Lanka Education And Research Network

Introduction to Security

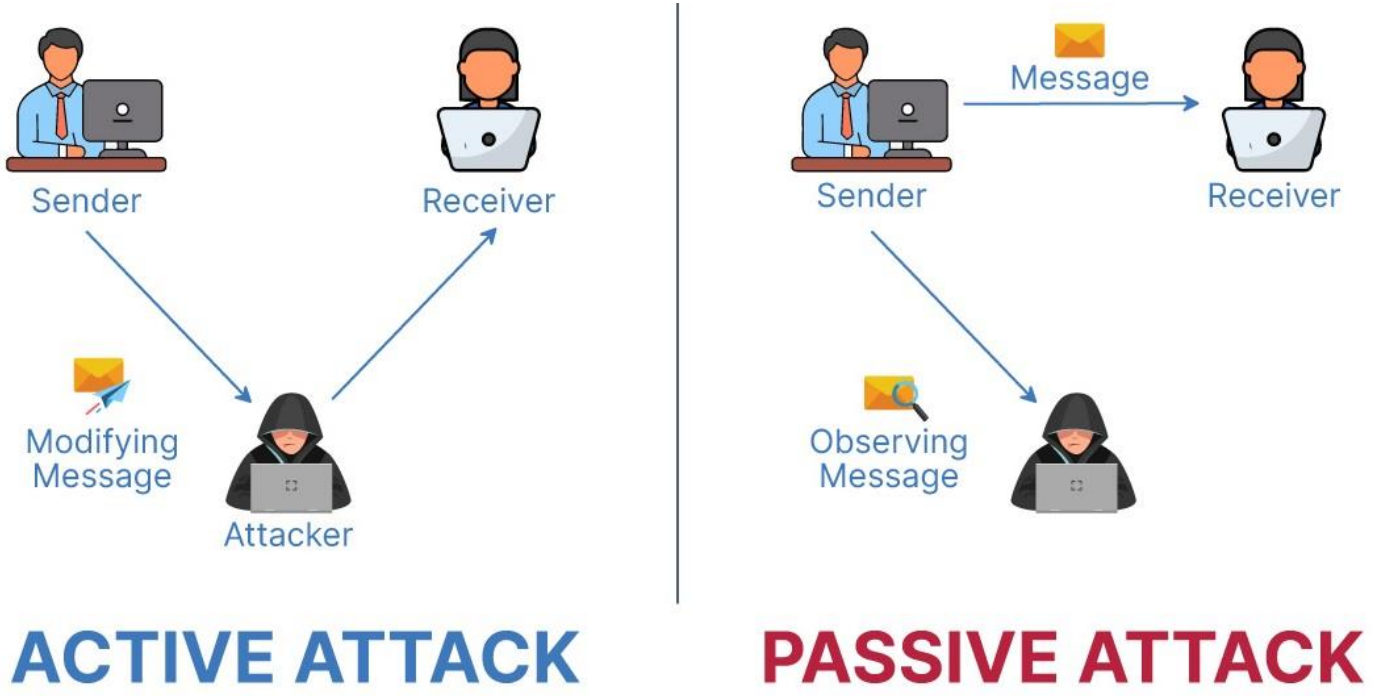
Definition of Information security

- Security is defined as the state of being free from danger or threat.

- **Information security** is defined as the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording, or the destruction of information.

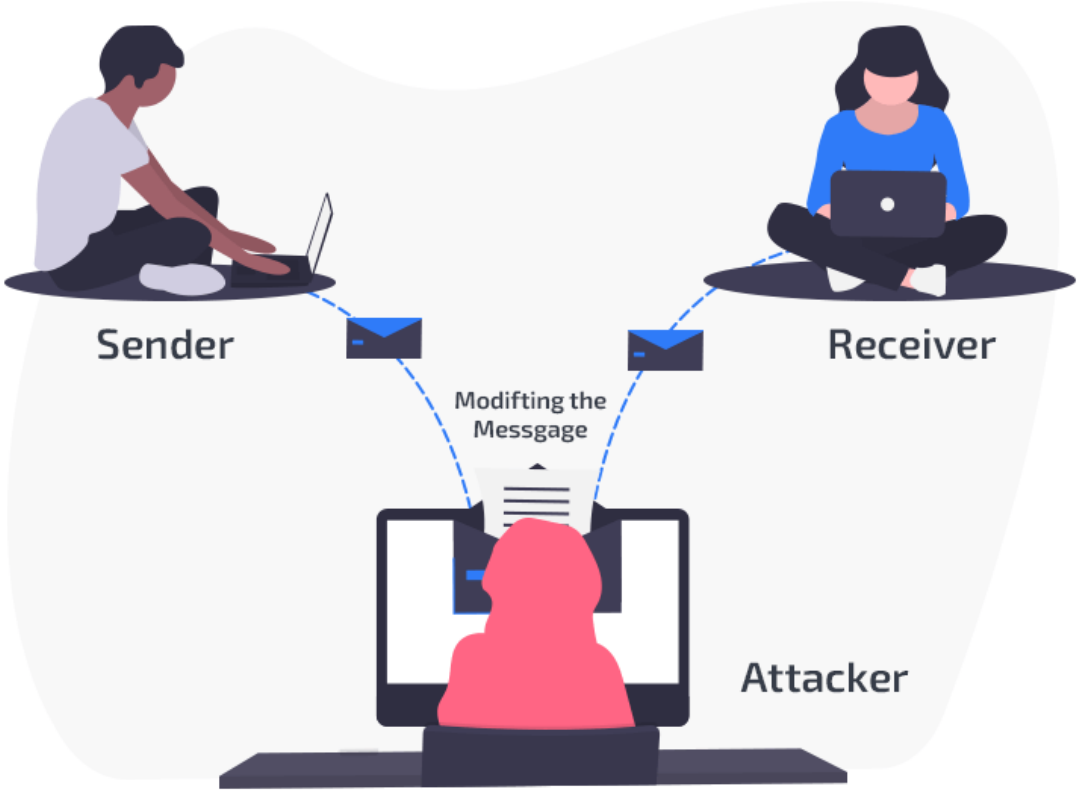
Types of Attacks

- An attack is any action that compromises the security of information owned by an organisation.



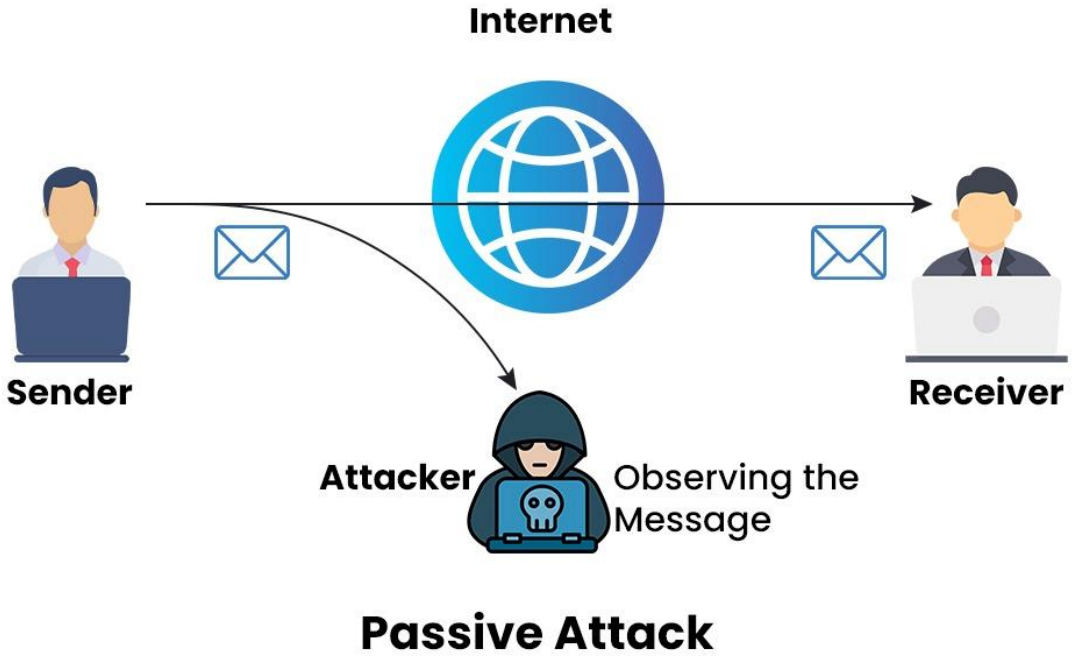
Active Attacks

- The attacker tries to modify the information or creates a false message.



Passive Attack

- Attackers do not affect or change the system operations.
- Spy or steal sensitive information from the system to learn important data about the system of the organization.



Key Security Concepts

Key Security Concepts

- **Confidentiality** – ensures that sensitive information are accessed only by an authorized person and kept away from those not authorized to possess them.

- It is implemented using security mechanisms such as usernames, passwords, access control lists (ACLs), and encryption.

Key Security Concepts

- **Integrity** – ensures that information are in a format that is true and correct to its original purposes. The receiver of the information must have the information the creator intended him to have.

- Integrity is implemented using security mechanism such as data encryption and hashing.

Key Security Concepts

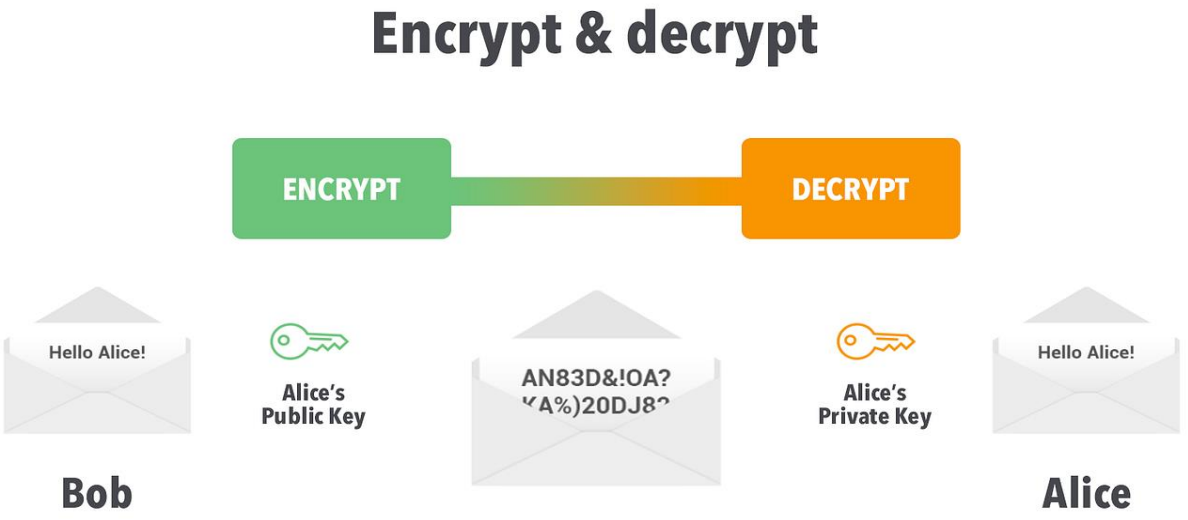
- **Availability** – ensures that information and resources are available to those who need them.

- It is implemented using methods such as hardware maintenance, software patching and network optimization.

Achieving Security

There are a number of approaches that we can take in order to achieve security.

- **Encryption**
- A process which converts plain text messages or data into cipher text.

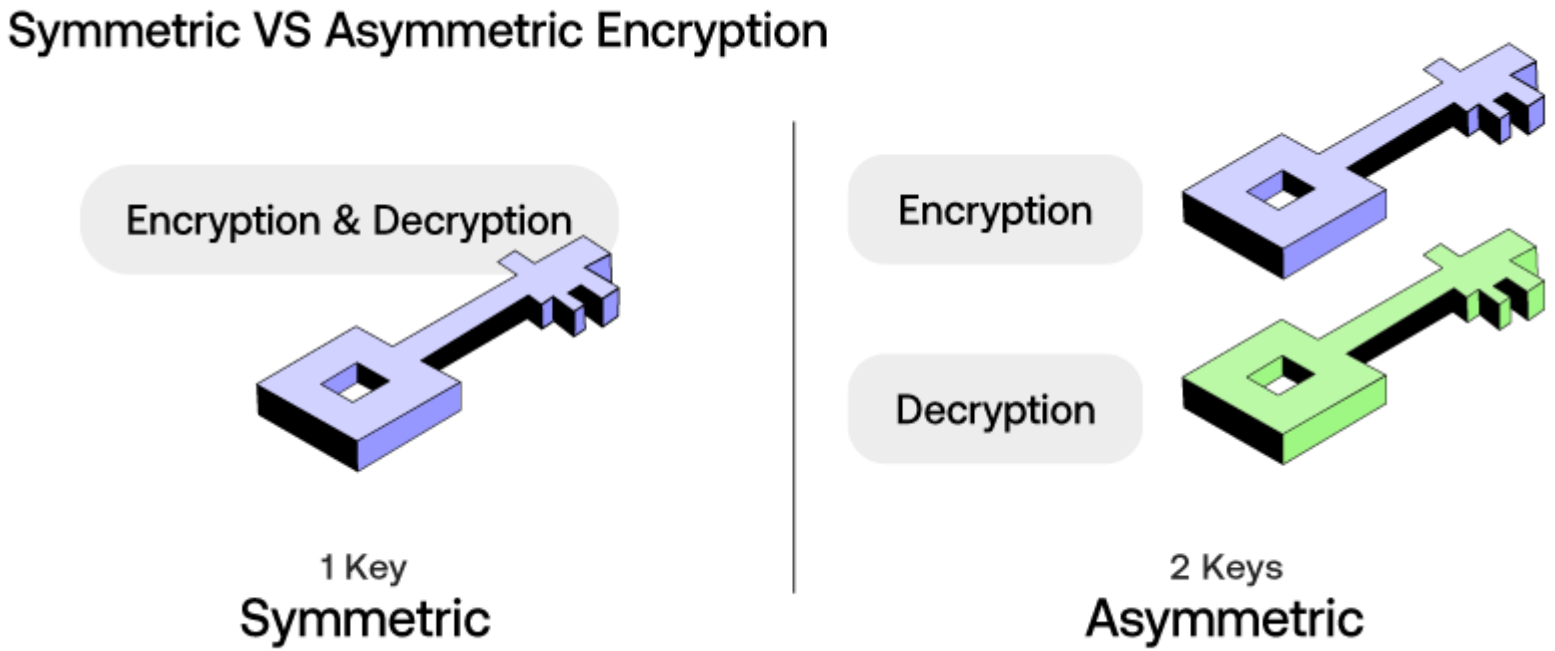


Achieving Security

- This is done by using an encryption algorithm with a key or a password.

- An encryption algorithm is the mathematical formula used to transform data into ciphertext.

Types of Encryption



Digital Signature

- Similar to a physical signature that place on a physical document such as a letter, users can digitally sign electronic documents and communications too.

- Digital signatures are used in e-commerce, software distribution, financial transactions and other situations that rely on forgery or tampering detection techniques.

- A digital signature is also known as an electronic signature.

Access Control

- Access control is a way of limiting access to a system or to physical or virtual resources.
- In computing, access control is a process by which users are granted access and certain privileges to systems, resources or information.
- The simplest access control method is to use a username and a password, so that only authorised people can gain entry to a system.

What is a REN

- REN => Research and Education Network
- High bandwidth, Low Latency, open networks with no Filtering
- Enable research or services that could not be accomplished otherwise
- Our goal is to build networking capacity to support Research and Education

  Remember: University = Research & Education
- Buying all service from your local ISP is a losing game – you will spend more money and not have control of the network
- The Campus Network is the foundation for all Research and Education Activity
- Without a good campus network, the Research and Education Network can't work as well as it should

What is a Campus Network

- High bandwidth Networks – can be 10G , 40G or may be 100G
- Can be multiple acres of ground, multiple multi-story buildings
- Low latency fiber networks
- High number of L3, L2 devices
- Can be wired, wireless or both
- High number of services
  - Public
  - Confidential
  - Valuable, copyrighted
- Large research data volumes
- High user base – technical/ non-technical

Security in campus network

- Securing and monitoring the security of a campus network is difficult
- Campus networks need to be fairly open
- Always will have viruses, attacks and people generally acting bad

You get a call from some agency (eg: LEARN/ CERT) saying that they have a report that one of your hosts is participating in a Denial of Service (DoS) attack

- What do you do?
- How do you find the host (very hard if NAT)

Security in campus network – Key things

- Assets – what are we protecting?
  - Many sorts of targets:
    - Network infrastructure
    - Network services
    - Application service (money!)
    - Data
    - User machines
- Attackers – from whom?
- Attacks - common attacks
- Defenses - defenses

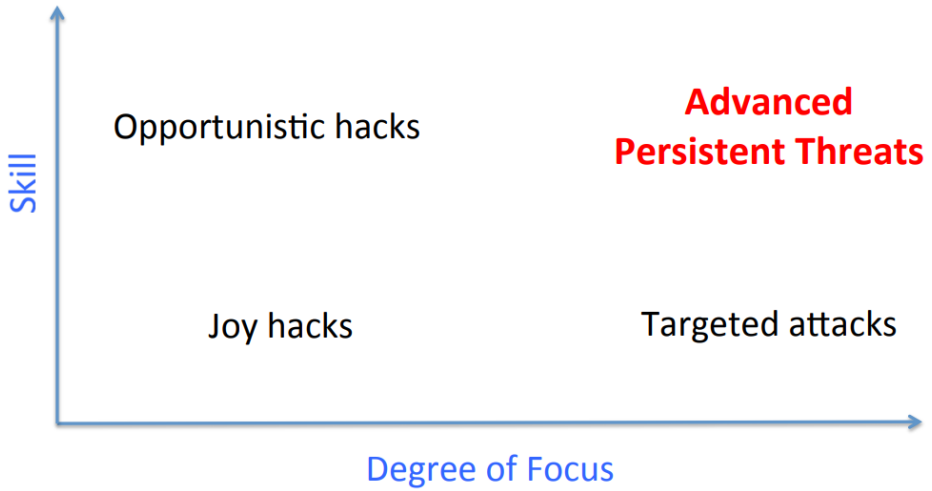
Security in campus network – Key things

- Assets – What are we protecting?
- Attackers – From whom?
  - Script kiddies: little real ability, but can cause damage if you're careless
  - Money makers: hack into machines; turn them into spam engines; etc.
  - Government intelligence agencies, AKA Nation State Adversaries
- Attacks – Common Attacks
- Defenses - Defenses

Security in campus network – Key things

- Assets – What are we protecting?
- Attackers – From whom?
- Attacks – Common Attacks – The Threat matrix

The Threat Matrix



Security in campus network – Key things

Joy Hacks:

⚠ Hacks done for fun, with little skill

⚠ Some chance for damage, especially on unpatched machines

⚠ Targets are random; no particular risk to your data (at least if it's backed up)

⚠ Ordinary care will suffice

⚠ Most hackers start this way

⚠ Common in many Campus Networks

Security in campus network – Key things

Opportunistic Hacks:

⚠ Most phishers, virus writers, etc.

⚠ Often quite skilled, but don't care much whom they hit

⚠ May have some "zero-days" attacks

⚠ The effects are random but can be serious

⚠ Consequences: bank account theft, Social account theft, machines turned into bots, etc.

Have your users reported these kind of attacks???

Security in campus network – Key things

Targeted Attacks:

⚠ Attackers want you. Sometimes, you have something they want

⚠ Other times, its someone with a grudge

⚠ Background research – learn a lot about the target

⚠ May do physical reconnaissance

⚠ Watch for things like “spear-phishing” or other carefully targeted attacks

Have your users reported these kind of attacks?

Security in campus network – Key things

Advanced Persistent Threats (APT):

⚠ Very skillful attackers who are aiming at a particular targets

⚠ Sometimes – though not always – working for a nation-state

⚠ very hard to defend against them

⚠ May use non-cyber means, including burglary bribery and blackmail

⚠ Note: many lesser attacks blamed on APTs

Have your users reported these kind of attacks?

Security in campus network – Key things

Assets – What are we protecting?

- Attackers – From whom?
- Attacks – Common Attacks
- Defenses – Defenses

—Defense strategies depend on the class of attacker, and what you're trying to protect

—Tactics that keep out script kiddies won't keep out an intelligence agency

—But stronger defenses are often much more expensive, and cause great inconvenience

Defense Strategies

Joy Hackers:

- By definition, joy hackers use existing tools that target known holes
  - Patches exist for most of these holes
  - These hacking tools are known to AV companies
- The best defense is staying up to date with patches
- Also, keep antivirus software up to date
- Ordinary enterprise-grade firewalls will also repel them

Defense Strategies

Opportunistic Hackers:

- Sophisticated techniques used
  - Possibly even some 0-days
- You may need multiple layers of defense
  - Up-to-date patches and anti-virus
  - Multiple firewalls
  - Intrusion detection
  - Lots of attention to logfiles
- Goal: contain the attack

Defense Strategies

Targeted Attacks:

- Targeted attacks exploit knowledge; try to block or detect the reconnaissance
- Security procedures matters a lot
- How do you respond to phone callers?
- What do people do with unexpected attachments?
- USBs in the parking lot
- Hardest case: disgruntled employee or ex-employee

Defense Strategies

Advanced Persistent Threats :

- Very, very hard problem!
- Use all of the previous defenses
- There are no sure answers — even air gaps aren't sufficient (Google Stuxnet)
- Pay special attention to procedures
- Investigate all oddities

Defense Strategies

- Don’t use the same defenses for everything
- Layer them; protect valuable systems more carefully
- Maybe you can’t afford to encrypt everything—but you probably can encrypt all communications among and to/from your high-value machines
- The defender has to think about the entire perimeter, all the weakness
- Because the attacker has to find only one weakness and it is not good news for defenders

Security in a Process

You can never achieve security – it is a process that you have to continually work on

– Assessment – what is at risk
– Protection – efforts to mitigate risk
– Detection – detect intrusions or problem
– Response – respond to intrusion or problem
– Do it all over again

Thank You