REVIEWER: INFORMATION ASSURANCE AND SECURITY

MODULE 1 PART 1: INTRODUCTION TO INFORMATION ASSURANCE AND SECURITY 1

ISO STANDARD -According to ISO (International Standard Organization) / IEC (International Electrotechnical Commission) standard 9126 – 1 (Software Engineering, Product Quality), the following are all aspects of system quality:

- FUNCTIONALITY
- USABILITY
- RELIABILITY
- PERFORMANCE
- SECURITY

INFORMATION ASSURANCE

Information in computer terms may tend be.

- Useful
- Gathered
- The result of processing data
- Assurance on the other hand means a positive declaration intended to give confidence or a promise.

INFORMATION ASSURANCE (IA)

is the study of how to protect your information assets from destruction, degradation, manipulation, and exploitation. But also, how to recover should any of those happen. Notice that it is both proactive and reactive.

BASIC SECURITY ISSUES

- **Availability** – timely, reliable access to data and information services for authorized users.
- **Integrity** – protection against unauthorized modification or destruction of information.
- **Confidentiality** - assurance that the information is not disclosed to unauthorized person.
- **authentication** – security measures to establish the validity of a transmission, message, or originator.
- **Non-repudiation** – assurance that the sender is provided with proof of a data delivery and recipient is provided with proof of the sender's identity, so that neither can later deny having processed the data.

DIFFERENT VIEW ON IA

According to **Debra Herrmann**, IA should be viewed as spanning four security engineering domains:

- Physical security
- Personnel security
- IT security
- Operational security

So, threats/risks to IA should be considered along these dimensions as well.

PHYSICAL SECURITY

- Locking sensitive documents in a safe

PERSONNEL SECURITY

- Stationing a marine guard outside an embassy

IT SECURITY

- encrypting your hard drive
- Using SSL (Secure Sockets Layer) for data transfers
- Having off-site backup of documents

OPERATIONAL SECURITY

- Enforcing hard-to-guess passwords
- Assigning security clearances to staffers

FOUR SECURITY CATEGORIES

PHYSICAL SECURITY

refers to the protection of hardware, software, and data against physical threats to reduce or prevent disruptions to operations and services and loss of assets.

PERSONNEL SECURITY

is a variety of ongoing measures taken to reduce the likelihood and severity of accidental and intentional alteration, destruction, misappropriation, misuse, misconfiguration, unauthorized distribution, and unavailability of an organization's logical and physical assets, as the result of action or inaction by insiders and known outsiders, such as business partners.

IT SECURITY

is the inherent technical features and functions that collectively contribute to an IT infrastructure achieving and sustaining confidentiality, integrity, availability, accountability, authenticity and reliability.

OPERATIONAL SECURITY

involves the implementation of standard operational security that defines the nature and frequency of the interaction between users, systems and system resources.

ANOTHER VIEW ON IA

According to Raggad's taxonomy of information security, a computing environment is made up of five continuously interacting components:

- Activities
- People
- Data
- Technology
- Networks

SECURITY STRATEGIES

- Risk Assessment and Management
- Access Control
- Encryption and Data Protection
- Incident Response and Recovery
- Security Awareness and Training
- Security Policies and Procedures

MODULE 1 – PART 2:

COMPUTER SECURITY

DIFFERENT ELEMENTS IN COMPUTER SECURITY

CONFIDENTIALITY
Confidentiality is the concealment of information or resources. Also, there is a need to keep information secret from other third parties that want to have access to it, so just the right people can access it.

INTEGRITY
Integrity is the trustworthiness of data in the systems or resources by the point of view of preventing unauthorized and improper changes.

Integrity is composed of two sub-elements – data-integrity, which it has to do with the content of the data and authentication which has to do with the origin of the data as such information has values only if it is correct.

AVAILABILITY
Availability refers to the ability to access data of a resource when it is needed, such as the information has value only if the authorized people can access at right time. Denying access to data nowadays has become a common attack. Imagine a downtime of a live server how costly it can be.

TERMINOLOGIES IN COMPUTER SECURITY

Unauthorized access − An unauthorized access is when someone gains access to a server, website, or other sensitive data using someone else's account details.

Hacker − Is a Person who tries and exploits a computer system for a reason which can be money, a social cause, fun etc.

Threat − Is an action or event that might compromise the security.

Vulnerability − It is a weakness, a design problem or implementation error in a system that can lead to an unexpected and undesirable event regarding security system.

Attack − Is an assault on the system security that is delivered by a person or a machine to a system. It violates security.

Antivirus or Antimalware − Is a software that operates on different OS which is used to prevent from malicious software.

Social Engineering − Is a technique that a hacker uses to stole data by a person for different for purposes by psychological manipulation combined with social scenes.

Virus − It is a malicious software that installs on your computer without your consent for a bad purpose.

Firewall − It is a software or hardware which is used to filter network traffic based on rules.

MAIN OBJECTIVES OF COMPUTER SECURITY

CONFIDENTIALITY

- of data (secrecy)
- of persons (privacy)
- access only by authorized parties

INTEGRITY

- data only correctly modified or deleted by authorized parties
- Availability
- correctly accessible in a timely manner
- the failure to meet this goal is called a denial of service

TOOLS FOR COMPUTER SECURITY

Tools for confidentiality Overview

- Authorization - Access policies - access control
- Authentication – identification
- Passwords
- Encryption - Virtual private networking
- Auditing – logging
- Backups
- Checksums
- Antivirus
- Disaster recovery planning
- Physical protections
- Anti-theft
- Uninterruptible Power Supply
- Redundancies
- Intrusion-detection systems
- Antivirus software
- Firewall

TOOLS FOR CONFIDENTIALITY

- Don't share them
- Not even with computer administrators
- Don't write them down
- Don't reuse them among different sites
- Change them often

Select wise:

- Easy to remember
- Hard to guess (resistant to dictionary attacks)
- Password length
- Large set of characters (caps, lower case, numbers, symbols)

Some notorious password leaks

- 2014: 5M Gmail passwords
- 2013: 38M Adobe passwords (and source code)
- 2013: 250K Twitter passwords
- 2012: 12M Apple User IDs stolen by FBI, 1M leaked
- 2012: 6M LinkedIn passwords
- 2012: 450K plaintext Yahoo passwords
- 2012: 1.5M plaintext Youporn passwords
- 2009: 10K MS Hotmail, MSN and Live passwords

BIOMETRIC IDENTIFICATION

- Fingerprint
- Voice print
- Iris scan
- Retinal scan

Danger of biometric identification

- You can't change your biometric password once it got leaked
- You can't legally refuse to give it, unlike a password (US fifth amendment)

TOOLS FOR CONFIDENTIALITY

- Lock your screen when you leave
- Cryptography Secret Writing
- Ciphertext (Cipher text is what encryption algorithms, or ciphers, transform an original message into.)
- Encryption Algorithm
- Asymmetric Encryption
- Public Key Encryption
- Digital Signature
- Avoid non encrypted protocols
- Virtual Private Network
- Private Browsing
- Apply software Updates
- Scan for Malware

BACKUPS

- Use off-site data protection = vaulting e.g., remote backup (compression, encryption!)
- First time and sometimes: full backup
- Most often: only incremental backup
- Use a good data retention scheme
- e.g., 7 daily, 4 weekly, 12 monthly, all yearly backups
- Reflect about your time for full restore.
- Test the restore procedure!
- “80% of backups fail to restore.”

INTEGRITY

DATA INTEGRITY

refers to the accuracy, consistency, and reliability of data over its entire lifecycle. It ensures that data remains unchanged and uncorrupted during storage, processing, and transmission.

KEY ASPECTS OF DATA INTEGRITY

- Preventing Unauthorized Changes
- Detecting Tampering
- Ensuring Data Accuracy
- Securing Data in Transit

COMMON THREATS TO DATA INTEGRITY

Malware and Viruses - Malicious software, such as viruses, worms, and Trojans, can infect systems and corrupt or steal data.

Data Breaches - Unauthorized access to sensitive data by hackers or insiders can lead to data theft, manipulation, or exposure.

Human Error- Mistakes made by employees or users, such as accidental data deletion or improper data entry, can compromise data integrity.

Hardware Failures - Hardware components, including hard drives and memory modules, can fail and result in data corruption or loss.

Cyberattacks - Cyberattacks like Distributed Denial of Service (DDoS) and ransomware can disrupt data availability and lead to data loss or corruption.

DATA ENCRYPTION

is the process of converting data into a coded or unreadable format, to protect it from unauthorized access. Encryption is a fundamental tool for ensuring data integrity and confidentiality.

Methods of Data Encryption There are various encryption methods, including:

Symmetric Encryption - Uses a single key for both encryption and decryption, e.g., AES (Advanced Encryption Standard).

Asymmetric Encryption - Utilizes a pair of public and private keys for encryption and decryption, e.g., RSA (Rivest-Shamir-Adleman).

End-to-End Encryption - Ensures that data is encrypted on the sender's side and can only be decrypted by the intended recipient, e.g., Signal Messenger.

A **Hash function** is a mathematical algorithm that takes an input (or "message") and returns a fixed-size string of characters, which is typically a hexadecimal number. The output, known as the hash value or digest, is unique to the input data, making it a valuable tool for data integrity.

PASSWORD STORAGE

When a user creates a password, it is run through a hash function and the resulting hash is stored in the database. When the user logs in, the entered password is hashed and compared to the stored hash. If they match, the login is successful.

FILE VERIFICATION

Popular software like WinMD5 and HashTab calculate and display hash values for files, allowing users to verify the file's integrity. For example, an SHA-256 hash value can be provided for a downloadable file, and users can verify it using hash functions

ACCESS CONTROL and **AUTHENTICATION** are essential components of data integrity and security. They involve mechanisms and processes for verifying the identity of users and regulating their access to data, systems, or resources.

ACCESS CONTROL METHODS

Access control mechanisms can be implemented in various ways, including role-based access control (RBAC), mandatory access control (MAC), and discretionary access control (DAC).

● Role-Based Access Control (RBAC)

In an organization, RBAC assigns specific roles (e.g., admin, user, manager) to individuals. These roles determine their access privileges. For example, an admin can access and modify all data, while a user has limited access.

AUTHENTICATION METHODS

Authentication methods include something you know (e.g., passwords), something you have (e.g., smart cards or tokens), something you are (e.g., biometrics), and multi-factor authentication (MFA) combining two or more of these methods.

● Multi-Factor Authentication (MFA)

Many online services, like Google and online banking, offer MFA. After entering a password, users receive a one-time code on their mobile device, which they must enter to access their accounts. This extra authentication layer enhances security.

AVAILABILITY

is one of the core principles of the CIA Triad. It refers to the concept that information and systems should be accessible and usable by authorized individuals whenever needed. The goal is to ensure that data and services are consistently available, preventing disruptions due to various threats.

Distributed Denial of Service (DDoS) Attacks: Explain how DDoS attacks flood a system with traffic to overwhelm and disrupt its services.

● The 2016 Dyn cyberattack, where major websites like Twitter and Netflix were rendered temporarily unavailable due to a massive DDoS attack.

Hardware Failures: Discuss how hardware components, such as hard drives or power supplies, can fail unexpectedly.

● The British Airways IT outage in 2017, caused by a power supply issue, which resulted in canceled flights and inconvenience to thousands of passengers.

Natural Disasters: Explain that natural disasters like earthquakes, hurricanes, and floods can disrupt data centers and infrastructure.

● Hurricane Katrina in 2005 severely affected data center availability, leading to data loss and downtime for many organizations.

Methods for Ensuring Availability

● Redundancy

● Disaster Recovery Plans

● Load Balancing

MODULE 2: CYBER SECURITY

CYBER SECURITY IS SAFETY

Security: We must protect our computers and data in the same way that we secure the doors to our homes.

Safety: We must behave in ways that protect us against risks and threats that come with technology.

LEADING THREATS

- Viruses
- Worms
- Trojan Horses / Logic Bombs
- Social Engineering
- Rootkits
- Botnets / Zombies

VIRUSES

◉ A virus attaches itself to a program, file, or disk.

◉ When the program is executed, the virus activates and replicates itself.

◉ The virus may be benign or malignant but executes its payload at some point (often upon contact). Viruses can cause computer crashes and loss of data.

◉ In order to recover or prevent virus attacks:

- Avoid potentially unreliable websites/emails.
- System Restore.
- Re-install operating system.
- Use and maintain anti-virus software.

WORMS

- Independent program that replicates itself and sends copies from computer to computer across network connections.
- Upon arrival, the worm may be activated to replicate.

LOGIC BOMBS AND TROJAN HORSES

LOGIC BOMB:

Malware logic executes upon certain conditions. The program is often used for otherwise legitimate reasons.

EXAMPLES:

Software which malfunctions if maintenance fee is not paid.

Employee triggers a database erase when he is fired. •

TROJAN HORSE

Masquerades as a benign program while quietly destroying data or damaging your system.

Download a game: It may be fun but contains hidden code that gathers personal information without your knowledge.

SOCIAL ENGINEERING

Social engineering manipulates people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems

PHISHING: COUNTERFEIT EMAIL

PHISHING

A seemingly trustworthy entity asks for sensitive information such as SSN, credit card numbers, login IDs or passwords via e-mail.

PHARMING: COUNTERFEIT WEB PAGES

The link provided in the e-mail leads to a counterfeit webpage which collects important information and submits it to the owner.

• The counterfeit web page looks like the real thing

• Extracts account information

MAN IN THE MIDDLE ATTACK

• An attacker pretends to be your final destination on the network. When a person tries to connect to a specific destination, an attacker can mislead him to a different service and pretend to be that network access point or server.

ROOTKIT

◉ Upon penetrating a computer, a hacker may install a collection of programs, called a rootkit.

◉ May enable:

- Easy access for the hacker (and others) into the enterprise
- Keystroke logger

◉ Eliminates evidence of break-in.

◉ Modifies the operating system.

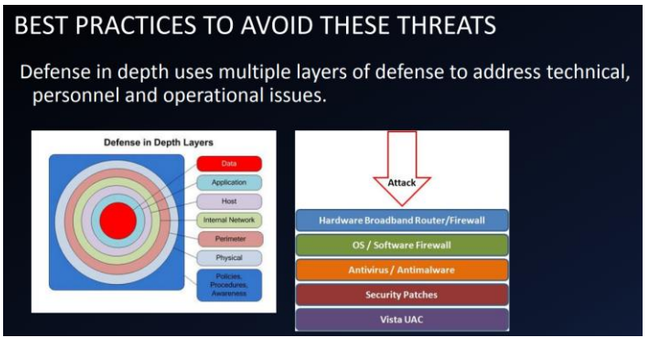
IDENTIFYING SECURITY COMPROMISES

◉ Symptoms:

- Antivirus software detects a problem.
- Disk space disappears unexpectedly.
- Pop-ups suddenly appear, sometimes selling security software.
- Files or transactions appear that should not be there.
- The computer slows down to a crawl.
- Unusual messages, sounds, or displays on your monitor.
- Stolen laptop: 1 stolen every 53 seconds; 97% never recovered.
- The mouse pointer moves by itself.
- The computer spontaneously shuts down or reboots.
- Often unrecognized or ignored problems.

MALWARE DETECTION

• Spyware symptoms:
• Changes to your browser homepage/start page.
• Ending up on a strange site when conducting a search.
• System-based firewall is turned off automatically.
• Lots of network activity while not particularly active.
• Excessive pop-up windows.
• New icons, programs, favorites which you did not add.
• Frequent firewall alerts about unknown programs when trying to access the Internet.
• Poor system performance.



ANTI-VIRUS AND ANTI-SPYWARE SOFTWARE

• Anti-virus software detects certain types of malwares and can destroy it before any damage is done.
• Install and maintain anti-virus and anti-spyware software.
• Be sure to keep anti-virus software updated.
• Many free and commercial options exist.
• Contact your Technology Support Professional for assistance.

HOST-BASED FIREWALLS

• A firewall acts as a barrier between your computer/private network and the internet. Hackers may use the internet to find, use, and install applications on your computer. A firewall prevents many hacker connections to your computer.
• Firewalls filter network packets that enter or leave your computer

PROTECT YOUR OPERATING SYSTEM

- Microsoft regularly issues patches or updates to solve security problems in their software. If these are not applied, it leaves your computer vulnerable to hackers.
- The Windows Update feature built into Windows can be set up to automatically download and install updates.
- Avoid logging in as administrator
- Apple provides regular updates to its operating system and software applications.
- Apply Apple updates using the App Store application.

USE STRONG PASSWORDS

• Make passwords easy to remember but hard to guess • USG standards:
• Be at least ten characters in length
• Must contain characters from at least two of the following four types of characters:
• English upper case (A-Z)
• English lower case (a-z)
• Numbers (0-9)
• Non-alphanumeric special characters ($, !, %, ^, …)
• Must not contain the user's name or part of the user's name
• Must not contain easily accessible or guessable personal information about the user or user's family, such as birthdays, children's names, addresses, etc.

AVOID SOCIAL ENGINEERING AND MALICIOUS SOFTWARE

• Do not open email attachments unless you are expecting the email with the attachment and you trust the sender.
• Do not click on links in emails unless you are absolutely sure of their validity.
• Only visit and/or download software from web pages you trust.

AVOID HACKER TRICKS

◉ Be sure to have a good firewall or pop-up blocker installed.
◉ Pop-up blockers do not always block ALL pop-ups so always close a pop-up window using the 'X' in the upper corner.
◉ Never click "yes," "accept" or even "cancel."
◉ Infected USB drives are often left unattended by hackers in public places

SECURE BUSINESS TRANSACTIONS

◉ Always use secure browser to do online activities.
◉ Frequently delete temp files, cookies, history, saved passwords etc.

BACKUP IMPORTANT INFORMATION

◉ No security measure is 100% reliable.
◉ Even the best hardware fails.
◉ What information is important to you?
◉ Is your backup: Recent? Off-site & Secure? Process Documented? Encrypted? Tested?