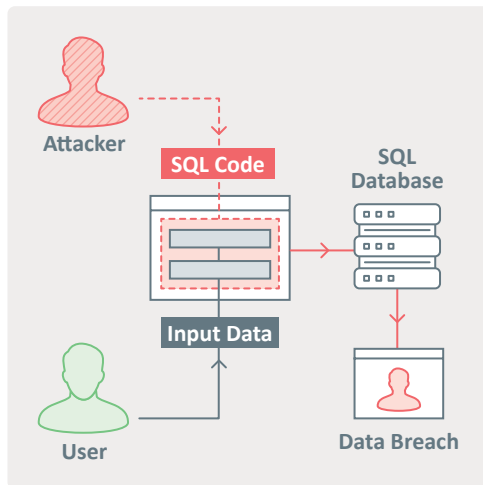


Figure 1.10: Example of an SQL injection

SQL Injections

SQL injection attacks exploit a web application's database vulnerabilities to gain unauthorized access or manipulate data. This can be done by inserting malicious code into a website's input fields, such as login forms, to gain access to the database. SQL injection attacks can have serious consequences, such as the theft of sensitive data or the modification of database records. Organizations can protect themselves against SQL injection attacks by implementing best practices for secure coding and using web application firewalls (WAFs) to detect and block malicious traffic. An example of an SQL injection attack occurred in 2019 when a vulnerability in the Magento e-commerce platform, now named Adobe Commerce, allowed attackers to gain unauthorized access to sensitive customer data, such as names and credit card information.

Cross-Site Scripting (XSS) Attacks

XSS attacks inject malicious code into a website to steal user information or manipulate displayed content. This can be done by inserting scripts into a website's input fields, such as search boxes or comment sections, that execute when the user interacts with the page. XSS attacks can have serious consequences, such as the theft of sensitive information or the manipulation of website content. Organizations can protect themselves against XSS attacks by implementing secure coding practices and using content security policies (CSPs) to detect and block malicious scripts. In 2018, attackers used an XSS attack to steal sensitive information from customers of a large ticket vendor company. The attackers injected malicious code into the company's payment page, allowing them to steal customer information, including names, addresses, and payment card information.

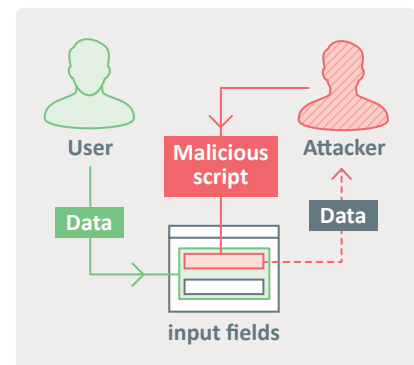


Figure 1.11: Example of an XSS attack

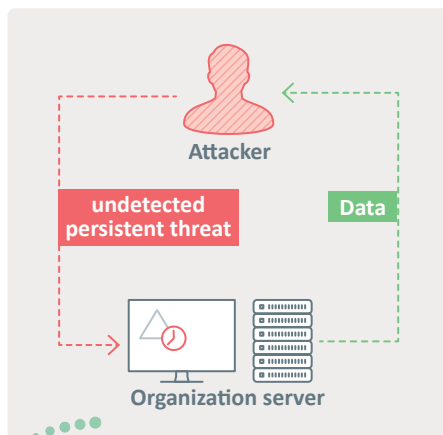


Figure 1.12: Example of an APT attack

Attacks by Advanced Persistent Threat (APT)

APT attacks are targeted attacks that use sophisticated techniques to gain unauthorized access to a system and remain undetected for long periods. APT attacks often use a combination of social engineering, malware, and other techniques to gain access to sensitive information or systems. These attacks can have serious consequences, such as the theft of intellectual property or sensitive customer data. Organizations can protect themselves against APT attacks by implementing a comprehensive security program that includes employee training, vulnerability management, and threat intelligence. An example of an APT attack occurred in 2015 when attackers exploited a previous medical data breach to steal the personal information of 80 million customers. The attackers were able to remain undetected for several months, highlighting the need for comprehensive security programs and threat intelligence.

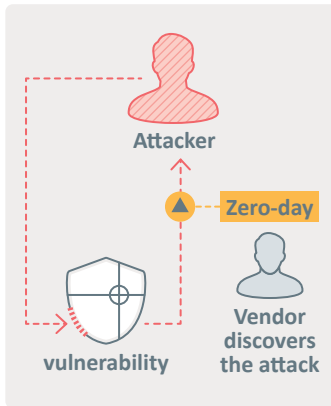


Figure 1.13: Example of Zero-day exploit

Zero-Day Exploits

Zero-day exploits take advantage of vulnerabilities in software before they are discovered and patched, making them particularly dangerous, since developers have had 0 days to fix the problem when the attack is launched. Zero-day exploits can be used to gain unauthorized access to a system, steal sensitive information, or cause damage to the system. These exploits are typically undertaken by attackers to carry out targeted attacks against organizations. Zero-day exploits can be difficult to protect against because they are unknown to the software vendor and cannot be patched until discovered. Organizations can protect themselves against zero-day exploits by implementing best practices for secure coding and by using security tools that can detect and block suspicious behavior. An example of a zero-day exploit occurred in 2021 when attackers used a vulnerability in Microsoft's new version of Exchange Server to install backdoors on targeted systems.

Password Attacks

Password attacks use techniques like brute force or phishing to guess or steal user passwords and gain unauthorized access to systems. Brute force attacks use automated tools to try thousands or millions of possible passwords until the correct one is found. Phishing attacks use social engineering techniques to trick users into revealing their passwords. Password attacks can have serious consequences, such as stealing sensitive data or compromising critical systems. Users can protect themselves against password attacks by using strong, complex passwords and multi-factor authentication (MFA), like SMS authentication or the Saudi Nafath to add a layer of security. In 2012, attackers used a brute force attack to gain access to the LinkedIn database, compromising millions of users' passwords.

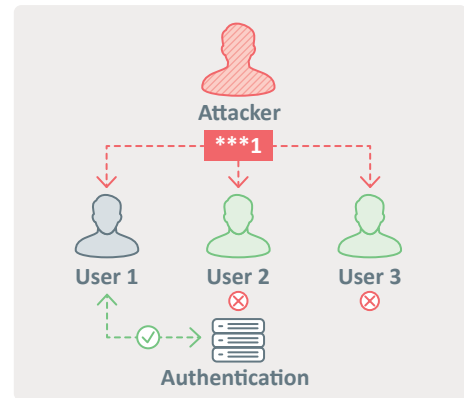


Figure 1.14: Example of a password attack

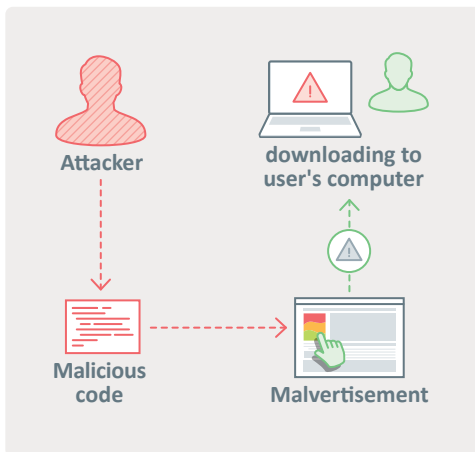


Figure 1.15: Example of malvertising practice

Malvertising

Malvertising is the practice of embedding malicious code in online advertisements to infect users' computers with malware.

Malvertisements can be difficult to detect because legitimate advertising networks often serve them. Once a user clicks on a malvertisement, malware is downloaded to their computer, which can be used to steal sensitive information or carry out other attacks. Users can protect themselves against malvertising by using advertisement blockers and being cautious when clicking on online advertisements. For example in 2016, the Angler exploit kit served malvertisements on popular websites, including the New York Times and the BBC. The malvertisements contained code that would download the Locky ransomware to users' computers, highlighting the need for users to use ad blockers and other security tools to protect against malvertising.



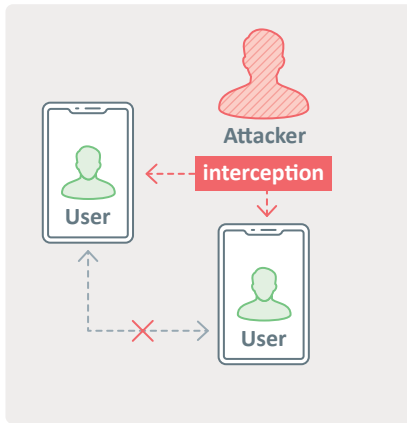


Figure 1.16: Example of an eavesdropping interception

Eavesdropping

Eavesdropping is the unauthorized interception of communication, such as emails, phone calls, or instant messages. Eavesdropping can be carried out using various techniques, such as packet sniffing or network tapping. Eavesdropping can have serious consequences, such as stealing sensitive information or compromising critical systems. Users can protect themselves against eavesdropping by using encryption technologies, such as HTTPS and VPNs, and being cautious when using public Wi-Fi networks. An example of eavesdropping occurred in 2020, when attackers exploited a vulnerability in a telecommunications protocol to intercept and eavesdrop on text messages and phone calls. The vulnerability, known for several years, highlighted the need for telecom companies to implement stronger security measures to protect against eavesdropping.

Security Information and Event Management (SIEM) System

A SIEM system is a set of software tools designed to help organizations and enterprises detect and respond to cyberattack threats in real time. A SIEM system collects and analyzes data from various sources, such as network devices, servers, and applications, to identify potential security incidents. The data is analyzed using machine learning and artificial intelligence algorithms to detect anomalies and patterns that may indicate a security threat.

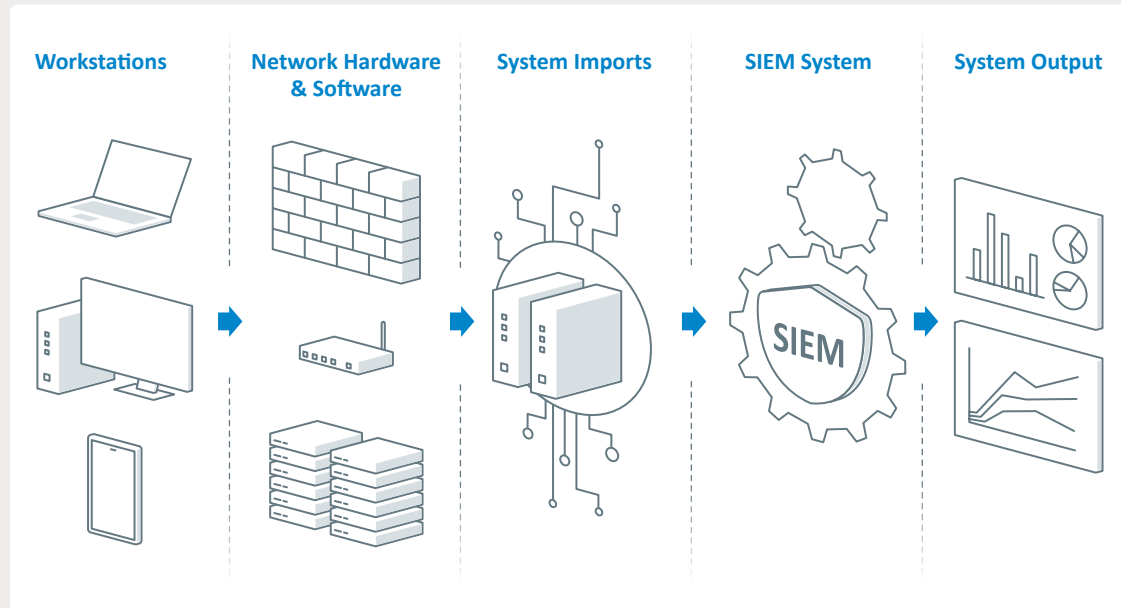


Figure 1.17: Representation of Security Information and Event Management (SIEM)



Cybersecurity Risk Identification, Mitigation, and Management

Cybersecurity risk identification, mitigation, and management are essential processes for organizations to safeguard their critical assets, protect sensitive information, and ensure the continuity of their operations.

Risk Identification

The first step in managing cybersecurity risks involves identifying potential threats and vulnerabilities that could affect an organization's digital assets. Key activities in risk identification include:

Asset Inventory

Creating a comprehensive list of an organization's digital assets, including hardware, software, data, and network infrastructure.

Threat Assessment

Identifying potential threat sources, such as cybercriminals, insider threats, or natural disasters, that could exploit vulnerabilities in the organization's systems.

Vulnerability Assessment

Discovering and documenting weaknesses in an organization's digital assets using vulnerability scanning, penetration testing, and manual assessments.

Risk Analysis

To prioritize risks based on their potential consequences, evaluate the likelihood and impact of identified threats and vulnerabilities.

Risk Management

Once risks have been identified, organizations should take steps to reduce or manage them. Risk management involves implementing security measures to address vulnerabilities and minimize the likelihood or impact of threats. Key risk mitigation strategies include:

Cybersecurity Awareness Training

Educating employees about cybersecurity best practices and their responsibilities in protecting the organization's digital assets.

Incident Response Planning

Developing a plan to detect, respond to, and recover from security incidents to minimize their impact on the organization.

Access Control

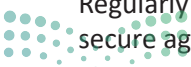
Implementing authentication and authorization mechanisms to restrict access to sensitive data and systems only to authorized users.

Encryption

Encryption converts plain text or data into encoded formats to prevent unauthorized access. Encrypting sensitive data and information at rest and in transit protects it from unauthorized access or theft.

Patch Management

Regularly updating software and hardware to address known vulnerabilities and ensure systems remain secure against emerging threats.



Risk Treatment

Selecting and implementing appropriate risk mitigation strategies based on the organization's risk tolerance and available resources and regularly reviewing the effectiveness of these strategies.

Governance and Compliance

Ensuring the organization's cybersecurity policies and practices align with relevant laws, regulations, and industry standards.

Reporting and Communication

Keeping stakeholders informed about the organization's cybersecurity risk responses and any changes to its risk management strategies.

Table 1.2 outlines the key tools for identifying cybersecurity risks.

Table 1.2: Tools for cybersecurity risk identification, mitigation, and management	
Category	Description
SIEM Systems	Security information and event management (SIEM) systems collect and analyze security-related data from various sources.
Penetration Testing Tools	Simulate attacks on systems or networks to identify vulnerabilities and test the effectiveness of security controls.
Security Risk Assessment	Identify and assess security risks across an organization's infrastructure, including networks, systems, and applications.
Data Loss Prevention	Monitor and control the flow of sensitive data within an organization to help prevent data breaches.
Firewall and IPS	Monitor and block incoming traffic that is identified as potentially harmful.
Endpoint Protection	Protect individual devices, such as laptops or smartphones, from malware and other threats.
Security Analytics Tools	Use machine learning and other advanced techniques to analyze security data and identify potential threats.

Exercises

1

Read the sentences and tick ✓ True or False.	True	False
1. A virus is a piece of code that attaches itself to another program or file and executes when that program or file is run.	☐	☐
2. Ransomware encrypts the user's files or device and demands payment for their restoration.	☐	☐
3. A trojan is a legitimate or useful program that performs beneficial actions in the background.	☐	☐
4. Multi-factor authentication (MFA) can add a layer of security to protect against password attacks.	☐	☐
5. Spyware is malware that protects the user's online privacy and security.	☐	☐
6. Phishing attacks are a form of social engineering that attempts to trick users into revealing sensitive information.	☐	☐
7. DoS attacks involve coordinating multiple devices to attack a network simultaneously.	☐	☐
8. SQL injection attacks exploit a web application's database vulnerabilities to gain authorized access or manipulate data.	☐	☐
9. Cross-site scripting (XSS) attacks inject malicious code into a website to steal user information or manipulate displayed content.	☐	☐
10. Public Wi-Fi networks are invulnerable to eavesdropping attacks.	☐	☐

2 Define what malware is.



3 Explain what a computer virus is and how it works.

4 Compare and contrast the characteristics of viruses, worms, trojans, and ransomware.

5 Analyze public Wi-Fi networks' potential risks and benefits and how users can protect their devices.



6 Explain the importance of staying aware for malvertising attacks.

7 Evaluate the effectiveness of Security Information and Event Management (SIEM) solutions in detecting and responding to security threats.

8 Compare and contrast DoS and DDoS attacks.



9 Identify and explain the steps an organization can take to protect against zero-day exploits.

10 Assess the impact of SQL injection attacks on a web application.

11 List two example activities that are part of risk identification, mitigation, and management.



Lesson 3

Cybersecurity Threats and Controls

Link to digital lesson



www.ien.edu.sa

Cybersecurity Threats

Cybersecurity threats have become an ever-present danger in our increasingly digitized world. As online activities become more commonplace and our personal data more easily accessible, it is imperative that we understand the risks associated with a range of cybersecurity issues, such as data threats, identity theft, and online tracking.

Data Threats

Data protection becomes crucial as more personal and sensitive information is stored digitally. Organizations must handle personal data securely and responsibly, protecting it from unauthorized access, alteration, or disclosure. Key data protection concerns include:

Data Breaches

Unauthorized access to or disclosure of personal data, often due to weak security measures or human error.

Data Retention

The duration and manner in which personal data is stored can raise concerns if the stored data is inadequately protected.

Data Sovereignty

The legal implications of storing data in different countries, which may cause different privacy laws and regulations to be applied to this data according to the laws of each country.

Identity Theft

Identity theft occurs when an individual's personal information is stolen and used fraudulently, often for financial gain. The digital age has made it easier for criminals to access and exploit personal data, increasing identity theft. Examples of identity theft include:

Spear-Phishing

Spear-phishing targets individuals or organizations with personalized messages to obtain sensitive information. The attacker uses the target's personal information to make the message appear legitimate.

Spoofing

Spoofing is when an attacker disguises themselves as a legitimate user in order to gain access to information.

Online Tracking

As people engage in various online activities, their actions are often tracked and monitored, raising concerns about privacy and surveillance. Online tracking can involve both legitimate and invasive practices, including:



وزارة التعليم
Ministry of Education

2026 - 1448

Cookies

Small text files placed on a user's device by websites, which can be used to track browsing activity and preferences for legitimate purposes, such as personalizing content, but can also be used for invasive tracking.

Behavioral Tracking

The monitoring and analysis of an individual's online activities to create a profile of their interests, habits, and preferences, often used for targeted advertising.

To address these cybersecurity threats, governments, organizations, and individuals must work together to develop and implement policies, regulations, and best practices that balance the benefits of digital technologies with the need to protect personal data.

Cybersecurity and Access Control

Access control is a fundamental defense measure in cybersecurity that aims to protect information systems and data privacy from unauthorized access and modification. Access control can also be based on different models, such as role-based, or attribute-based. Access control can help achieve various security objectives, such as authentication, authorization, and nonrepudiation. These concepts are further explained below.

Role-Based Access Control (RBAC)

RBAC is a method in cybersecurity that restricts system access to authorized users based on their roles within an organization. In this model, permissions to perform certain operations are assigned to specific roles, and users are assigned appropriate roles, thereby obtaining these permissions. For example, developers could have access to write and modify code in a software company.

In contrast, a quality assurance tester would only have access to view and test the code but not modify it. RBAC simplifies the management and auditing of user rights, and it is less prone to errors than individually assigned permissions.

Attribute-Based Access Control (ABAC)

ABAC is a more flexible, fine-grained access control method that grants permissions based on attributes associated with a user, the assets they are trying to access, and the conditions under which access is being requested. These attributes can be user attributes (such as role, department, or location), resource attributes (such as data classification), and environmental attributes (such as time of day and location of access).

For example, a sensitive document in a corporation may be accessible to a manager (user attribute) only if the document is tagged as belonging to their department (resource attribute) and access is attempted during office hours (environmental attribute). ABAC allows for a highly dynamic and contextual access control system.

Identification

Identification is the means of verifying the identity of a user, process, or device, typically as a pre-requisite for granting access to resources in a system. The identification step is usually done outside the system as a pre-step. For example, issuing a new employee with a username and password once they join an organization, and the identification happens in person or via a verified way the organization establishes.



Authentication

Authentication is the verification of the identity of a user, device, or system attempting to access resources within an organization. Strong authentication mechanisms help ensure that only legitimate users gain access to the organization's resources.

Authorization

Once a user, device, or system has been authenticated, the authorization process determines the level of access they should be granted. This involves assigning permissions based on predefined access policies, user roles, or group memberships. Proper authorization ensures that users can only access the resources and perform the actions they are explicitly permitted to, limiting the potential for unauthorized access or misuse of sensitive data.

Nonrepudiation

Nonrepudiation is a critical aspect of access control and cybersecurity, ensuring that a user cannot deny the authenticity of their actions or transactions within a system. This is particularly important in situations where the integrity of data or the validity of transactions must be maintained, such as in financial services, healthcare, or legal settings. Implementing nonrepudiation mechanisms can help prevent disputes, fraud, and unauthorized activities by providing irrefutable evidence of user actions.

Principle of Least Privilege

Access control systems should adhere to the principle of least privilege, which states that users should only be granted the minimum level of access necessary to perform their job functions. This limits the potential for unauthorized access or misuse of sensitive data and reduces the potential damage caused by compromised user accounts or insider threats.

Need to Know

Only those who have an operational need to know certain information should have access to that information. It is an important security and privacy measure because it limits the amount of data that can potentially be accessed inappropriately. This principle is used in both public and private organizations alike to ensure the safety of important assets.

Layering

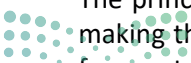
By adding different forms of security at multiple levels, users can ensure that important data and systems are protected from unauthorized access and manipulation. This principle is a key part of information security systems because it helps to reduce the risks of a single security measure being breached.

Diversification

This principle recommends that organizations should implement a variety of security mechanisms to reduce risk from attack or other threats. By having different forms of security, organizations are able to identify where weaknesses and vulnerabilities may occur and respond accordingly. By diversifying the security measures implemented, organizations can minimize the risk of a single flaw leading to a breach.

Obscurity

The principle of obscurity is the practice of providing limited visibility to sensitive data or systems. By making them hard to find or preventing direct access to them, organizations can protect certain assets from potential attackers or intruders.



This principle also includes hiding necessary authentication data from plain sight and is an important form of application defense for preventing unauthorized access to important information and data.

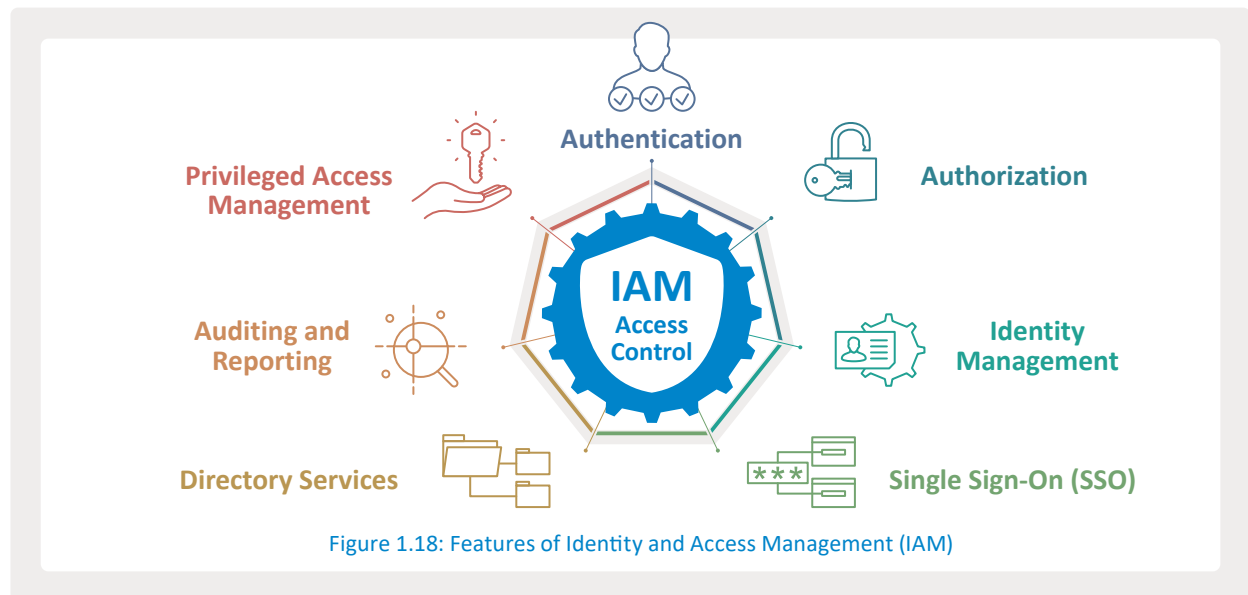
Auditing and Monitoring

Access control systems should include auditing and monitoring capabilities to track user activities and access attempts. By logging and reviewing access events, organizations can identify suspicious activities, detect potential security breaches, and ensure compliance with internal policies and external regulations.

Cybersecurity Access Control Tools

IAM Access Control

Identity and Access Management (IAM) is a critical component of cybersecurity that helps organizations to manage and protect user identities and access to resources. IAM solutions are designed to provide centralized control over user identities and access to resources and automate user account provisioning and de-provisioning. Enterprise-grade IAM solutions typically include various features to help organizations manage and protect user identities and resource access. These features include:



■ Authentication

Including multi-factor authentication (MFA) capabilities to help protect against identity theft and unauthorized access. Authentication can begin with processes outside the system, such as issuing a new employee with a username and password once they join an organization, and the identification happens in person or via verified methods established by the organization.

■ Authorization

Allowing organizations to manage resource access based on role-based access controls (RBAC) and other access control models.

■ Identity Management

Managing user identities across various platforms and applications and automating the provisioning and de-provisioning of user accounts.

■ Single Sign-On (SSO)

Accessing multiple applications and resources with a single set of credentials, simplifying the login process and reducing the risk of password-related security incidents.

■ Directory Services

Directory services provide centralized management of user identities and resource access.

■ Auditing and Reporting

Providing detailed auditing and reporting capabilities, which allow organizations to track user activity, detect suspicious activity, and meet compliance requirements.

■ Privileged Access Management (PAM)

PAM helps organizations secure, manage, and monitor privileged access to sensitive systems and data.

Active Directory Example

Active Directory allows administrators to create and manage user accounts, groups, and computers and control resource access based on RBAC. It also includes a built-in authentication system, which provides secure authentication for Windows-based servers and clients.

Active Directory is organized into a hierarchical structure of domains, trees, and forests. A domain is a logical group of network resources, such as user accounts and computers, that share a common namespace. A tree is a group of domains that share a contiguous namespace, and a forest is a tree with a common schema.

Active Directory can also be used to implement identity federation, which allows users to access resources across multiple domains or forests using a single set of credentials. This can be useful for organizations with multiple subsidiaries or that need to share resources with partners or customers.

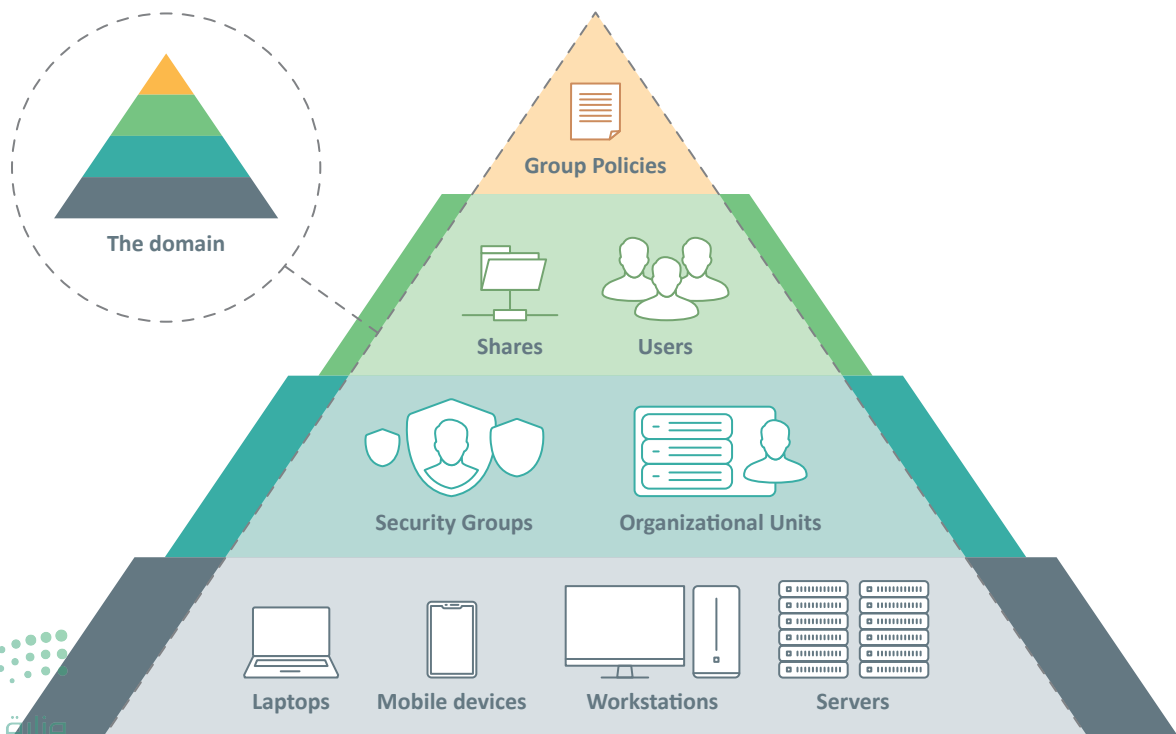


Figure 1.19: Active Directory structure

Table 1.3: Advantages and potential issues of IAM systems

Advantages	Potential issues
IAM solutions provide centralized control over user identities and resource access. This allows organizations to enforce security policies, such as multi-factor authentication, and to manage access to resources based on role-based access controls.	IAM solutions can be complex to implement and maintain, requiring specialized knowledge and resources.
IAM solutions can automate the provisioning and de-provisioning of user accounts, reducing the risk of errors and improving the efficiency of the process.	IAM solutions may require integration with existing systems and applications, which can be time-consuming and difficult.
IAM solutions can provide detailed auditing and reporting capabilities, which allow organizations to track user activity and detect suspicious activity, helping to meet compliance requirements.	IAM solutions are typically targets for attackers, meaning they must be constantly updated and monitored to protect against new threats.
IAM solutions can also provide Single Sign-On (SSO) capabilities, simplifying the login process and reducing the risk of password-related security incidents.	IAM solutions rely heavily on accurate, up-to-date data, which can be difficult to maintain, especially in large and complex environments.

Attacking an IAM

There are several ways that an attacker can attempt to attack an IAM system:

Social Engineering

An attacker can use social engineering techniques, such as phishing or pretexting, to trick users into revealing their credentials or to convince them to perform actions that compromise security.

Brute-force attacks

An attacker can use automated tools to try different combinations of usernames and passwords to guess the correct login credentials.

Privilege escalation

An attacker can attempt to exploit vulnerabilities in the IAM system or in other systems to gain elevated privileges and access sensitive resources.

Insider threats

An attacker can be someone already authenticated and has access to the system. They can use their access to steal sensitive data, disrupt the system, or use the system to launch attacks on other resources.

Man-in-the-middle (MitM) attacks

An attacker can intercept network communications and use them to intercept or steal sensitive information, such as login credentials.

Distributed Denial of Service (DDoS) attacks

An attacker can use a DDoS attack to overwhelm the IAM system and disrupt its operations, making it unable to process requests and authenticate users data.

Single Sign-On (SSO)

Single Sign-On (SSO) is a method of authentication that allows users to access multiple applications and resources with a single set of credentials rather than having to remember and enter separate login information for each application. This can simplify the login process for users and reduce the risk of password-related security incidents. An example of an SSO control is the Saudi Nafath portal.

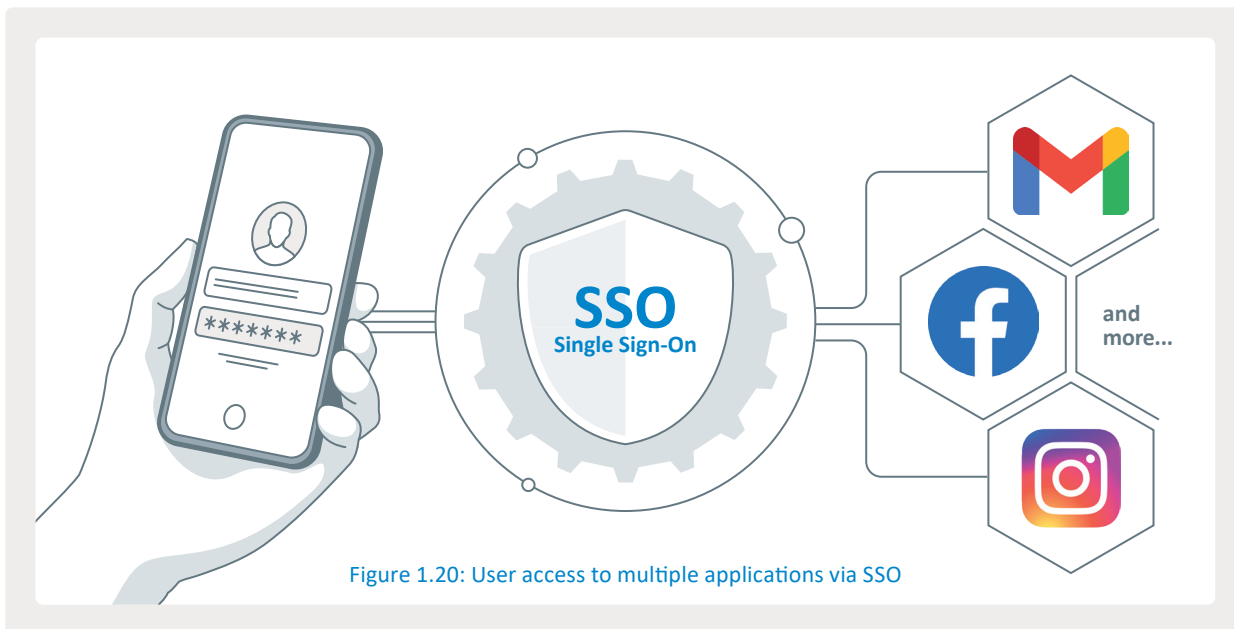


Table 1.4: Advantages and potential issues of SSO authentication

Advantages	Potential issues
SSO can make it easier for users to access the resources they need, as they only need to remember one set of login credentials.	SSO relies on a central authentication server. If this server becomes unavailable, users cannot access the necessary resources.
SSO can reduce the risk of password-related security incidents, such as password reuse and phishing attacks, as users only need to remember one password.	SSO can be complex to implement and maintain, requiring specialized knowledge and resources.
SSO can help organizations to comply with regulatory requirements for password management, as users only need to remember one password.	SSO can create a higher security risk, as an attacker who compromises a user's credentials can gain access to multiple resources.



Assessing and Identifying Vulnerabilities of Systems

There are various cybersecurity strategies and techniques to assess and identify the vulnerabilities and weaknesses of information systems. Two of the most prominent are Vulnerability Assessment (VA) and Penetration Testing (PT). VA and PT are essential cybersecurity practices that help organizations assess and identify vulnerabilities and weaknesses in their systems. These proactive measures allow organizations to address potential security risks before malicious actors can exploit them. The following is an explanation of these strategies.

Vulnerability Assessment (VA)

A vulnerability assessment systematically identifies, analyzes, and prioritizes vulnerabilities in an organization's systems, applications, or networks. The goal of a VA is to discover weaknesses that could be exploited by attackers and provide insights into potential attack vectors. Key aspects of a vulnerability assessment include:

Scanning

Using automated tools or manual techniques, vulnerability scanners inspect systems and applications for known vulnerabilities or misconfigurations.

Reporting

After scanning, a detailed report is generated, listing identified vulnerabilities, their severity, and potential impact on the organization.

Prioritization

Vulnerabilities are ranked based on their severity and potential impact, helping organizations prioritize their remediation efforts.

Remediation

Organizations use the findings from the vulnerability assessment to address and fix the identified vulnerabilities, often through patching, configuration changes, or other security improvements.

Penetration Testing (PT)

Penetration testing, or ethical hacking, is a more in-depth and targeted assessment of an organization's security posture. It involves simulating real-world attacks to test the effectiveness of security controls and identify exploitable vulnerabilities. PT aims to uncover weaknesses that automated vulnerability scans may not detect and to evaluate the organization's overall defense capabilities. Key aspects of penetration testing include:

Planning and Scope

A clear plan and scope for the penetration test are established, including objectives, target systems, and testing boundaries.

Reconnaissance

The penetration tester gathers information about the target systems and environment to identify potential vulnerabilities and attack vectors.

Exploitation

The tester attempts to exploit identified vulnerabilities, simulating the actions of a real attacker to gain unauthorized access, escalate privileges, or compromise sensitive data.

Reporting

After the test, a detailed report is generated, outlining the vulnerabilities discovered, successful exploits, and recommendations for remediation.

Cybersecurity and Ethical Hacking

Ethical hackers or white-hat hackers, use techniques and tools to identify vulnerabilities and weaknesses in an organization's systems, networks, or applications. The primary difference between ethical hacking and malicious hacking is the intent behind the actions and the permission granted by the target organization. Ethical hackers work within legal and moral boundaries to help organizations improve their security posture, whereas malicious hackers aim to exploit vulnerabilities for personal gain or malicious purposes.

It is important to strike a balance when discussing ethical hacking, as the term can be misunderstood or misused. While ethical hacking plays a crucial role in identifying vulnerabilities, it should not be encouraged as a free-for-all activity, nor should it be confused with the illegal practices of traditional hackers. The following points highlight the critical aspects of maintaining a balanced view of ethical hacking:

Permission and Authorization

Working with the explicit permission of the organization they are testing. They should have a clear agreement outlining their activities' scope, objectives, and boundaries.

Legal and Regulatory Compliance

Complying with relevant laws, regulations, and industry standards. This ensures that the activities are within legal and ethical boundaries and helps to avoid potential legal issues or unintended consequences.

Professionalism and Responsibility

Adhering to a strict code of conduct and demonstrate professionalism. They must be accountable for their actions and take care not to cause any harm to the systems they are testing.

Disclosure and Remediation

Upon discovering vulnerabilities, ethical hackers should promptly report their findings to the target organization and provide recommendations for remediation. This collaborative approach helps to address security issues effectively while maintaining trust between the ethical hacker and the organization.

Education and Certification

Encouraging the pursuit of ethical hacking education and certifications helps to establish a clear understanding of the ethical and professional standards that should be maintained.

In conclusion, security professionals play a vital role in identifying cybersecurity vulnerabilities and helping organizations to improve their security posture. However, it is essential to maintain a balanced perspective on the practice to ensure that it remains within ethical and legal boundaries and to discourage any potential misuse of the term or the skills involved.



Table 1.5: Main activities performed by security professionals

Activity	Description
 Penetration Testing	Executing penetration tests to simulate attacks on an organization's systems, networks, or applications. This helps to identify exploitable vulnerabilities and assess the effectiveness of existing security controls.
 Vulnerability Assessments	Performing vulnerability assessments by scanning systems and applications for known vulnerabilities, misconfigurations, or weaknesses. They then provide a detailed report of their findings and prioritize the vulnerabilities for remediation.
 Security Audits	Conducting comprehensive security audits of an organization's infrastructure, policies, and procedures to evaluate their overall security posture and identify areas for improvement.
 Social Engineering Assessments	Conducting social engineering assessments to evaluate an organization's susceptibility to human-based attacks, such as phishing, pretexting, or physical security breaches. They can also provide recommendations for improving employee security awareness and training.
 Wireless Network Assessments	Assessing the security of an organization's wireless networks, including Wi-Fi and Bluetooth, to identify vulnerabilities, weak encryption, or misconfigurations that attackers could exploit.
 Web Application Testing	Testing web applications for vulnerabilities such as SQL injection, cross-site scripting, or authentication bypasses, helping organizations to secure their online services and protect sensitive data.
 Red Team Exercises	Participating in red team exercises, acting as attackers in a simulated scenario to test an organization's incident response capabilities, security defenses, and overall resilience.
 Secure Code Review	Reviewing an organization's software code for potential security flaws or vulnerabilities, providing recommendations for improving code security and reducing the risk of exploitation.
 Security Training and Awareness	Helping organizations develop and deliver security training programs, sharing their expertise and knowledge to educate employees on cybersecurity best practices and common attack techniques.

Exercises

1

Read the sentences and tick ✓ True or False.	True	False
1. Spear-phishing attacks are distributed attacks sent to masses of people.	☐	☐
2. Cookies are small text files placed on a user's device by websites to track browsing activity.	☐	☐
3. Behavioral tracking is used exclusively for security purposes and not for targeted advertising.	☐	☐
4. Access control is not important for protecting information systems and data privacy from unauthorized access and modification.	☐	☐
5. The principle of least privilege states that users should be granted the maximum level of access necessary to perform their job functions.	☐	☐
6. Access control models, such as ABAC and RBAC, are responsible for enforcing security policies and managing user access within an organization.	☐	☐
7. Ethical hacking is identical to malicious hacking in terms of intent and permission.	☐	☐
8. Ethical hackers should always work with the explicit permission of the organization they are testing.	☐	☐
9. Disclosure and remediation are essential aspects of ethical hacking to maintain trust and address security issues effectively.	☐	☐
10. Social engineering assessments by white-hat hackers evaluate an organization's susceptibility to human-based attacks.	☐	☐

2

Analyze the role of data protection in addressing data threat issues in the digital age. What are the key data protection concerns?



3 Evaluate the use of cookies in online tracking. How can cookies both enhance user experience and raise privacy concerns?

4 Analyze the significance of nonrepudiation in access control and cybersecurity.



5 Evaluate the principle of least privilege and its impact on access control. How does adhering to this principle reduce security risks within an organization?

6 Describe the role of ethical hacking in maintaining a strong cybersecurity posture. How does ethical hacking contribute to the overall security of an organization?



7 Outline the roles of professionalism and responsibility in ethical hacking.

8 Evaluate the role of white-hat hackers in conducting security audits and red team exercises.



Project

You are working at a large financial company and you are tasked with creating a comprehensive security analysis for the company board. You will present the threats from malware and advanced cyberattacks and how risk management strategies can help your company mitigate their impact. You will analyze the threats companies like yours face and the steps they can take to secure their information systems.

1

Introduce malware and advanced cyberattacks by defining them, providing examples, and explaining the consequences of malicious attacks on the company's information system.

2

Outline the processes of risk identification and assessment and describe various strategies that can be used to mitigate risks associated with malware and advanced cyberattacks.

3

Highlight the importance of ongoing risk management and monitoring in cybersecurity and present case studies of organizations that have effectively managed the risks posed by malware and advanced cyberattacks.

4

Create a PowerPoint presentation for the company board of directors that includes the above notes and summarizes why an effective cybersecurity strategy is crucial in the digital age.



Wrap up

Now you have learned to:

- > Define cybersecurity.
- > Outline the key principles of cybersecurity.
- > List the main career paths in cybersecurity.
- > Describe how Saudi Arabia became a prominent authority on cybersecurity.
- > Analyze the various types of malware.
- > Outline how cybercriminals utilize advanced cyberattacks.
- > Distinguish different processes and activities for risk identification, mitigation, and management.
- > Outline the data threat issues that cybersecurity systems are tasked with securing.
- > Summarize access control techniques for securing information systems.
- > Describe how ethical hacking helps protect organizations and companies.

KEY TERMS

Access Control

Authentication

Authorization

Availability

CIA Triad

**Chief Information
Security Officer (CISO)**

Confidentiality

Data Threat

Data Protection

Ethical Hacking

**Identity and Access
Management (IAM)**

Integrity

Malware

Nonrepudiation

Penetration Testing (PT)

Risk Identification

Risk Management

Risk Mitigation

Single Sign-On (SSO)

**Vulnerability Assessment
(VA)**

White-Hat Hacking

2. Cybersecurity Protection and Response

In this unit, you will learn about the threats affecting the security of hardware, software, and operating systems, and how to protect against them. You will then learn about how network systems are attacked and how to analyze and protect them with secure protocols and techniques. Then you will analyze how Digital Forensics and Incident Response are employed to protect large-scale systems from cyberattacks.

Learning Objectives

In this unit, you will learn to:

- > Outline the threats and vulnerabilities affecting hardware, operating and software system security.
- > Analyze secure system design techniques.
- > Protect Windows machines and data using basic security measures.
- > Describe how network structures and web technologies affect cybersecurity systems.
- > Outline network security protocols and techniques.
- > Analyze network traffic with Wireshark.
- > Utilize the Windows VPN service.
- > Analyze how Digital Forensics and Incident Response are used to protect digital systems.

Tools

- > Wireshark
- > Windows Defender Firewall
- > DB Browser for SQLite



Lesson 1

Hardware, Software and Operating System Security

Link to digital lesson



www.iem.edu.sa

Hardware, Software and Operating System Security

In cybersecurity, it is important to understand the necessity of protecting hardware, software, and operating systems from potential threats. These three components, as well as information and networks, are the foundation of any digital system, and securing them is essential to ensure the safety and privacy of users. In this lesson, hardware, software, and OS security will be discussed, and in the next lesson, network security will be presented.

Hardware Security

Hardware security involves safeguarding the physical components of a computer system, such as processors, memory, and storage devices. This includes implementing measures to prevent unauthorized access or tampering, and protecting hardware from damage due to environmental factors, power surges, or other hazards. Some common hardware security techniques include using secure boot processes, Trusted Platform Modules (TPMs) for encryption, and hardware security keys for authentication.

Main threats to hardware systems:

- **Physical attacks:** Unauthorized access to, modification of, or theft of hardware components.
- **Counterfeit components:** Fake or substandard hardware components introduced into the supply chain, potentially compromising security.
- **Hardware Trojans:** Malicious circuits or components hidden within hardware, capable of compromising the system or leaking sensitive data.
- **Side-channel attacks:** Attacks that exploit information leakage from the hardware, such as power consumption, electromagnetic radiation, or timing.

Security practices for protecting hardware systems:

- **Secure boot process:** Ensuring the boot process uses a digital signature to verify the authenticity of the OS.
- **Trusted Platform Modules (TPMs):** Integrating TPMs to enable hardware-based encryption and secure storage of encryption keys.

- **Hardware security keys:** Using hardware tokens or biometric devices for multi-factor authentication.
- **Firmware security:** Ensuring firmware updates are cryptographically signed and securely delivered.
- **Hardware-based virtualization:** Utilizing hardware features to isolate and secure virtual environments.
- **Network Air Gap:** This is a security measure that physically disconnects a hardware device from other networks to prevent hacking.

Table 2.1: Examples of hardware security threats and security best practices

Threat example	Security best practice example
An unauthorized person gains access to a server room and tampers with the hardware.	Implement a boot process that uses digital signatures to verify the authenticity of the operating system.
A fake RAM chip is introduced into a computer, which undermines the system's performance and security.	Incorporate a TPM into the system to provide hardware-based encryption and a secure storage location for encryption keys.

Operating System Security

The operating system (OS) is the core software that manages a computer's hardware and software resources, acting as an intermediary between the user and the system components. Securing the OS is vital to maintaining overall system security. Modern operating systems have built-in security features that help protect against common threats. These features may include user authentication, file and folder permissions, encryption, and firewall protection. Regularly updating the OS with security patches and using strong, unique passwords for user accounts are essential best practices for maintaining operating system security.

Main threats to operating systems:

- **Unauthorized access:** Gaining unauthorized access to an operating system, potentially leading to data theft, system compromise, or disruption.
- **Privilege escalation attacks:** Exploiting vulnerabilities to gain higher levels of access or control within the operating system.
- **Rootkits:** Rootkits are malicious software programs made to gain access to and control of a computer's operating system without the owner's knowledge.
- **Boot sector attacks:** Attacks targeting the boot sector of a system, potentially preventing the operating system from loading or functioning.

Security practices for protecting operating systems:

- **User authentication:** Requiring a unique username and strong, complex password for each user account.
- **File and folder permissions:** Setting appropriate access controls to restrict access to sensitive files and folders.
- **Encryption:** Using built-in OS encryption tools to protect sensitive data on storage devices.
- **Firewall protection:** Configuring the OS firewall to monitor and control incoming and outgoing network traffic coming from or to the OS.
- **Regular OS updates:** Installing the latest OS patches and security updates to address vulnerabilities.
- **Security baselines and hardening:** Applying security best practices and configurations to minimize attack surfaces.

Table 2.2: Examples of operating system security threats and security best practices

Threat example	Security best practice example
Malware is installed on a system that hides its existence and gives an attacker unrestricted access to the operating system.	Use the built-in encryption tools of the OS to protect sensitive data on storage devices.
An attacker uses malware to alter the boot sector of a system, preventing it from starting up correctly.	Configure the OS firewall to monitor and control incoming and outgoing network traffic.

Software Security

Software security involves protecting the programs and applications running on a computer system from vulnerabilities, bugs, and potential exploits. This includes developing secure coding practices, regularly updating software with security patches, and using antivirus programs to detect and remove malicious software. Additionally, software security ensures that only trusted and verified applications are installed on a system and that proper access controls are in place to prevent unauthorized use or modification.

Main threats to software systems:

- **Exploitation of vulnerabilities:** Attackers taking advantage of software vulnerabilities to compromise systems or gain unauthorized access.

- **Malware:** Malicious software, such as viruses, worms, ransomware, or spyware, that can cause harm or steal sensitive data.
- **Injection Attacks:** Attacks where malicious code or commands are inserted into a software system, leading to unauthorized access or control.
- **Backdoor:** A backdoor is a security flaw in software that establishes a path of access to a system or device that bypasses normal authentication procedures.
- **Buffer Overflows:** An overly large input that is not correctly handled by the software's code can cause a program to crash or execute unintended code, potentially allowing malicious code to run.

Security practices for protecting software systems:

- **Secure coding practices:** Adopting practices such as input validation and proper error handling in software development.
- **Regular software updates:** Applying security patches and updates as soon as they are released by vendors.
- **Antivirus programs:** Installing and updating antivirus software to detect and remove malware.
- **Application sandboxing:** Isolating applications in a restricted environment to minimize potential damage.
- **Intrusion detection/prevention:** Intruders use network gateways to infect the software of a system. An IDS is a system that monitors networks for any potentially harmful activity and takes appropriate action in response.

Table 2.3: Examples of software security threats and security best practices

Threat example	Security best practice example
An attacker uses a known vulnerability in a web application to gain unauthorized access to user data.	Use input validation and proper error handling during software development to minimize the potential for exploitation.
A software developer unknowingly includes code that allows remote access without authentication in a software update.	Run potentially unsafe applications in a restricted environment to minimize the potential for harm.



The threats and the best practices described above for hardware, software and operating system security are related to several challenges that need to be confronted when protecting IT systems. Table 2.4 illustrates the main challenges of protecting hardware, software, and operating systems.

Table 2.4: Main challenges of protecting hardware, software, and operating systems	
Challenge	Description
Hardware system security	
Physical tampering	Protecting hardware from unauthorized physical access, modification, or theft.
Supply chain security	Ensuring the security and integrity of hardware components throughout the supply chain, from manufacturing to deployment.
Firmware vulnerabilities	Identifying and mitigating vulnerabilities in firmware, which can be exploited by attackers to compromise hardware.
Hardware obsolescence	Addressing the security risks associated with outdated or unsupported hardware components.
Software systems security	
Zero-day vulnerabilities	Identifying and mitigating previously unknown software vulnerabilities before they can be exploited by attackers.
Software complexity	Managing the increasing complexity of software systems, which can introduce new vulnerabilities and make security harder to achieve.
Software supply chain attacks	Securing the software supply chain against compromises, which can lead to the introduction of malicious code or vulnerabilities.
Operating system security	
OS vulnerabilities	Identifying and addressing vulnerabilities in the operating system that can be exploited by attackers.
Privilege escalation	Preventing attackers from gaining higher levels of access or control within the operating system.
OS hardening	Implementing and maintaining the necessary security configurations and best practices to protect the operating system.
Compatibility issues	Ensuring that security measures do not negatively impact the performance or compatibility of applications running on the OS.

Secure System Design Techniques

Secure system design is a fundamental approach in cybersecurity that emphasizes building security into systems from the ground up. It involves considering potential threats and vulnerabilities during the development process and implementing measures to mitigate risks proactively. The following are some of the most common techniques for secure system design.

Security by Design

Security by Design is a principle that advocates for integrating security measures and considerations from the initial stages of system or software development. Instead of being an afterthought or an addition, security protocols and safeguards are built into the product from the outset. This proactive approach emphasizes the creation of systems and applications in such a way that they are inherently secure. This includes defining policies, roles, and responsibilities, ensuring data integrity and privacy, and implementing user access controls, encryption, and secure coding practices. Security by Design aims to minimize security vulnerabilities and limit the impact of potential security breaches.

Defense in Depth

Defense in depth is a comprehensive approach to cybersecurity where multiple layers of security controls and measures are placed throughout an information technology system. It is based on the military principle that it's more difficult for an enemy to penetrate a complex and multi-layered defense system than to breach a single barrier. This strategy aims to protect information integrity, availability, and confidentiality by implementing a series of defensive mechanisms, including firewalls, intrusion detection systems, data encryption, anti-virus software, and physical security measures. The concept relies on the notion that if one layer of defense is ineffective or breached, the next layer should be able to prevent the attack, giving an organization multiple opportunities to mitigate potential threats.

Security by design and defense in depth seem similar, but there are differences in their application. The following examples show their differences in various scenarios.

Website development with security by design

In the development of a new e-commerce website, security by design would entail the use of secure coding practices, input validation to prevent SQL injection or cross-site scripting attacks, and implementing strong user authentication and access controls from the outset.

Network infrastructure setup with defense in depth

Deploying firewalls at the network perimeter, implementing intrusion detection/prevention systems (IDS/IPS), using strong endpoint protection software, and having a strong incident response plan in place. Regular audits and penetration testing would also be part of the strategy.

Cloud-based service development with security by design

When developing cloud-based services, best practices would include the use of secure APIs, robust authentication and access control mechanisms, and built-in data encryption techniques.

Physical data center security with defense in depth

To protect the physical security of a data center, defense in depth will use segmentation to divide the network into smaller, isolated subsections. The network is segmented on multiple levels, typically by firewalls, public-facing networks, and virtual LANs (VLANs). Each segment should have its security controls, such as authentication, traffic inspection, and monitoring protocols, to reduce the risk of attacks.



Secure Programming

Secure programming involves writing software code resistant to vulnerabilities and exploits. It involves using secure coding techniques, best practices, and development methodologies to minimize the risk of introducing security flaws into the software. Table 2.5 shows scenarios in which the secure programming technique is applied.

Table 2.5: Applications of security by secure programming technique	
Scenario	Application
Web Application Development	Developers are creating a new web application for a banking system. Secure programming in this context would involve input validation, using secure and encrypted connections (HTTPS), and implementing proper session management.
Mobile Application Development	Developers are working on a new mobile app for a healthcare provider. Here, secure programming might involve ensuring that the app does not store sensitive data insecurely on the device, implementing strong access controls, and encrypting all data transmitted between the app and the server.

Passkeys and Device Security

There are multiple tools and techniques used to protect hardware devices and their data. Even the simplest protection measures can be effective against security vulnerabilities. One modern example are **passkeys**. A passkey is a digital credential that replaces traditional passwords and allows users to sign in to apps and websites using biometric sensors, PINs, or patterns. Passkeys provide robust protection against phishing attacks and are standardized across browsers and operating systems. When users want to sign in to a passkey service, their browser or operating system will help them select and use the right passkey.

The system will ask users to unlock their devices using a biometric sensor, PIN, or pattern. This ensures that only the rightful owner can use the passkey. Passkeys use public key cryptography, reducing potential data breach threats. When a user creates a passkey with a site or application, this generates a public-private key pair on the user's device. Only the site stores the public key, but this alone is useless to an attacker. An attacker can't derive the user's private key from the data stored on the server, which is required to complete authentication. Because passkeys are bound to a website or app's identity, they're safe from phishing attacks. The browser and operating system ensure that a passkey can only be used with the website or app that created them. This frees users from the worry of signing in to a fake website or app designed to fool them. One example is FIDO2 (Fast Identity Online), an open authentication standard that supports passwordless authentication using biometrics and external security keys. The use of a passkey is illustrated in figure 2.1.

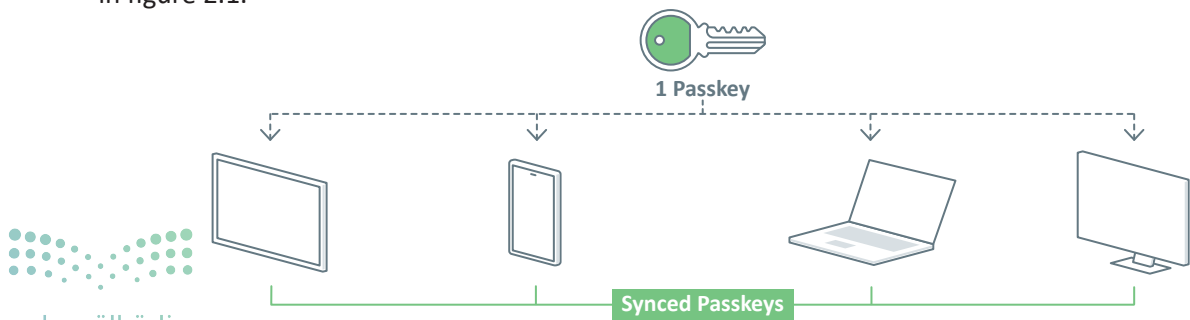


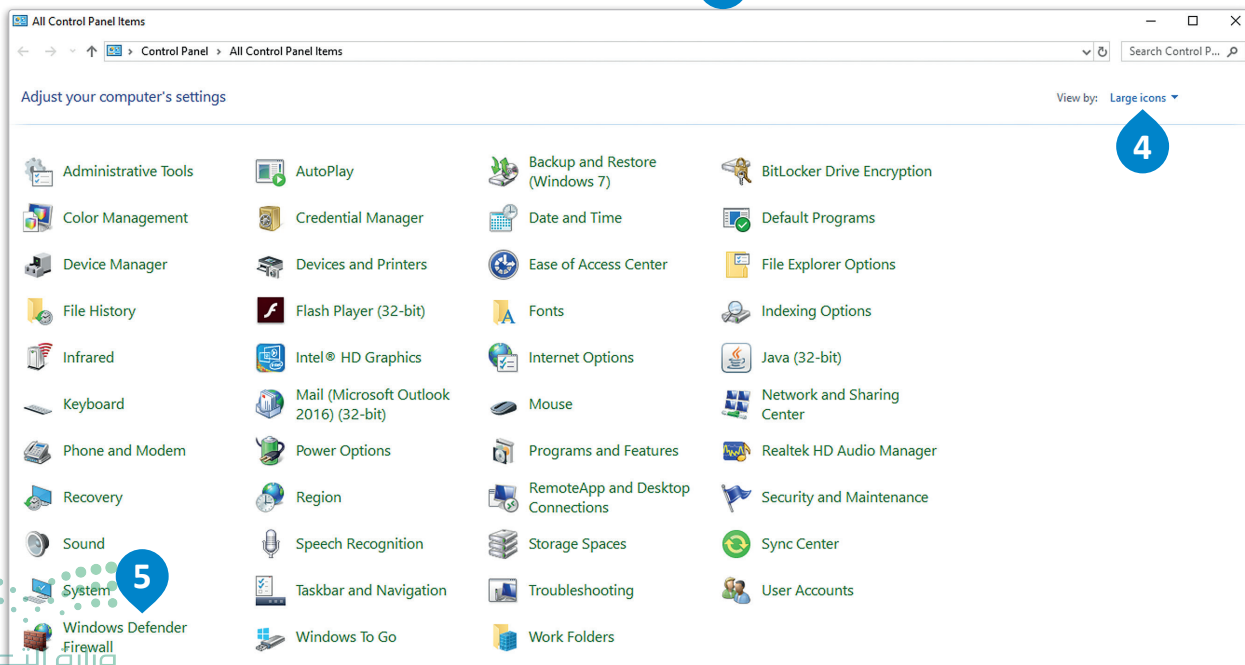
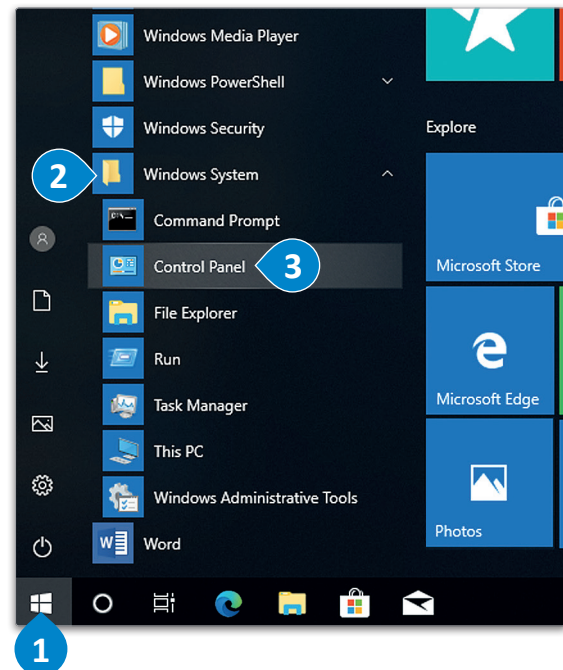
Figure 2.1: Authentication of mobile devices with the use of a passkey

Windows Firewall

The built-in Windows firewall is a software application that helps protect the OS on your PC by monitoring incoming and outgoing network traffic and allowing or blocking it based on a set of rules. It acts as a barrier between your computer and the Internet or other networks, preventing unauthorized access to your system. Carry out the following steps to see how to activate the Windows firewall on your PC. The following steps might have a slight variation, depending on the Windows OS version that you use. For this example, we will use **Windows 10**.

Activating the Windows Firewall:

- > Click on the **Windows Start** button. **1**
- > Click on **2** the **Control Panel** application. **3**
- > Change the settings view to **Large icons**. **4**
- > Click on the **Windows Defender Firewall** option. **5**
- > Check if the shield is **green**, which means that the firewall is **enabled**. **6**
- > Click on the **Turn Windows Defender Firewall on or off** option. **7**
- > Click on the **radio buttons** to toggle between **activating** and **deactivating** the firewall. **8**
- > Click **OK**. **9**



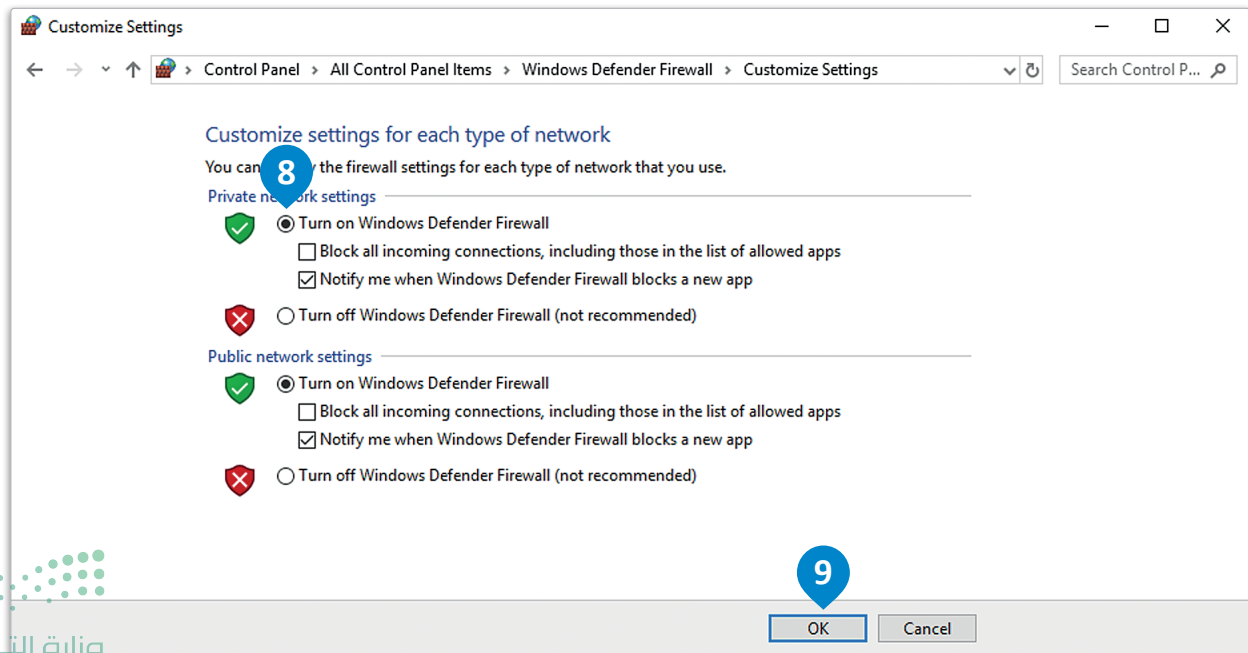
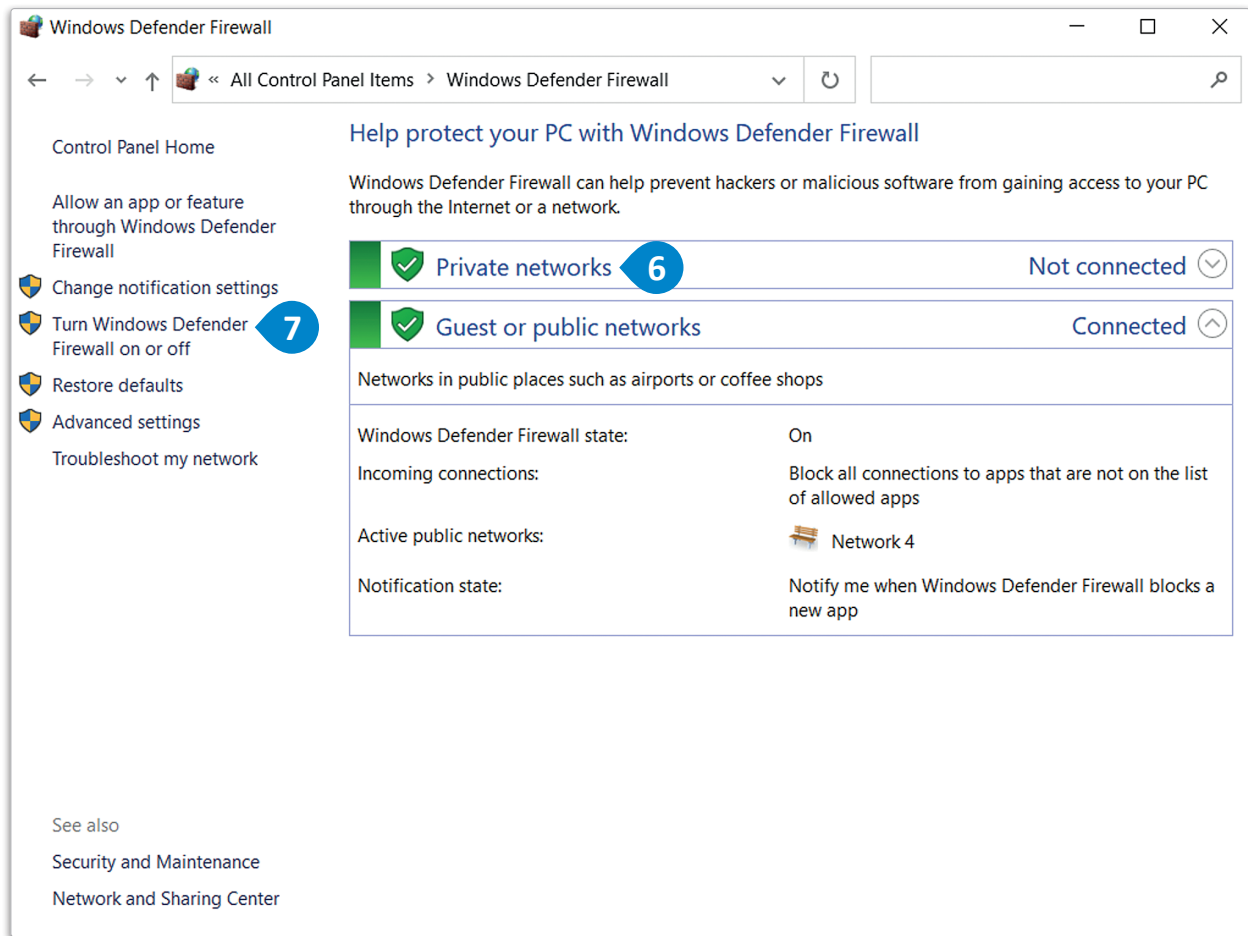


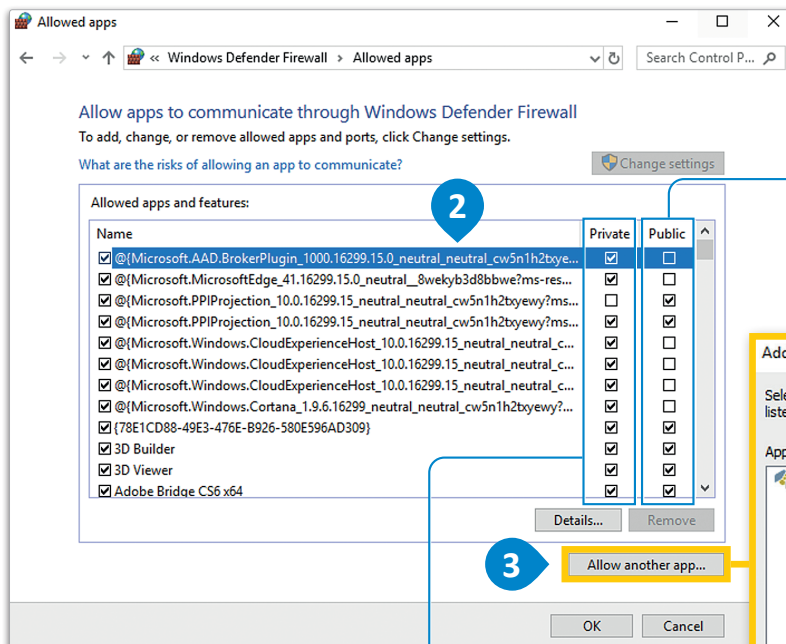
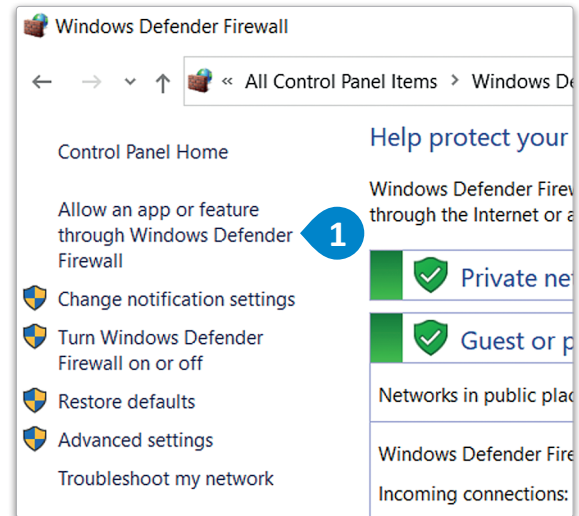
Figure 2.2: Activating the Windows Firewall

Allowing Internet Access to Applications on your PC

Windows provides several security features to protect your device and your data from unauthorized access, malware, and other attacks. Although this firewall works well when managing applications and limiting network connections, sometimes a security measure may require you to allow or block applications manually.

Allowing Internet access to applications:

- > In the **Windows Defender Firewall** window, click **Allow an app or feature through Windows Defender Firewall**. **1**
- > A list of installed apps requesting Internet access will appear. **2**
- > To allow an application to connect to the Internet, click **Allow another application**. **3**
- > If there is an application to which you want to allow access to the Internet, select it. **4**
- > Click **Add**. **5**



This option allows a specific application to connect to the Internet and is usually used for public networks.

This option blocks access to the Internet.

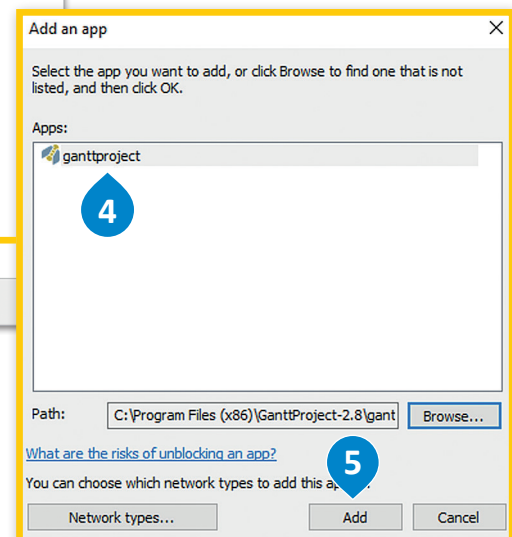
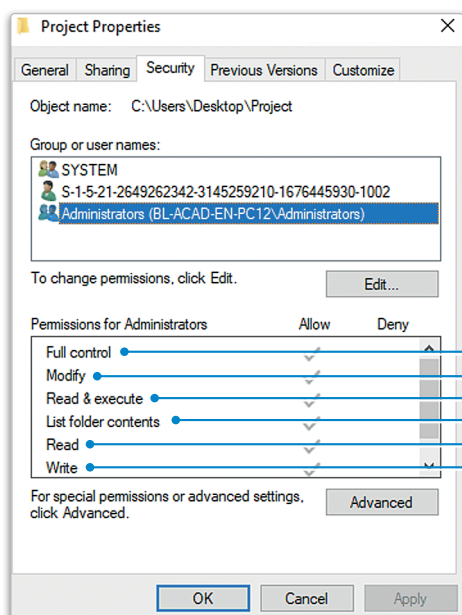


Figure 2.3: Allowing Internet access to applications



Modifying File and Folder Permissions on your PC

Controlling access to files and folders is one of the fundamental measures for securing information systems. Windows provides an interface for setting permissions and access to different folders and files on a system. This will prevent malicious users from accessing sensitive data. Windows systems use the NTFS permissions system. NTFS (New Technology File System) permissions are a set of access controls used to restrict or grant permissions to users and groups accessing files and folders. NTFS permissions enable administrators to set granular permissions for users and groups at the file and folder level, allowing for fine-grained control over who can access, modify, or delete specific files and folders. The most common NTFS permissions are the following:



Full Control: Provides the user or group with complete control over the file or folder, including the ability to modify permissions, delete, and take ownership.

Modify: Allows users to modify files or folders, including creating new files and subfolders.

Read & Execute: Allows users to view and execute files and folders.

List Folder Contents: Allows users to view the contents of a folder but not to read, modify or execute the files within the folder.

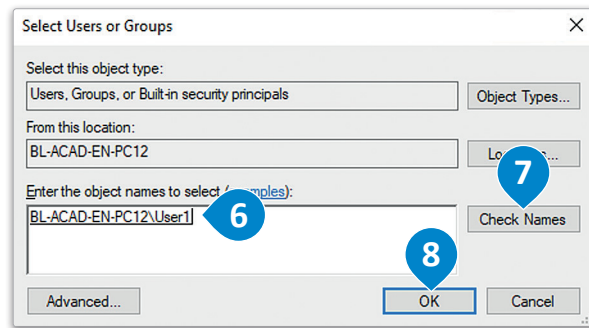
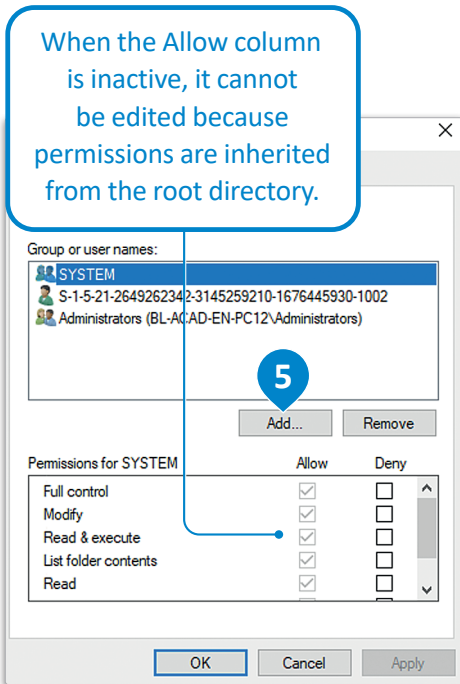
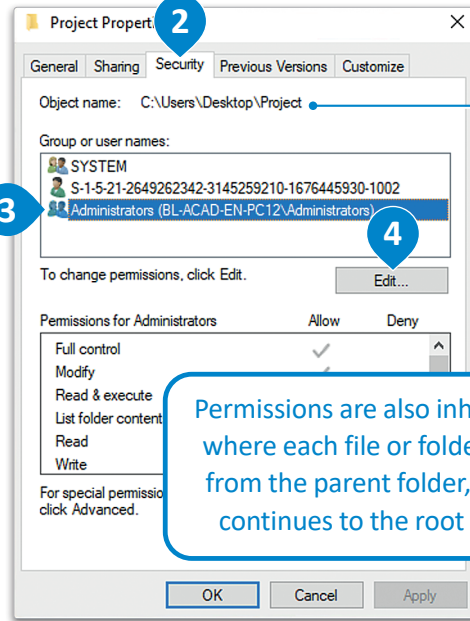
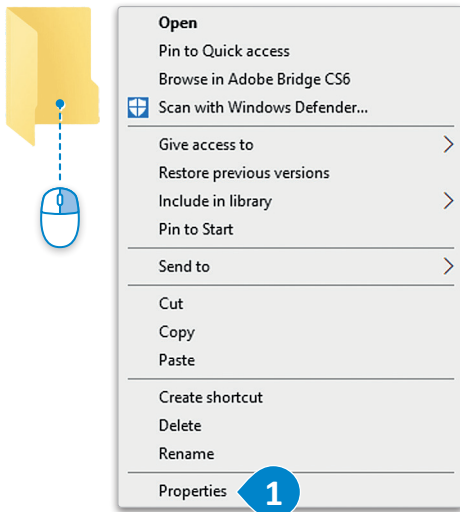
Read: Allows users to view files and folders.

Write: Allows users to create new files and folders.

The following instructions show how to modify the permissions and access to a folder for a specific user or group.

Modifying file and folder permissions for a specific user:

- > Right-click on the file or folder that you want and click **Properties**. ①
- > Click on the **Security** tab. ②
- > You can view a list of all the users that have permissions. ③
- > Click on the **Edit** button to edit the permissions of a user or group. ④
- > Click on the **Add** button to add a new user or group. ⑤
- > If you need to change the permissions of a user or a group, type the name. ⑥
- > Click on the **Check Names** button to check that your inputted text is correct. ⑦
- > Click **OK**. ⑧
- > You can view the new user or group in the updated list. ⑨
- > Use the checkboxes to assign the permissions that you want. ⑩



To be able to edit any permissions, you must have ownership of the file or folder, so if the owner is another user account or a system account such as a local system, you will not be able to modify the permissions.

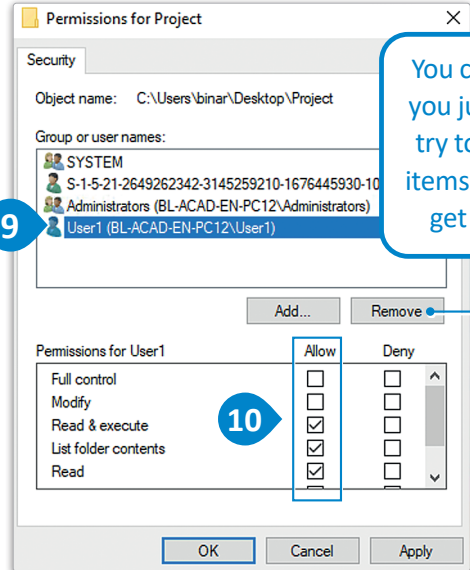


Figure 2.4: Modifying file and folder permissions for a specific user

Exercises

1

Read the sentences and tick ✓ True or False.	True	False
1. Hardware security involves safeguarding the physical components of a computer system.	☐	☐
2. Malware is malicious code that is triggered by a specific condition or event.	☐	☐
3. Sandboxing is a technique for isolating applications from the main operating system.	☐	☐
4. Software security includes installing antivirus programs to detect and remove malicious software.	☐	☐
5. Secure boot processes are used to verify the authenticity of the operating system before it boots up.	☐	☐
6. Passkeys do not use biometric data for user authentication.	☐	☐
7. Firmware security involves ensuring that firmware updates are cryptographically signed and securely delivered.	☐	☐
8. Encryption is used to protect sensitive data on storage devices.	☐	☐
9. Regular operating system updates should be installed to address any vulnerabilities.	☐	☐
10. Security by design is a proactive approach to developing secure systems and applications by integrating security measures and considerations after the development process.	☐	☐



2 Evaluate the risks associated with outdated or unsupported hardware components.

3 Compare the challenges faced in ensuring the security of hardware and software systems.

4 Analyze the main best practices for protecting operating systems.



5 Evaluate the effectiveness of secure system design techniques for protecting digital systems.

6 List examples of the applications of security by design.

7 Describe how passkeys are used as a modern authentication method.



Lesson 2

Network and Web Security

Link to digital lesson



www.iem.edu.sa

Network Structures and Web Technologies in Cybersecurity

In cybersecurity, understanding the structure of networks and web technologies is crucial, as these elements shape the nature of the threats and the protective measures that can be taken to mitigate them. Networks consist of interconnected devices that exchange information with each other, while web technologies enable the creation and sharing of content and applications over the Internet. The Internet can be viewed as a network of networks. As the number of devices and web services increases, so does these systems' complexity and potential vulnerability.

The structure of networks and web technologies directly impacts the types of threats that can be encountered in the cybersecurity landscape. For instance, networks may face distributed denial-of-service (DDoS) attacks, which can overwhelm and disrupt services by flooding them with traffic. Similarly, web technologies can be vulnerable to threats like cross-site scripting (XSS) and SQL injection attacks, where hackers exploit vulnerabilities in web applications to gain unauthorized access to sensitive data.

On the other hand, the structure of networks and web technologies also shapes the protective measures that can be employed to secure them. For example, network segmentation can isolate critical systems and reduce the potential attack surface. In contrast, firewalls and intrusion detection systems (IDSs) can help monitor and control traffic flow in and out of a network. In web technologies, secure programming practices, such as input validation and proper error handling, can help prevent vulnerabilities from being exploited.

The following presents the basic networking and web technology concepts that influence cybersecurity threats and protective measures:

Fundamental Networking Concepts

Network Topologies

The physical or logical arrangement of devices in a network. Common topologies include star, ring, bus, mesh, and hybrid.

Network Devices

Essential hardware components that facilitate communication and connectivity within networks, such as switches, routers, firewalls, and access points.

Transmission Media

The physical or wireless means through which data is transmitted between devices in a network. Examples include Ethernet cables (e.g., twisted-pair, coaxial, or fiber-optic cables) and wireless technologies (e.g., Wi-Fi, Bluetooth, or cellular networks).

Network Protocols

Sets of rules and conventions that dictate how devices communicate and exchange information within a network. Protocols operate at different layers of the Open Systems Interconnection (OSI) or TCP/IP models. Examples include HTTP/S, FTP, TCP, UDP, and IP.

Fundamental Networking Components

Switches

Network devices responsible for directing traffic within a local area network (LAN), connecting devices and ensuring that data packets reach their intended destinations.

Routers

Devices that forward data packets between different networks, determining the most efficient path for the data to travel.

Firewalls

Security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules, protecting internal networks from unauthorized access and potential cyberattacks.

Access Points

Network devices that provide wireless connectivity to other devices, enabling them to connect to the network and communicate with other devices or systems.

Fundamental Networking Protocols

IP (Internet Protocol)

Responsible for addressing and routing data packets across networks, ensuring that they reach their intended destinations.

Internet Protocol Security (IPSec)

IPSec is a suite of protocols used to secure IP communications by authenticating and encrypting each IP packet in a data stream. It operates at the network layer of the Internet Protocol Suite, enabling it to protect any application traffic across an IP network.

TCP (Transmission Control Protocol)

Ensures reliable data transmission by establishing a connection between devices, sequencing data packets, and managing the information flow.

SSL/TLS (Secure Sockets Layer / Transport Layer Security)

Cryptographic protocols that provide secure communication over a network by encrypting data exchanged between a client and a server, commonly used in web browsing, email, and other applications that require secure data transmission.

UDP (User Datagram Protocol)

This is an unreliable protocol used by applications that require faster delivery of data but do not require the complex features of the TCP.

HTTP (Hypertext Transfer Protocol)

Used for transmitting web-based content between a client (e.g., a web browser) and a server using a TCP connection, enabling the exchange of text, images, and other multimedia elements.

HTTPS (Hypertext Transfer Protocol Secure)

An encrypted version of HTTP that uses TLS/SSL protocol instead of using TCP directly. It is currently used in the majority of Internet services.

FTP (File Transfer Protocol)

A standard protocol for transferring files between a client and a server over a network, allowing users to upload, download, and manage files on a remote system.

SFTP (Secure File Transfer Protocol)

A secure version of FTP that uses SSH (Secure Shell) to encrypt data during transmission, providing an additional layer of security for file transfers.

DNS (Domain Name System)

A protocol that translates human-readable domain names (e.g., www.example.com) into IP addresses, allowing users to access websites and other network resources using easily understandable names as URLs (Unified Resource Locator).

DHCP (Dynamic Host Configuration Protocol)

A network management protocol that automatically assigns IP addresses and other network configuration information to devices on a network, simplifying network administration and reducing the risk of IP address conflicts.

SNMP (Simple Network Management Protocol)

A protocol for monitoring and managing network devices, such as routers, switches, and servers, by collecting and organizing information about their performance, use, and status.

Network and Web Security Technologies

In cybersecurity, it is important to understand and employ various network security protocols and technologies to protect the integrity, confidentiality, and availability of data and systems. The following are the most common and essential network security measures.

Intrusion Detection Systems (IDSs)

An Intrusion Detection System (IDS) is a security technology that monitors network traffic for any signs of malicious activity or policy violations. Intrusion Detection Systems can generate alerts when potential threats are detected, allowing network administrators to respond quickly and mitigate the impact of an attack. There are two types of IDSs:

- **Network-based IDS (NIDS):**

This type of IDS analyzes network traffic, looking for suspicious patterns or signs of unauthorized access.

- **Host-based IDS (HIDS):**

This type of IDS is installed on individual devices, such as servers or workstations, and monitors local system activity for any signs of intrusion or unauthorized access.

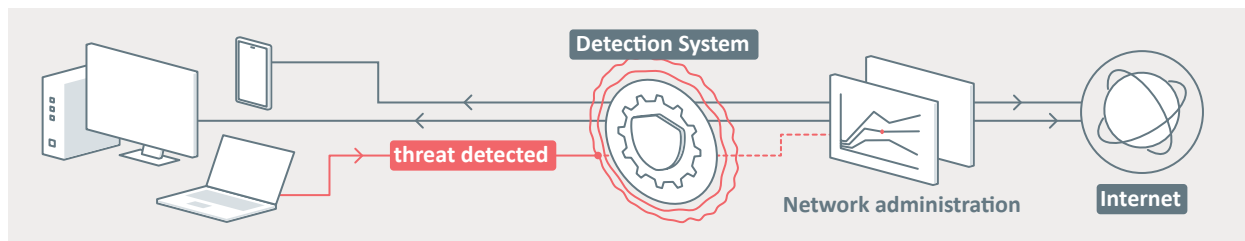


Figure 2.5: Representation of an IDS

Demilitarized Zones (DMZs)

A Demilitarized Zone (DMZ) is a specific network segment between an organization's internal network and the external, untrusted network, such as the Internet. The DMZ is designed to provide an additional layer of security by isolating services that need to be accessible from the Internet, such as web servers or email servers, from the organization's internal network.

By placing these services in the DMZ, any potential attacks or vulnerabilities are contained within the DMZ and are less likely to impact the internal network. This setup allows organizations to maintain a higher level of security for their critical systems and data.

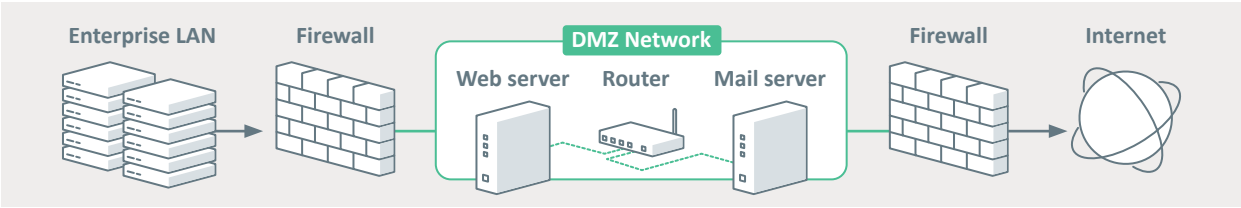


Figure 2.6: DMZ Network architecture

Virtual Private Networks (VPNs)

A Virtual Private Network (VPN) is a technology that establishes a secure and encrypted connection between a user's device and a remote network, often over the Internet. VPNs protect the confidentiality and integrity of data transmitted between the user's device and the remote network, ensuring that sensitive information remains private even when transmitted over unsecured networks.

VPNs also provide additional benefits, such as bypassing geo-restrictions, protecting user privacy, and allowing remote access to secure networks. These technologies are commonly employed by businesses and individuals alike to maintain security and privacy while using the Internet.

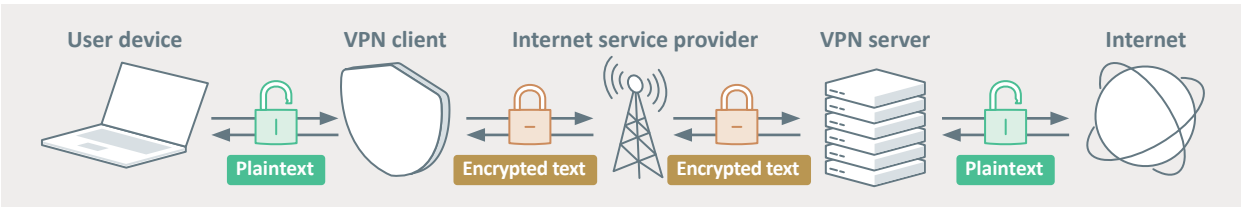


Figure 2.7: Representation of a VPN

Protecting your Devices on a Public Wi-Fi Network

Using public WiFi networks is convenient, but creates various security risks for your devices and your data. The following are best practices for protecting your devices on a public WiFi network.

- Use your cellphone as a mobile hotspot.
- Turn off your WiFi connection when you are not planning to connect to a WiFi network.
- Do not perform tasks that require the transmission of sensitive information, like financial or medical data, over public WiFi.
- Do not reset passwords for your accounts over a public WiFi network.
- Use a VPN service.
- Avoid web pages that use HTTP protocol instead of the more secure HTTPS.
- Turn off resource sharing on your devices.

Network Monitoring and Packet Sniffing

There are tools that are used to monitor the traffic on a network and track and analyze the packets that are transmitted through the network. These actions are performed by tools called Packet Analyzers. One of the most popular packet analyzer tools is **Wireshark**. Wireshark is an open-source packet analyzer used to examine details of traffic at several levels, from connection-level information to single packet-level information. It provides information to the network administrator regarding individual packets, such as transmission time, source and destination, protocol type, and packet header data which can be very important for evaluating and diagnosing security issues. You can download and install Wireshark from the following link:

<https://www.wireshark.org/download.html>



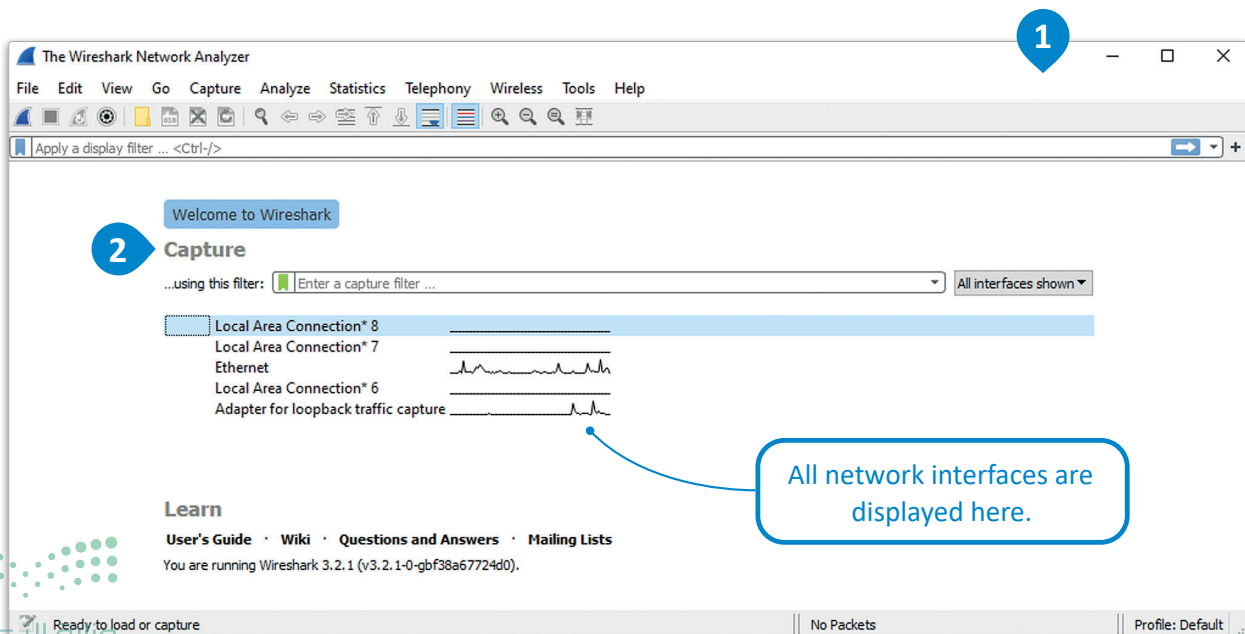
Figure 2.8: QR code to download Wireshark

Monitoring a Network with Wireshark

You will now familiarize yourself with the interface of the Wireshark network analyzer.

Monitoring a network with Wireshark:

- > Open the **Wireshark** application and view the **available networks** list. **1**
- > Click on the **Capture** command. **2**
- > In the **Capture Interfaces** window, click on the **network** you want to monitor. **3**
- > Click on the **Start** button. **4**
- > Monitor the flow of data packets in the network. **5**
- > Click the **Stop** button to end the network monitoring. **6**



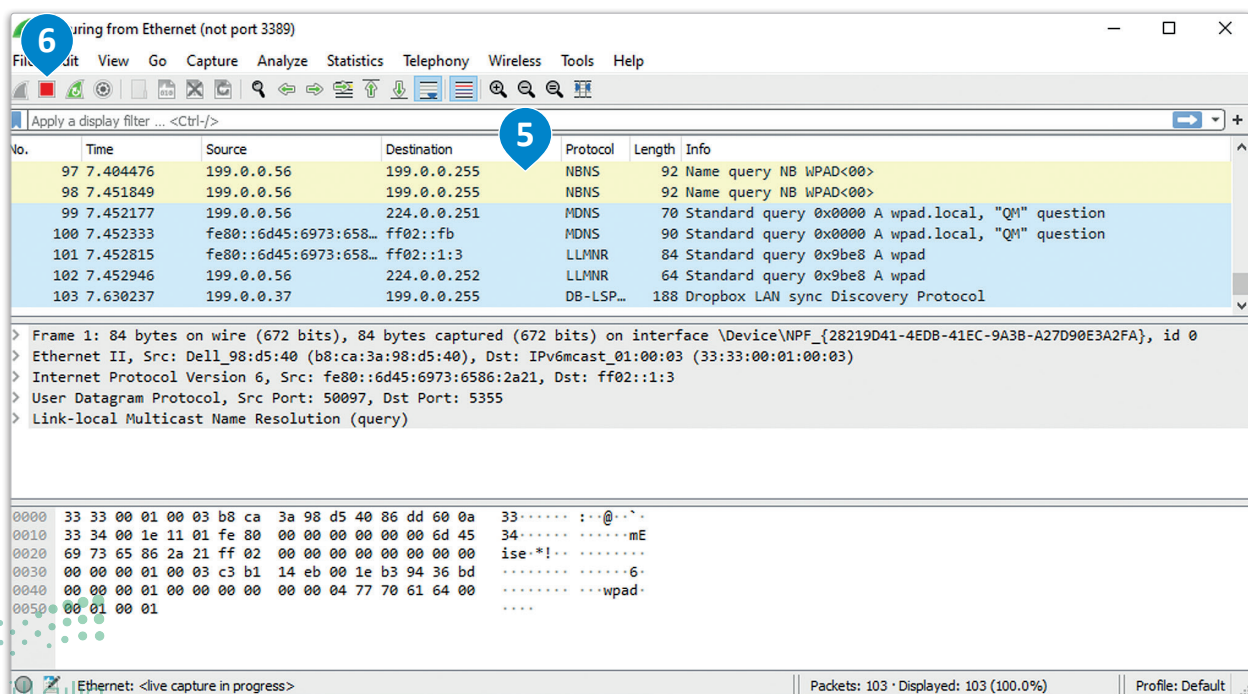
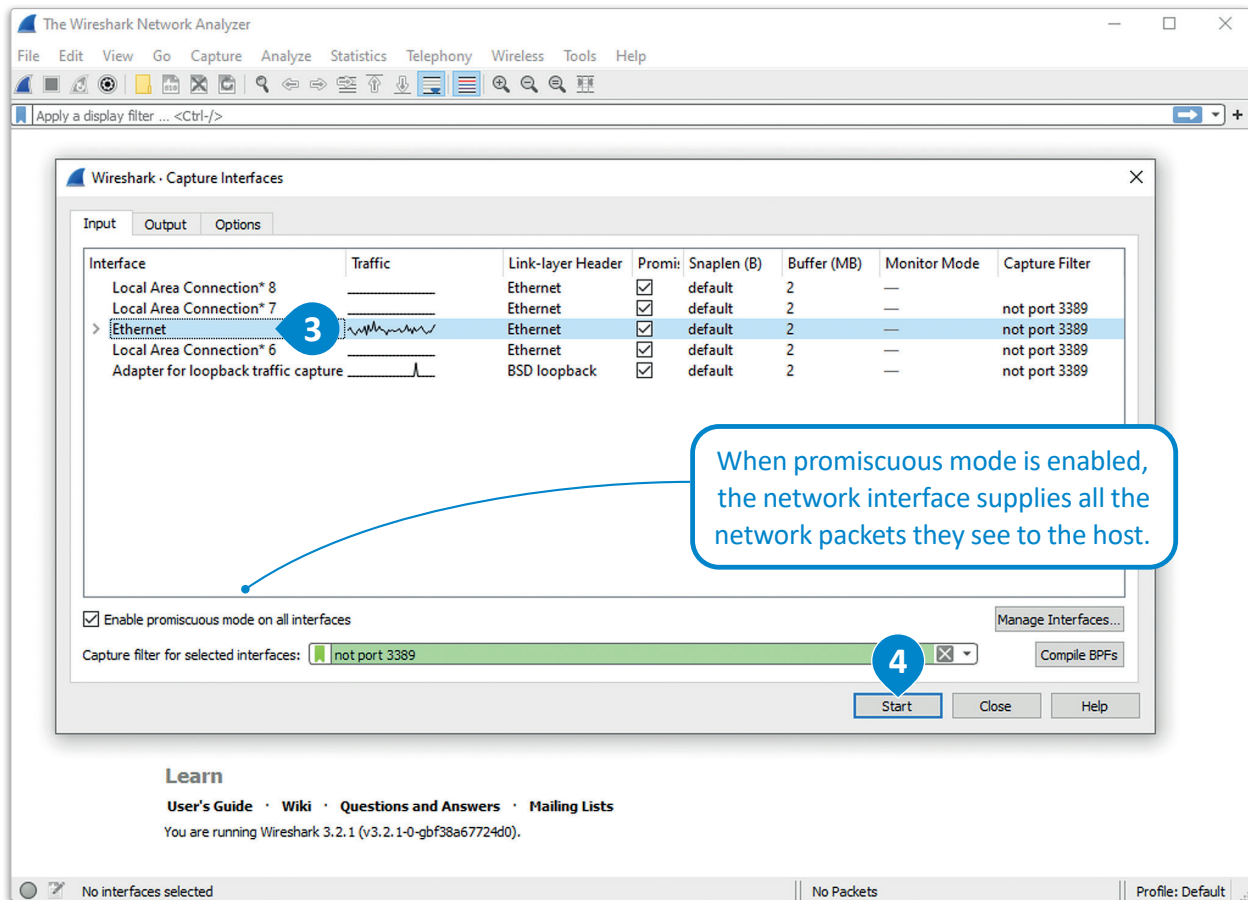


Figure 2.9: Monitoring a network with Wireshark

Analyzing the Wireshark Output

The Wireshark Network analyzer offers a lot of data about the flow of packets through the network, grouped into three different panes. These are the **Packet List Pane**, the **Packet Details Pane**, and the **Packet Byte Pane**.

The Packet List Pane

Time: The Time column refers to the time the packet was received or sent, measured in seconds since the start of the capture.

Source: The Source column indicates the IP address of the source.

Destination: The Destination column indicates the destination IP address.

Protocol: The Protocol column indicates the communication protocol that was used.

Length: The Length column refers to the length of the package.

Info: The Info column contains additional information about the package.

The screenshot displays the Wireshark network analyzer interface. The top pane, 'The Packet List Pane', shows a table of captured packets. The bottom pane, 'The Packet Details Pane', shows the hierarchical structure of the selected packet (Frame 24). The bottom-most pane, 'The Packet Byte Pane', shows the raw byte data of the selected packet.

Time	Source	Destination	Protocol	Length	Info
19.0.454862	199.0.0.154	199.0.0.46	UDP	973	3389 → 56890 Len=931
20.0.595584	199.0.0.42	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
21.0.607092	199.0.0.46	199.0.0.154	UDP	60	56890 → 3389 Len=11
22.0.655524	199.0.0.154	40.69.222.109	TCP	54	57103 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1026 Len=0
23.0.720223	199.0.0.154	199.0.0.46	UDP	1219	3389 → 56890 Len=1177
24.0.738046	40.69.222.109	199.0.0.154	TCP	60	443 → 57103 [FIN, ACK] Seq=1 Ack=2 Win=1022 Len=0
25.0.738110	199.0.0.154	40.69.222.109	TCP	54	57103 → 443 [ACK] Seq=2 Ack=2 Win=1026 Len=0
26.0.744110	199.0.0.46	199.0.0.154	TLSv1.2	97	Application Data
27.0.751879	199.0.0.46	199.0.0.154	TLSv1.2	97	Application Data
28.0.751950	199.0.0.154	199.0.0.46	TCP	54	3389 → 59329 [ACK] Seq=1 Ack=1 Win=1026 Len=0
29.0.768463	199.0.0.46	199.0.0.154	TLSv1.2	104	Application Data
30.0.773324	199.0.0.154	199.0.0.46	UDP	1282	3389 → 56890 Len=1240
31.0.773367	199.0.0.154	199.0.0.46	UDP	1279	3389 → 56890 Len=1237

The Packet Details Pane shows the following details for Frame 24:

- Frame 24: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{28219D41-4EDB-41EC-9A3B-A27D90E3A2FA}, id 0
- Ethernet II, Src: VMware_55:6f:07 (00:0c:29:55:6f:07), Dst: Dell_9c:e5:c3 (f8:b1:56:9c:e5:c3)
- Internet Protocol Version 4, Src: 40.69.222.109, Dst: 199.0.0.154
- Transmission Control Protocol, Src Port: 443, Dst Port: 57103, Seq: 1, Ack: 2, Len: 0

The Packet Byte Pane shows the raw byte data of the selected packet:

```

0000 f8 b1 56 9c e5 c3 00 0c 29 55 6f 07 08 00 45 00 ..V.... )Uo...
0010 00 28 3a 3d 40 00 65 06 0d 46 28 45 de 6d c7 00 .(:@.e..F(E.m..
0020 00 9a 01 bb df 0f fa 64 c6 7e 6a 18 fa ab 50 11 .....d~j...P.
0030 03 fe d7 15 00 00 00 00 00 00 00 00 00 00 00 .....
  
```

Figure 2.10: Network monitoring output

The Packet Details Pane

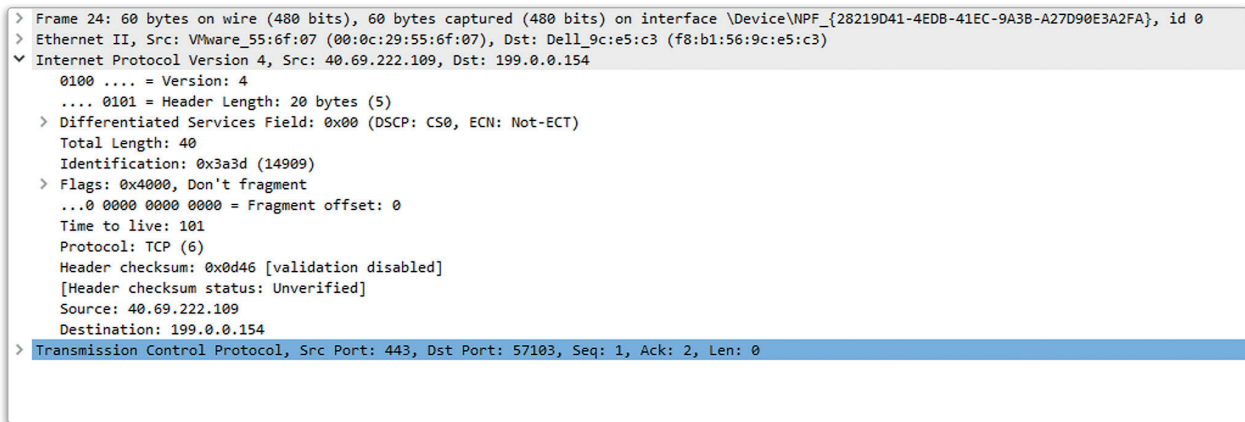
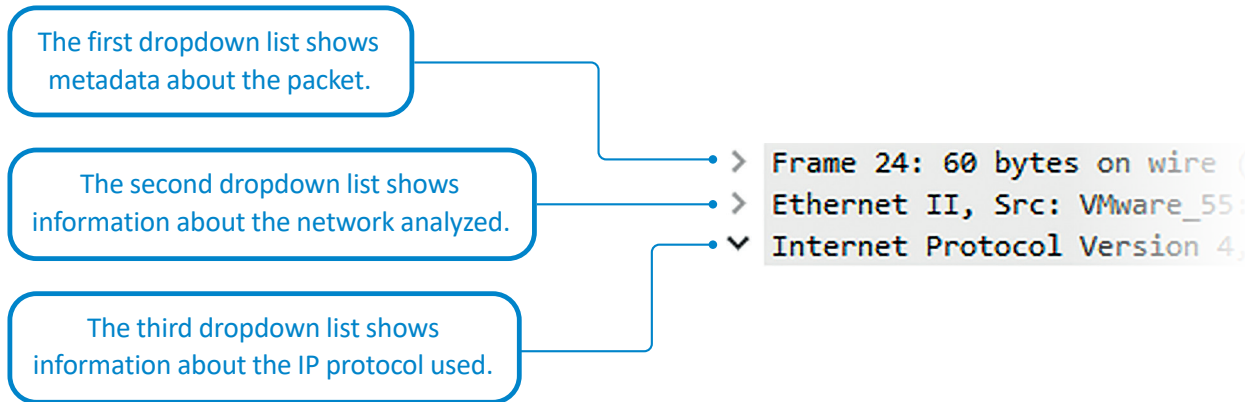


Figure 2.11: The Packet Details Pane



The Packet Byte Pane

The Packet Byte Pane box displays packet data defined in hexadecimal format.

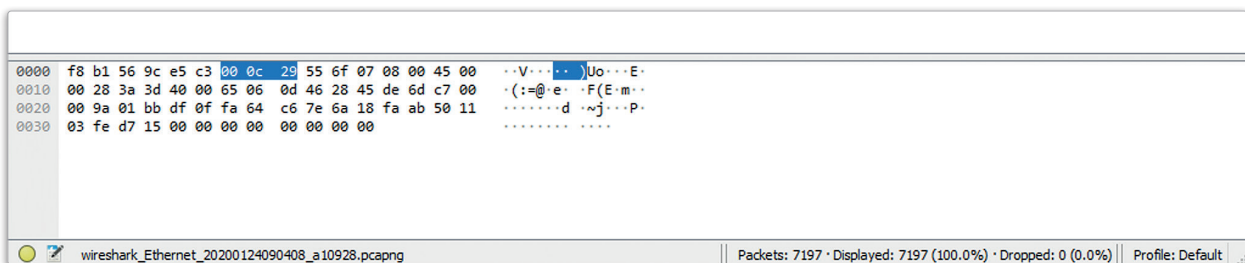


Figure 2.12: The Packet Byte Pane

INFORMATION

Wireshark shows the packet byte pane in hexadecimal format because it provides a more compact and readable representation of the data transmitted on the network. In the hexadecimal system, each byte of data is represented by two digits (0-9 and A-F), which provides a concise way to display and analyze the contents of packets. The hexadecimal format is commonly used in networking protocols and standards, allowing easy data comparison and analysis across different systems and platforms.

Analyzing a Wireshark scan

Wireshark can be used to analyze the network data flow from scans of a network that were carried out previously and then saved. You will use a file from a saved scan to find suspicious activity on the network. You can download a network scan file from the following download link:

https://bl-xtrtransfer.s3.amazonaws.com/KSA/G12/CYB/U2/L2/Scan_results.pcapng



To open a Wireshark file:

- > In the **File** tab, click the **Open** option. 1
- > In the **Open Capture File** window, select the **Scan_results.pcapng** file. 2
- > Click **Open**. 3
- > The scan file will output all the recorded network traffic. 4

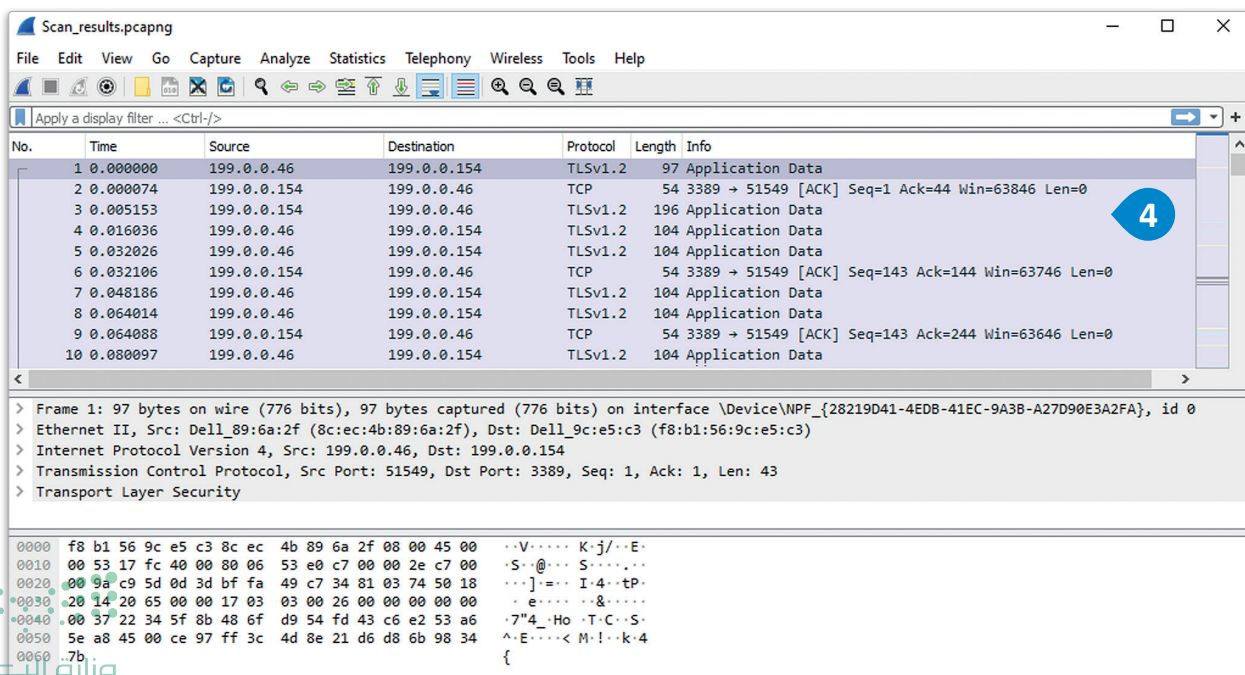
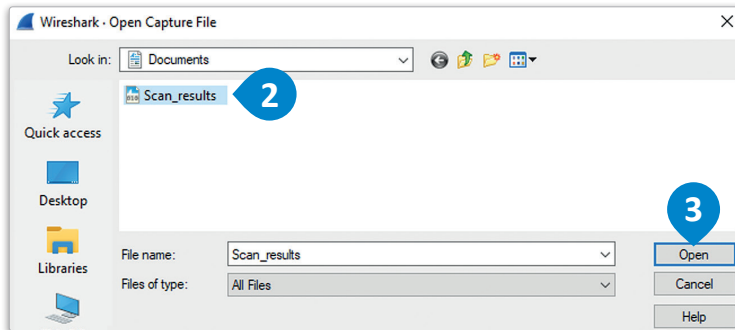
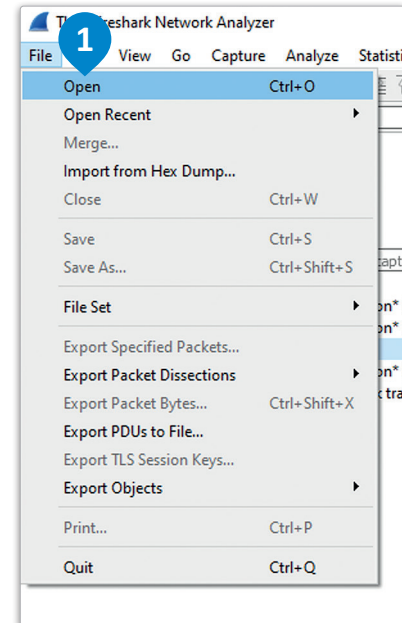


Figure 2.13: Open a Wireshark file

Taking a closer look at the Packet List Pane that displays the scan results, you can see that the scan file contains packets describing conversations between users' machines (clients) and central servers.

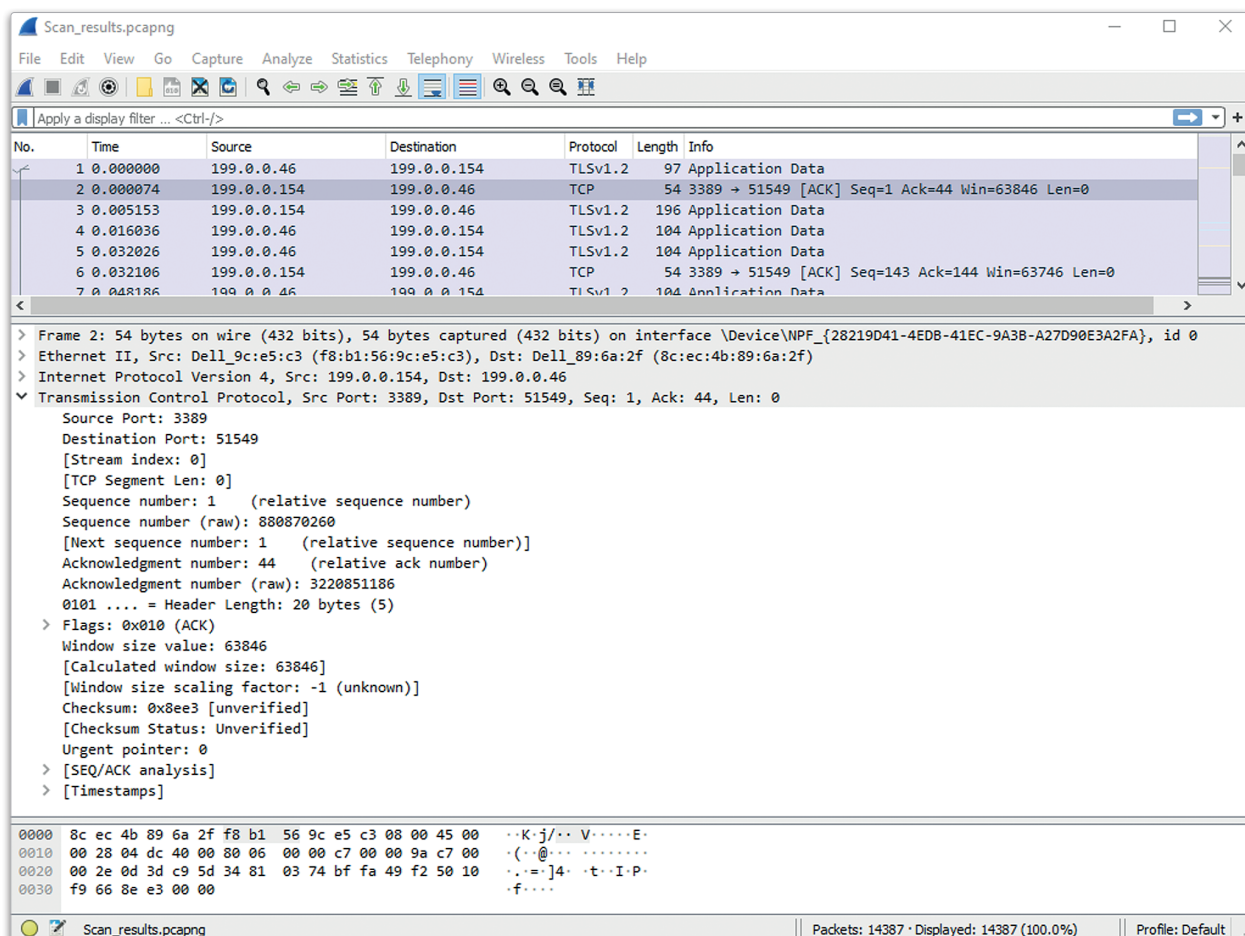
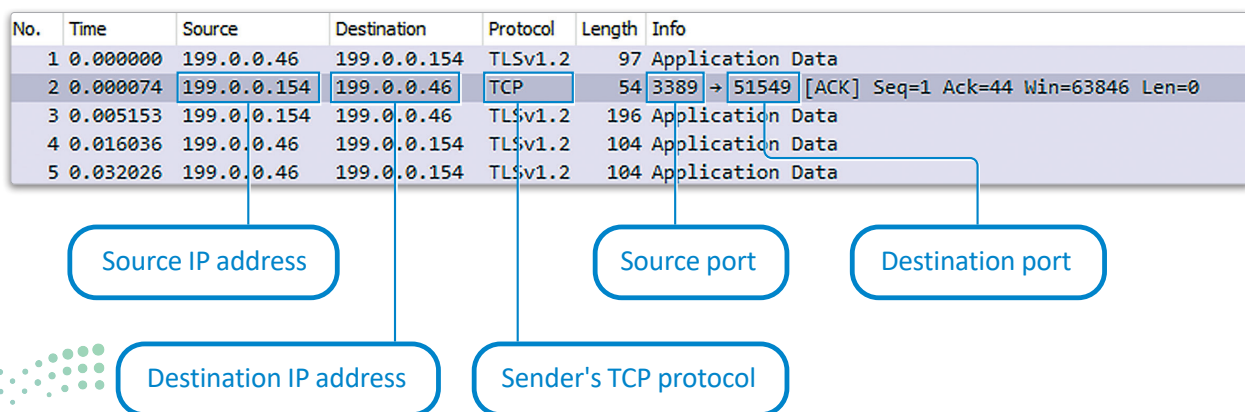


Figure 2.14: Detailed output of Packet Details Pane

In **packet #2**, the **source IP address** is **199.0.0.154**, and the **destination IP address** is **199.0.0.46**. The **receiver** sends a packet using the **sender's TCP protocol** over port **3389** as the **source port** (the sender's port) and port **51549** as the **destination port** (the receiver's port).



In another example, in **packet #10214**, you can notice that the **source IP address** is **172.217.23.99**, and the **destination IP address** is **199.0.0.154**. The packet information also shows that the transmission protocol used is **TCP**, and the port number is **80**, which indicates that the **Hypertext Transfer Protocol (HTTP)** is being used. This means the user is visiting a web page. The IP address **172.217.23.99** belongs to a **Google search engine page**, meaning you received a data packet from Google.

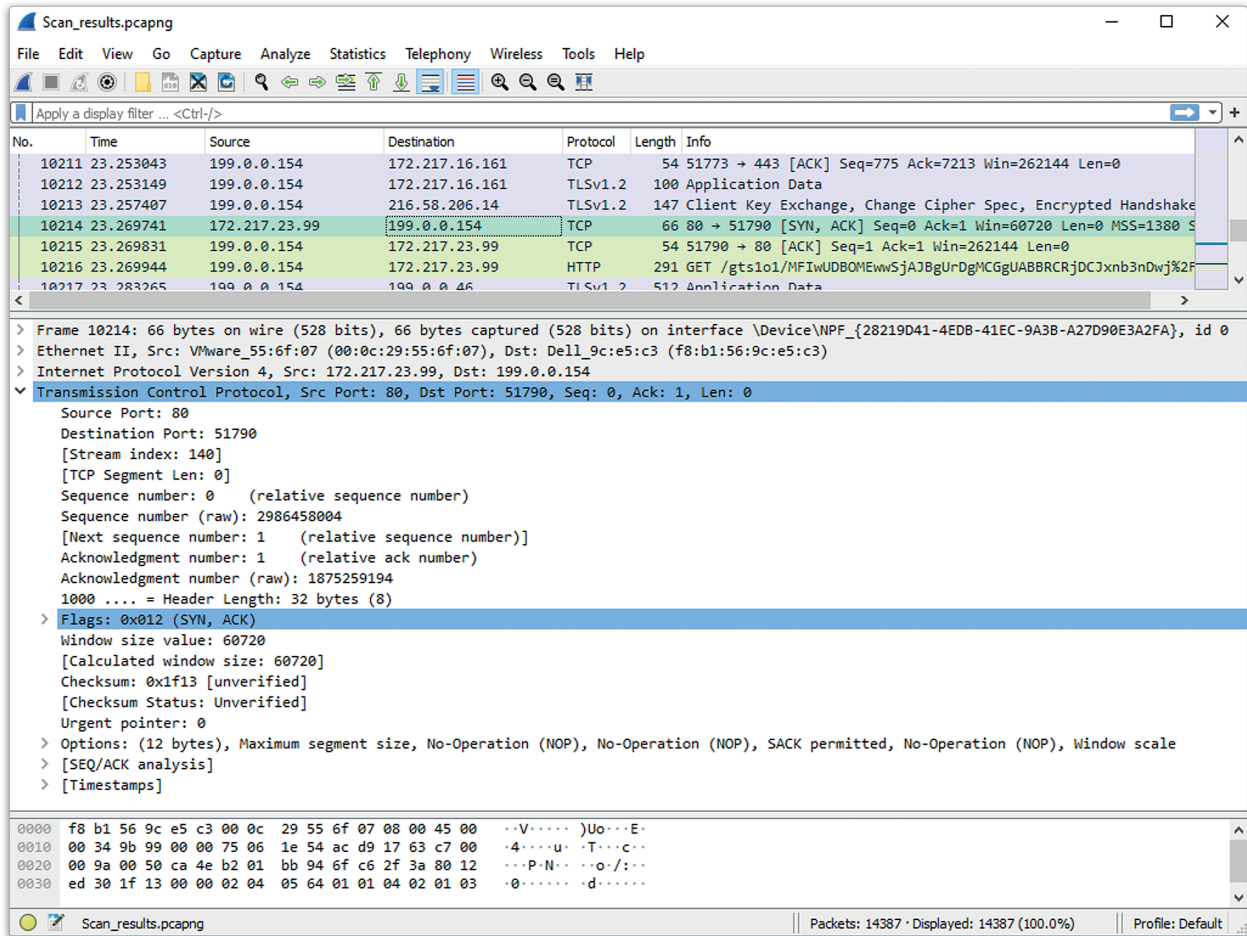


Figure 2.15: Analysis of IP addresses



Detecting Suspicious Activity on a Network

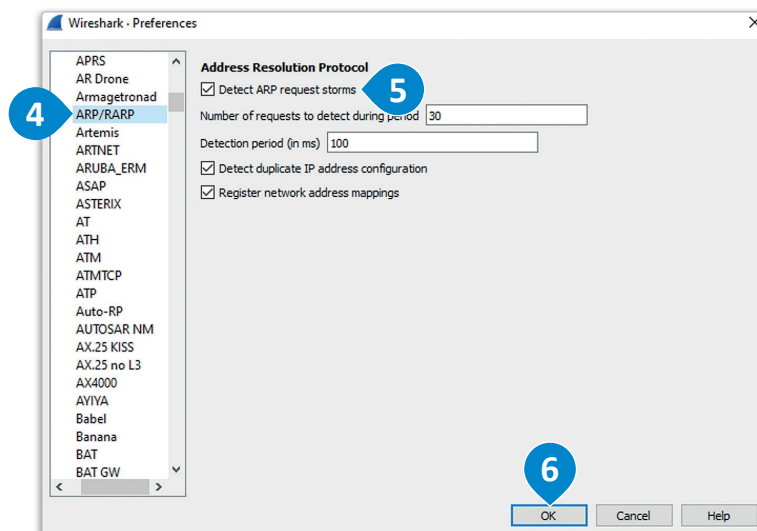
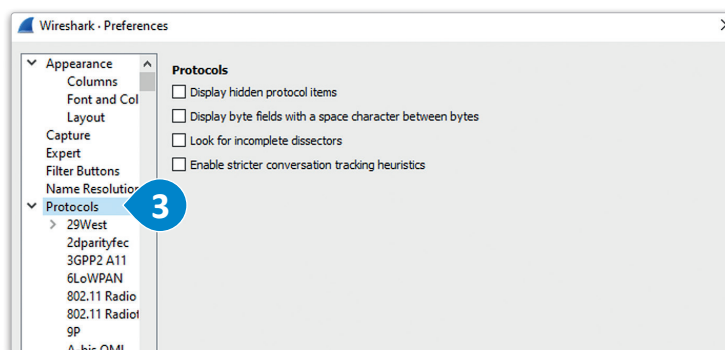
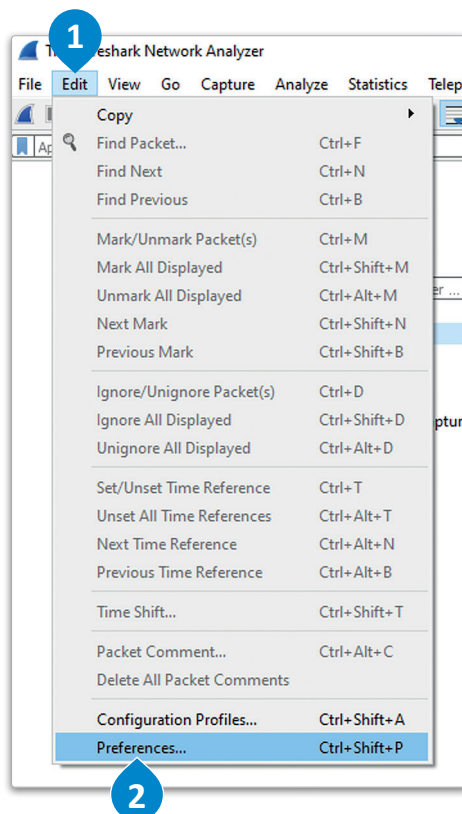
Wireshark is used to detect suspicious activities on the network. You will check Address Resolution Protocol (ARP) messages and packets that pass using this protocol to detect devices that are trying to perform suspicious operations.

To detect ARP requests:

- > In the Edit tab **1**, click Preferences. **2**
- > In the **Preferences** window, select the **Protocols** option. **3**
- > Choose the **ARP/RARP** protocol. **4**
- > Check the **Detect ARP request storms** box. **5**
- > Click **OK**. **6**
- > In the **Packet List Pane**, you can check for suspicious activity. **7**

Address Resolution Protocol (ARP)

The Address Resolution Protocol (ARP) is a communication protocol used for resolving the network layer addresses (IPv4 addresses) of a device to its corresponding data link layer address (MAC address) on a local network. ARP is essential for enabling devices to communicate with each other on a local network by mapping IP addresses to MAC addresses.



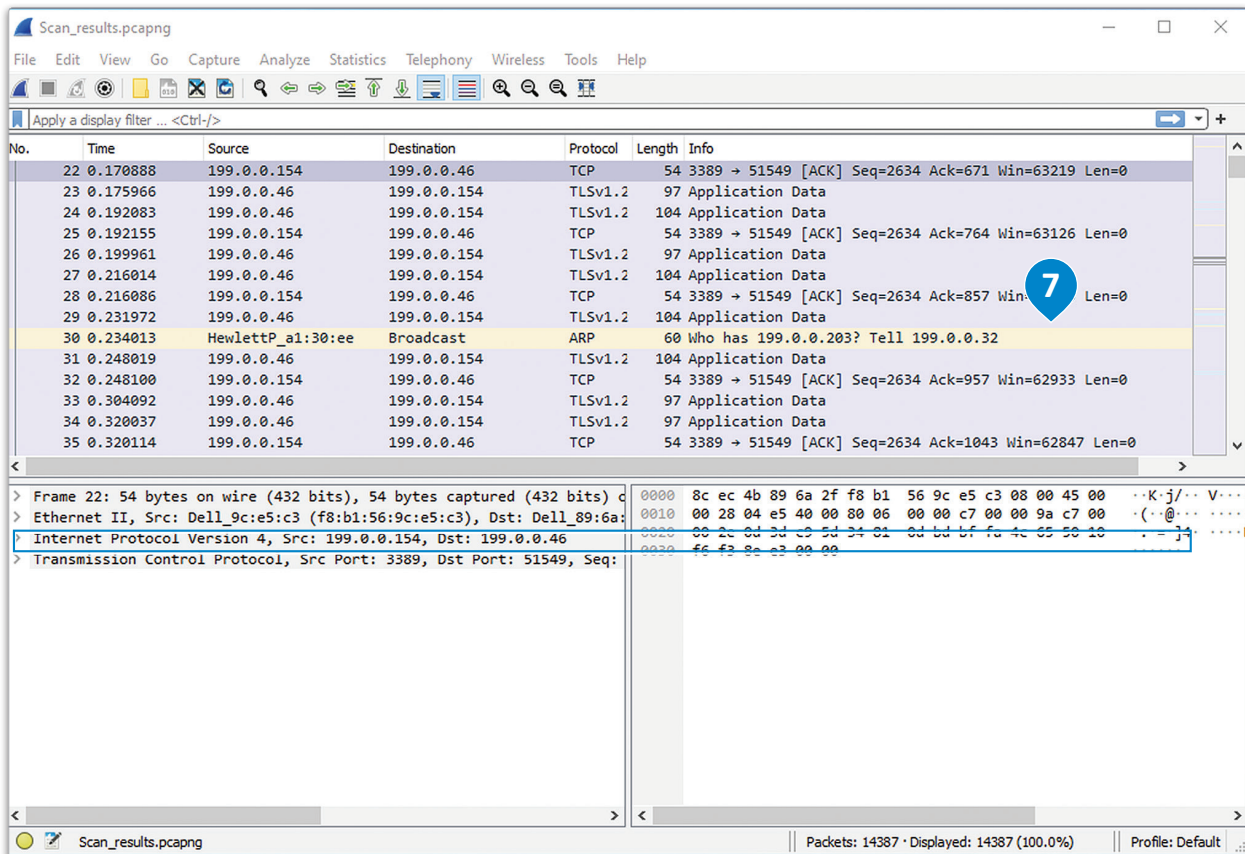


Figure 2.16: Detect ARP requests

In the Packet List Pane, the capture results show that suspicious network activity has been detected. More specifically, there is a device that sends data without showing the destination to which it is sent, and it eavesdrops on other devices on the network. It checks if IP 199.0.0.203 is in use, and the response is returned to IP 199.0.0.32. From this information, we can conclude that someone may be trying to detect if IP 199.0.0.203 is in use, as shown in figure 2.17. If it isn't, a potential intruder can use this IP address to connect to the network.

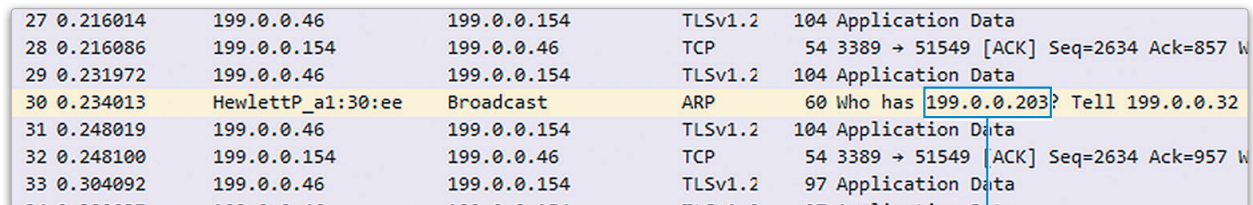


Figure 2.17: An unknown user trying to detect if IP 199.0.0.203 is in use



Someone may be trying to detect if IP 199.0.0.203 is in use.



Analyzing Data Flow with Expert Information

Wireshark offers an Expert Information option to identify network problems and suspicious behavior, which aids non-professionals in recognizing such activity.

To activate the Expert Information option:

- > In the **Analyze** tab, click the **Expert Information** option. 1
- > Suspicious activity is recognized by the Expert Information system. 2

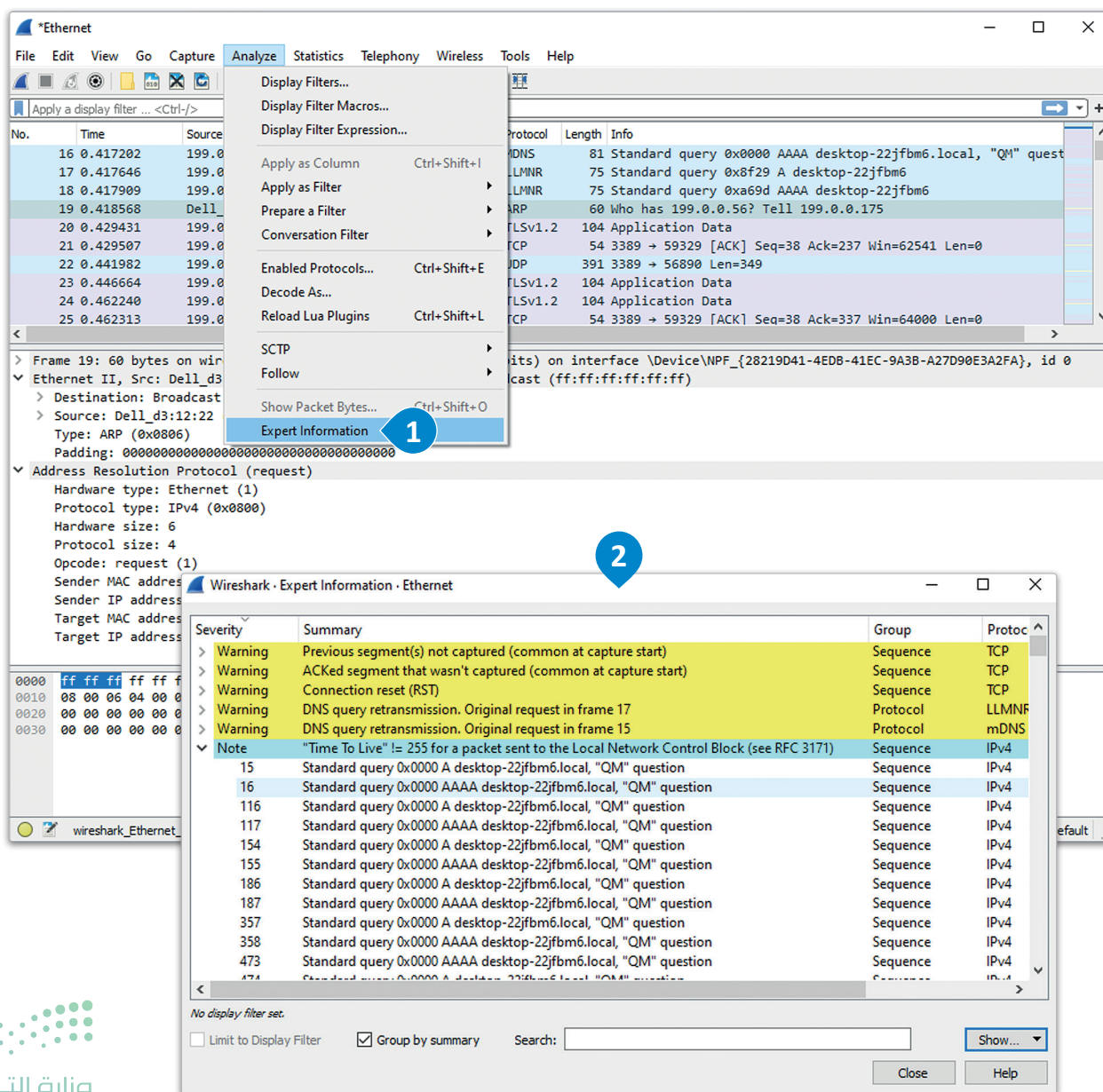


Figure 2.18: Activating Expert Information

Connecting to a VPN Service on your Windows Machine

The Windows operating system has a built-in VPN connector that you can use to protect your machine. This method is widely used, as it allows users to securely access remote resources, especially after the increase in the need for employees to work remotely from their homes. This means the organizations need to provide secure access for their remote employees.

An employee can securely connect to the organization's servers through a VPN service without worrying about their login data or other sensitive data being intercepted if they connect from home or anywhere outside the organization's building.

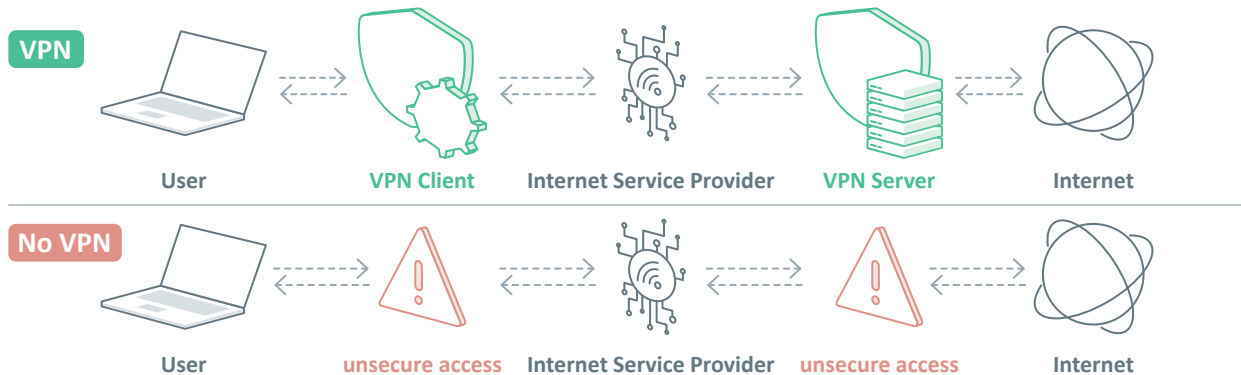
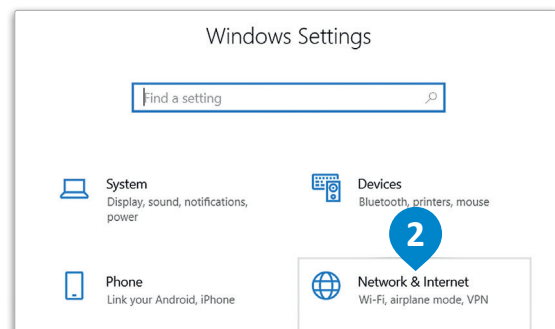
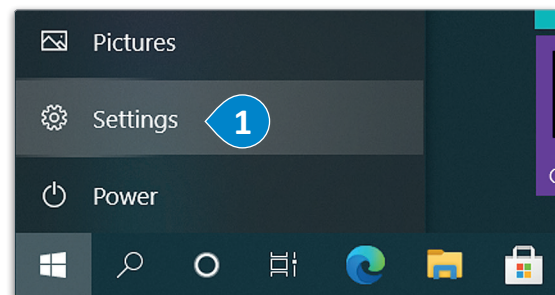


Figure 2.19: VPN service is a secure method for a remote employee

Your Windows computer can connect to a VPN for business or personal use. A VPN connection provides more security in accessing your corporate network and the Internet in public places or through unsecured networks such as in restaurants and airports. Suppose you have a VPN service installed on your computer which is named **my-vpn-server**, and you want to connect to it.

To connect to a VPN Service:

- > In the **Windows Start** menu, click **Settings**. **1**
- > In the **Windows Settings** window, click **Network & internet**. **2**
- > Click on the **VPN** tab. **3**
- > Click on the **Add a VPN connection** button. **4**
- > In the **VPN provider** dropdown, select the **Windows (built-in)** option. **5**
- > Type **VPN** in the **Connection name** field. **6**
- > Type **my-vpn-server** in the **Server name or address** field. **7**
- > In the **Type of sign-in info** field, choose the **User name and password** field. **8**
- > Click **Save**. **9**



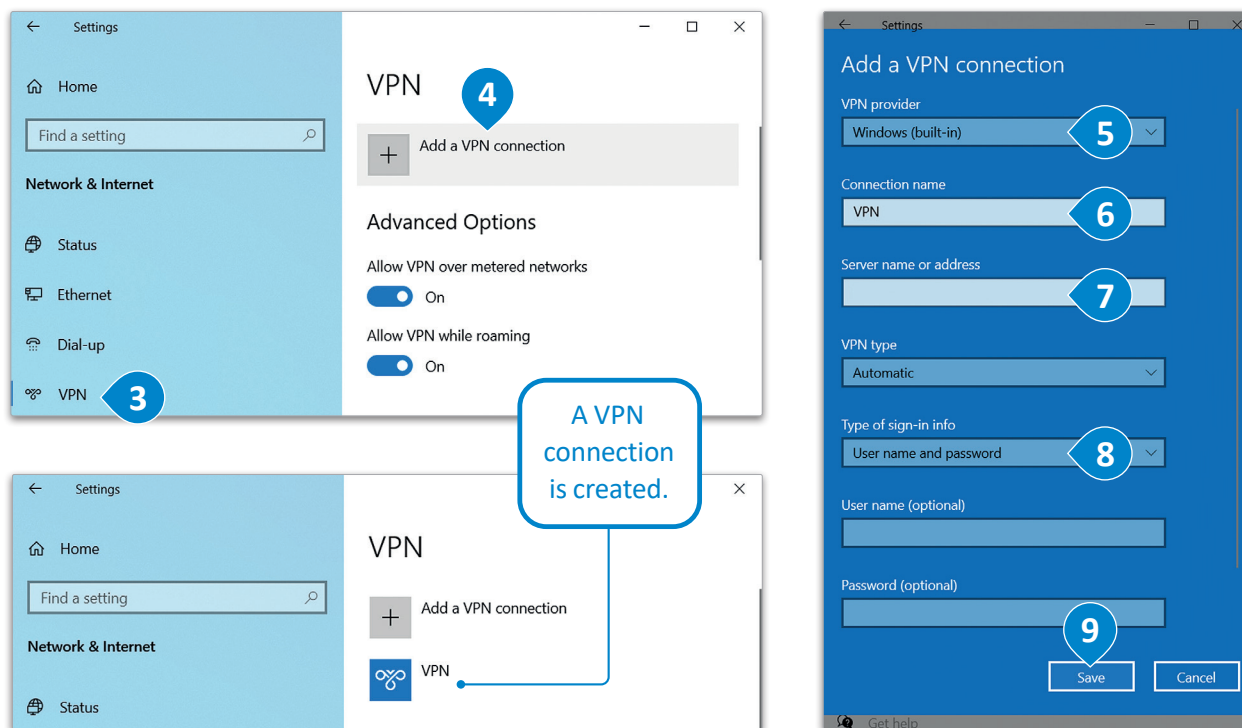


Figure 2.20: Connecting to a VPN Service

Activating the VPN service

After configuring the VPN service, you must connect to it to activate its features.

To activate a VPN service:

- > In the **Windows Notification** area, click the **Network** button. **1**
- > Choose the VPN connection you want to use, in this case: **VPN**. **2**
- > Click **Connect**. **3**
- > Enter the username and password. **4**
- > Click **OK**. **5**
- > When the connection is established, the word **Connected** will appear below the name of the VPN network. **6**

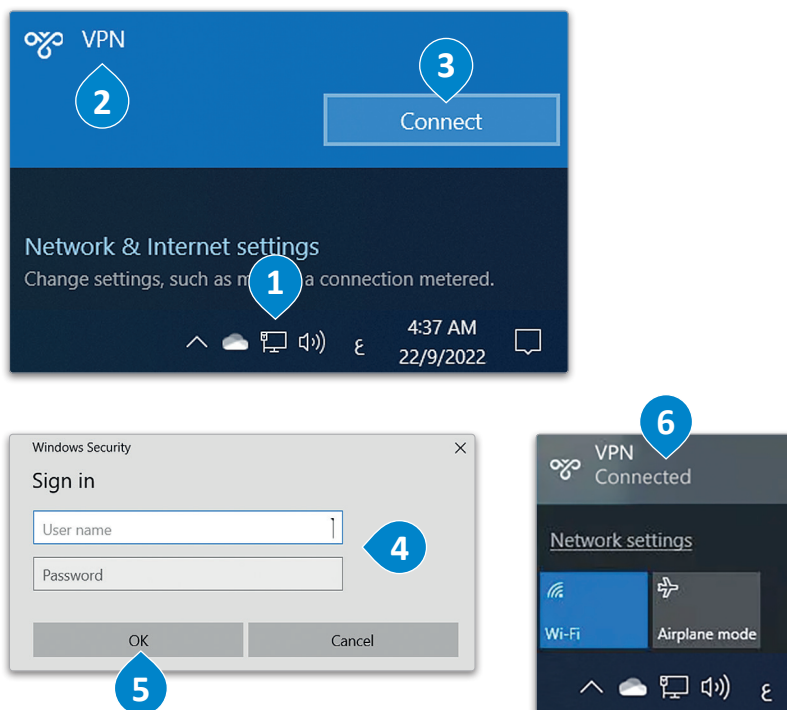


Figure 2.21: Activating a VPN service

Exercises

1

Read the sentences and tick ✓ True or False.	True	False
1. Network transmission media include twisted-pair, coaxial, and fiber-optic cables.	☐	☐
2. Routers are responsible for directing traffic within a local area network (LAN).	☐	☐
3. Cross-site scripting (XSS) is a type of web-based attack.	☐	☐
4. IPSec is a commonly used network protocol.	☐	☐
5. Firewalls can be implemented as software or hardware.	☐	☐
6. Intrusion Detection Systems (IDSs) monitor file transfers.	☐	☐
7. Secure Sockets Layer (SSL) is a protocol for encrypting data during transmission.	☐	☐
8. The Domain Name System (DNS) translates IP addresses into human-readable domain names.	☐	☐
9. Wireshark is used for packet sniffing processes.	☐	☐

2

List the difference between the HTTP and HTTPS protocols in terms of security.



وزارة التعليم

Ministry of Education

2026 - 1448

- 3 Explain how Demilitarized Zones (DMZs) are used to protect internal networks from external threats.

- 4 Evaluate the effectiveness of Virtual Private Networks (VPNs) in maintaining user privacy.



5 Evaluate how firewalls and Intrusion Detection Systems (IDSs) can be used to protect networks from attacks.

6 Explain the difference between network-based and host-based Intrusion Detection Systems (IDSs).



7 Capture and analyze network traffic:

- Start Wireshark and select your network interface. Start the packet capture.
 - Browse the Internet for a few minutes. Open a few websites, watch a video, etc.
 - Stop the packet capture and save the data.
 - Analyze the traffic. Extract some header info such as the source IP/Port, destination IP/Port, and capture time.
-
-

8 ARP request analysis:

- Start a new live capture on your Ethernet interface.
 - Filter the results for ARP by typing "arp" into the filter bar.
 - Analyze the results. How many ARP requests are there? Can you identify the source and destination MAC addresses?
-
-
-

9 Detecting unusual network activity in Wireshark:

- Load the file Scan_results.pcapng provided by your teacher.
 - Use the Expert Information option to identify any potential issues or unusual activity.
 - Take note of any anomalies and try to identify what might be causing them. Could any of these be a sign of a potential security threat?
-
-
-



Lesson 3

Digital Forensics and Incident Response

Link to digital lesson



www.iien.edu.sa

Introduction to Digital Forensics (DF) and Incident Response (IR)

Digital Forensics and Incident Response (DFIR) are important branches of cybersecurity that focus on identifying, investigating, containing, and remediating cyberattacks, and on providing information for legal cases or other digital investigations. DFIR services are made up of two main components:

Digital Forensics

As an investigative field within forensic science, digital forensics involves collecting, analyzing, and presenting digital evidence on computer systems, network devices, phones, or tablets. This evidence can help reveal the truth about events that occurred on these devices. Digital forensics is often employed in legal proceedings, regulatory investigations, internal company investigations, and criminal activity cases, among other types of digital investigations.

Incident Response

While also involving the investigation of computer systems through the collection and analysis of data, incident response specifically focuses on addressing security incidents. In these cases, investigators must balance various steps, such as containment and recovery, to effectively respond to the situation.

Both digital forensics and incident response play crucial roles in uncovering the facts surrounding digital events and addressing potential security incidents to ensure the safety and integrity of digital systems and data.

Cyber Kill Chain

The Cyber Kill Chain is a methodology used to understand and analyze malicious cyberattacks. It identifies the stages that enable attackers to gain control of their target and ultimately perform their objectives. Understanding the cyber kill chain is an essential part of the DFIR process. By understanding the cyber kill chain, defenders of the networks can identify attack patterns, recognize known techniques used by the attackers, and respond accordingly. The phases of the Cyber Kill Chain are as follows:

Phase 1: Reconnaissance

During Reconnaissance, attackers identify targets and explore vulnerabilities to exploit. This process may involve harvesting credentials and collecting information like email addresses, user IDs, locations, software apps, and OS. More information gathered leads to more successful attacks.

Phase 2: Weaponization

During Weaponization, an attacker creates an attack vector (e.g., malware, ransomware, virus, worm) to exploit a known vulnerability. They may also set up backdoors for continued access if their entry is closed by administrators.



Phase 3: Delivery

In the Delivery step, an intruder may send malicious attachments or links to users to spur activity. They may also use social engineering techniques to try to increase the effectiveness of their attack.

Phase 4: Exploitation

During the Exploitation phase, the harmful code is run on the system of the targeted individual.

Phase 5: Installation

Immediately after Exploitation, the attack vector will be installed on the victim's system, allowing the threat actor to gain control.

Phase 6: Command and Control

In Command and Control, the attacker takes remote control of a device/identity within the network and moves laterally, expanding access and creating new entry points.

Phase 7: Actions on Objective

During this phase, the perpetrator proceeds with their desired objectives, which could involve stealing data, causing damage, encrypting information, or extracting data.

DFIR Processes

Digital forensics and incident response, while distinct functions, are closely related and often combined in practice. Both are essential components of cybersecurity, with digital forensics focusing on collecting and analyzing evidence to determine what happened during a computer security incident, while incident response involves investigating, containing, and recovering from such security incidents. These techniques are frequently used together by Computer Security Incident Response Teams (CSIRTs) in handling cyberattacks, litigations, and various digital investigations. DFIR processes include the following:

Computer Security Incident Response Teams (CSIRTs)

Computer Security Incident Response Teams (CSIRTs) are specialized groups of technical professionals who investigate, analyze, and respond to digital security incidents. They play a critical role in protecting and recovering computer networks after identifying security issues.

Forensic collection

This involves the process of gathering, examining, and analyzing data from various sources, such as networks, applications, data stores, and endpoints, both on-premises and in the cloud.

Chain of custody

A procedure that continues forensic collection by keeping track of the evidence's journey from collection to analysis. It involves documenting every individual interacting with the evidence, the date and time of collection or transfer, and the reason for the transfer.

Root cause investigation

In this step, the organization determines whether it has been the target of a breach and identifies the root cause, scope, timeline, and impact of the incident.

Notification and reporting

Depending on the organization's compliance obligations, it may need to notify and report breaches to the appropriate authorities.

Post-incident review

This stage may require the organization to negotiate with attackers, communicate with stakeholders, customers, and the press, or implement changes to systems and processes to address vulnerabilities, depending on the nature of the incident.

Digital Forensics Process

A typical DF process will go through the following steps:



Identification

Potential digital evidence related to an incident or investigation is identified and documented. This involves pinpointing the sources of relevant data, such as computers, mobile devices, servers, or network logs, and determining the scope of the investigation.



Preservation

The digital evidence that is identified is safeguarded to prevent alteration, damage, or loss. This includes creating forensic images or copies of the data, isolating affected systems from networks, and maintaining a proper chain of custody to ensure the integrity of the evidence.



Analysis

The collected evidence is then examined to uncover relevant information and identify patterns or connections. This may involve using specialized forensic tools and techniques to recover deleted files, decrypt encrypted data, or analyze system logs and artifacts. Analysts must also interpret the findings, considering the context of the investigation and potential alternative explanations. Analysis includes the following methods:

- File system forensics: Investigating endpoint file systems to identify signs of a security breach or compromise.
- Memory forensics: Examining system memory to uncover indicators of compromise that may not be present in file systems.
- Network forensics: Analyzing network activity, such as emails, messages, and browsing history, to recognize an attack, understand the attacker's methods, and determine the scope of the incident.
- Log analysis: Reviewing and interpreting activity records or logs to detect unusual events or suspicious behavior that could indicate a security incident.

Documentation

The entire digital forensics process must be documented, including the steps taken, tools used, and conclusions made. Detailed documentation ensures that the forensic analysis can be reviewed, replicated, and challenged if necessary while demonstrating the investigator's adherence to best practices and industry standards.





Reporting

After the digital forensics process, teams present their evidence and findings. This final step usually details the analysis methodology and procedures followed during the investigation, ensuring the information is presented clearly and accurately for further review or potential legal proceedings.

Incident Response (IR) Process

A typical IR process will go through the following steps:



Scoping

In this stage, the goal is to assess the incident's severity, scope, and breadth and identify all indicators of compromise (IoC). This step helps to understand the extent of the attack and prioritize response actions accordingly.



Investigation

This involves using advanced systems and threat intelligence to detect threats, collect evidence, and provide in-depth information about the incident. It is a crucial step in understanding the nature of the attack and gathering essential data for further analysis.



Securing

Organizations still need to continuously monitor their cyber health even after the threats have been addressed. This stage often involves containing and eradicating active threats identified during the investigation and closing any identified security gaps to prevent future attacks.



Support and Reporting

The Support and Reporting stage ideally concludes each security incident with a detailed plan for ongoing support and customized reporting. A DFIR service provider may also examine the organization and provide expert advice on the next steps to enhance security measures and ensure preparedness for potential future incidents.



Transformation

Finally, the Transformation stage involves DFIR teams identifying gaps in the organization's security posture, advising on effectively strengthening areas of weakness, and mitigating vulnerabilities. This stage aims to improve the organization's security posture and increase its resilience against future cyber threats.

Digital Forensics and Incident Response Challenges

As computer systems have progressed, so have the difficulties associated with DFIR. Today, digital forensics and incident response experts face several significant obstacles. Table 2.6 illustrates the main challenges of DFIR.



Table 2.6: Main challenges of Digital Forensics and Incident Response

Challenge	Description
Digital Forensics	
Scattered evidence	The reconstruction of digital evidence is no longer dependent on a single host; it is dispersed across numerous physical and virtual locations. As a result, digital forensics requires more expertise, tools, and time to collect and investigate threats thoroughly and accurately.
The fast pace of technology	Digital devices, software applications, and operating systems are constantly changing, evolving, and expanding. Due to the rapid rate of change, experts in digital forensics must be able to manage digital evidence in a wide variety of application versions and file formats.
Incident Response	
Growing data, scarce support	Organizations are confronted with an increasing number of security alerts. However, they often do not possess the cybersecurity expertise necessary to address the volume of information and, ultimately, the relevant threat data. Organizations increasingly rely on external DFIR experts to bridge the skills divide and maintain critical threat support.
Increased attack surface	The expansive attack surface of modern computing and software systems makes obtaining an accurate network overview harder and increases the risk of misconfigurations and user error.

Digital Forensics and Incident Response Best Practices

DF Best Practices

The effectiveness of DFIR depends on responding quickly and thoroughly. It is essential that digital forensics teams have extensive experience and appropriate tools and processes in place to provide a practical, prompt response to any issue.

Expertise in digital forensics has a number of advantages, including the ability to determine an incident's root cause and precisely determine its scope and impact. Employing the appropriate investigative tools will optimize the identification of vulnerabilities that led to an attack or accidental exposure.

IR Best Practices

Incident response services are customized for real-time incident management. To reduce reputational damage, financial loss, and business downtime, the best practices for IR include preparation and planning, as well as timely, accurate, and trustworthy mitigation and response.

Best practices for digital forensics and incident response include determining the fundamental cause of issues, correctly identifying and locating all available evidence/data, and providing ongoing support to ensure that the organization's security defenses are strengthened for the future.

Zero-Trust Security

IR also covers the prevention of malicious attacks in a system. Enterprises have developed security architectures called **zero-trust security models**. The zero-trust model is an information security model that has gained popularity recently. Unlike traditional methods that rely on perimeter defenses, such as firewalls, to protect the internal network, zero-trust assumes that no device or user should be inherently trusted. This means that even if a user accesses a system from a valid account and an internal device, their request must still be authenticated and authorized. In a zero-trust model, authorization is not granted by default and should only be given if there is a legitimate need. This approach has become more popular due to changes in technology and society, such as remote workforces and the rise of cyberattacks, making perimeter defenses less effective.

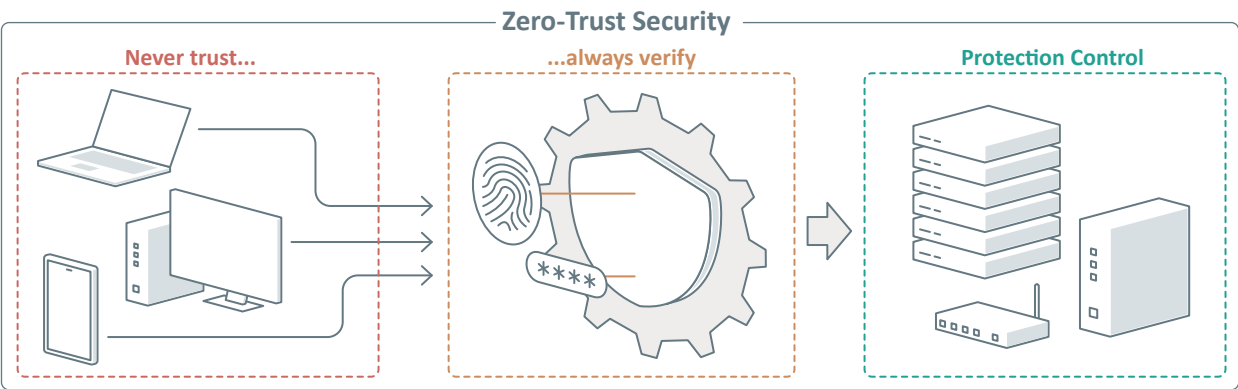


Figure 2.22: Representation of Zero-Trust Security

Table 2.7: Main principles for implementing a zero-trust security model	
Principle	Description
Identity verification	All users, devices, and applications must be authenticated and authorized before granting access to resources. Multi-factor authentication (MFA) is often used to provide an additional layer of security beyond usernames and passwords.
Least privilege	Access to resources should be granted on a need-to-know basis and only for the minimum time required to complete a specific task.
Network segmentation	Networks should be segmented to limit lateral movement by attackers. This is often accomplished through micro-segmentation, which divides a network into small, isolated zones that can be individually secured.
Continuous monitoring	Zero-Trust security requires continuous monitoring of user and device behavior, network traffic, and security events to detect and respond to threats in real time.
Data protection	Data should be protected using encryption and other security measures at rest and in transit.
Policy enforcement	Policies should be defined to ensure that all users, devices, and applications comply with security requirements.

Analyzing the Web Activity of a Device

Many cyberattacks that occur originate from an infection that occurs through the web activity of a user. After an incident has occurred, the digital forensics process follows. One of the main tasks is investigating and analyzing the web activity of a device that was affected by the incident.

Web browsers store log files that contain data and information about the activities that were performed with that browser. These log files are structured in a way that they can be accessed and read by data analysis tools.

In the scenario that follows, you will analyze the web activity for your device that occurred with the Chrome web browser. You will utilize DB Browser for SQLite, which is a database management system tool. This tool will be used to access the log files and read the activity data. You can download and install DB Browser from the following link:

<https://sqlitebrowser.org/dl/>



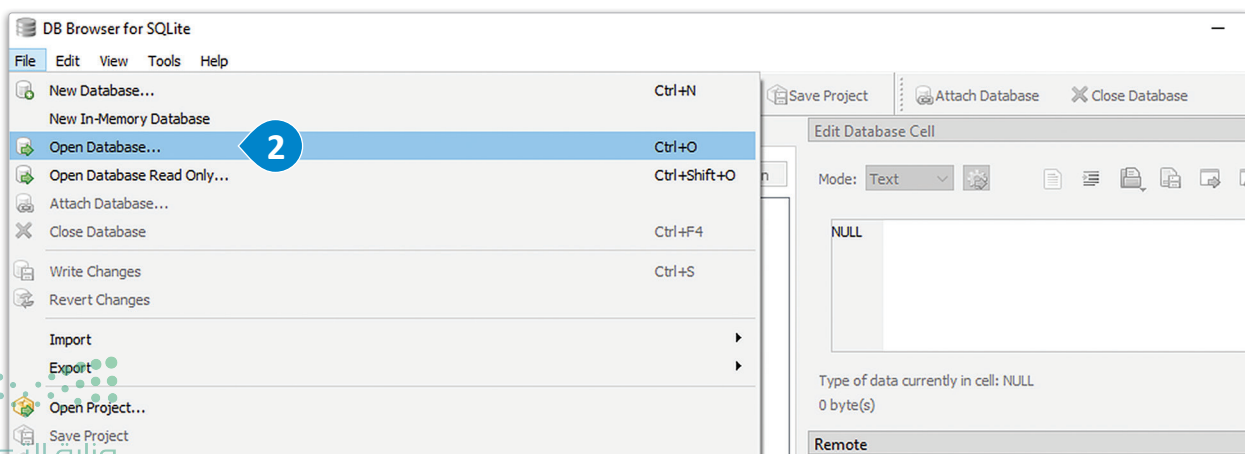
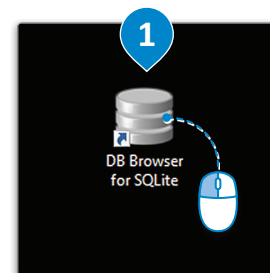
Figure 2.23: QR code to download DB Browser for SQLite

Getting Started with DB Browser

To view the activity of your browser, you will first have to find and open the log files of Chrome. The log files are databases that contain multiple tables, where each table holds information about your activity, like the websites you have visited and the files you have downloaded. Always make sure that you follow security and protection best practices for your own PC when browsing on the Internet.

To open DB Browser and load a log file:

- > Double-click the **DB Browser** shortcut on your **Desktop**. **1**
- > Click on **File** and then click **Open Database...** **2**
- > Enter "**C:\Users\[username]\AppData\Local\Google\Chrome\User Data\Default**" in the location path, at [username] insert the your computer's username. **3**
- > Choose **All files (*)** from the dropdown menu. **4**
- > Click on **History** **5**, to select the History log file, and click **Open**. **6**



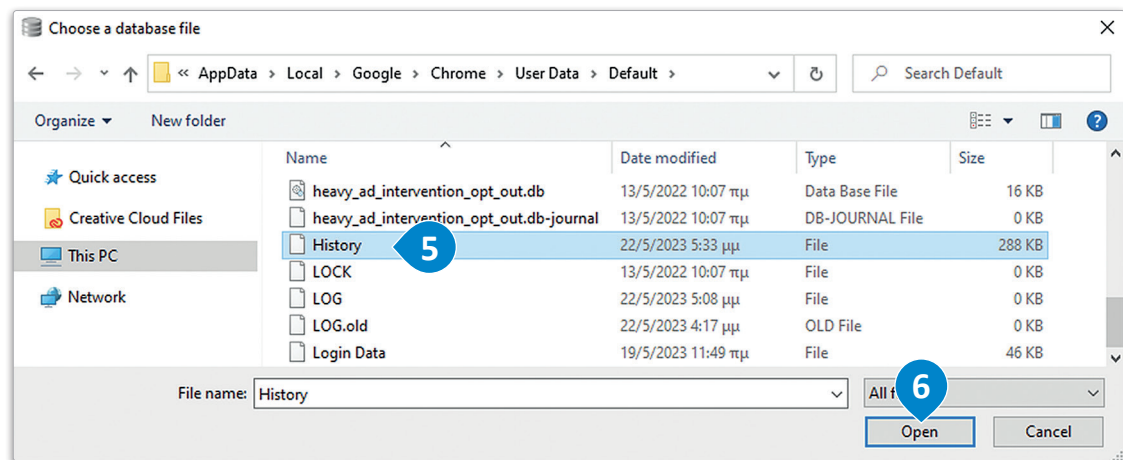
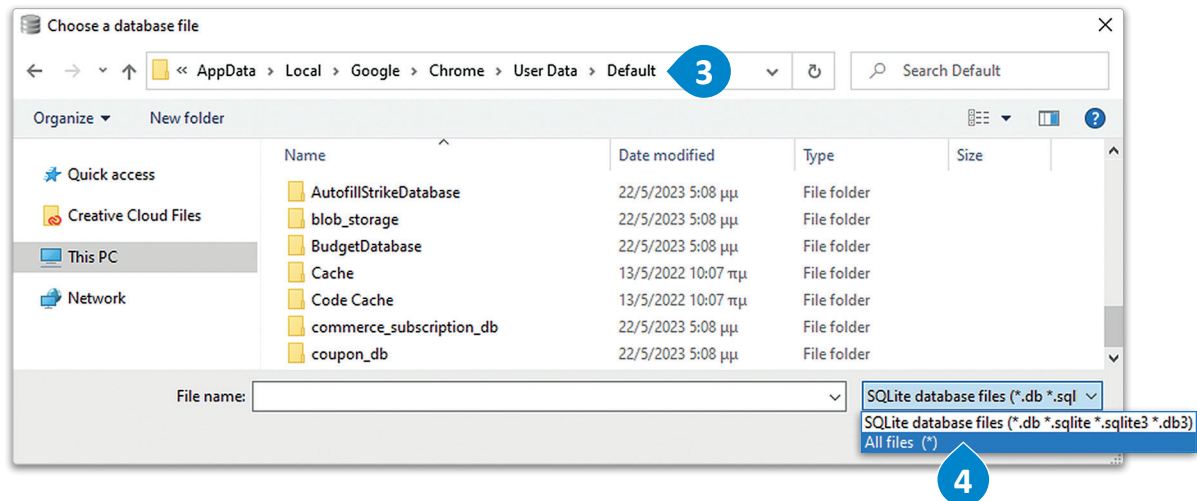


Figure 2.24: Open DB Browser and load a log file

To view a table:

- > Click on the **Browse Data** tab. 1
- > Click the **dropdown menu** 2 and select **urls** to view the **urls** table. 3

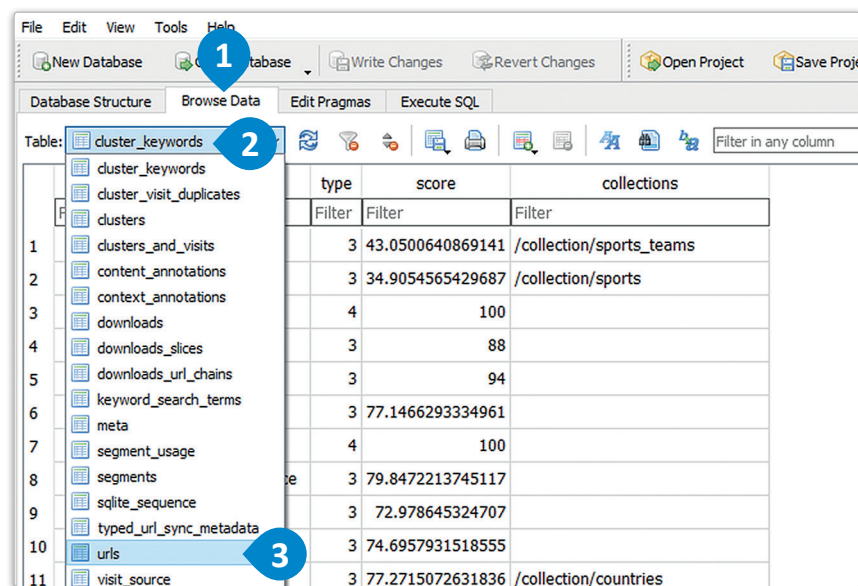


Figure 2.25: View a table



The Uniform Resource Locators (URLs) table

In cybersecurity forensics, the **urls** table plays a significant role in investigating and analyzing user browsing activities. The **urls** table, found within the Chrome history log file, contains valuable information about the web addresses visited by a user during their browsing sessions. By examining the data stored in the **urls** table, investigators can gain insights into the websites accessed, track user behavior, and uncover crucial evidence related to cybercrimes.

The **urls** table consists of several key columns that provide specific details about each visited URL. Let's explore these columns and understand their significance in the realm of cybersecurity forensics:

- url:**
The **url** column stores specific web addresses of the visited websites. Analyzing the URLs allows investigators to identify the exact web pages accessed and retrieve critical information related to a particular online activity.
- title:**
The **title** column holds the titles or names of the visited web pages. This information offers additional context and helps investigators understand the content and purpose of the accessed websites. Analyzing the titles can provide valuable insights into the user's interests, browsing habits, and potential areas of focus during an investigation.
- visit_count:**
The **visit_count** column records the number of times a specific URL has been visited by the user. This count allows investigators to determine the frequency and level of engagement with a particular website. Analyzing it helps in identifying frequently accessed resources, prioritizing investigation efforts, and identifying patterns or trends in user behavior.
- last_visit_time:**
The **last_visit_time** column provides the timestamp or date and time of the most recent visit to a particular URL. This information enables investigators to establish timelines, track the chronology of user activities, and potentially correlate website visits with other events or actions.

Table: **urls**

	id	url	title	visit_count	last_visit_time
	Filter	Filter	Filter	Filter	Filter
1	1	https://www.google.com/search?...	ksa ministry of education - ...	2	13331026045492522
2	2	https://moe.gov.sa/en	Ministry of Education	1	13331026047091166
3	3	https://moe.gov.sa/en/Pages/...	Ministry of Education	1	13331026047091166
4	4	https://nca.gov.sa/en	National Cybersecurity ...	2	13331026071307456
5	5	https://sdaia.gov.sa/en/default.aspx	Saudi Authority for Data and...	1	13331026134530124

Reading a Timestamp

A timestamp is a numeric value that represents a specific point in time. It is commonly used in databases and computer systems to record and track the occurrence of events or the creation/modification of data. Timestamps are often stored as the number of seconds or milliseconds since a specific reference point, known as the epoch.

You can use the following script in the Execute SQL tab of DB Browser to view the date of an input, by substituting "timestamp" with the value you want to view:

```
SELECT datetime (timestamp/1000000 +  
                (strftime('%s', '1601-01-01')), 'unixepoch', 'localtime')
```

To read a timestamp:

- > Click on the **Execute SQL** tab. **1**
- > Enter the **script** with the timestamp you wish to view in the **field** below. **2**
- > Click the **Run** button to run the script. **3**

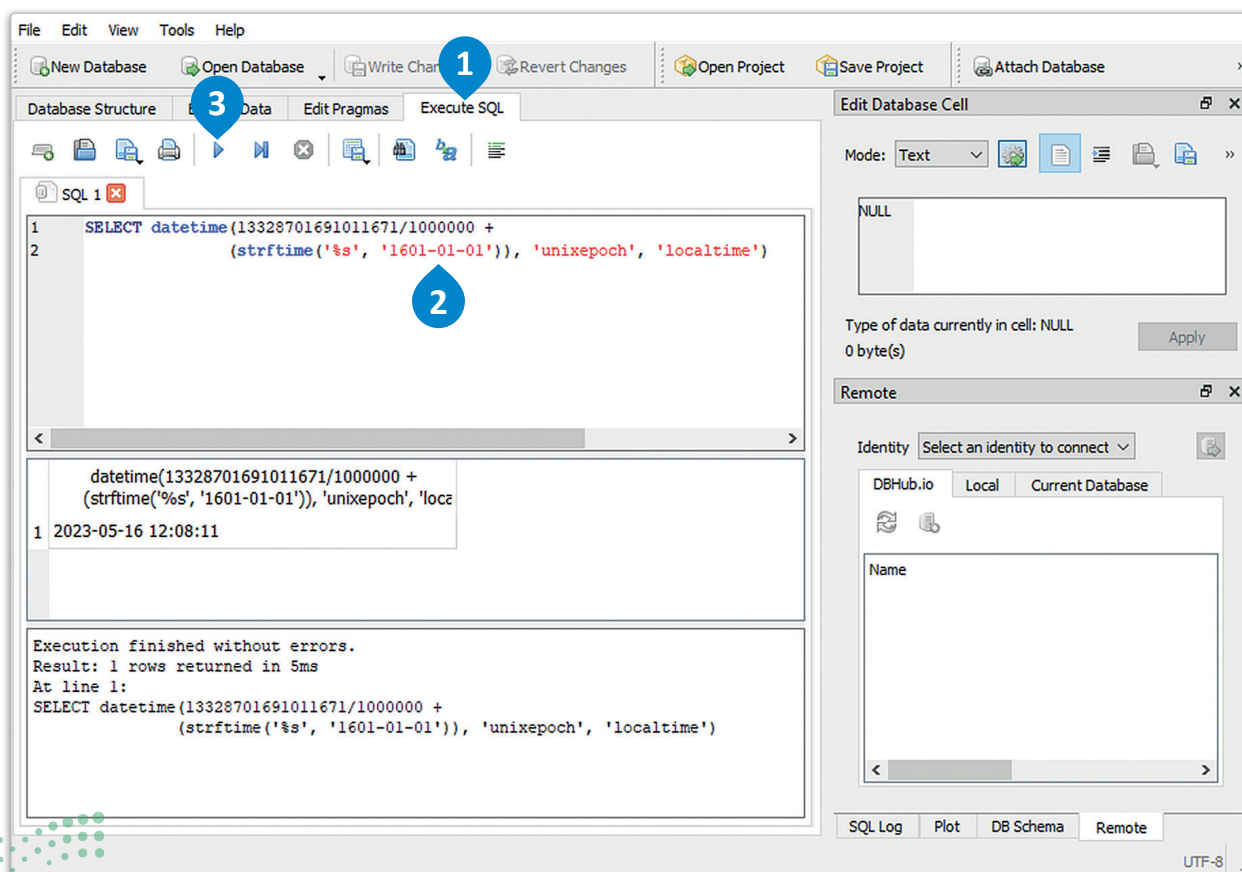


Figure 2.26: Read a timestamp

The Keyword_search_terms Table

The **keyword_search_terms** table is a significant component of cybersecurity forensics investigations as it holds crucial information about the search terms or keywords used by users during their browsing activities. The **term** column in this table specifically captures the individual search queries entered by users.

The **term** column provides valuable insights into users' interests, information needs, and online behavior. Analyzing the **term** column allows investigators to understand the specific keywords or phrases users use when searching for information. These search terms can range from simple keywords to more complex queries, offering valuable clues about the users' intentions and the type of information they were seeking.

Downloads Table

Another important table that holds crucial information in forensics is the **downloads** table. The **downloads** table contains information about downloaded files and associated metadata. It plays a significant role in managing and tracking downloaded content. The table includes several important fields that provide insights into the downloaded files and related details:

current_path
Filter
C:\Users\binar\Downloads\ICT_Brochure.pdf

target_path
Filter
C:\Users\binar\Downloads\ICT_Brochure.pdf

tab_url
Filter
http://binarylogic.net/brochures/1

total_bytes
Filter
1769706

start_time
Filter
13328797041529572

end_time
Filter
13328797042103677

current_path and target_path columns:

These fields store the current and target paths of the downloaded file on the user's local system. The **current_path** represents the temporary or in-progress location of the file during the download, while the **target_path** indicates the final destination where the file is stored after the download is completed.

tab_url column:

The **tab_url** field stores the URL or web address of the webpage where the download originated. It helps identify the specific webpage or online source from which the file was downloaded.

total_bytes column:

The **total_bytes** field represents the total size of the downloaded file in bytes. It provides information about the file's size, which can be helpful in assessing the impact on storage resources and understanding the nature of the downloaded content.

start_time and **end_time** columns:

These fields capture the start and end times of the download process. The **start_time** indicates when the download was initiated, while the **end_time** represents when the download was completed. Analyzing these timestamps can provide insights into the duration of the download process and potentially correlate it with other events or user activities.

id	current_path	target_path	start_time	total_bytes	end_time	tab_url
1	C:\Users\binar\Downloads\ICT_Brochure.pdf	C:\Users\binar\Downloads\ICT_Brochure.pdf	13328797041529572	1769706	13328797042103677	http://binarylogic.net/brochures/1

Logins Table

In the **Login Data** log file, you can find the **logins** table. The **logins** table contains information related to user logins and stored credentials. It is commonly found in web browsers' databases and plays a crucial role in managing and auto filling login details. The table includes several important fields that provide insights into user credentials and associated metadata:

origin_url

Filter

https://login.live.com/oauth20_authorize.srf

username_element

Filter

loginfmt

username_value

Filter

saadsa.bl@outlook.com

password_element

Filter

passwd

password_value

Filter

BLOB

date_created

Filter

13328890149058235

date_last_used

Filter

13328890141382119

The value of the password is encrypted and shown here as BLOB.

origin_url column:

The **origin_url** field stores the URL or web address of the website where the login credentials were used or saved. It helps identify the specific website or online service associated with the stored login information.

username_element and username_value columns:

These fields capture the HTML element name and corresponding value for the username or user identifier used during login. They provide information about the structure and values of the username fields in the web form.

password_element and password_value columns:

Similar to the username fields, these fields capture the HTML element name and corresponding value for the password used during login. They provide insights into the structure and values of the password fields in the web form.

date_created column:

The **date_created** field indicates the date and time when the login credentials were created or saved. It helps establish the timestamp of when the credentials were initially stored in the browser's database.

date_last_used column:

The **date_last_used** field records the most recent date and time when the login credentials were used for authentication. It provides insights into the last time the credentials were utilized for logging into the associated website.

Table: logins						
	origin_url	username_element	username_value	password_element	password_value	date_created
	Filter	Filter	Filter	Filter	Filter	Filter
1	https://login.live.com/oauth20_authorize.srf	loginfmt	saadsa.bl@outlook.com	passwd	BLOB	13328890149058235

Exercises

1

Read the sentences and tick ✓ True or False.	True	False
1. Digital forensics focuses on restoring deleted files and decrypting encrypted data.	☐	☐
2. Digital forensics and incident response are distinct processes.	☐	☐
3. Digital forensics is only used in legal proceedings.	☐	☐
4. Incident response involves gathering and analyzing data to determine what happened in a security incident.	☐	☐
5. Computer Security Incident Response Teams (CSIRTs) play an essential role in cybersecurity.	☐	☐
6. Post-incident review is not necessary for a DFIR process.	☐	☐
7. Forensic collection only involves collecting data from a single source.	☐	☐
8. Memory forensics is the same as file system forensics.	☐	☐

2 Outline the sources of evidence that must be identified when conducting a digital forensics investigation.

3 Analyze the role of Computer Security Incident Response Teams (CSIRTs) in protecting machine networks.



4 Describe the steps of a typical DFIR process.

5 Describe the main challenges associated with Digital Forensics and Incident Response.

6 In a web browser with large quantities of activity data, analyze the results from the urls table and try to deduce if there are specific patterns the user follows in their web browsing activity.

7 For the same data as in the previous exercise, evaluate the data from the logins table and list the sites where the user has entered their credentials. After that, categorize them as secure or potentially unsecured sites.

Project

Suppose you are a cybersecurity professional at a large enterprise organization dealing with a new worm outbreak. The worm spreads through removable media and infects hosts, installing a DDoS agent. The organization has already suffered widespread infections before antivirus signatures become available. You must devise strategies to identify and contain the worm and protect sensitive data.

1

Identify the methods the incident response team could use to find all infected hosts and discuss how the organization could have attempted to prevent the worm from entering the organization devices before antivirus signatures were released.

2

Explain the steps the organization could take to prevent the worm from spreading further via infected hosts before antivirus signatures are released. Discuss how the handling of this incident would change if hosts infected with the DDoS agent had been configured to attack another organization's website the next morning.

3

Analyze how the handling of this incident would change if one or more of the infected hosts contained sensitive, personally identifiable information regarding the organization's employees. What additional precautions and actions would be necessary to protect this sensitive data?

4

Describe the measures the incident response team would need to perform for hosts not currently connected to the network to ensure they are not infected or do not spread the worm upon reconnection.

5

Collect the notes you have written and create a PowerPoint presentation showing the scenario analysis and the DFIR response.



Wrap up

Now you have learned to:

- > Recognize the vulnerabilities of hardware, operating, and software systems.
- > Describe techniques for secure system design.
- > Protect a Windows system using various security techniques.
- > Outline the relationship between network structures, web technologies and cybersecurity systems.
- > Identify how to secure network systems through protocols and best practices.
- > Analyze the data flow through a network with Wireshark.
- > Activate the Windows VPN service.
- > Analyze how DFIR is used to respond to and defend against sophisticated cyberattacks.
- > Evaluate the web activity of a browser with DB Browser for SQLite.

KEY TERMS

**Address Resolution
Protocol (ARP)**

**Computer Security
Incident Response Teams
(CSIRTs)**

Defense In-Depth

**Demilitarized Zones
(DMZs)**

Digital Forensics (DF)

Firewalls

Incident Response (IR)

**Intrusion Detection
Systems (IDSs)**

Packet Analyzers

Passkeys

Secure Programming

Security by Design

**Virtual Private Networks
(VPNs)**

Zero-Trust Security



3. Advanced Topics in Cybersecurity

In this unit, you will learn about how cybersecurity legislation influences the modern technological landscape both in Saudi Arabia and internationally. You will then be introduced to cryptography and you will implement cryptographic algorithms with Python. Finally, you will learn the importance of robust cybersecurity systems for applications built with emerging technologies.

Learning Objectives

In this unit, you will learn to:

- > Outline the main points of standardized cybersecurity legislation.
- > Identify the main cybersecurity laws and regulations that are present in Saudi Arabia and in other countries.
- > Explain what cryptography is and its uses.
- > Identify the types of cryptography and their potential threats from hackers.
- > Implement cryptographic algorithms with Python.
- > Analyze how cybersecurity systems protect systems created with emerging technologies.

Tools

- > Python



Lesson 1

Cybersecurity Regulations and Laws

Link to digital lesson



www.ien.edu.sa

The Importance of Laws and Regulations in Cybersecurity

As technology systems have advanced, so has the need to ensure that individuals and businesses stay secure online. Cybersecurity laws and regulations exist as a way to make sure that companies and individuals are held liable for any security incidents that may occur. Organizations and governments can more effectively protect data and remain compliant by understanding the laws, regulations, and other existing guidelines. Understanding the laws and regulations will help individuals and organizations play an active role in keeping the Internet safe. This knowledge can be used to strengthen security practices, create more secure products, and increase customer trust in their products and services.

The most important points for the correct use of legislation and regulation in cybersecurity are the following:



Data Privacy and Protection

With vast amounts of personal and sensitive data being collected, stored, and transmitted digitally, laws and regulations help ensure that this information is handled securely and responsibly. This protects individuals' privacy rights and prevents unauthorized access or misuse of their data.



Standardization

Cybersecurity regulations and laws provide a common set of standards and best practices for organizations to follow, promoting a baseline level of security across industries. This standardization facilitates better collaboration between organizations and enables more effective response strategies to cyber threats.



Compliance and Accountability

Legal frameworks hold organizations accountable for their security posture by requiring them to implement specific security measures and report breaches when they occur. This promotes a culture of compliance and encourages organizations to continually assess and improve their cybersecurity practices.





Deterrence and Prosecution

Cybersecurity laws define and classify various cybercrimes, allowing law enforcement agencies to pursue and prosecute offenders. This serves as a deterrent against malicious cyber activities and ensures that cybercriminals are held accountable for their actions.



International Cooperation

Because cyber threats and attacks cover multiple countries, international collaboration is essential in combating cybercrime. Cybersecurity laws and regulations help facilitate cooperation between nations, enabling the sharing of intelligence, resources, and best practices in addressing global cyber threats.

Cybersecurity Laws and Regulations in KSA

Cybersecurity Controls

The National Cybersecurity Authority (NCA) in Saudi Arabia has published various cybersecurity controls that public and private entities operating in Saudi Arabia must adhere to. Cybersecurity controls are technical and non-technical measures designed to protect computer systems, networks, and data from unauthorized access, misuse, modification, destruction, or disruption. The following is an overview of these controls.

Essential Cybersecurity Controls (ECC)

Providing the minimum basic requirements for cybersecurity is the main objective of these requirements, which are designed based on best practices and standards to protect the information assets of the entities from internal and external threats and reduce cyber risks. These controls also address various aspects of cybersecurity, including asset management, identity and access management, cybersecurity incidents and threats management, and cybersecurity awareness and training. These controls are binding on all government agencies in the Kingdom of Saudi Arabia, including ministries, agencies, institutions, and others, and their subsidiaries and companies, and private sector entities that have Critical National Infrastructure (CNIs) or work to operate or host them. This is to ensure the protection of their information systems.

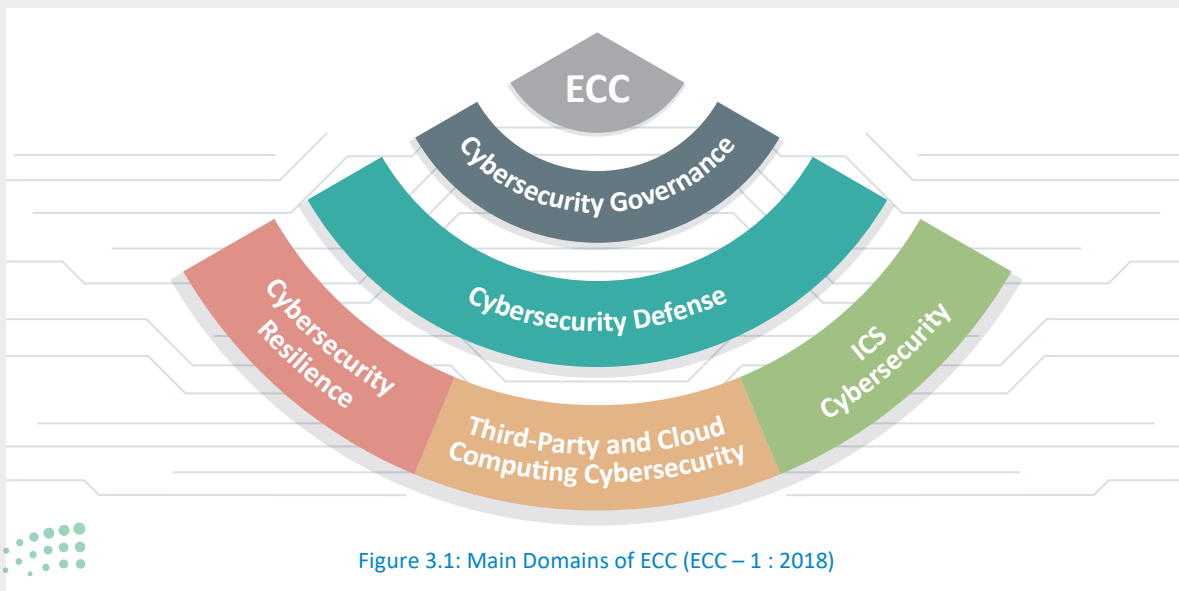


Figure 3.1: Main Domains of ECC (ECC – 1 : 2018)



Data Cybersecurity Controls (DCC)

The NCA has issued the Data Cybersecurity Controls (DCC) to improve the regulation and security of cyberspace in the Kingdom. The DCC controls aim to raise the level of cybersecurity protection for national data and to enhance the cybersecurity of the entities during the stages of the data life cycle, in order to ensure the protection of their data and information assets from cyber threats and risks.

1. Cybersecurity Governance	1-1	Periodical Cybersecurity Review and Audit	1-2	Cybersecurity in Human Resources
	1-3	Cybersecurity Awareness and Training Program		
2. Cybersecurity Defense	2-1	Identity and Access Management	2-2	Information System and Information Processing Facilities Protection
	2-3	Mobile Devices Security	2-4	Data and information Protection
	2-5	Cryptography	2-6	Secure Data Disposal
	2-7	Cybersecurity for Printers, Scanners and Copy Machines		
3. Third-Party and Cloud Computing Cybersecurity	31	Third-Party Cybersecurity		

Figure 3.2: DCC Main domains and subdomains

Cloud Cybersecurity Controls

The NCA has developed the Cloud Cybersecurity Controls, which is an extension of the ECC controls. This is in order to reduce cyber risks to Cloud Service Providers (CSOs) and Cloud Service Tenants (CSTs).

Telework Cybersecurity Controls

The purpose of this document is to raise the readiness of entities to work remotely safely and adapt to changes in remote work environments and systems, in addition to enhancing the cybersecurity capabilities of entities to withstand cyber threats when working remotely.

Critical Systems Cybersecurity Controls

These controls aim to develop protection and resilience capabilities against cyberattacks in order to enable entities with sensitive systems to preserve their information and technical assets to meet current security needs and to enhance the readiness of entities in the face of increasing cyber risks that may result in harmful effects at the national level.

Operational Technology Cybersecurity Controls

These controls aim to raise the readiness of the entities so that they can protect their operational systems. The document also specifies the minimum cybersecurity requirements for sensitive industrial control systems in government and private entities to prevent unauthorized access to these systems.

Cybercrime Regulation

In the Kingdom of Saudi Arabia, several laws and standards have been established to address cybercrime and protect the privacy and security of individuals and organizations. The following is an overview of the most prominent of these:

Personal Data Protection Law (PDPL)

The Personal Data Protection Law (PDPL) and its executive regulations are relevant to protecting the privacy of individuals in Saudi Arabia and set the legal basis for the protection of your rights regarding the processing of personal data by all entities in the Kingdom, as well as all entities outside the Kingdom that process personal data related to individuals residing in the Kingdom using any means, including online personal data processing.

Anti-Cyber Crime Law

The Saudi Arabian Anti-Cyber Crime Law is a set of laws and regulations that criminalize a wide range of cybercrime activities in Saudi Arabia. The law was enacted to protect the country's national security and economic interests from cyber threats and ensure the safety of citizens and residents from cybercrime.

The Anti-Cyber Crime Law criminalizes cybercrime activities such as hacking, online fraud, identity theft, and privacy invasion. It also includes provisions for the protection of personal data and the investigation and prosecution of cybercrime.

Under the Anti-Cyber Crime Law, cybercrime is considered a serious offense punishable by fines, imprisonment, and other penalties. The law also authorizes the government to take measures to block access to websites that are deemed to be involved in cybercrime.



International Cybersecurity Laws and Regulations

International cybersecurity laws and regulations have become increasingly important in protecting data and information globally, in addition to the laws and regulations already in place in the Kingdom of Saudi Arabia. Following are some of the most prominent international cybersecurity and data laws.



USA

CFAA

The Computer Fraud and Abuse Act is a federal law that deals with computer crime and data privacy. The law prohibits unauthorized access to computers and any form of intentional harm or damage to any computer system. It is one of the first federal laws to criminalize computer misuse and focus on data protection.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law requiring national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

COPPA

The Children's Online Privacy Protection Act (COPPA) is a law in the United States that establishes rules for collecting and using personal data from children under the age of 13. It requires websites, mobile applications, and other online services to obtain parental consent before collecting, using, or sharing children's personal information.



EU

EU Cybersecurity Act

The EU Cybersecurity Act strengthens the EU Agency for Cybersecurity (ENISA) and creates a framework for certifying the cybersecurity of products and services. ENISA will prepare the technical foundations for certification schemes, and the act establishes an EU-wide certification framework for ICT products, services, and processes. This means companies operating in the EU must only certify their ICT products, processes, and services once, and their certificates will be recognized throughout the European Union.

GDPR

The General Data Protection Regulation is a Regulation (GDPR) in EU law on data protection and privacy in the EU and the European Economic Area. The GDPR applies to the processing of personal data wholly or partly by automated and non-automated means either they form part of a filing system or are intended to form part of a filing system.



UK

NIS Regulations

The Security of Network & Information Systems Regulations (NIS Regulations) are laws aimed at increasing the security of digital and physical networks and information systems. They are intended to safeguard essential and digital services from cyberattacks, protecting citizens, businesses, and public services. The regulations apply to companies providing essential services, such as transport, energy, water, health, and digital infrastructure, as well as digital service providers, including online marketplaces, search engines, and cloud computing services.



Exercises

1

Read the sentences and tick ✓ True or False.	True	False
1. Laws and regulations are only used to protect companies from cyber threats.	☐	☐
2. Standardization of cybersecurity laws and regulations promotes the highest level of security.	☐	☐
3. Organizations and governments are not held accountable for security breaches.	☐	☐
4. International cooperation is not essential for combating cybercrime.	☐	☐
5. Cybersecurity laws and regulations have no effect on customer trust in products and services.	☐	☐
6. The NCA aims to protect the Kingdom's interests by strengthening its cybersecurity infrastructure.	☐	☐
7. ECC controls only address identity and access management.	☐	☐
8. The PDPL offers guidelines for cloud cybersecurity governance.	☐	☐
9. The HIPPA regulates the unauthorized access of digital financial data.	☐	☐
10. The Saudi Anti-Cyber Crime Law covers both personal and enterprise security.	☐	☐



2 Explain how standardization of cybersecurity laws benefits businesses and organizations.

3 Analyze two subcategories of Data Cybersecurity Control guidelines.



4 Evaluate the implications of not adhering to cybersecurity laws and regulations.

5 Define the Anti-Cyber Crime Law in Saudi Arabia.



6 Search the Internet for the ECC controls and list the main controls for a cybersecurity awareness and training program.

7 Evaluate the implications of the GDPR for businesses operating across borders.



Lesson 2

Cryptography in Cybersecurity

Link to digital lesson



www.ien.edu.sa

Introduction to Cryptography

The Importance of Cryptography

Cryptography is the science of secret writing with the goal of hiding the meaning of a message. It is the science of keeping information secure and secret through codes, algorithms, and encryption. Cryptography has a long history, evolving from simple substitution ciphers used by ancient civilizations to sophisticated encryption algorithms employed in modern digital communication. The evolution of cryptography throughout history reflects the continuous innovation and adaptation of encryption techniques in response to changing needs and technological advances.

At its core, cryptography relies on two fundamental concepts: encryption and decryption. Encryption converts readable information, *plaintext*, into unreadable information, *ciphertext*, using a secret key and a specific algorithm. Decryption, conversely, is the process of converting ciphertext back into plaintext. Cryptography remains vital to secure communication and data protection in an increasingly connected world. The following points outline the importance of cryptography:

Data Confidentiality

Cryptography encrypts sensitive data so only authorized parties with the correct keys can access it, safeguarding personal, financial, and confidential information from unauthorized access. This is essential for sectors such as finance, healthcare institutions, and government agencies.

Authentication

Cryptography enables the use of digital signatures to verify the authenticity of messages, establishing sender identity and preventing tampering during transmission.

Integrity

Cryptography helps ensure data integrity, using advanced techniques for verification and change detection.

Nonrepudiation

Cryptographic techniques provide nonrepudiation, ensuring parties cannot deny the authenticity of their actions or transactions. This is important in legal, financial, and other settings where maintaining data and transaction integrity is essential.

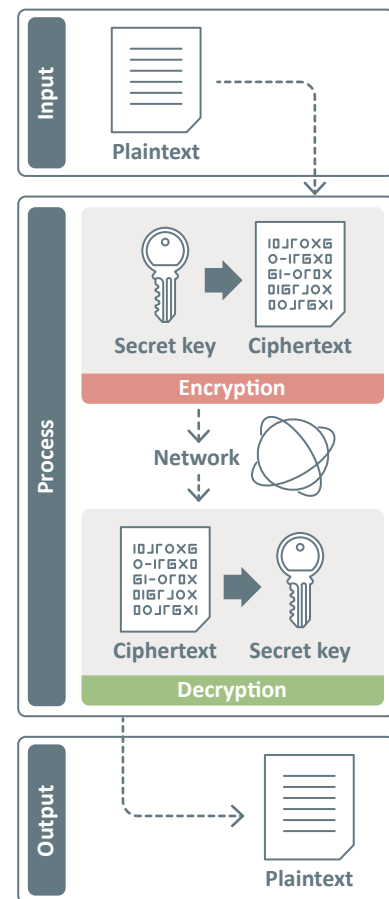


Figure 3.3: Representation of a typical encryption-decryption process



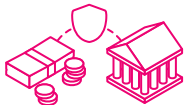
وزارة التعليم
Ministry of Education

2026 - 1448

Applications of Cryptography

The applications of cryptography are vast and diverse, playing a critical role in securing communications, protecting sensitive data, and ensuring trust across a wide range of industries and technologies in the digital landscape. Table 3.1 illustrates the most common applications of cryptography.

Table 3.1: Common applications of cryptography	
Application	Description
 Secure Messaging	Cryptography is essential for securing communication channels between users, ensuring the confidentiality and integrity of messages. For example, applications like Signal and WhatsApp use end-to-end encryption (E2EE) to protect messages from unauthorized access or eavesdropping. With E2EE, only the intended recipients can decrypt and read the messages, providing a high level of security and privacy.
 Email Security	Cryptographic techniques, such as PGP (Pretty Good Privacy), are instrumental in securing email communications. PGP encrypts both the messages and attachments, ensuring the confidentiality and integrity of the content. It allows only the intended recipient to access and decipher the information, providing robust security for email communication. Additionally, digital signatures provided by PGP help verify the authenticity of the sender, establishing trust in the email exchange.
 Secure Web Browsing	Cryptography, particularly through the use of HTTPS, is essential for securing web browsing sessions. It encrypts the connection between the user's browser and the web server, providing confidentiality and integrity for sensitive data exchanged during the browsing session.
 E-commerce Security	Cryptography protects sensitive data in e-commerce. It encrypts information like credit card details, ensuring confidentiality and non-repudiation. It also verifies website authenticity, using methods like Kerberos and Public Key Infrastructure (PKI), for a safe shopping experience.
 Virtual Private Network	Cryptography, along with the IPsec (Internet Protocol Security) protocol, is used in VPNs to create secure, encrypted connections between remote devices and a private network. IPsec is a suite of protocols that provides authentication, encryption, and integrity verification for IP communications. With cryptography, IPsec ensures the confidentiality and integrity of the data transmitted over a VPN.
 Internet of Things (IoT) Security	With the rapid growth of IoT devices, cryptography plays a crucial role in ensuring secure communication and data protection. Lightweight cryptographic techniques encrypt data transmitted between IoT devices and backend servers.

Application	Description
 Blockchain and Digital Currencies	Cryptography is a core component of blockchain technology and digital currencies. It is used to secure transactions, maintain the integrity of the distributed ledger, and ensure the authenticity of participants.

Types of Cryptography

Cryptography encompasses a variety of techniques that can be broadly classified into three main types: symmetric key cryptography, asymmetric key cryptography, and hash functions. Each type serves a distinct purpose and has advantages and limitations depending on the specific security requirements and use cases. The following is an introduction to each one of these types:

Symmetric Key Cryptography

Symmetric key cryptography, or secret key cryptography, uses a single key for encryption and decryption processes and its main operation is substitution and transposition. When a sender wants to transmit encrypted data, they use the shared secret key to encrypt the plaintext, turning it into ciphertext. The recipient, who also possesses the same secret key, then decrypts the ciphertext back into plaintext. The length of the key is very important in symmetric key cryptography. One common symmetric key algorithm is Advanced Encryption Standard (AES).

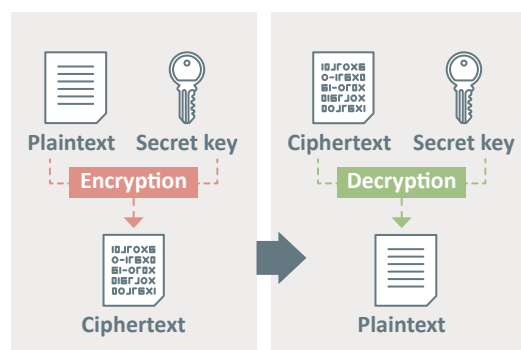


Figure 3.4: Process of Symmetric Key Cryptography

Asymmetric Key Cryptography

Asymmetric key cryptography, or public key cryptography, involves using two distinct but mathematically related keys: public and private keys. The public key is openly distributed, while the private key remains confidential to the owner and it is infeasible to find the private key from the public key. For asymmetric key cryptography to work properly, there must be trust in public key providers. When a sender wants to encrypt data, they use the recipient's public key. Upon receiving the encrypted data, the recipient uses their private key to decrypt the message. Conversely, the private key can be used to sign data for authentication purposes, and the public key can verify the signature. Some widely used asymmetric key algorithms include RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC). It is important to note that the length of the key in bits directly affects the security of the encryption, with longer key lengths providing stronger protection against attacks.

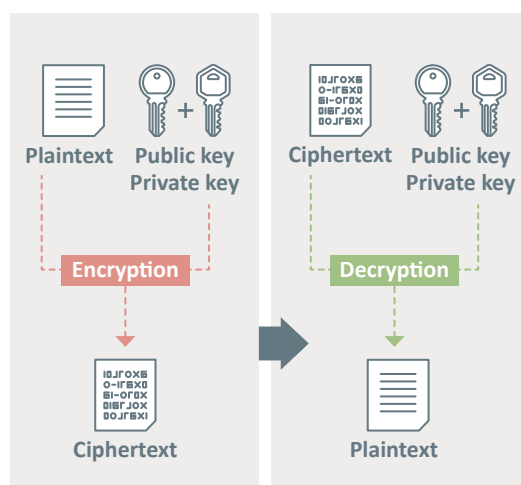
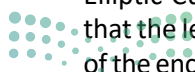


Figure 3.5: Process of Asymmetric Key Cryptography



Hash Functions

Hash functions are a cryptographic technique that takes variable-size input and generates fixed-size output. Hash functions are one-way, meaning it is computationally infeasible to reverse engineer the original input from the hash and any change in the input most likely results in changes in the output. This makes hashing particularly useful for ensuring data integrity and authentication.

When data is transmitted or stored, a hash can be generated and sent along with the data. The recipient can then compute a new hash for the received data and compare it with the original hash. The data has not been tampered with or altered if the hashes match. Some popular hashing algorithms include the Secure Hash Algorithm 3 (SHA3) family, Message-Digest Algorithm 5 (MD5), and the Hash-based Message Authentication Code (HMAC) hash functions.

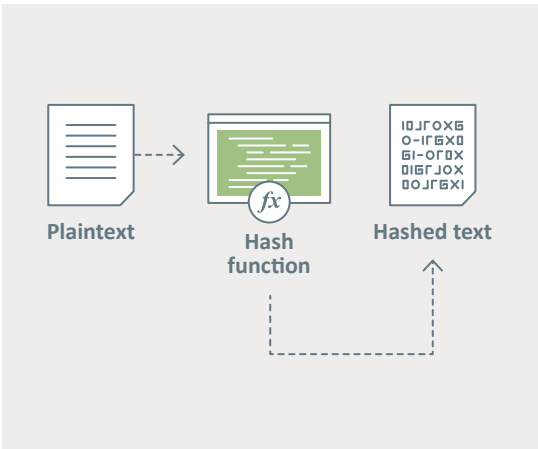


Figure 3.6: Process of Hash function

Table 3.2: Advantages and disadvantages of cryptography types

Type	Advantages	Disadvantages
Symmetric Key Cryptography	• Faster and more computationally efficient • Suitable for large-scale data encryption	• Key distribution and management challenges • Not providing a digital signature, can't guarantee the correctness of user identity
Asymmetric Key Cryptography	• Simplified key distribution (public key sharing) • Enables digital signatures and authentication	• Slower and more computationally intensive • Less suitable for large-scale data encryption
Hashing	• Fast process • Hard to reverse-engineer • Fixed length output regardless of input size	• Vulnerable to collisions in weak algorithms, meaning two different inputs produce the same output

Validation of Public Keys

One of the challenges of asymmetric key cryptography is the validation of the public key that is used for the encryption and decryption of a message. In order to verify that a public key does not come from a hacker, the two following methods are used:

Webs of trust

Webs of trust are a decentralized approach used in cryptography to validate the authenticity of public keys. This concept can be explained through the following example:

Suppose Khalid wants to verify the public key of Ahmed. Instead of relying on a centralized authority, Khalid checks the web of trust. He finds that Fahd, a trusted entity on the web, has signed off on Ahmed's public key, affirming its authenticity. Khalid knows and trusts Fahd, so he can now trust that the public key belongs to Ahmed. Furthermore, Khalid notices that other web members have vouched for Ahmed's key, establishing a stronger web of trust. This means that the more users confirm the validity of a public key, the more trustworthy it becomes within the network. This decentralized approach helps prevent malicious actors from using fake or unauthorized public keys to gain access to encrypted data. By relying on a network of trusted entities, cryptography leverages webs of trust to validate public keys and ensure the security and integrity of communications.

Certificate Authorities

A Certificate Authority (CA) is a trusted entity that validates public keys in cryptography. It plays a central role in authenticating digital certificates, such as SSL (Secure Sockets Layer) certificates, which establish secure connections between websites and users.

For example, when a website wants to obtain an SSL digital certificate, the website owner submits a request to a trusted CA. The CA verifies the owner's identity through various authentication methods, including domain ownership verification. Once the owner's identity and associated public key are verified, the CA issues an SSL digital certificate for the website. This certificate binds the website's identity to its public key, enabling secure communication and encryption between the website and its users.

Cryptography Attacks

There are numerous methods and techniques that are used by hackers to gain access to data that is encrypted by cryptographic algorithms. The following are two of the most common methods used:

Brute Force Attacks

Brute force attacks are used in cryptography attacks as an exhaustive trial-and-error method to crack encrypted data. In these attacks, the attacker systematically tries all possible combinations of the encryption key until he finds the correct combination with which he can decrypt the data.

For example, in a brute force attack against an encrypted password, the attacker would attempt different combinations of characters until they discover the key that decrypts the password. This method can be time-consuming and resource-intensive, especially if the encryption algorithm employs strong, lengthy keys. The National Institute of Standards and Technology (NIST) recommends a minimum key size of 2048 bits for RSA and 224 bits for Elliptic Curve Cryptography (ECC) to secure against brute force attacks.

Cryptanalysis

Cryptanalysis analyzes encrypted data to find weaknesses in the encryption scheme that can be exploited for data extraction or manipulation. Hackers use it to access encrypted data, such as passwords, credit card numbers, and confidential documents. Hackers often employ techniques to break encryption schemes, including analytical, brute-force, and side-channel attacks.

Analytical attacks involve algorithms to determine the likely keys to encrypt data. Brute-force attacks probe all possible keys until the correct key is found. Side-channel attacks exploit known flaws in hardware or software to bypass security measures.

Implementing Cryptographic Algorithms

You will now implement some cryptographic algorithms with the use of the Python programming language.

Caesar Cipher Algorithm

This is a simple substitution cipher where each letter is replaced by another letter based on the key. It is a very simple cryptographic algorithm that is not used in production systems.

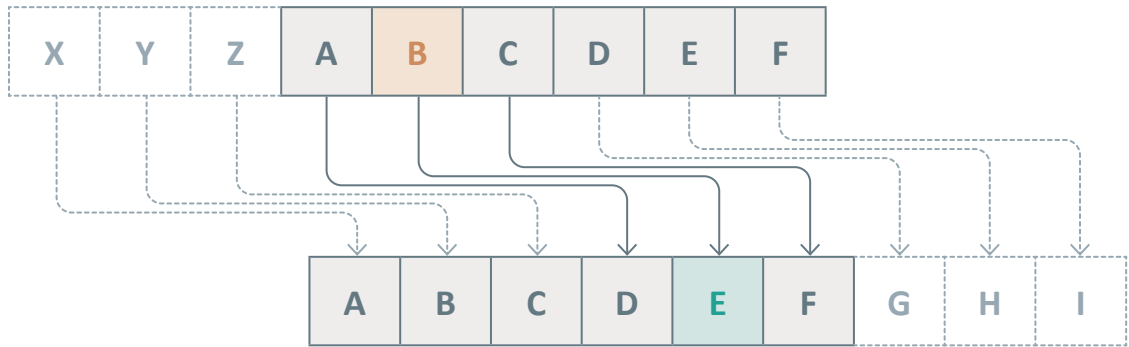
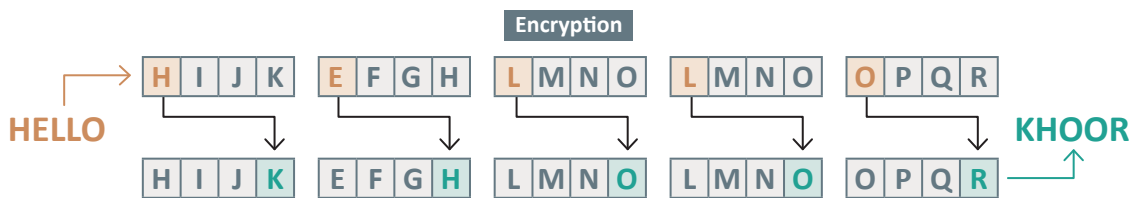


Figure 3.7: Representation of Caesar Cipher cryptographic algorithm using the variable key = 3

Example

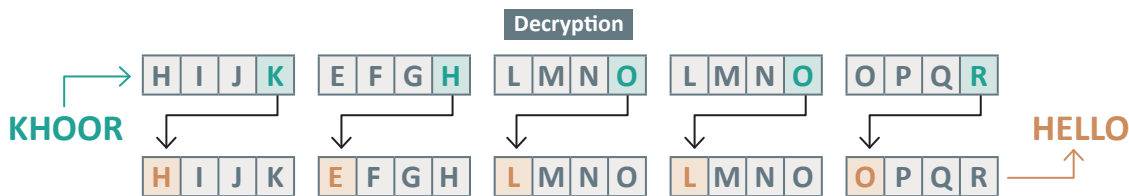
For example, let's use a right shift of 3 (also known as a key of 3) in our Caesar cipher. Our plaintext (the original message) is **HELLO**

We then shift each letter in "HELLO" three places to the right:



So, in this case, "HELLO" encrypted with a Caesar cipher using a shift of 3 becomes "KHOOR".

To decrypt the message, we just do the opposite operation: we shift each letter 3 places to the left (or 23 places to the right, as the effect is the same in a 26 letter alphabet).



And we get back our original message, "HELLO".

Encrypting the message

```
def caesar_encrypt(message, key):  
    # Create a list of alphabet characters  
    alphabet_lower = "abcdefghijklmnopqrstuvwxyz"  
    alphabet_upper = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"  
    # Create an empty string to store the encrypted message  
    encrypted_message = ""  
    # Iterate through each character in the message  
    for char in message:  
        # Check if character is a lowercase letter  
        if char in alphabet_lower:  
            # Find index of the character in alphabet list  
            char_index = alphabet_lower.find(char)  
            # Move the character to the right by the key  
            new_char_index = (char_index + key) % 26  
            # Add the replaced character to the encrypted message  
            encrypted_message += alphabet_lower[new_char_index]  
        # Check if character is an uppercase letter  
        elif char in alphabet_upper:  
            char_index = alphabet_upper.find(char)  
            new_char_index = (char_index + key) % 26  
            encrypted_message += alphabet_upper[new_char_index]  
        else:  
            # Add the character to the encrypted message as it is  
            encrypted_message += char  
    # Return the encrypted message  
    return encrypted_message
```

Decrypting the Message

```
def caesar_decrypt(encrypted_message, key):  
    # Create a list of lowercase alphabet characters  
    alphabet_lower = "abcdefghijklmnopqrstuvwxyz"  
    # Create a list of uppercase alphabet characters  
    alphabet_upper = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"  
    # Create an empty string to store the decrypted message  
    decrypted_message = ""
```

```

# Iterate through each character in the encrypted message
for char in encrypted_message:
    # Check if character is a lowercase letter
    if char in alphabet_lower:
        # Find the index of the character in the lowercase alphabet list
        char_index = alphabet_lower.find(char)
        # Move the character to the left by the key
        new_char_index = (char_index - key) % 26
        # Add the replaced character to the decrypted message
        decrypted_message += alphabet_lower[new_char_index]
    # Check if character is an uppercase letter
    elif char in alphabet_upper:
        # Find the index of the character in the uppercase alphabet list
        char_index = alphabet_upper.find(char)
        # Move the character to the left by the key
        new_char_index = (char_index - key) % 26
        # Add the replaced character to the decrypted message
        decrypted_message += alphabet_upper[new_char_index]
    else:
        # If the character is not a letter, add it to the decrypted message as it is
        decrypted_message += char
    # Return the decrypted message
return decrypted_message

```

Testing the Cipher

```

# Testing the Caesar cipher
message = "There are twenty three items in the inventory."
key = 5

encrypted_message = caesar_encrypt(message, key)
decrypted_message = caesar_decrypt(encrypted_message, key)

print(encrypted_message)
print(decrypted_message)

```

```

Ymjwj fwj ybjsyd ymwjj nyjrx ns ymj nsajsytd.
There are twenty three items in the inventory.

```



Vigenère Cipher Algorithm

This is an extension of the Caesar cipher, where each letter is shifted based on a keyword. Like the Caesar cipher, it can encrypt messages but its complexity is inadequate for production systems.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

The Key: S

The Encrypted Letter: E

The Decrypted Letter: M

Figure 3.8: Representation of Vigenère Cipher cryptographic algorithm

Example

Let's say our plaintext (the original message) is **HELLO** and we'll use the keyword **KEY**. First, you align the keyword with your plaintext, repeating the keyword as necessary:

plaintext
HELLO
| | | | |
KEYKE
keyword

So, for our keyword "KEY", the shifts would be K=10, E=4, Y=24.
Applying these shifts to each letter in "HELLO" yields:

"H" (shifted by 10 places) becomes "R"

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

"E" (shifted by 4 places) becomes "I"

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D



"L" (shifted by 24 places) becomes "J"

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

"L" (shifted by 10 places) becomes "V"

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

"O" (shifted by 4 places) becomes "S"

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N

So, in this case, "HELLO" encrypted with a Vigenère cipher using the keyword "KEY" becomes "RIJVS".

To decrypt the message, we perform the reverse operation: shifting each letter in "RIJVS" back by the amount specified by the corresponding letter in the keyword "KEY".

Encrypting the message

```
def vigenere_encrypt(plaintext, keyword):
    # Calculate the length of the keyword
    keyword_length = len(keyword)
    # Convert each character in the keyword to its ASCII value
    keyword_as_int = [ord(i) for i in keyword]
    # Convert each character in the plaintext to its ASCII value
```

ASCII is an encoding system, which is a standard code for representing all English alphanumeric characters.

```

plaintext_int = [ord(i) for i in plaintext]
ciphertext = ''
# Loop over each character in the plaintext
for i in range(len(plaintext_int)):
    # Calculate the new character by adding the ASCII value of the plaintext
    # character and the corresponding keyword character (modulo 26)
    value = (plaintext_int[i] + keyword_as_int[i % keyword_length]) % 26
    # Convert the new character back to a string and append it to the ciphertext
    # Adding 65 converts the value to its ASCII representation as an uppercase letter
    ciphertext += chr(value + 65)
return ciphertext

```

Decrypting the Message

```

def vigenere_decrypt(ciphertext, keyword):
    # Calculate the length of the keyword
    keyword_length = len(keyword)
    # Convert each character in the keyword to its ASCII value
    keyword_as_int = [ord(i) for i in keyword]
    # Convert each character in the ciphertext to its ASCII value
    ciphertext_int = [ord(i) for i in ciphertext]
    plaintext = ''
    # Loop over each character in the ciphertext
    for i in range(len(ciphertext_int)):
        # Calculate the original character by subtracting the ASCII value of the
        # corresponding keyword character from the ciphertext character (modulo 26)
        value = (ciphertext_int[i] - keyword_as_int[i % keyword_length]) % 26
        # Convert the original character back to a string and append it to the plaintext
        # Adding 65 converts the decrypted value back to its ASCII representation as an uppercase letter
        plaintext += chr(value + 65)
    return plaintext

```

Testing the Cipher

```

encrypted_message = vigenere_encrypt("THERE ARE TWENTY THREE ITEMS IN THE
INVENTORY", "LEMON")
print(encrypted_message)
decrypted_message = vigenere_decrypt(encrypted_message, "LEMON")
print(decrypted_message)

```

```

ELQFREEDSGEABGJXFVEPIFWGPQEHVYXFVREMZJRYXAF
L
THERETARETTWENTYTTTHREETITEMSTINTTTHETINVENTORY

```



The Diffie-Hellman (DH) Key Exchange Algorithm

The Diffie-Hellman (DH) Key Exchange Algorithm is a cryptographic protocol for secure communication over an unsecured network. It allows two parties to establish a shared secret key that can be used to encrypt and decrypt messages exchanged between them.

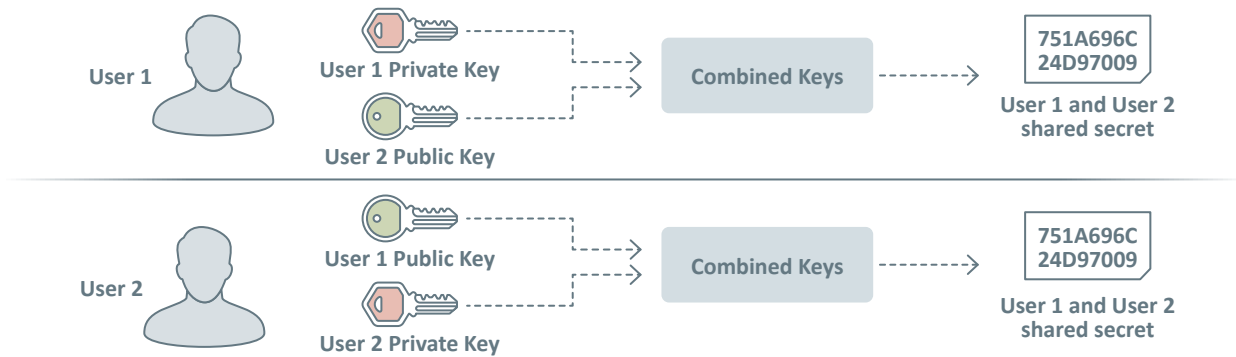


Figure 3.9: Representation of DH Key Exchange Algorithm

Example

For simplicity, let's use small numbers as an example. In real life, much larger numbers would be used to provide sufficient security.

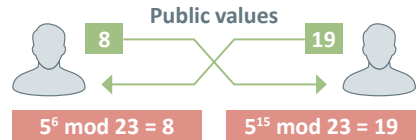
1. First, both parties agree on two large prime numbers. For our example, let's use 5 (a primitive root modulo) and 23 (the modulus). These numbers can be public.



2. Next, each party chooses a secret number. Ali chooses 6 and Ahmed chooses 15. These numbers are private and should not be shared.



3. Both parties calculate a public value to share with each other. Ali calculates $(5^6 \bmod 23)$ which equals 8, and Ahmed calculates $(5^{15} \bmod 23)$ which equals 19.



4. Ali and Ahmed exchange these public values.

5. Now, each party calculates the shared secret. Ali calculates $(19^6 \bmod 23)$ and gets 2, and Ahmed calculates $(8^{15} \bmod 23)$ and also gets 2.



So, Ali and Ahmed have now agreed on a shared secret (2 in this case) over an unsecured channel without sending the secret itself. An eavesdropper would need to solve a discrete logarithm problem to figure out the secret, which is computationally difficult and time-consuming, especially with larger numbers.

Preparing the Algorithm

```
import random
import hashlib

# Modular exponentiation: (base^exponent) % modulus
def mod_exp(base, exponent, modulus):
    return pow(base, exponent, modulus)

# Generate a large prime number
def generate_large_prime(bits=2048):
    return random.getrandbits(bits) | 1 # Command to create a prime number
```

Implementing the Key Exchange

```
def dh_key_exchange():
    # Agree on large prime numbers p and g
    p = generate_large_prime()
    g = generate_large_prime()

    # Each party selects a private key
    ali_private_key = generate_large_prime()
    ahmed_private_key = generate_large_prime()

    # Each party computes their public key
    ali_public_key = mod_exp(g, ali_private_key, p)
    ahmed_public_key = mod_exp(g, ahmed_private_key, p)

    # Each party exchanges their public key and computes the shared secret
    ali_shared_secret = mod_exp(ahmed_public_key, ali_private_key, p)
    ahmed_shared_secret = mod_exp(ali_public_key, ahmed_private_key, p)

    # Verify that the shared secrets match
    assert ali_shared_secret == ahmed_shared_secret

    # Optionally, hash the shared secret to derive a symmetric key
    shared_secret_hash = hashlib.sha256(str(ali_shared_secret).encode()).hexdigest()

    return shared_secret_hash
```

Generating the Secret Shared Key

```
# Produce the shared secret key
shared_secret = dh_key_exchange()
print("Shared secret:", shared_secret)
```

Shared secret: 74b40ad75c4d76edcef424bcb1e27be104c60c22072e0aad65b5a29b60d1ddab



Cybersecurity, Cryptography and Blockchain

In recent years, blockchain technology has gained attention in cybersecurity systems. Blockchain is a decentralized and transparent ledger that securely records transactions. However, it is not immune to vulnerabilities and cyberattacks.

One area of concern is smart contracts, which are self-executing contracts written in code and executed on a blockchain. For example, imagine a smart contract designed to manage supply chain transactions. If a coding error or vulnerability exists in the smart contract, an attacker could exploit it to manipulate or disrupt the supply chain process. This could lead to fraudulent activities or unauthorized access to sensitive information. A visual explanation of the processes that blockchain technologies use is illustrated in figure 3.10.

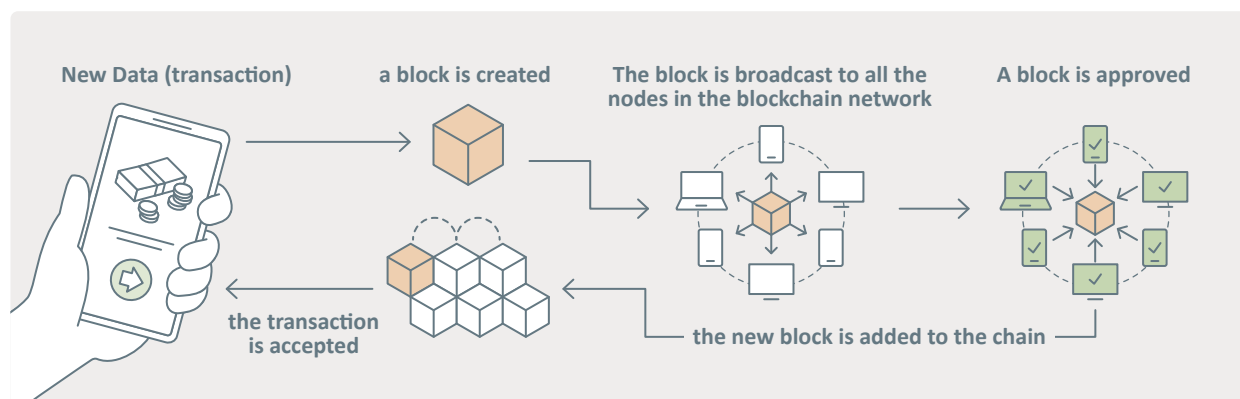


Figure 3.10: Representation of Blockchain technology

Blockchain technologies can help in cybersecurity in several ways, including:

Identity management

Blockchain can create a secure and decentralized identity management system where users can control their data and share it with others as needed. For example, blockchain-based identity systems can store and verify user identities, making it more difficult for attackers to steal or alter user data.

Supply chain management

Blockchain can create a secure and transparent supply chain management system that records all transactions in a tamper-resistant ledger. For example, blockchain-based supply chain systems can track the movement of goods and ensure that they are not tampered with or counterfeited.

Smart contracts

Blockchain can create secure and automated smart contracts, which can help reduce the risk of fraud and ensure that transactions are executed as intended. For example, blockchain-based smart contracts can automate payment processing, reducing the risk of payment fraud.

Distributed networks

Blockchain can create secure and decentralized networks, which can help reduce the risk of single points of failure and ensure that data is distributed across multiple nodes. For example, blockchain-based networks can create more secure and efficient peer-to-peer file-sharing systems.

Data storage

Blockchain can be used to create secure and decentralized data storage systems, which can help reduce the risk of data breaches and ensure that stored data is tamper-resistant. For example, blockchain-based data storage systems can store sensitive data such as medical records or financial information.

Exercises

1

Read the sentences and tick ✓ True or False.	True	False
1. Encryption converts plaintext into readable information.	☐	☐
2. Authentication is used to verify the integrity of messages.	☐	☐
3. Data confidentiality is essential for communications within the finance industry.	☐	☐
4. Cryptography plays a vital role in securing web browsing sessions.	☐	☐
5. VPNs do not use cryptography for secure connections.	☐	☐
6. Symmetric key cryptography is faster and more computationally efficient than asymmetric key cryptography.	☐	☐
7. Hashing is primarily used for data encryption.	☐	☐
8. Cryptanalysis is a technique used by hackers to gain access to encrypted data.	☐	☐
9. A web of trust is made up of users who have agreed to sign off on one another's public keys.	☐	☐
10. A certificate authority issues a digital certificate that binds a public key to an identity.	☐	☐

2

Describe the core principles of cryptography and how it works.



3 Outline the various applications of cryptography in the modern digital world.

4 List the three main types of cryptographic algorithms.



5

6



7 Analyze how webs of trust are used to validate public keys in cryptography.

8 Explain how hackers can use cryptanalysis to gain access to encrypted data.



Lesson 3

Cybersecurity in Emerging Technologies

Link to digital lesson



www.ien.edu.sa

Cybersecurity Systems in Emerging Technologies

Emerging technologies are transforming the world very quickly. However, these technologies also pose significant challenges and risks to the security and privacy of individuals, organizations, and nations. Cybersecurity systems are essential to protect the data, systems, and networks that enable these technologies from malicious attacks and unauthorized access. The following is an introduction to some of the vulnerabilities in actively used emerging technologies and to why cybersecurity systems are important to protect them.

IoT Devices

The Internet of Things (IoT) is the network of interconnected devices, sensors, and appliances that collect, transmit, and exchange data with each other. These devices range from smart home appliances, such as thermostats and security systems, to industrial machinery, health monitoring devices, and wearables. As the number of IoT devices grows, so does the potential attack surface for cybercriminals. For example, IoT devices in edge computing environments may have limited resources for implementing robust security measures, making them more susceptible to attacks. Organizations utilizing edge computing must adopt strong security practices, such as encryption, secure device management, and network segmentation, to protect their data and systems from potential threats. Some of the risks associated with IoT include:

Weak authentication and authorization

IoT devices often lack strong authentication and authorization mechanisms, making them easy targets for attackers, so using strong passwords and MFA protects IoT devices from unauthorized access.

Lack of encryption

Many IoT devices lack encryption capabilities, which can result in the interception of data by attackers, so advanced encryption measures should be implemented.

Firmware vulnerabilities

Firmware is a form of microcode or program embedded into hardware devices to help them operate effectively. IoT devices often have firmware that can be easily compromised, allowing attackers to gain control over the device.

Outdated software

Many IoT devices are not designed with security in mind and may run outdated software with known vulnerabilities. Regularly updating IoT device firmware and software ensures known vulnerabilities are patched.



Privacy concerns

IoT devices often collect sensitive personal data, such as location information and biometric data, which can be used for malicious purposes if it falls into the wrong hands. Organizations should limit the amount of personal data collected and stored by IoT devices to minimize privacy concerns.

Smart Cities

Smart cities utilize interconnected technologies and the Internet of Things (IoT) to enhance urban living, optimize resource consumption, and improve public services. They rely on data collected from sensors, devices, and systems to enable real-time decision-making and to automate processes. However, the increasing connectivity and reliance on technology also make smart cities vulnerable to cyberattacks, which could result in disrupted services, stolen data, or compromised infrastructure.

For example, an attacker could compromise a smart city's traffic management system, causing gridlock or accidents, or take control of a city's water supply system, contaminating the water or disrupting its distribution. To ensure the security of smart cities, it is crucial to implement robust cybersecurity measures, such as network segmentation, secure communication protocols, and continuous monitoring, to protect the city's infrastructure and the data it collects. Some of the security risks associated with smart cities include:

Vulnerable devices

IoT devices are often not designed with security in mind and can be easily compromised. These devices could be used to launch attacks on other devices or gain access to sensitive data.

Data privacy

Smart city systems collect a lot of data about citizens, such as location data and other personal information. This data is valuable to advertisers and other third parties, but it also raises concerns about privacy and data security.

Cyberattacks

Smart city systems are vulnerable to cyberattacks that could disrupt services or cause damage to infrastructure. For example, hackers could shut down traffic lights, causing traffic chaos and accidents.

Lack of standardization

Smart city systems are often developed by different vendors, using different technologies and protocols. This lack of standardization makes it difficult to integrate systems and can create security vulnerabilities.

To mitigate these risks, it is important to implement best practices for smart city security, for example:

Regularly updating and patching all devices and systems to ensure they are secure and functioning properly.



Implementing strong authentication and access controls to prevent unauthorized access to devices and systems.

Conducting regular security assessments to identify and address vulnerabilities.

Developing comprehensive incident response plans to respond to and mitigate security incidents quickly.

Ensuring that data privacy policies are in place and that data is collected, stored, and used in compliance with applicable regulations.

Developing standardization frameworks to ensure that systems are compatible and secure.

Autonomous Vehicles

Autonomous vehicles, or self-driving cars, rely on advanced technologies and sensors to navigate and operate without human intervention. However, as vehicles become more connected and automated, they become more vulnerable to cyberattacks, which could result in vehicle theft, privacy breaches, or even physical harm to passengers and pedestrians. Autonomous vehicles collect a lot of data about passengers and their surroundings. This data is valuable to advertisers and other third parties, but it also raises concerns about privacy and data security.

For instance, a cybercriminal could exploit a vulnerability in an autonomous vehicle's communication system to gain control, causing it to crash or endangering its occupants. Ensuring the security of autonomous vehicles requires implementing multi-layered security measures, such as strong encryption for communication, secure software development practices, and regular monitoring for potential threats. Protecting autonomous vehicles from cyber threats is crucial for their safe and successful integration into our transportation systems.

To mitigate the risks, it is important to implement the following best practices for autonomous vehicle security:

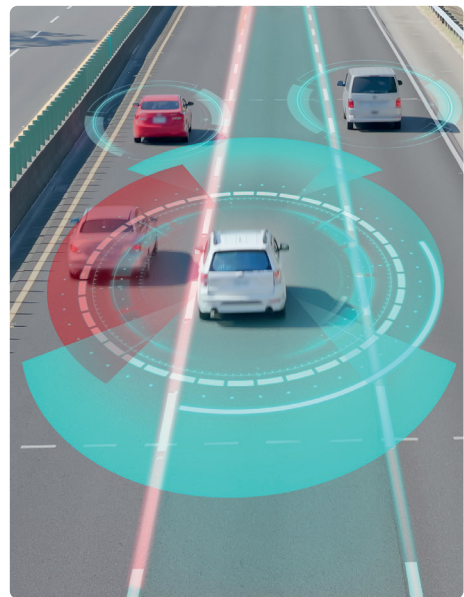


Figure 3.11: Protecting autonomous vehicles is crucial for the safety of the passengers

Encrypting all data transmitted between the vehicle and external systems.

Regularly updating the vehicle's software and hardware to ensure they are secure and functioning properly.

Conducting regular security assessments to identify and address vulnerabilities.

Conducting rigorous testing and validation of all components to identify and fix vulnerabilities.



Implementing strong authentication and access controls to prevent unauthorized access to the vehicle's systems.

Developing comprehensive incident response plans to respond to and mitigate security incidents quickly.

Ensuring that data privacy policies are in place and that data is collected, stored, and used in compliance with applicable regulations.

5G Networks

5G networks promise faster Internet speeds, lower latency, and increased capacity, enabling innovations such as autonomous vehicles, smart cities, and IoT applications. However, the rollout of 5G networks also presents new cybersecurity challenges. The increased attack surface, supply chain risks, and potential exploitation of network components create the need for robust cybersecurity measures to protect the infrastructure.

The complexity of 5G networks and the vast number of interconnected devices create opportunities for cybercriminals to exploit weak points, potentially disrupting critical services or stealing sensitive data.

Cloud Computing

Cloud computing enables businesses and individuals to store, process, and manage their data on remote servers, providing scalability, cost savings, and flexibility. However, the reliance on cloud-based services and infrastructure also demands strong cybersecurity measures to protect the data and applications hosted in the cloud.

Cloud-related cybersecurity risks include data breaches, unauthorized access, and account hijacking. For example, misconfigured cloud storage buckets can expose sensitive information to the public, leading to data leaks and potential legal consequences. Additionally, insider threats can pose a significant risk to cloud environments, as privileged users with malicious intent can abuse their access to steal data or disrupt services.

Another concern relating to cloud computing is the shared responsibility model, where the cloud service provider is responsible for securing the underlying infrastructure while the customer is responsible for securing their data and applications hosted on the cloud. This division of responsibility can sometimes lead to confusion or gaps in security, making successful attacks more likely. Organizations must understand their responsibilities and implement appropriate security measures to protect their assets in the cloud.

Quantum Computing

Quantum computing leverages the principles of quantum mechanics to perform computations exponentially faster than classical computers. This breakthrough technology holds immense potential for various industries, including cryptography, pharmaceuticals, and financial services. However, quantum computers also pose cybersecurity risks, particularly in the field of encryption. Once sufficiently powerful, quantum computers could break many of the current cryptographic algorithms, rendering encrypted data vulnerable to interception and decryption.



To prepare for this potential threat, researchers are developing quantum-resistant algorithms that are believed to be secure even against quantum computers. Implementing these algorithms in advance will help ensure the confidentiality and integrity of sensitive data.

Artificial Intelligence (AI) and Machine Learning (ML) Systems

AI and ML systems are transforming various industries by enabling machines to learn from data, make predictions, and improve their performance over time. These systems have applications in diverse sectors, including healthcare, finance, transportation, and manufacturing. AI-based technologies can help security professionals analyze large volumes of data and identify patterns that might go unnoticed. This can enable organizations to respond more quickly and effectively to security incidents.

One way in which AI is being used in cybersecurity is through machine learning. Machine learning algorithms can analyze security data, such as network traffic or user behavior, and identify patterns or anomalies that may indicate a security threat. This can help security teams detect and respond to attacks in real time.

Another way in which AI is being used in cybersecurity is through predictive analytics. Predictive analytics can help organizations identify potential security threats before they occur. Predictive analytics can help security teams anticipate and prevent attacks by analyzing historical data and identifying patterns.

The following are some practical examples of AI and ML applications in cybersecurity:

Malware detection

AI can detect malware by analyzing behavior patterns and identifying anomalous activity. For example, an AI-based system might flag a program accessing many files or communicating with unknown servers as potential malware.

Network intrusion detection

AI can detect network intrusions by analyzing traffic and identifying patterns that may indicate an attack. For example, an AI-based system might flag an unusually large number of failed login attempts as potential network intrusion attempts.

User behavior analysis

AI can be used to analyze user behavior and identify potential security risks. For example, an AI-based system might flag an employee accessing sensitive data outside of normal working hours as a potential insider threat.

Threat intelligence analysis

AI can analyze threat intelligence data and identify emerging threats. For example, an AI-based system might flag a new malware variant spreading rapidly across the Internet as a potential emerging threat.

Fraud detection

AI can detect fraudulent activity, such as credit card fraud or identity theft. For example, an AI-based system might flag a credit card transaction being made from an unusual location or outside of the user's normal spending patterns as potential fraud.



However, the growing reliance on AI and ML systems also raises security concerns. Cybercriminals can target these systems and attempt to manipulate or compromise them for malicious purposes. Hackers can use machine learning and other AI-based technologies to identify vulnerabilities in systems and launch more sophisticated attacks. For example, attackers can use machine learning algorithms to generate convincing phishing emails or to bypass security controls by impersonating legitimate users.

One other potential risk associated with AI and ML systems is adversarial attacks, where cybercriminals create malicious inputs designed to deceive or exploit the vulnerabilities of AI models. For instance, an attacker might add subtle noise to an image that causes a facial recognition system to misidentify the subject. Another example is the manipulation of recommendation algorithms on social media platforms, where an attacker can spread false information or create fake profiles to influence users' behavior.

To mitigate the risks associated with AI-powered attacks, developing and implementing strong cybersecurity measures is important. This can include using AI-powered technologies to detect and respond to real-time threats and implementing measures such as multi-factor authentication and access controls to prevent unauthorized access.

Robotics and Autonomous Systems

Robotics and autonomous systems are increasingly integrated into various industries, from manufacturing to agriculture and transportation. As these technologies become more sophisticated and connected, they become more vulnerable to cyberattacks. Cybersecurity risks associated with robotics and autonomous systems include unauthorized access, data theft, and system manipulation to cause physical harm or disrupt operations.

For instance, an attacker could compromise a factory robot's control system, causing it to endanger or hurt workers. Ensuring the security of robotics and autonomous systems requires strong access controls, secure communication protocols, and regular monitoring for potential threats. Addressing these cybersecurity challenges is critical to safely and successfully adopting robotics and autonomous systems across various sectors.

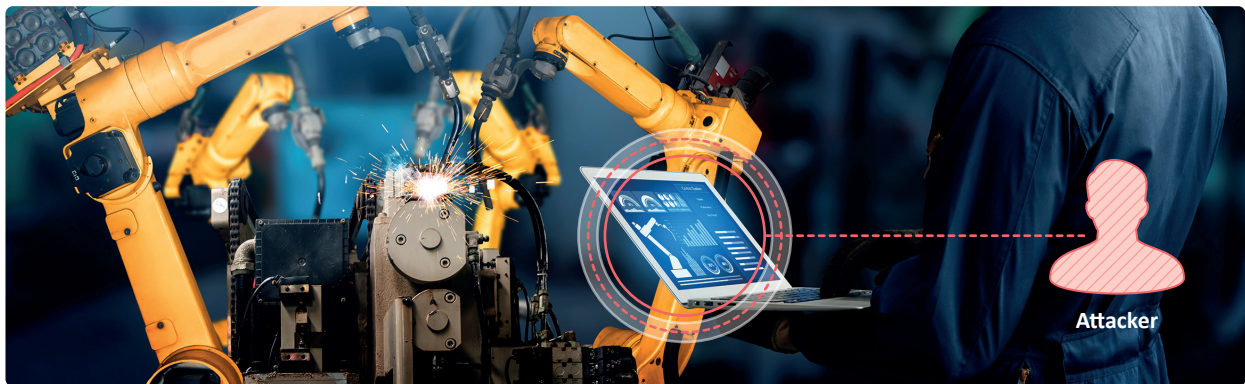


Figure 3.12: A cybercriminal can manipulate a system to cause physical harm or disrupt operations

Augmented Reality (AR), Virtual Reality (VR) and the Metaverse

AR, VR, and metaverse technologies have rapidly evolved, expanding their applications from gaming to various industries such as healthcare, education, manufacturing, and the emerging concept of the metaverse. These immersive technologies can collect vast amounts of personal and sensitive data, making them prime targets for cybercriminals. Therefore, ensuring data privacy and security in AR, VR, and metaverse environments is crucial to protect user information from unauthorized access or misuse.

One example of a potential security risk in these immersive environments is the use of biometric data for authentication, such as facial recognition or eye tracking. While these methods may enhance user

experiences, they also introduce new vulnerabilities and privacy concerns. Organizations implementing AR, VR, and metaverse technologies must employ robust security measures to safeguard user data and maintain trust in these transformative technologies.

As the metaverse continues to develop, with interconnected virtual environments and seamless user interactions, it becomes even more critical to prioritize cybersecurity. The interconnected nature of the metaverse creates a complex landscape where protecting user data, preventing unauthorized access, and mitigating potential threats require comprehensive security measures.



Figure 3.13: Biometric data in AR and VR environments are commonly targeted by cyberattacks

Digital Twins

Digital twins are virtual replicas of physical assets, systems, or processes that can be used for simulation, analysis, and optimization. These digital models have various applications, including smart cities, manufacturing, and healthcare. As digital twins become more interconnected and store vast amounts of sensitive data, they become prime targets for cybercriminals.

Potential cybersecurity risks for digital twins include unauthorized access, data tampering, and attacks on the underlying infrastructure supporting the digital twin. For example, an attacker could manipulate a digital twin's data to cause operational disruptions or mislead decision-makers. To protect digital twins from cyber threats, organizations must implement strong access controls, data encryption, and continuous monitoring to ensure the security and integrity of their digital assets.

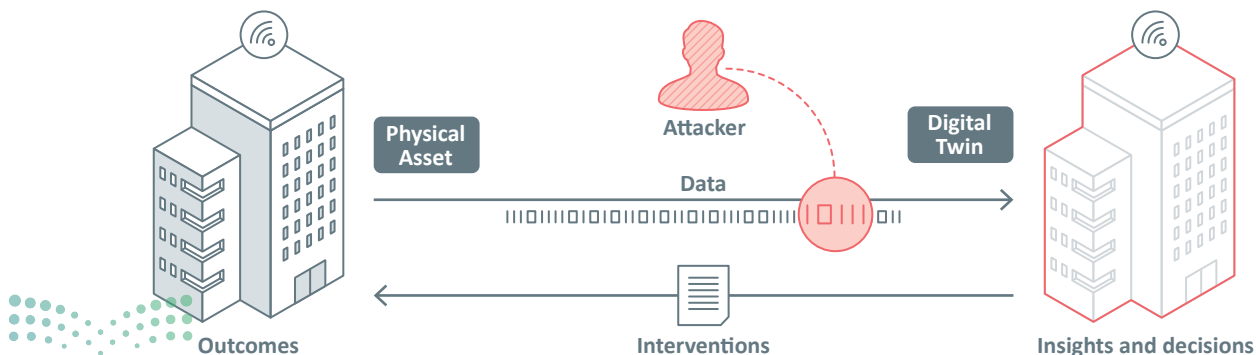


Figure 3.14: Digital twins store vast amounts of sensitive data making them prime targets for cybercriminals

Exercises

1

Read the sentences and tick ✓ True or False.	True	False
1. Cybersecurity is important to protect data, systems, and networks from malicious attacks and unauthorized access.	☐	☐
2. Smart cities rely on data collected from sensors and devices to enable real-time decision-making.	☐	☐
3. Autonomous vehicles can be adversely affected by cyberattacks.	☐	☐
4. Quantum computing has the potential to break current cryptographic algorithms.	☐	☐
5. Cloud computing does not introduce new cybersecurity challenges.	☐	☐
6. 5G networks create increased attack surfaces.	☐	☐
7. Artificial Intelligence and Machine Learning systems are not vulnerable to adversarial attacks.	☐	☐
8. Robotics and autonomous systems do not pose security risks.	☐	☐
9. Smart contracts are safe from potential attacks.	☐	☐
10. Augmented Reality and Virtual Reality applications do not collect personal data.	☐	☐

2 Describe the unique vulnerabilities faced by Internet of Things (IoT) devices.



3 Assess the security measures necessary to protect 5G networks from cyber threats.

4 Provide examples of cybersecurity risks associated with AI and ML systems.

5 Evaluate the shared responsibility model between the cloud service provider and their customers.



6 Describe the need for quantum-resistant algorithms in the era of quantum computing.

7 Explain the type of information digital twins store and the dangers posed by their use.



Project

Smart cities are revolutionizing how people live, work, and interact with their environment by leveraging cutting-edge technologies to create more efficient, sustainable, and connected urban spaces. However, this reliance on technology also brings forth a myriad of cybersecurity challenges that must be addressed to ensure citizens' safety, privacy, and well-being.

1

Provide an overview of a smart city, its components, and its benefits to citizens and governments.

2

Identify and describe smart cities' main cybersecurity challenges, including potential threats to critical infrastructure, data privacy, and communication networks.

3

Analyze various components of smart cities, such as energy management systems, transportation systems, public safety, and healthcare, and discuss the specific cybersecurity measures required to protect each component.

4

Research and present emerging technologies, tools, and strategies that can enhance the cybersecurity posture of smart cities, such as artificial intelligence, blockchain, or intrusion detection systems.

5

Summarize the main findings and recommendations for securing smart cities, and use your notes to create a PowerPoint presentation.



Wrap up

Now you have learned to:

- > Identify the importance of standardized cybersecurity legislation.
- > Analyze the main domestic and international cybersecurity laws.
- > Describe cryptography and its use cases.
- > Classify the types of cryptography and the methods hackers use to access encrypted data.
- > Implement cryptographic algorithms with Python.
- > Describe the importance of cybersecurity systems for the protection of applications built with emerging technologies.

KEY TERMS

5G Networks	Hashing	Smart Cities
Artificial Intelligence (AI)	Internet of Things (IoT)	Symmetric Key Cryptography
Asymmetric Key Cryptography	Machine Learning (ML)	Threat Intelligence Analysis
Cloud Computing	Private Key	User Behavior Analysis
Cryptography	Public Key	
Cybercrime Regulation	Quantum Computing	
Digital Twins	Robotics and Autonomous Systems	