NCC education®
Awarding Great British Qualifications

Network Security and Cryptography

Topic 1:

Network Security and Cryptography Fundamentals

The Unit Roadmap

Unit Aim: The unit to provide a comprehensive understanding of the fundamental principles, techniques, and best practices employed to safeguard computer networks from cyber threats. It explores the concepts of secure communication, cryptographic algorithms, encryption, and authentication protocols, etc. equipping learners with essential knowledge to protect network infrastructure and data integrity in an increasingly interconnected digital landscape.

Unit Syllabus

- **Network Security and Cryptography Fundamentals**
- Cryptography Techniques
- Operating System Security and Vulnerabilities
- Software Vulnerabilities and attacks
- Network Security and Defense
- Email and Web Security
- Firewalls
- VLAN and VPN
- Wireless Security
- Information Security Management

Unit Delivery

- The teacher-led time for this module is comprised of lectures and Tutorial/laboratory sessions.
- Lectures are designed to start each topic.
  - ✓ You will be encouraged to be active during lectures by raising questions and taking part in discussions.
- Tutorial/Laboratory sessions are designed to follow the respective topic lecture.
  - ✓ During these sessions, you will be required to work through practical tutorials and various exercises.

Private Study

- You are also expected to undertake private study to consolidate and extend your understanding.

- Exercises are provided in your Student Guide for you to complete during this time.

Assessment

This unit will be assessed by:

- An examination worth 50% of the total mark
- An assignment worth 50% of the total mark

Scope and Coverage

This topic will cover:

- What is Network Security?
- Principles of Network Security
- Model for Network Security
- Approaches of Network Security
- Introduction to Cryptography
- Cryptography Fundamentals

Learning Outcomes

By the end of this topic students will be able to:

- Demonstrate a systematic understanding of the concept of network security and cryptography.
- Understand the principle and model of network security.
- Identify different approaches for network security.
- Understand the role of cryptography in network security.

Introduction

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—The Art of War, Sun Tzu

What is Security?

In the most general terms, security could mean “protection of Person or Property (assets) against harm (threats.)”

- What assets?
- What kinds of threats?
- What does “protection” mean?
- Does the nature of protection vary depending on the threat?

Terminology

- **Asset:** is anything that has value
- **Threat:** is a type of action that has potential to cause harm
- **Threat Agent:** is a person or element that has the power to carry out the threat
- **Vulnerability:** is a flaw or weakness that allows a threat agent to bypass security
- **Exploit:** is the act of exploiting the security weakness

Security Attacks, Mechanisms & Services

- **Security Attack**

  Any action that compromises the security of information.

- **Security Mechanism**

  A process / device that is designed to detect, prevent or recover from a security attack.

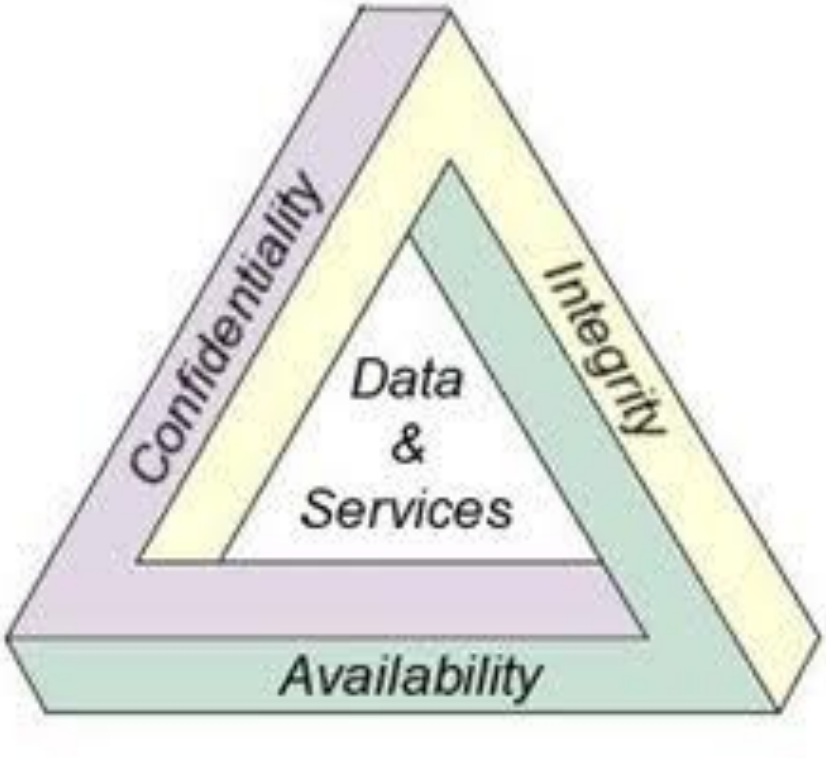
- **Security Service**

  A service intended to counter security attacks, typically by implementing one or more mechanisms.

Principle of Security - CIA Triad

C.I.A. Triangle – 3 key characteristics of information that must be protected:

- Confidentiality - only authorized parties can view private information
- Integrity - to preserve the accuracy and completeness of information and the methods that are used to process and manage it.
- Availability - information is accessible to authorized users whenever needed



Data Confidentiality

Examples

- Student records
- Patient records, etc.

How to ensure confidentiality?

- Cryptography
- Strong access control
- Limiting number of places where data can appear (only on servers, read-only, cannot be copied to USB sticks, etc.)

Data Integrity

Examples

- Patient information in a hospital – the doctor should be able to trust that the information is correct and current.
- Inaccurate info could result in serious harm to the patient and expose the hospital to massive liability.

How to ensure integrity?

- Strong access control
- Cryptography
- Documenting system activity

Data Availability

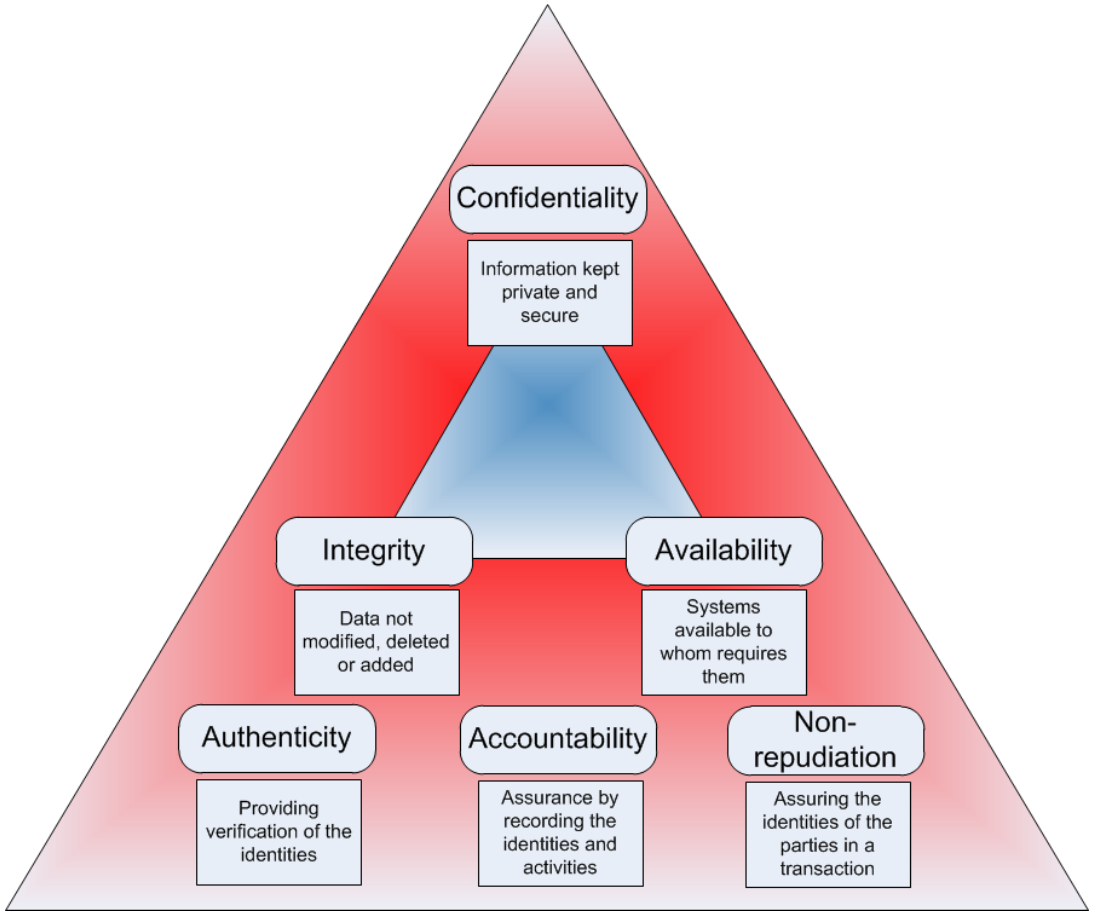
Examples

- Accessible and properly functioning web site – a key asset for an e-commerce company. A DoS attack could make the site unavailable and cause significant loss in revenue and reputation.

How to ensure availability?

- Well established backup procedure
- Effective data-recovery procedure
- Anti-DoS Systems

Extended CIA Triangle



Extended CIA Triangle

Authenticity: Proving that you are who you say you are.

Authentication may be obtained by the provision of a password or a scan of your retina.

Accountability: The traceability of actions performed on a system to a specific system entity (user, process, device).

Audit trails must be selectively kept and protected so that actions affecting security can be traced back to the responsible party.

Non-repudiation: The prevention of either the sender or the receiver denying a transmitted message.

System must be able to prove that certain messages were sent and received.

Goals of Attacker

- **Unauthorized Data Access**

  From business perspective: breach of data protection mandates (e.g., DPA2018, GDPR)

- **Espionage, Spying**

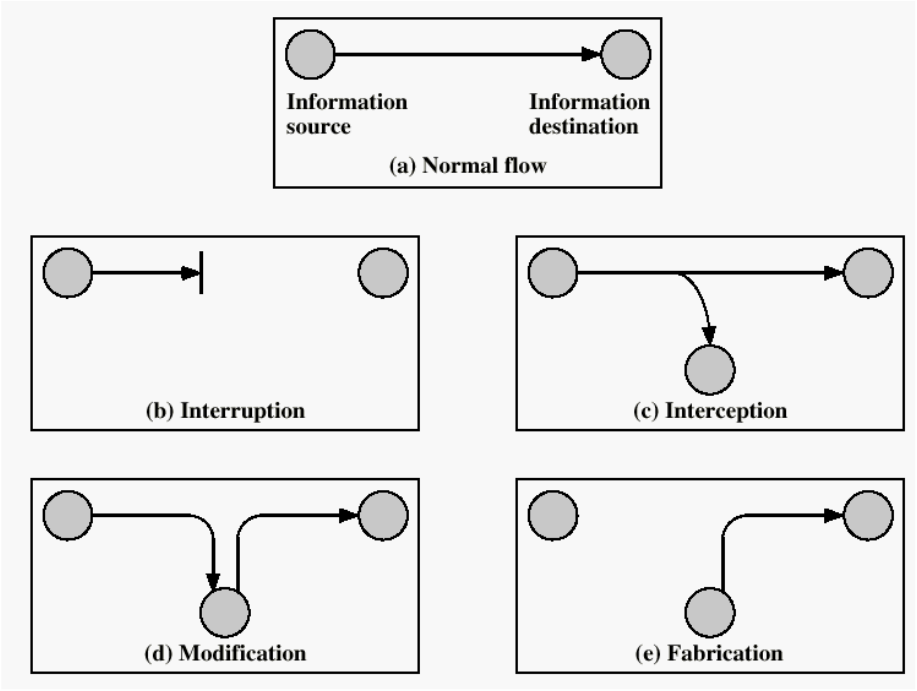
  Intellectual property, confidential information, privacy.

- **Denial of Service (DoS)**

  Disruption of businesses, financial loss.

Type of Security Attacks

- **Interruption:** This is an attack on availability
- **Interception:** This is an attack on confidentiality
- **Modification:** This is an attack on integrity
- **Fabrication:** This is an attack on authenticity



Class Activity

Which of the following forms of security attack is most severe?

- Interruption
- Interception
- Modification
- Fabrication

Create a group of 2-3 students, discuss and provide example why the selected form of attack is more severe.

Solution:

All forms of security attacks have the potential to cause significant damage, but the severity of an attack depends on the specific context and the consequences it produces. However, in terms of the potential impact without context, the most severe form of security attack among the options listed is likely "Interruption."

Let’s now see breakdown of each attack form and their potential severity

Interruption

- This form of attack aims to disrupt or deny the availability of a system, service, or network, rendering it inaccessible or unusable.
- Significant interruptions can lead to financial losses, reputational damage, and potential safety risks, depending on the affected system or service.
- Examples include Distributed Denial of Service (DDoS) attacks that overwhelm a network with traffic, rendering it inaccessible to legitimate users.

Interception

- Interception attacks involve unauthorized access to and monitoring of data transmissions between systems or networks.

- While interception can lead to the exposure of sensitive information and privacy breaches, it may not always cause immediate severe consequences, as the attacker's intentions and the specific data intercepted play a crucial role.

Modification

- Modification attacks involve unauthorized alterations or tampering with data or system configurations.
- The severity of this attack depends on the type of modifications made and the impact they have on the integrity and reliability of the affected systems or data.
- For example, unauthorized modification of critical system files can lead to system instability, data corruption, or the introduction of malicious code.

Fabrication:

- Fabrication attacks involve the creation or insertion of false or counterfeit information into a system or network.

- While fabrication attacks can lead to confusion, misinformation, or the compromise of system integrity, their severity may vary depending on the purpose and impact of the fabricated information.

Why the Increasing Number of Attacks?

- Increased connectivity
- Many valuable assets online
- Sophisticated attack tools and strategies available
- Faster detection of Vulnerabilities
- Delays in security updates
- User Confusion - Users are called upon to make difficult security decisions with little or no guidance
- Others?

Why Should We Care?

- Reputation
- Financial Loss
- Customer Loyalty
- Loss of Valuable Data
- Legal issues – Data Protection Regulations

Cyber Attacks on the Rise

According to the Cyber Security breaches survey, published by the Department for Culture Media & Sport:

- 46% of all UK businesses identified at least one cyber security breach or attack in the last 12 months.
- This rises to two-thirds among medium firms (66%) and large firms (68%).

Why Learn About Security?

- Curiosity
- Impact on our lives and world
- Job Prospect!
- Apply to all networks
- Change/ Reinvention

Human Aspect

- Refer to the role that people play in the security of network and information systems.
- This aspect of security recognizes that technology alone is not sufficient to protect sensitive data and systems.
- Human behavior, psychology, and interactions are equally important in safeguarding against security threats.

Physical Security

- Dumpster Diving which involves digging through trash to find information that can be useful in an attack.
- Inexpensive hardware such as USB flash drives, hard drives, CD-ROMS
- Memos – May help in impersonation
- Organizational charts – Gives away details of people in authority
- Phone directories
- Policy/system manuals
- Shoulder Surfing

Physical Security – Counter Measures

- Always put papers in shredder machine.
- Graphical Passwords.
- One-time passwords & Multi-factor authentication.
- Destroy your hardware's.
- **Training**

Class Activity

Could you tell me some relevant security incidents?

Example - British Airways

Typical unauthorized data access case:

- 400,000 affected customers.
- Stolen: Log in, payment card and travel booking details, name and address information.
- Payment page gives access to third- party scripts (with no protection).
- Vulnerability in third-party Javascript used on the website, exploited by a hacking group called Magecart.
- The third-party piece of Javascript (22 lines), Modernizr, sent data to baways.com.

£20M Fined

British Airways fined £20m over data breach

16 October 2020

Example - NHS

A denial of service (DoS) case:

- Hundreds of thousands computers (> 150 countries affected).
- Computer worm.
- Windows SMB protocol.
- Stolen NSA hacking tools/backdoor.
- DoublePulsar backdoor to create a persistent backdoor that was used to deliver the WannaCry ransomware.
- Using the EternalBlue exploit, the ransomware spread to every other unpatched computer on the network.
- Kill switch (visited some predefined website.)

12.10.18

WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled

https://www.nationalhealthexecutive.com/News/wannacry-cyber-attack-cost-the- nhs-92m-after-19000-appointments-were-cancelled

How to Protect from Cyber Attacks?

Protecting against cyber attacks involves implementing a multi-layered approach that addresses various aspects of security.

Broadly speaking, it is categorized as:

- Information Security
- Cybersecurity
- Network Security

Information Security

- Protects information from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Ensures the confidentiality, integrity, and availability of information.
- Involves policies, procedures, and technologies to secure information.

Cybersecurity

- Focuses on protecting computer systems, networks, and data from digital threats and attacks.
- Safeguards against malware, hacking, phishing, ransomware, and other cyber threats.
- Includes measures like antivirus software, firewalls, intrusion detection systems, and security awareness training.

Network Security

- Concentrates on protecting the integrity and confidentiality of computer networks and their data.
- Prevents unauthorized access, misuse, or modification of network resources.
- Utilizes measures like firewalls, VPNs, network segmentation, access controls, and encryption.

Comparison

- Information security is a broader term that encompasses cybersecurity and network security.
- Cybersecurity specifically deals with digital threats and attacks, while network security focuses on securing computer networks and their data.
- Information security applies to all types of information, while cybersecurity and network security are specific to computer systems, networks, and data.
- Cybersecurity includes measures like antivirus software, intrusion detection systems, and security awareness training, while network security includes technologies like firewalls, VPNs, and access controls.

Checkpoint Summary

- In today's digital world, protection against cyber threats is curial.
- Protecting against cyber attacks involves implementing information security, cybersecurity, network security.
- Key characteristics of information that must be protected: Confidentiality, Integrity, Availability, Authenticity, Accountability and Non-repudiation.
- Common types of attacks: Interruption, Interception, Modification, Fabrication.

NCC education®
Awarding Great British Qualifications

Network Security and Cryptography

Topic 1: Lecture 2

Network Models and Cryptography

Network Attack Models

Passive attacks

- Observe, intercept, overhear, eavesdrop.
- Offline analysis.
- Hard to protect against.

Active attacks

- Modify, forge messages.
- Replay or relay messages.
- Real-time attendance in protocols/system run.

Network Attack Models cont'd

External Attackers

- Not part of the system.
- No privilege, no valid password, no valid signature, decryption keys, and authorised access granted by default.

Insider Attackers

- Part of the system.
- Can be an employee.
- Can be compromised nodes/devices that are under control of the attacker.
- Depending on the role of the compromised device/node
  - Privilege, valid password, no valid signature, decryption keys, and some level of authorised access.
- Protection against an insider attacker is much harder compared to external attackers.

OSI Model Corresponding Attacks

Layer 2 (data link) Attacks
- MAC Spoofing Attack
- DHCP Starvation

Layer 3 (network) Attacks
- IP Spoofing
- Denial of Service attack
- Mail bomb
- Ping of Death
- Smurf Attack

Layer 4 (transport) Attacks
- SYN Flooding
- Sniffing
- Man-in-the-middle
- Session Replay
- Session Hijacking
- Domain Hijacking

Layer 7 (application) Attacks

Typical Application Attacks
- Reverse Engineering
- Password Attacks
- Buffer Overflow
- Malware
  - ✓ Viruses
  - ✓ Worms
  - ✓ Trojan Horses
  - ✓ Ransomware
  - ✓ Logic bomb
- Web Application Attacks
  - ✓ SQL injection
  - ✓ Cross site Scripting
  - ✓ Cross site Request Forgery
  - ✓ Man in the browser

People Attacks
- Trusted Insiders
- Social Engineering
- Identity Theft

MAC Spoofing

Goal

- To impersonate other devices for receiving sensitive information.
- Avoid firewall/router address filter list

Method

- Changing the MAC address of a device.
- The MAC address is hard-coded on a network interface controller (NIC).
- However, some drivers allow the MAC address to be changed.
- Some specialized tools can mislead the operating system to accept a fake MAC address
- E.g., SMAC, https://www.klcconsulting.net/smac/
- E.g., Change MAC address in Windows 7 https://www.ionos.co.uk/digitalguide/server/know-how/what-is-mac-spoofing/
- Difficult to detect.
- Analyze log files and traffic (e.g., with Wireshark)
- Check if there are several IP addresses link to the same MAC address (can be false detection).

Denial of Service Attack (DoS)

Goal

- Prevent a system to provide a service as normal.

Method

- Saturation – deprives a computer of needed resources
- Misconfiguration – destroys or alters configuration to prevent correct operation
- Destructive – physically destroy or damage network components
- Disruptive – interrupts communication between network nodes

Mail-Bomb

Send huge amount of emails to an email account

- Prevent the user from accessing emails.
- It is likely to affect productivity.
- Not always malicious.
- Can be also spam.

Ping of Death Attack

Saturation and destructive DoS attack

- The “ping” command is a common command used to identify another node on the network.

Sending a huge number (thousands) of pings at the same time can cause a drain on CPU usage

- Draining the CPU means the computer is less able to respond to other service requests.

If the attacker exceeds the upper limit of TCP connection, this may cause the ping target to crash

- If the computer crashes, then it is not able to provide any services.

Smurf Attack

A disruptive DoS attack using "broadcast addresses" and spoofing a return to address

- The attacker pretends to be the intended target
- Sends an ICMP ECHO request to the broadcast address of network routers
  - The router will then forward this to all the devices it is connected to (can be 255 further devices)
- Those 255 devices then reply to the request to the spoofed IP address
- The spoofed IP address (the intended victim) then gets overloaded.

SYN Attack

A disruptive DoS attack that prevents network handshake

- The TCP protocol utilises a 3-stage-handshake to ensure data sent is received
- Handshake occurs between client and server
  - Client -> SYN
  - Server -> SYN-ACK
  - Client -> ACK
- Withholding the final ACK will cause the server to wait

Social Engineering

Tricking people into doing things they wouldn't normally do

- Non-technical in nature; using confidence trickery to fool people
- E.g., phoning up and saying "I'm from your bank, we've detected a fraudulent activity on your account and need to check…just confirm your details…"
- Counter-measures…
  - Policy and procedures – must be clear and must be understood and followed
  - Education is really important – don't assume people are aware of this
  - Multi-person authorisation for important resources
  - Technical access controls – e.g., biometrics

Insider Threat

Don't focus on the 'external' (intruder) threat; often the biggest threat comes from trusted individuals

- They have specific knowledge about infrastructure
- Might have privileged access to resources – inside the security perimeter
- Doesn't need to be malicious – employees often make mistakes
  - Some work recently discovered that overwork and tiredness can lead to security vulnerabilities being exploited
- Can also be malicious
  - "About to be made redundant"
  - "Didn't get the pay rise I had hoped for"
  - "I want to set up my own competitor business"

Mitigation Measures

- Risk assessment – understanding where the most important risks are
- Cultural – “important risks” will depend on company culture
  - Might be financial, but might be risk to life
- Education of users
- Keeping computers/devices up to date with patches
- Engage with services that offer support (e.g., traffic-scrubbing), packet analysis/examination
- Gather evidence to take remedial action / learn
- Build incident response plans
- Harden security after incidents

Approaches for Network Security

- **Encryption (Cryptography)**
- Software Controls (access limitations in a database, in operating system protect each user from other users)
- Hardware Controls (smart access cards)
- Policies (frequent changes of passwords)
- Physical Controls

Cryptography

Cryptography is the science and practice of **secure** communication and data protection through the use of mathematical techniques and algorithms. It involves the **transformation/encryption** of **plaintext** (human-readable data) into **ciphertext** (encrypted data) to ensure that sensitive information remains confidential and secure from unauthorized access or malicious attacks during transmission or storage.

Cryptanalysis

Cryptanalysis is the science and art of studying and **breaking cryptographic systems/decryption** to gain unauthorized access to encrypted information. Also known as **code-breaking**, cryptanalysis involves analyzing the structure and properties of cryptographic algorithms and encrypted data to discover weaknesses, vulnerabilities, or the actual decryption key.

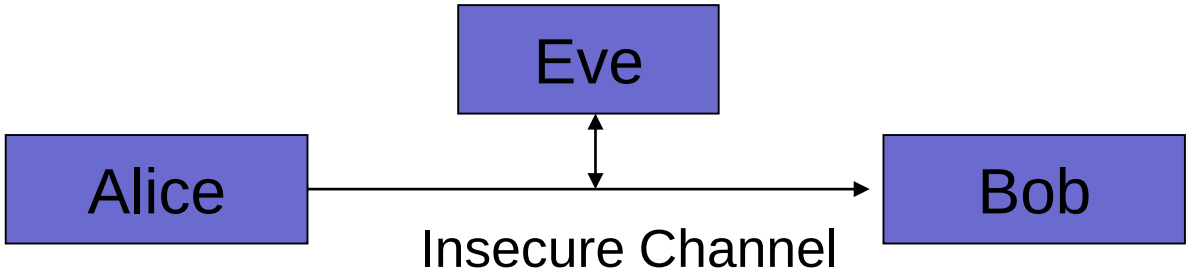
Cryptography Vs Steganography

Cryptography - Science of transforming information into secure form such that unauthorized persons cannot access it.

Steganography – Hides the existence of data

Image, audio, video files containing hidden messages embedded in the file. Achieved by dividing data and hiding In the unused portions of the file.

Cryptography Goals



Confidentiality: Cryptography aims to ensure confidentiality, which means that sensitive information remains private and only accessible to authorized parties. Prevent Eve from access to information.

Integrity: Cryptography ensures data integrity, which means that information remains unchanged and unaltered during transmission or storage. Eve is not able to alter the information.

Authentication: Cryptography enables authentication, which means verifying the identity of a user or system. Bob should be able to confirm that packet is coming from Alice and Eve is not able to alter or pretend to be Alice.

Non-repudiation: Cryptography achieves non-repudiation, which prevents a party from denying their involvement in a communication or transaction. Alice is not able to deny later that the information is not sent by him/her.

Basic Cryptography Principle

Cryptographic scheme has five ingredients:

- Plaintext
- Encryption Algorithm
- Secret Key
- Cipher Text
- Decryption Algorithm

The security of an encryption system must depend only on the key, not on the secrecy of the algorithm.

Kerckhoffs' Principle

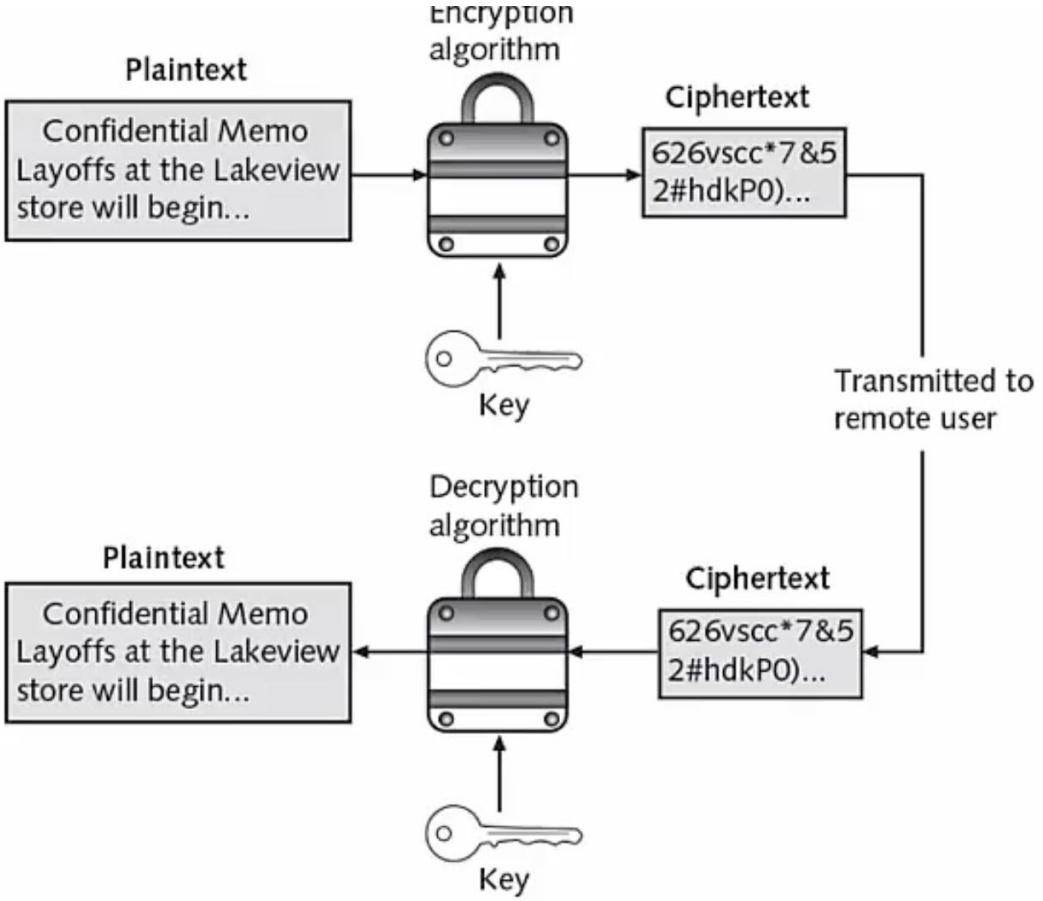
Basic Terminologies

- **Plaintext** - the original message
- **Ciphertext** - the coded message
- **Cipher** - algorithm for transforming plaintext to ciphertext
- **Key** - info used in cipher known only to sender/receiver
- **Encipher (encrypt)** - converting plaintext to ciphertext
- **Decipher (decrypt)** - recovering ciphertext from plaintext
- **Cryptography** - study of encryption principles/methods
- **Cryptanalysis (codebreaking)** - the study of principles/ methods of deciphering ciphertext without knowing key
- **Cryptology** - the field of both cryptography and cryptanalysis

Provable Security

- There is no such thing as a provably secure system.
- Proof of unbreakable encryption does not prove the system is secure.
- The only provably secure encryption is the one-time pad: C = P + K, where K is as long as P and never reused.
- Systems are believed secure only when many people try and fail to break them.

Generic Cryptography



Classification of Cryptographic Algorithms

- Classical Cryptography
- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Hash Function/digital signatures

In the next lectures, we will do into the details of these algorithms

Discussion Session

What are some common social engineering tactics that attackers use to deceive users and gain unauthorized access to sensitive information? How can users be more vigilant and avoid falling victim to these tactics?

Discussion Session

Some common social engineering tactics employed by attackers:

Phishing: Attackers send deceptive emails, messages, or websites that appear to be from a trusted source, such as a bank or a well-known company. The aim is to trick users into revealing personal information like passwords, credit card numbers, or account details.

Pretexting: In pretexting, attackers create a fabricated scenario to gain the target's trust. They may impersonate authority figures, IT support, or customer service representatives to extract sensitive information or access privileges.

Baiting: Attackers offer something enticing, such as a free USB drive or a tempting link, to lure users into downloading malicious software or visiting compromised websites.

Discussion Session

Some common social engineering tactics employed by attackers:

Tailgating: In a tailgating attack, the attacker gains physical access to a restricted area by following an authorized person without proper authorization.

Spear Phishing: This is a targeted form of phishing that focuses on specific individuals or organizations. Attackers gather information about their targets to create more personalized and convincing phishing messages.

Impersonation: Attackers may impersonate someone the target knows or trusts, such as a coworker, friend, or family member, to manipulate them into divulging sensitive information or performing actions on their behalf.

Discussion Session

Tips for Users to Stay Vigilant and Avoid Falling Victim:

- **Be Cautious with Email Links and Attachments**: Avoid clicking on links or downloading attachments from unknown or suspicious sources. Hover over links to check their URLs before clicking.
- **Verify Requests**: If someone asks for sensitive information or actions, independently verify their identity or request through a trusted channel, like a known phone number or official website.
- **Limit Personal Information**: Be cautious about sharing personal information on social media or other public platforms, as attackers can use this information for targeted attacks.

Discussion Session

Tips for Users to Stay Vigilant and Avoid Falling Victim:

- **Use Multi-Factor Authentication (MFA)**: Enable MFA whenever possible to add an extra layer of protection to your online accounts.
- **Stay Informed:** Stay updated about common social engineering tactics and educate yourself and others about potential threats and how to recognize them.
- **Report Suspicious Activity**: If you suspect social engineering attempts, report them to your organization's IT/security team or to relevant authorities.
- **Keep Software Updated**: Regularly update your devices and software to patch security vulnerabilities that attackers might exploit.

Topic Summary

- Network Attack Models : Passive, Active, Internal, External.
- At each layer of OSI model, there is a potential threat that need to be addressed.
- One of the potential techniques to address the security threats is **Cryptography.**
- Cryptography: Science of transforming information into secure form such that unauthorized persons cannot access it.

Next Topic 2: Cryptographic Techniques

- Classical Cryptography – Substitution, Transposition
- Symmetric Key Cryptography – Block and Steam Cipher

References

- CHARLES J. B., Christopher G., Philip C., Donald S. 2018. Cybersecurity Essentials, John Wiley & Sons, Inc.
- CIAMPA, M. (2012). Security+ guide to network security fundamentals. Cengage Learning.
- HOFFMAN, A. 2020. Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O'Reilly.
- OZKAYA, E. 2019. Cybersecurity: The Beginner's Guide. Packet Publishing Ltd.
- STALLINGS, W. 2022. Cryptography and Network Security: Principles and Practice, Global Edition, 8th edition, Pearson.

Topic 1 – Network Security and Cryptography Fundamentals

Any Questions?