BAIT1093 Introduction to Computer Security

Chapter 1: Introduction

Topics

1.1 Security Problems
1.2 Computer Security Concepts
1.3 Vulnerabilities, Threats and Attacks
1.4 Security Functional Requirement
1.5 Computer Security Trends
1.6 Computer Security Strategy

1.1 Security Problems

Note: The list shown above is not exhaustive

1.2 Computer Security Concepts

Computer Security

The **protection** afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity, availability and confidentiality** of **information system resources** (includes hardware, software, firmware, information/data, and telecommunications).

Source: https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter1.html

1.2 Computer Security Concepts

SIX PRINCIPLES OF SECURITY [1]

- Confidentiality
- Authentication
- Integrity
- Non-Repudiation
- Access Control
- Availability

1.2 Computer Security Concepts

Confidentiality [1]

- Only the sender and the intended recipient(s) should be able to access the content of a message
- Confidentiality gets compromised if an unauthorized person is able to access a message. Example of an attack is **interception**.

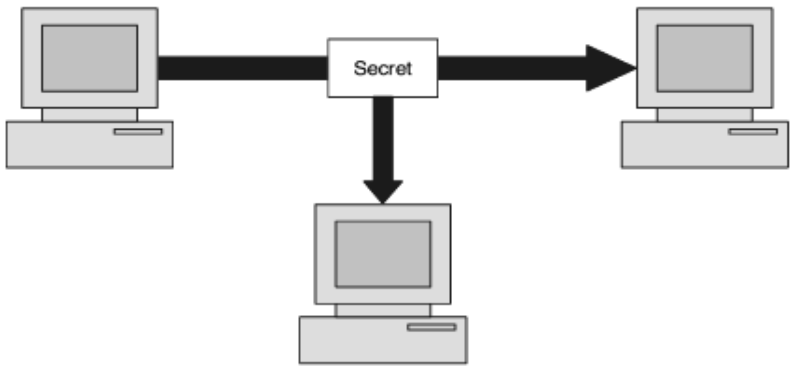


FIGURE 1.2 The loss of confidentiality: Interception causes the loss of the message's confidentiality.

1.2 Computer Security Concepts

Authentication [1]

- Help establish proof of identities.
- Ensures that the origin of an electronic message or document is correctly identified.
- Authentication is compromised via **fabrication**.

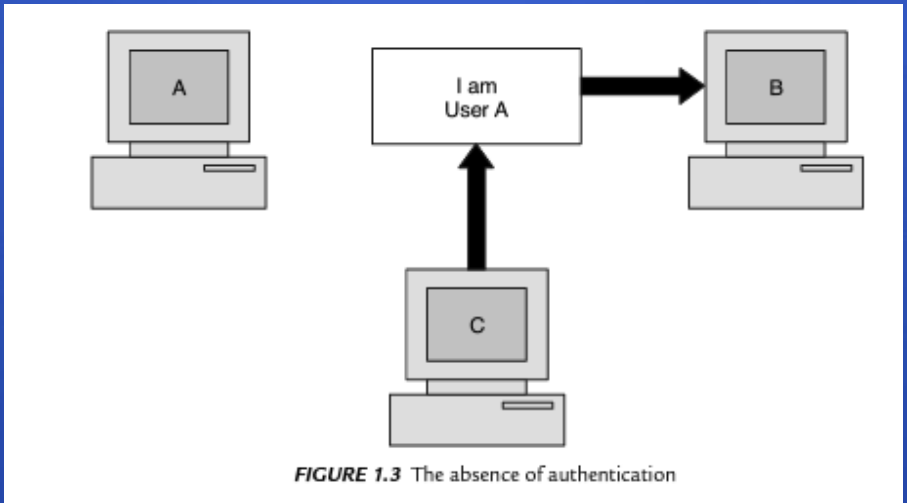


FIGURE 1.3 The absence of authentication

1.2 Computer Security Concepts

Integrity [1]

- Integrity is lost when the contents of a message are changed during the transmission from sender to receiver. This type of attack is called **modification**.

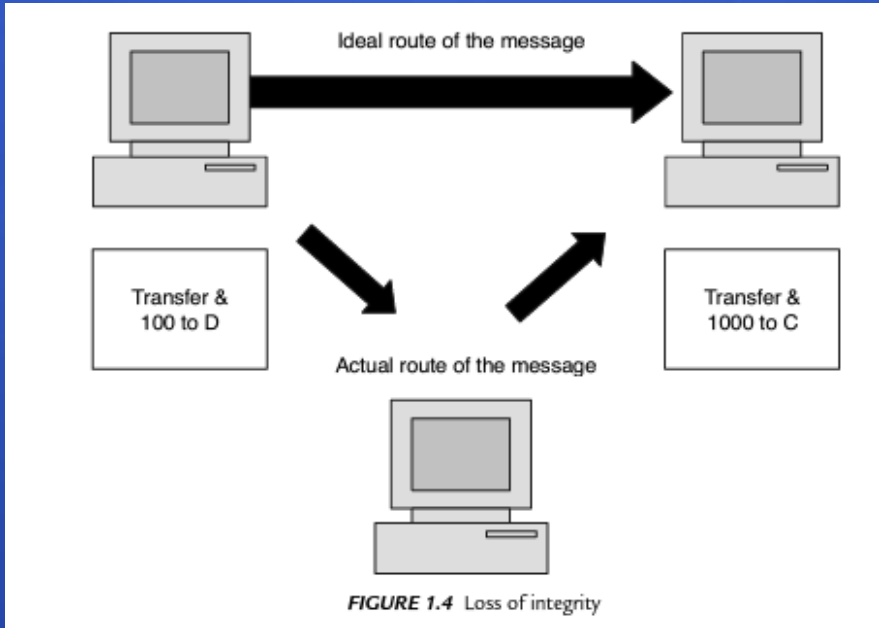


FIGURE 1.4 Loss of integrity

1.2 Computer Security Concepts

Non-Repudiation [1]

- Situations where users deny or repudiate sending messages to recipients.
- The principle of non-repudiation defeats the possibility of denying something after having done it.

1.2 Computer Security Concepts

Access Control [1]

- Determines who should be able to access what.
- Access control is broadly related to two areas:
  - Role management
    - Concentrates on the user side (which user can do what)
  - Rule management
    - Focuses on the resource side (which resource is available)
- Access control matrix which list users against list of items that they can access. An Access Control List (ACL) is a subset of an access control matrix.

1.2 Computer Security Concepts

Access Control

- Example of an Access Control Matrix

	File A	File B	File C	Printer 1
Alice	RW	RW	RW	OK
Bob	R	R	RW	OK
Carol	RW			
David			RW	OK
Faculty	RW		RW	OK

Source: https://oktatas.iit.uni-miskolc.hu/lib/exe/fetch.php?media=tanszek:oktatas:w2_software_system_security.pdf

1.2 Computer Security Concepts

Access Control

- Example of an Access Control List within an Access Control Matrix

	File A	File B	File C	Printer 1
Alice	RW	RW	RW	OK
Bob	R	R	RW	OK
Carol	RW			
David			RW	OK
Faculty	RW		RW	OK

Access Control List

Source: https://oktatas.iit.uni-miskolc.hu/lib/exe/fetch.php?media=tanszek:oktatas:w2_software_system_security.pdf

1.2 Computer Security Concepts

Availability [1]

- Resources should be available to authorized parties at all times.
- Attack called interruption will defeat the principle of availability.

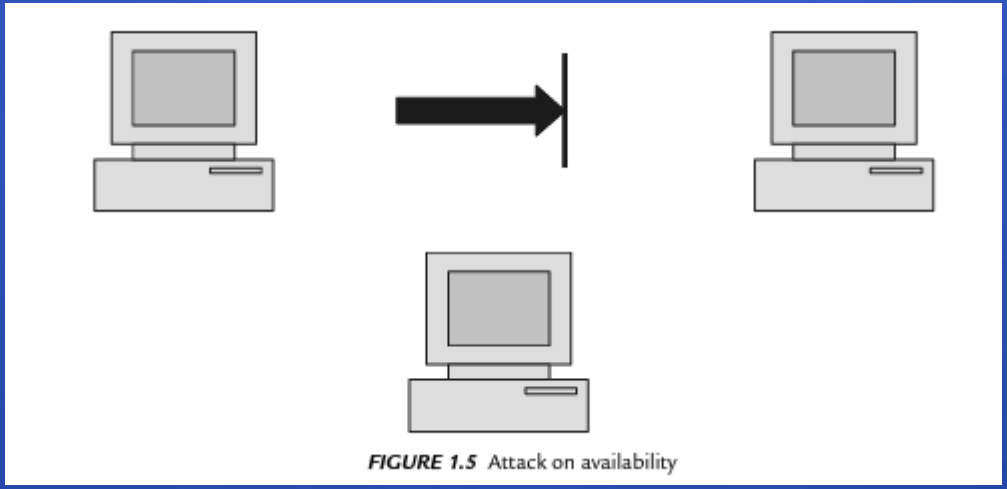


FIGURE 1.5 Attack on availability

1.3 Vulnerabilities, Threats and Attacks

Vulnerability [2]

- Defined as the state of being exposed to the possibility of being attacked or harmed.
- Cybersecurity vulnerabilities can be categorized into:
  - Platforms
  - Configurations
  - Third parties
  - Patches
  - Zero-day vulnerabilities

1.3 Vulnerabilities, Threats and Attacks

Vulnerability → 1) Platforms [2]

- A computer platform is a system that consists of the hardware device and an operation system (OS) that runs software such as applications, programs, or processes.
- Examples of platforms with serious vulnerabilities:
  - Legacy Platforms
  - On-Premises Platforms
  - Cloud Platforms

1.3 Vulnerabilities, Threats and Attacks

Vulnerability → 1) Platforms [2]

- Examples of platforms with serious vulnerabilities:
  - **Legacy Platforms**
    - No longer in widespread use
    - Vulnerabilities often found from legacy software, such as an OS or program
    - Example, Microsoft Windows, Apple macOS, Linux which are not updated with the latest version, ie depriving it of security fixes.

1.3 Vulnerabilities, Threats and Attacks

Vulnerability → 1) Platforms [2]

- Examples of platforms with serious vulnerabilities:
  - **On-Premises (On-Prem) Platforms**
    - Software and technology located within the physical confines of an enterprise, which is usually consolidated in the company's data center.
    - Security concern: more servers, network resources, support for remote access, new software to be added to support emerging business process and user needs which resulted inadequate configuration for security over time.
    - Numerous entry points from outside into the on-prem platform (through USB flash drives, wireless network transmissions, mobile devices, and email messages) creates more vulnerabilities.

1.3 Vulnerabilities, Threats and Attacks

Vulnerability → 1) Platforms [2]

- Examples of platforms with serious vulnerabilities:
  - Cloud Platforms
    - this is a pay-per-use computing model in which customers pay only for the online computing resources they need. Cloud computing resources can be scaled up or scaled back based on needs.
    - Vulnerabilities of cloud platforms are related to misconfigurations by the company personnel responsible for securing the cloud platform. Cloud resources are accessible from virtually anywhere, putting cloud computing platforms constantly under attack from threat actors probing for vulnerabilities.

1.3 Vulnerabilities, Threats and Attacks

Vulnerability → 2) Configurations [2]

- Modern hardware and software platforms provide an array of features and security settings that must be properly configured to repel attacks.
- However, the configuration settings are often not properly implemented, resulting in weak configurations.

1.3 Vulnerabilities, Threats and Attacks

Vulnerability → 2) Configurations [2]

Table 1-3 Weak configurations

Configuration	Explanation	Example
Default settings	Default settings are predetermined by the vendor for usability and ease of use (not for security) so the user can immediately begin using the product.	A router comes with a default password that is widely known.
Open ports and services	Devices and services are often configured to allow the most access so that the user can close ports that are specific to that organization.	A firewall comes with FTP ports 20 and 21 open.
Unsecured root accounts	A root account can give a user unfettered access to all resources.	A misconfigured cloud storage repository could give any user access to all data.

1.3 Vulnerabilities, Threats and Attacks

Vulnerability → 2) Configurations [2]

Table 1-3 Weak configurations *(continued)*

Configuration	Explanation	Example
Open permissions	Open permissions are user access over files that should be restricted.	A user could be given *Read*, *Write*, and *Execute* privileges when she should have only *Read* privileges.
Unsecure protocols	Also called *insecure protocols*, this configuration uses protocols for telecommunications that do not provide adequate protections.	An employee could use devices that run services with unsecure protocols such as *Telnet* or *SNMPv1*.
Weak encryption	Users choosing a known vulnerable encryption mechanism.	A user could select an encryption scheme that has a known weakness or a key value that is too short.
Errors	Human mistakes in selecting one setting over another without considering the security implications.	An employee could use deprecated settings instead of current configurations.

1.3 Vulnerabilities, Threats and Attacks

Vulnerability → 3) Third Parties [2]

- Most businesses use external entities known as third parties, to assist in providing services that the businesses lack the expertise. Example, contract with third parties to assist them in developing and writing a software program or app. Organizations rely on third-party data storage facilities for storing important data.
- Almost all third parties require access to the organization's company network. Connectivity between the organization and the third party is known as system integration.

1.3 Vulnerabilities, Threats and Attacks

Vulnerability → 3) Third Parties [2]

- The major risk of third-party system integration involves the principle of the weakest link. That is, if the security of the third party has any weaknesses, it can provide an opening for attackers to infiltrate the organization's computer network.
- Example: attack to third-party vulnerable integration between Target retail chain and a refrigeration, heating and air-conditioning third party, happened in 2013, where 40 million credit card numbers are stolen.

1.3 Vulnerabilities, Threats and Attacks

Vulnerability → 4) Patches [2]

- To address the vulnerabilities in OSs that are uncovered after the software has been released, software developers usually deploy a software "fix". A security patch is an officially released software security update intended to repair a vulnerability.
- However, they can also create vulnerabilities although it is important:
  - Difficulty patching firmware
  - Few patches for application software
  - Delays in patching OSs

1.3 Vulnerabilities, Threats and Attacks

Vulnerability → 5) Zero Day [2]

- Vulnerabilities that can be exploited by attackers before anyone else knows it exists are called as Zero Day, because it provides zero day of warning.
- Zero-day vulnerabilities are considered extremely serious. Systems are opened to attack with no specific patches available.
- Example of protections that can mitigate zero-day attack using machine learning to collect data from previously detected exploits and create a baseline of safe system behavior that may help detect an attack based on a zero-day vulnerability.

1.3 Vulnerabilities, Threats and Attacks

Threats

A threat is a potentially dangerous event that has not occurred but has the potential to cause damage if it does.

Cybersecurity threats are the actual means by which cyber attackers exploit vulnerabilities. Example of threats:

- Gain unauthorized access to servers
- Ransomware
- Denial of Service (DoS) attack

Source: https://www.simplilearn.com/vulnerability-in-security-article

1.3 Vulnerabilities, Threats and Attacks

Threat Actors [2]

- ***Threat actors are individuals or entities responsible for cyber incidents against the technology equipment of enterprises and users. Threat actors are also known as attackers or hackers.***
- ***Targets by threat actors:***
  - ***Individual users***
  - ***Enterprises***
  - ***Governments***

1.3 Vulnerabilities, Threats and Attacks

Threat Actors [2]

Table 1-1 Types of hackers

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

Today, threat actors are classified in more distinct categories, such as script kiddies, hacktivists, state actors, insiders and others.

1.3 Vulnerabilities, Threats and Attacks

Threat Actors → 1) Script Kiddies [2]

- Individuals who want to perform attacks, yet lack the technical knowledge to carry them out.
- Use freely available automated attack software (scripts) and use it to perform malicious acts.
- Attack may not be always successful due to lack of technical knowledge.

1.3 Vulnerabilities, Threats and Attacks

Threat Actors → 2) Hacktivists [2]

- Individuals who are stongly motivated by ideology (for the sake of their principles or activism)
- Examples of attacks by hacktivists:
  - Breaking into a website and changing its contents as a means of making a political statement.
  - Work through disinformation campaigns by spreading fake news and supporting conspiracy theories.
  - Demand in exchange of stolen data. “Hacktivists Release Iran Nuclear Documents After Deadline” https://www.iranintl.com/en/202210225387
- Motivation: Political, social, or ideological
- Affiliation: Non-governmental individuals or organizations
- Common TTPs: DDoS attacks, doxing, website defacements

Source: https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-cyber-threat-actors

1.3 Vulnerabilities, Threats and Attacks

Threat Actors → 3) State Actors [2]

- Governments are employing their own state-sponsored attackers for launching cyberattacks against their foes, known as state actors.
- Foes may be foreign governments or even citizens of their own nation that government considers hostile or threatening.
- A growing number of attacks from state actors are directed toward businesses in foreign countries with the goal of causing financial harm or damage to the enterprise's reputation.
- State actors might be the deadliest of all threat actors as they are highly skilled and have enough government resources to breach almost any security defense.

1.3 Vulnerabilities, Threats and Attacks

Threat Actors → 3) Nation-State Actors [2]

- Nation-State actors are often involved in multiyear intrusion campaign targeting highly sensitive economic, proprietary or national security information.
- The campaign have created a new class of attacks called advanced persistent threat (APT).
- The attacks use innovative tools (advanced) and once a system is infected, they silently extract data over an extended period of time (persistent).
- APTs are most commonly associated with state actors
- Motivation: Espionage, political, economic, or military
- Affiliation: Nation-states or organizations with nation-state ties
- Common TTPs: Spear-phishing password attacks, social engineering, direct compromise, data exfiltration, remote access trojans, and destructive malware.

Source: https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-cyber-threat-actors

1.3 Vulnerabilities, Threats and Attacks

Threat Actors → 4) Insiders [2]

- Serious threat to an enterprise comes from its own employees, contractors, and business partners, called insiders, who pose as insider threat of manipulating data from the position of a trusted employee.
- Six of out 10 enterprises reported being a victim of at least one insider attack during 2019. The focus of the insiders are intellectual property (IP) theft (43%), sabotage (41%), and espionage (32%).
- Motivation: Financial gain or to seek revenge
- Affiliation: Current or former employee, contractor, or other partner who has authorized access.
- Common TTPs: data exfiltration or privilege misuse

Source: https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-cyber-threat-actors

1.3 Vulnerabilities, Threats and Attacks

Threat Actors → 5) Cybercriminals

- Cybercriminals are largely profit-driven and represent a long-term, global, and common threat. They target data to sell, hold for ransom, or otherwise exploit for monetary gain. Cybercriminals may work individually or in groups to achieve their purposes.
- Motivation: Financial gain or reputation enhancement
- Affiliation: Individuals or with collaborators
- Common TTPs: Phishing, social engineering, business email compromise (BEC) scams, botnets, password attacks, exploit kits, malware, ransomware

Source: https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-cyber-threat-actors

1.3 Vulnerabilities, Threats and Attacks

Attacks – Theoretical Concepts [1]

- The principle of security faces threats from various attacks. These attacks are generally classified into four categories. They are:
  - Interception → compromising confidentiality
  - Fabrication → compromising authentication
  - Modification→ compromising integrity
  - Interruption → compromising availability
- These attacks are further grouped into two types: passive attacks and active attacks.

1.3 Vulnerabilities, Threats and Attacks

Attacks – Theoretical Concepts

Passive Attack

- Attempts to learn or make use of information from the system but does not affect system resources
- Eavesdropping on, or monitoring of data transmissions
- Goal of attacker is to obtain information that is being transmitted
- Two types of passive attacks (interception):
  - **Release of message contents**
  - **Traffic analysis**

Active Attack

- Attempts to alter system resources or affect their operation
- Involve some modification of the data stream or the creation of a false stream
- Three categories:
  - **Fabrication (Masquerade)**
  - **Modification**
    - **Replay attacks**
    - **Alterations**
  - **Interruption (DoS attacks)**

1.3 Vulnerabilities, Threats and Attacks

Attack Vectors [2]

- An attack vector is a pathway or avenue used by a threat actor to penetrate a system.
- Attack vectors categories:
  - Email
  - Wireless
  - Removable Media
  - Direct Access
  - Social Media
  - Supply Chain
  - Cloud

1.3 Vulnerabilities, Threats and Attacks

Attack Vectors → 1) Email [2]

- Almost 94 percent of all malware is delivered through email to an unsuspecting user. The goal is to trick the user to open an attachment that contains malware or click a hyperlink that takes the user to a fictitious website.

Attack Vectors → 2) Wireless [2]

- Because wireless data transmissions “float” through the airwaves, they can be intercepted and read or altered by a threat actor if the transmission is not properly protected.

1.3 Vulnerabilities, Threats and Attacks

Attack Vectors → 3) Removable Media [2]

- A removable media device, such as a USB flash drive, is a common attack vector. Threat actors have been known to infect USB flash drives with malware and leave them scattered in a parking lot or cafeteria. A well-intentioned employee will find the drive and insert it into his computer to determine its owner. However, once inserted, the USB flash drive will infect the computer.

1.3 Vulnerabilities, Threats and Attacks

Attack Vectors → 4) Direct Access [2]

- A direct access vector occurs when a threat actor can gain direct physical access to the computer. Once the attacker can "touch" the machine, she can insert a USB flash drive with an alternative operating system and reboot the computer under the alternate OS to bypass the security on the computer.

1.3 Vulnerabilities, Threats and Attacks

Attack Vectors → 5) Social Media [2]

- Threat actors often use social media as a vector for attacks. For example, an attacker may read social media posts to determine when an employee will be on vacation and then call the organization's help desk pretending to be that employee to ask for "emergency" access to an account.

1.3 Vulnerabilities, Threats and Attacks

Attack Vectors → 6) Supply Chain [2]

- A supply chain is a network that moves a product from the supplier to the customer and is made up of vendors that supply raw material, manufacturers who convert the material into products, warehouses that store products, distribution centers that deliver them to the retailers, and retailers who bring the product to the consumer.
- Today's supply chains are global in scope: manufacturers are usually thousands of miles away overseas and not under the direct supervision of the enterprise selling the product.

1.3 Vulnerabilities, Threats and Attacks

Attack Vectors → 6) Supply Chain [2]

- The fact that products move through many steps in the supply chain—and that some steps are not closely supervised—has opened the door for malware to be injected into products during their manufacturing or storage (called supply chain infections).
- Supply chains also serve as third-party vulnerabilities

1.3 Vulnerabilities, Threats and Attacks

Attack Vectors → 7) Cloud [2]

- As enterprises move their computing resources to remote cloud servers and storage devices, threat actors take advantage of the complexity of these systems to find security weaknesses

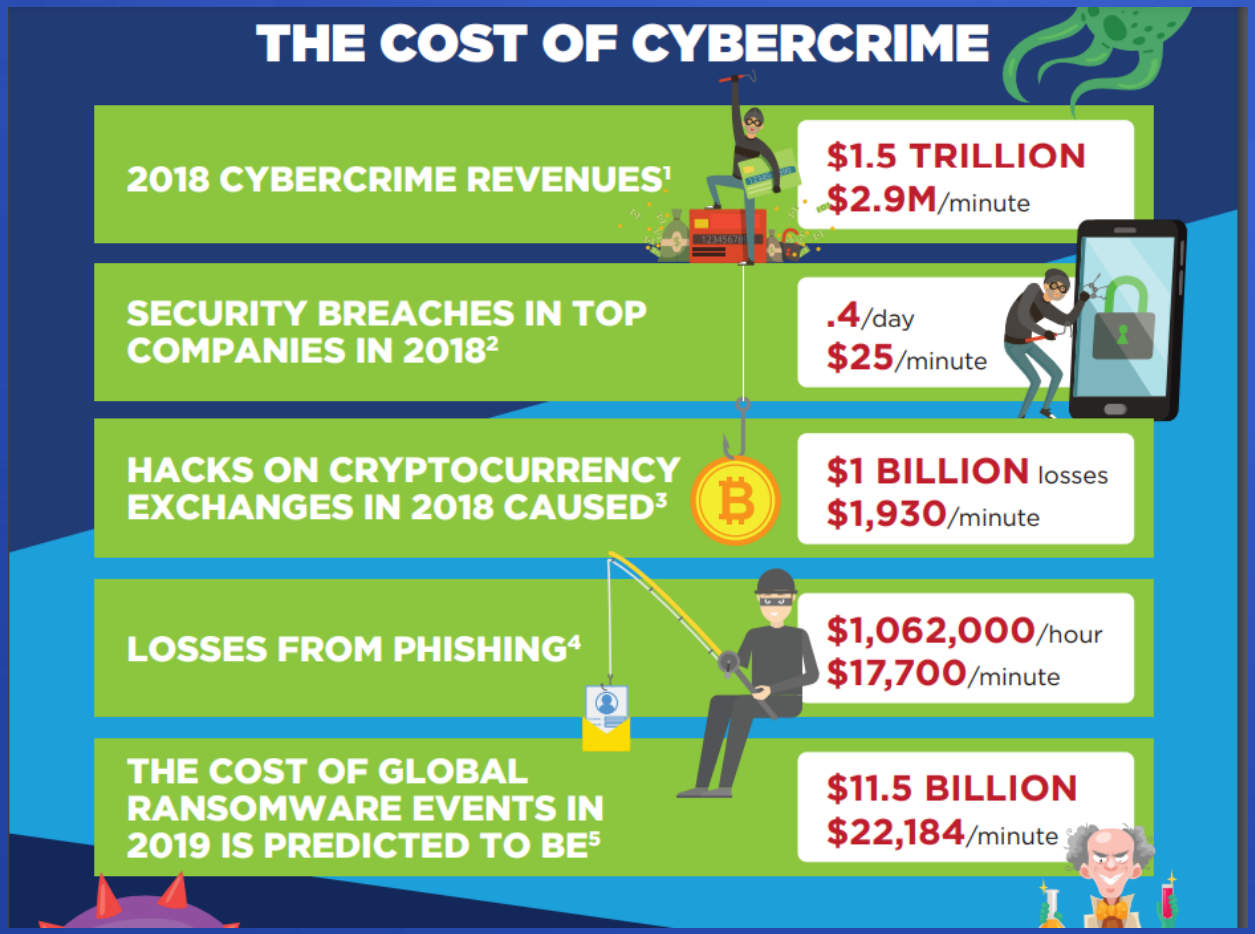
1.4 Security Functional Requirement

- Security Functional Requirement (SFR) describes functional behaviour (what a system has to do) that enforces security.
- Security functional requirement may include functional requirement related to access control, data integrity, authentication and wrong password lockouts.
- SRF is needed to comply to external regulatory requirements (Common Criteria for Information Technology Security Evaluation, referred to as Common Criteria or CC – international standard (ISO/IEC 15408)), in addition to adopting security best practices internally among developers.

Source: https://www.synopsys.com/blogs/software-security/software-security-requirements/

1.5 Computer Security Trends

- The cost of cybercrime is ever increasing.

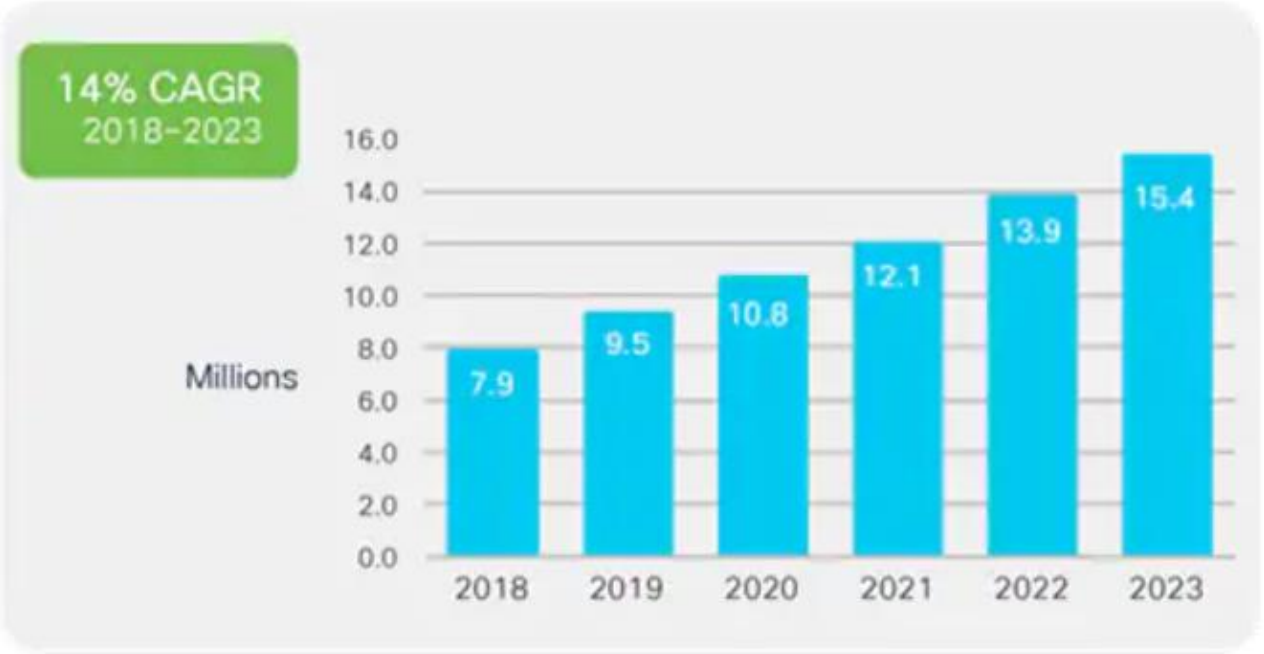


Source: https://www.riskiq.com/wp-content/uploads/2020/07/Evil-Internet-Minute-RiskIQ-Infographic-2019.pdf

1.5 Computer Security Trends

- The cyber attack will never stop.

Figure 21. Number of DDoS attacks: Attacks will double to 15.4 million by 2023 globally



Source: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

1.5 Computer Security Trends

- Live Cyber Attack Maps.
  - https://threatmap.checkpoint.com/
  - https://livethreatmap.radware.com/
  - https://threatmap.bitdefender.com/
  - https://cybermap.kaspersky.com/

1.5 Computer Security Trends

New Targets for Attacks

- Banks, e-commerce and databases will continue to be attacked with new targets as shown below:
  - Critical Infrastructure
  - Digital Assets
  - Higher Education
  - Online Gambling
  - Supply Chain

Source: https://www.purdueglobal.edu/blog/information-technology/cybersecurity-trends/

1.5 Computer Security Trends

New Types of Attacks

- Phishing and Social Engineering top causes of breaches
- 85% of attacks involved a human element, such as responding to a scam email or clicking on a link
- Due to remote work during the Covid-19 pandemic, cybercrime has gone up to 600%
- Attacks are getting more sophisticated
  - Phishing emails and malicious URLs are more specific, personalized, and geo-targeted.
  - Focus on mobile users, exploiting their vulnerabilities to access other platforms

Source: https://www.purdueglobal.edu/blog/information-technology/cybersecurity-trends/

1.5 Computer Security Trends

New Tactics in Security

- More companies are adopting “assume breach” mindset, meaning not trusting anything on or off the company network. This will encourage businesses to emphasize compliance with security policies, including how to spot a phishing attempt or how to respond to ransomware.
- More companies will adopt security solutions related to artificial intelligence (AI). With the adoption of AI and machine learning, less human effort is needed to anticipate and respond to attacks quickly.

Source: https://www.purdueglobal.edu/blog/information-technology/cybersecurity-trends/

1.5 Computer Security Trends

New Regulations to Come

- Governments will continue to tighten cybersecurity.
- Modern privacy laws will cover personal digital information of 75% of the world's population by the end of 2023.
- 30% of the world's governments are expected to pass legislation to regulate ransomware payments, fines, and negotiation by end of 2025.
- Organizations will have to demonstrate a high level of cybersecurity to obtain cyberinsurance coverage. Challenge: 77% of organizations do not have a cybersecurity incident response plan.
- New cryptocurrency regulation in several countries will discourage ransomware.

Source: https://www.purdueglobal.edu/blog/information-technology/cybersecurity-trends/

1.6 Computer Security Strategy

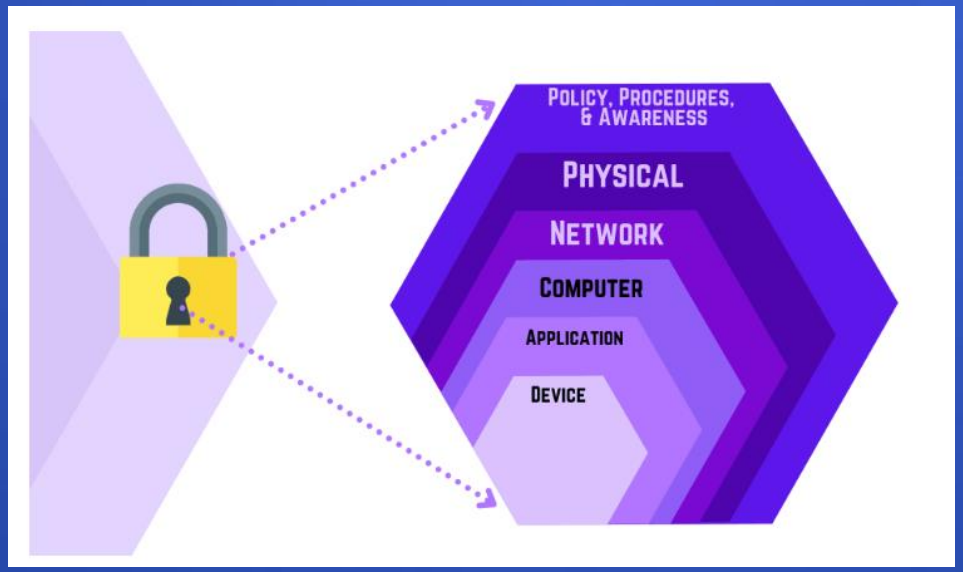
- Computer Security Strategy or known as Cyber Security Strategy nowadays is a plan that involves selecting and implementing best practices to protect a business from internal and external threat.

- **Defense in Depth Strategy** is implemented to effectively manage emerging threats and risks.

Source: https://purplesec.us/learn/cyber-security-strategy/#What

1.6 Computer Security Strategy

- The goal of implementing Defense In Depth Strategy encompasses the layering of security defenses.
- A combination of multiple security tools may be implemented, such as antivirus, anti-spam, VPN, and a host firewall.



Source: https://purplesec.us/learn/cyber-security-strategy/#What

1.6 Computer Security Strategy

Zero Trust Security + Defense in Depth

- Company must have resources available to support and monitor the functionality of the security tools used for defense in depth. This may introduce additional complexity.
- To address this issue, a zero trust model should be implemented as well.
- Zero trust implies, never trust, always verify.
- Multifactor Authentication and machine learning are components of zero trust, which provides company with visibility on who and how the assets are being utilized within the network.

Source: https://purplesec.us/learn/cyber-security-strategy/#What

1.6 Computer Security Strategy

Information Security Policy

- An important element of an effective security strategy is the **information security policy.**

- Security policies are a set of written practices and procedures that all employees must follow to ensure the confidentiality, integrity, and availability of data and resources. Security policies provide what the expectations are for business, how they are to be achieved, and describe the consequences for failure with the goal of protecting organizations.

- Many organizations opt for specific policy instead of one large policy, to make it easier for users to digest.

Source: https://purplesec.us/learn/cyber-security-strategy/#What

1.6 Computer Security Strategy

Information Security Policy

- Examples of information security policy:
  - Network Security Policy
  - Workstation Policy
  - Acceptable Use Policy
  - Clean Desk Policy
  - Remote Access Policy
  - Password Policy
  - Account Management Policy
  - Email Security Policy
  - Security Incident Management Policy
  - Log Management Policy
  - Personal Device Acceptable Use And Security (BYOD) Policy
  - Patch Management Policy
  - Server Security Policy
  - Systems Monitoring and Auditing Policy

Source:
https://purplesec.us/learn/cyber-security-strategy/#What
https://purplesec.us/network-security-policies/

1.6 Computer Security Strategy

Information Security Policy → 1) Network Security Policy

- These are a general set of security policy templates that set of standardized practices and procedures that outlines rules of network access, the architecture of the network, and security environments, as well as determine how policies are enforced.

Source:
https://purplesec.us/learn/cyber-security-strategy/#What
https://purplesec.us/network-security-policies/

1.6 Computer Security Strategy

Information Security Policy → 2) Workstation Policy

- General security (use an antivirus, lock unattended, password usage, patching)

Information Security Policy → 3) Acceptable Use Policy

- Acceptable/unacceptable Internet browsing and use
- Acceptable/unacceptable email use
- Acceptable/unacceptable usage of social networking
- Electronic file transfer of confidential information

Source:
https://purplesec.us/learn/cyber-security-strategy/#What
https://purplesec.us/network-security-policies/

1.6 Computer Security Strategy

Information Security Policy → 4) Clean Desk Policy

- Describes reasons for a clean, uncluttered desk that may have sensitive notes laying on a desk or taped to monitors.

Information Security Policy → 5) Remote Access Policy

- Definition of remote access
- Who is permitted (employees/vendors)
- Types of permitted devices/operating systems
- Methods permitted (Remote access VPN, site-to-site VPN)

Source:
https://purplesec.us/learn/cyber-security-strategy/#What
https://purplesec.us/network-security-policies/

1.6 Computer Security Strategy

Information Security Policy → 6) Password Policy

- The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Information Security Policy → 7) Account Management Policy

- The purpose of this policy is to establish a standard for the creation, administration, use, and removal of accounts that facilitate access to information and technology resources at the company.

Source:
https://purplesec.us/learn/cyber-security-strategy/#What
https://purplesec.us/network-security-policies/

1.6 Computer Security Strategy

Information Security Policy → 8) Email Security Policy

- The purpose of this policy is to establish rules for the use of the company email for sending, receiving, or storing of electronic mail.

Information Security Policy → 9) Log Management Policy

- Log management can be of great benefit in a variety of scenarios, with proper management, to enhance security, system performance, resource management, and regulatory compliance.

Source:
https://purplesec.us/network-security-policies/

1.6 Computer Security Strategy

Information Security Policy → 10) Security Incident Management Policy

- This policy defines the requirement for reporting and responding to incidents related to the company's information systems and operations. Incident response provides the company with the capability to identify when a security incident occurs. If monitoring were not in place, the magnitude of harm associated with the incident would be significantly greater than if the incident were noted and corrected.

Source:
https://purplesec.us/network-security-policies/

1.6 Computer Security Strategy

Information Security Policy → 11) Personal Device Acceptable Use And Security (BYOD) Policy

- This policy defines the standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data using their personal device. This policy applies to, but is not limited to, any mobile devices owned by any users listed above participating in the company BYOD program which contains stored data owned by the company.

Source:
https://purplesec.us/network-security-policies/

1.6 Computer Security Strategy

Information Security Policy → 12) Patch Management Policy

- Security vulnerabilities are inherent in computing systems and applications. These flaws allow the development and propagation of malicious software, which can disrupt normal business operations, in addition to placing companies at risk. In order to effectively mitigate this risk, software "patches" are made available to remove a given security vulnerability.

Source:
https://purplesec.us/network-security-policies/

1.6 Computer Security Strategy

Information Security Policy → 13) Server Security Policy

- The purpose of this policy is to define standards and restrictions for the base configuration of internal server equipment owned and/or operated by or on the company's internal network(s) or related technology resources via any means.

Source:
https://purplesec.us/network-security-policies/

1.6 Computer Security Strategy

Information Security Policy → 14) Systems Monitoring And Auditing Policy

- System monitoring and auditing is used to determine if inappropriate actions have occurred within an information system. System monitoring is used to look for these actions in real time while system auditing looks for them after the fact.

Source:
https://purplesec.us/network-security-policies/

1.6 Computer Security Strategy

Example of an information security policy template.

https://purplesec.us/wp-content/uploads/2021/02/Comprehensive-IT-Security-Policy-Template.pdf

1.6 Computer Security Strategy

Steps to implement a successful computer or cyber security strategy: [will go through in detail in Chapter 7 and Chapter 8]

- Conduct A Security Risk Assessment
- Set Your Security Goals
- Evaluate Your Technology
- Select A Security Framework
- Review Security Policies
- Create A Risk Management Plan
- Implement Your Security Strategy
- Evaluate Your Security Strategy

Source: https://purplesec.us/learn/cyber-security-strategy/#What

Main References

[1] Chauhan, S. R., and Jangra S., 2020, Computer Security and Encryption: An Introduction, Mercury Learning & Information. https://tarc.idm.oclc.org/login?url=https://ebookcentral.proquest.com/lib/tarc-ebooks/detail.action?docID=6404902

[2] Mark Ciampa. 2022. CompTIA Security+ Guide To Network Security Fundamentals. Cengage Learning.