



**SOMAIYA**  
VIDYAVIHAR UNIVERSITY

K J Somaiya College of Engineering

# Applied Cryptography

Ms. Swati Mali

B-215

swatimali@gmail.com

Assistant Professor, Department of Computer Engineering  
K. J. Somaiya College of Engineering  
Somaiya Vidyavihar University

**SOMAIYA**  
VIDYAVIHAR UNIVERSITY

K J Somaiya College of Engineering



# Applied Cryptography



# What is this course about?

- Objectives
  - Security needs / threats
  - Security Goals
  - Cryptography

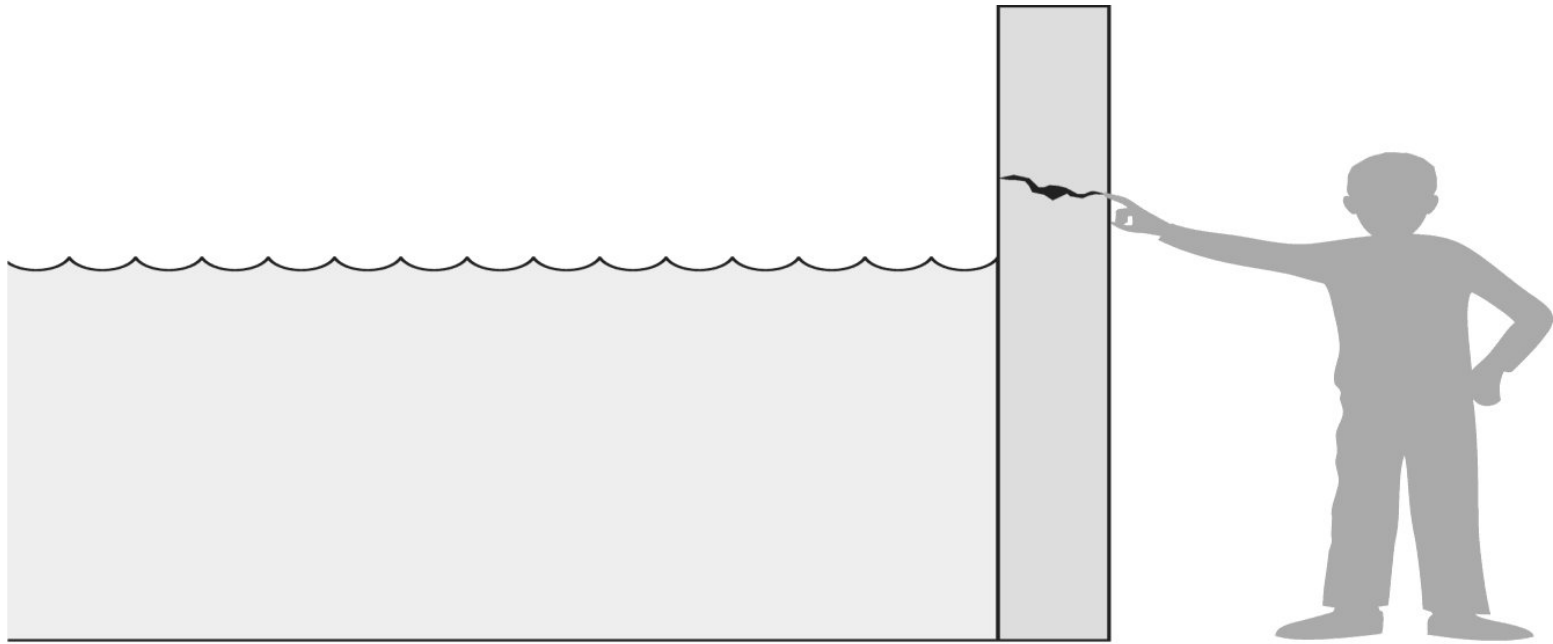
# What we will cover?

- –Vulnerabilities, threats, security Goals, and methods of defense
- –Cryptography
- –Symmetric
- –Asymmetric
- –Message authentication and digital signature
- –Advances in Cryptography

# Vulnerability, Threat and Control

- A vulnerability is a weakness in the security system, in procedure, design, or implementation that might be exploited to cause loss or harm
- A threat to a computer system is a set of circumstances that has the potential to cause loss or harm
- Control is an action, device, procedure, or technique that removes or reduces a vulnerability
- A threat is blocked by control of a vulnerability

# Threats, Controls, and Vulnerabilities



Pfleeger/Pfleeger Fig. 01-01

# Threats, Controls, and Vulnerabilities

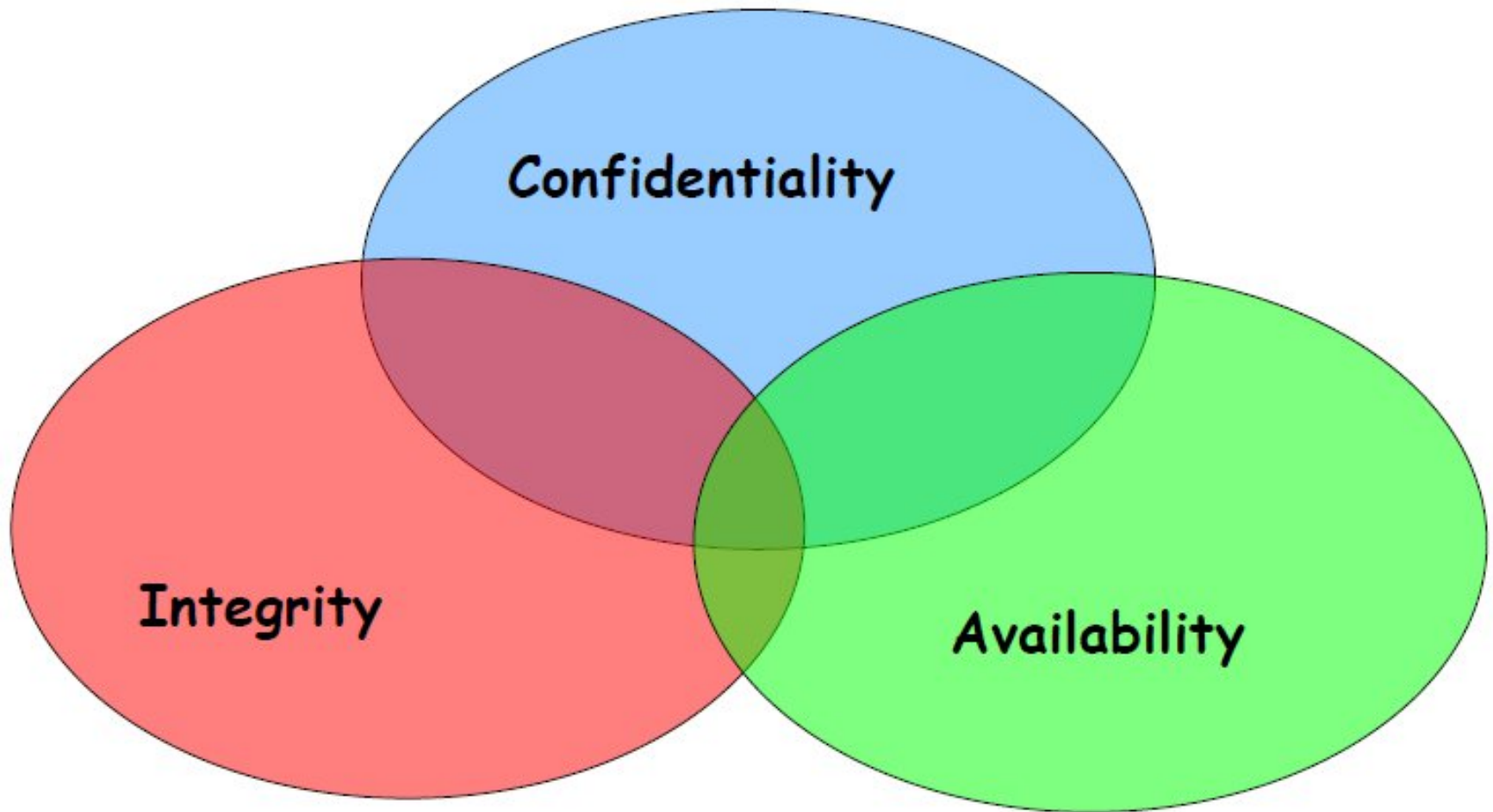
- Glass home
- Social media
- Land slide
- Bank transaction
- Covid vaccine booking
- Online zoom calls

# Attacks, Services and Mechanisms

- Security Attack: Any action that compromises the security of information.
- Security Mechanism: A mechanism that is designed to detect, prevent, or recover from a security attack.
- Security Service: A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

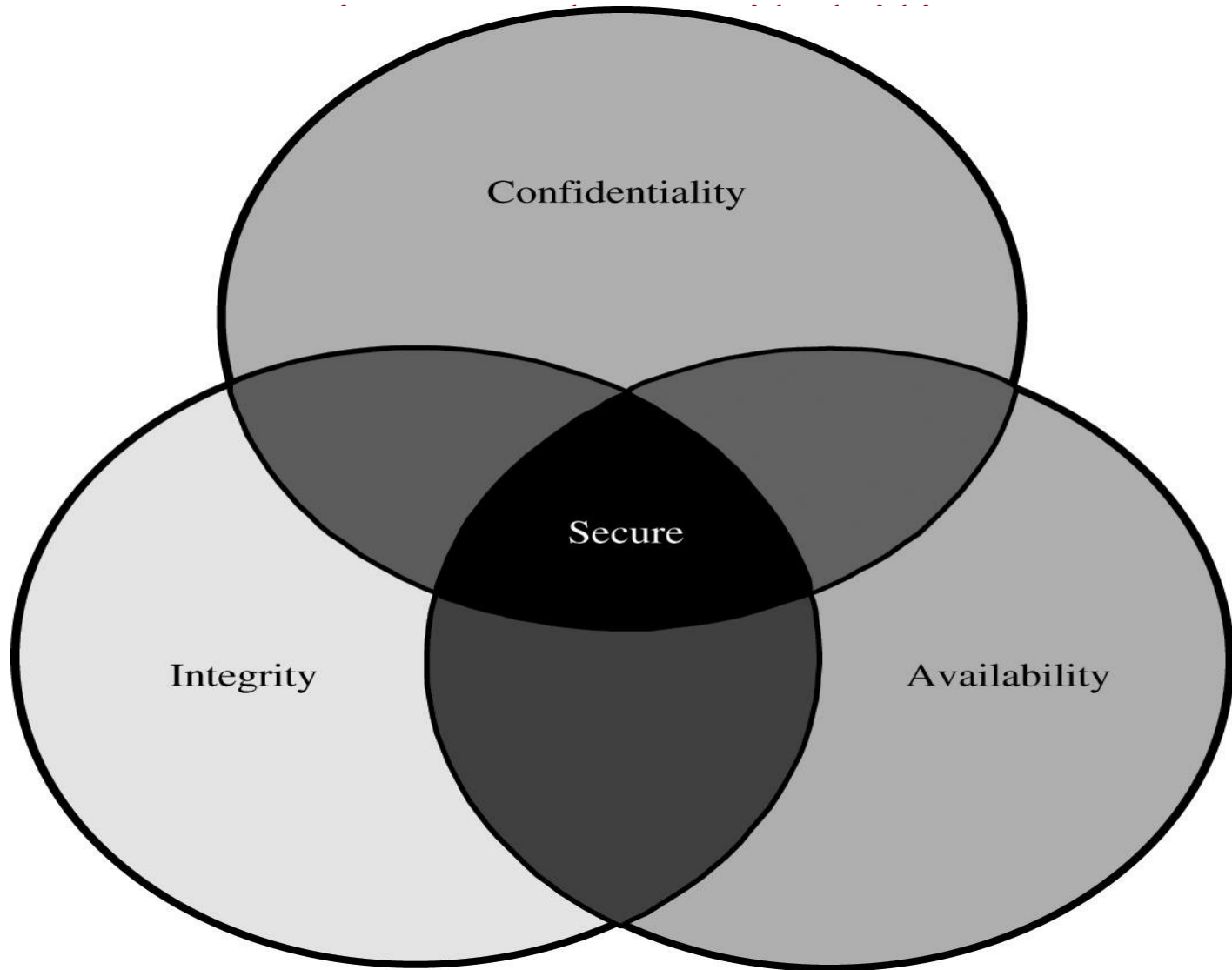


# Security Goals



Ms. Swati Mali

# Relationship Between Confidentiality,



# Confidentiality

- It ensures that computer-related assets are accessed only by authorized parties
- Access means reading, viewing, printing, or simply knowing that a particular asset exists
- It is sometimes also called secrecy or privacy

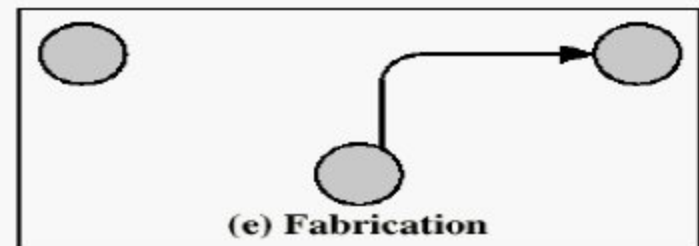
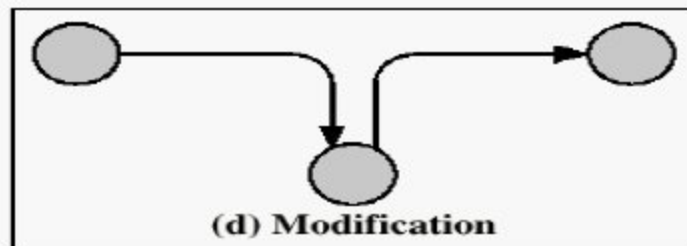
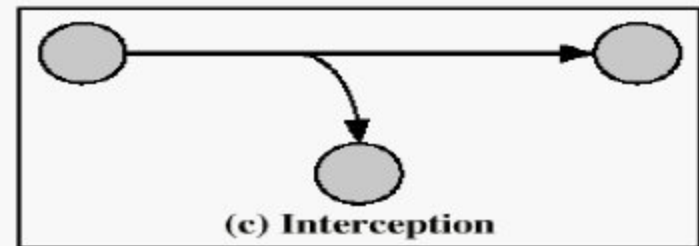
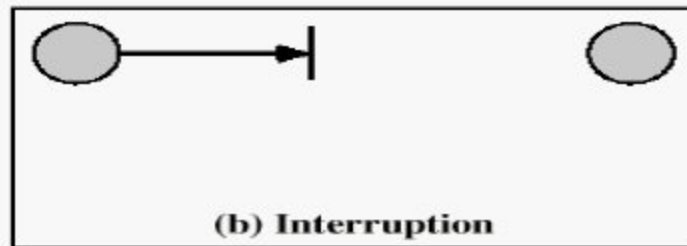
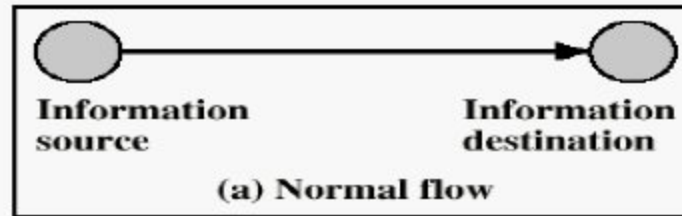
# Integrity

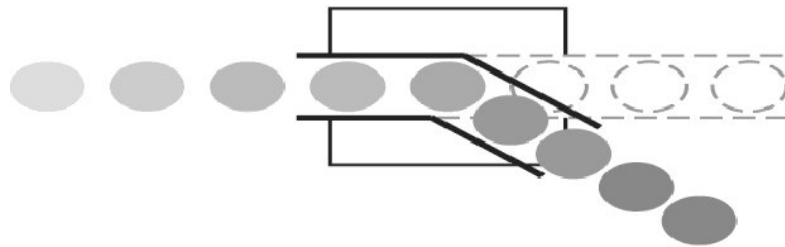
- It means that assets can be modified only by authorized parties only in authorized ways.
- The integrity of an item is preserved if it is:
  - Precise, accurate, unmodified, modified only in acceptable ways, modified by authorized people, modified by authorized processes, consistent, meaningful and usable.

# Availability

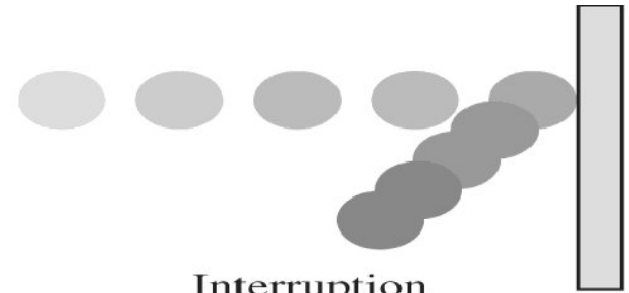
- It applies to both data and data processing
- A data item, service or system is available if
  - There is a timely response to our request
  - Fair to all i.e. some requesters are not favored over others
  - Fault tolerant
  - There is controlled concurrency, deadlock management, and exclusive access as required

# Security Attacks

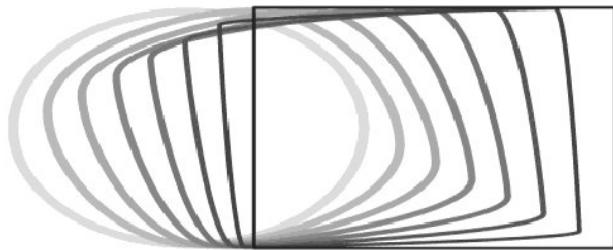




Interception



Interruption



Modification



Fabrication

Pfleeger/Pfleeger Fig. 01-02

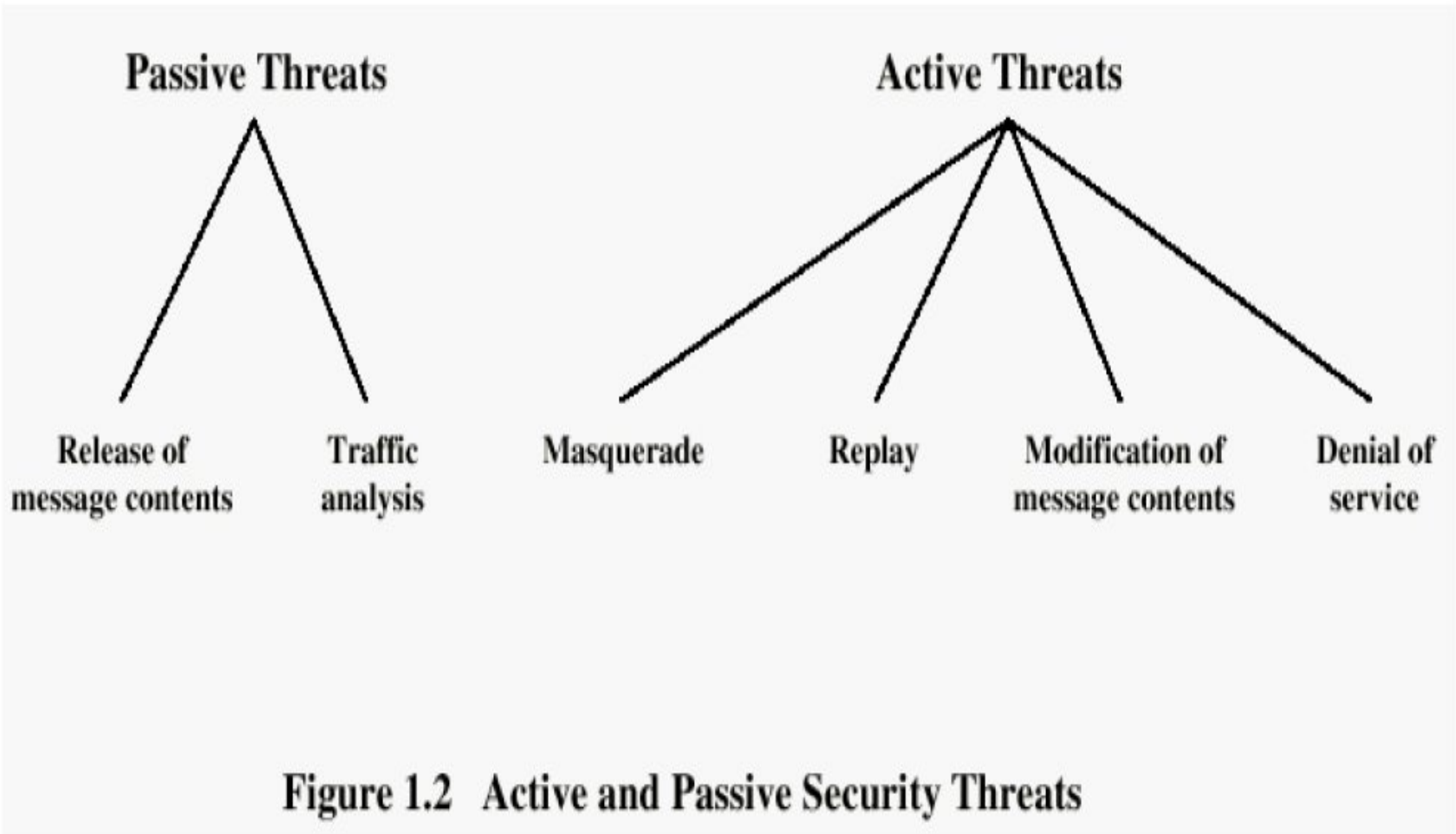
# Security Attacks

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



# Classical attacks on security

- Eavesdropping
- Traffic Analysis attack
- Replay attack
- non-repudiation attack
- Man-in-the-Middle attack
- Data Tampering
- Denial of Service (DoS) attack
- Brute Force Attack
- zero day exploit attack,
- Phishing and social engineering
- Spoofing
- Malware
- Session hijacking attack



Ms. Swati Mali

# Attacks

- Cryptanalytic Attacks
  - Exploit mathematical weakness of cryptographic algorithm
- Non-cryptanalytic Attacks
  - Threats to goal of security

# Security Attacks

Snooping

Traffic  
analysis

**Threat to  
confidentiality**

Modification

Masquerading

Replaying

Repudiation

**Threat to integrity**

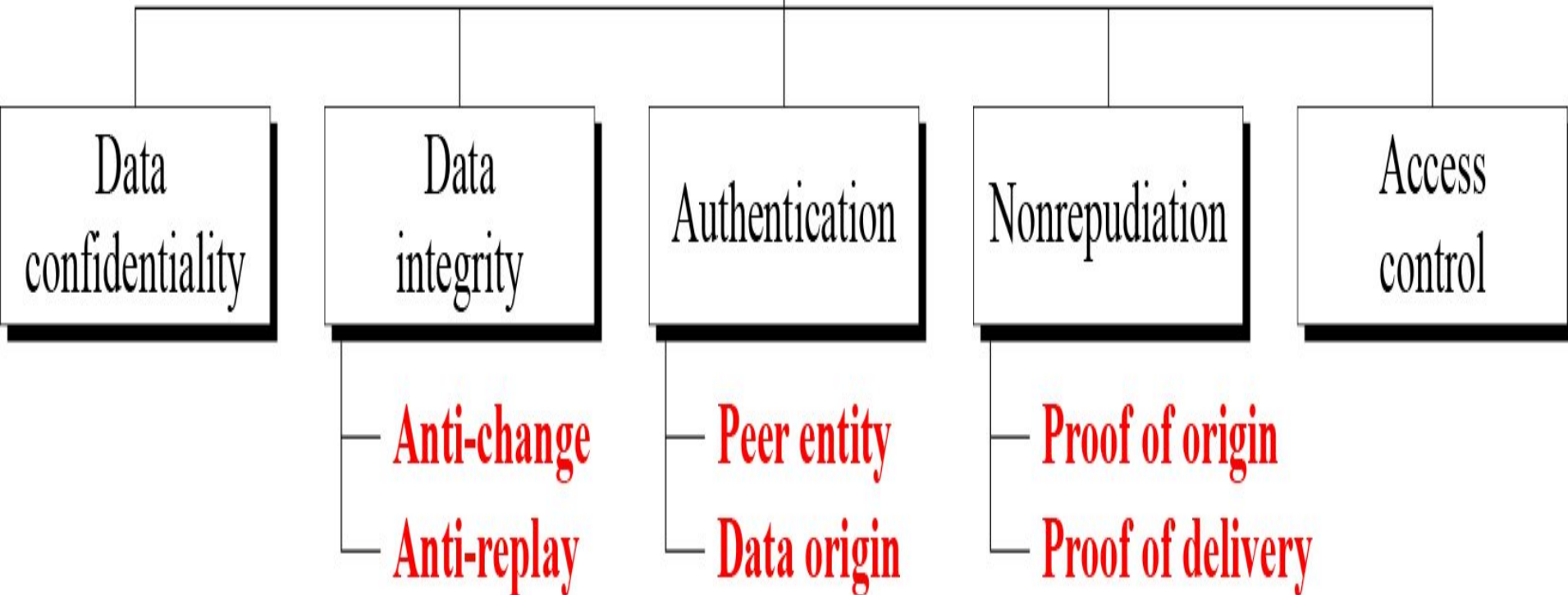
Denial of  
service

**Threat to  
availability**

# Security Services

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

# Security Services



## Security Mechanisms

Encipherment

Data integrity

Digital signature

Authentication exchange

Traffic padding

Routing control

Notarization

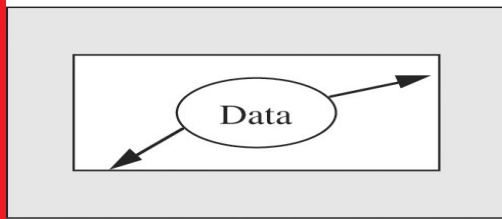
Access control

# Vulnerabilities

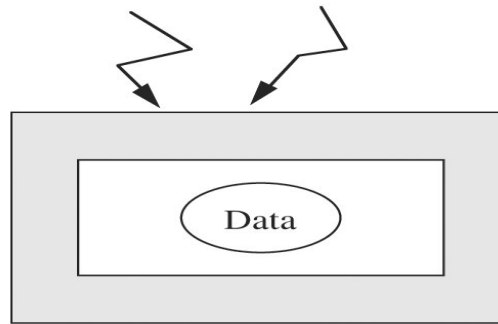
- Hardware vulnerabilities
- Software vulnerabilities
  - Software deletion
  - Software modification
    - Viruses etc.
  - Software theft
- Unauthorized copying etc.
- Data vulnerabilities



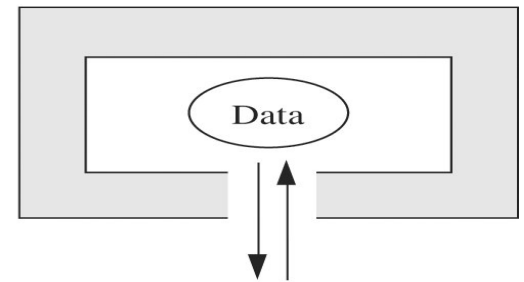
# Data Security



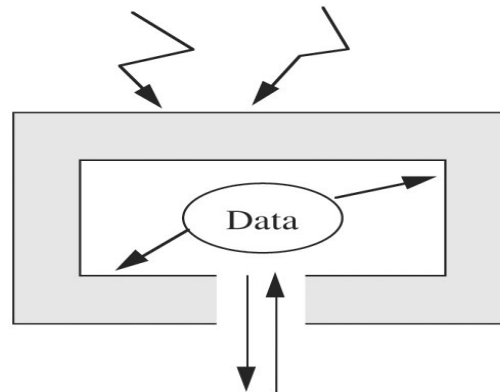
Confidentiality



Integrity

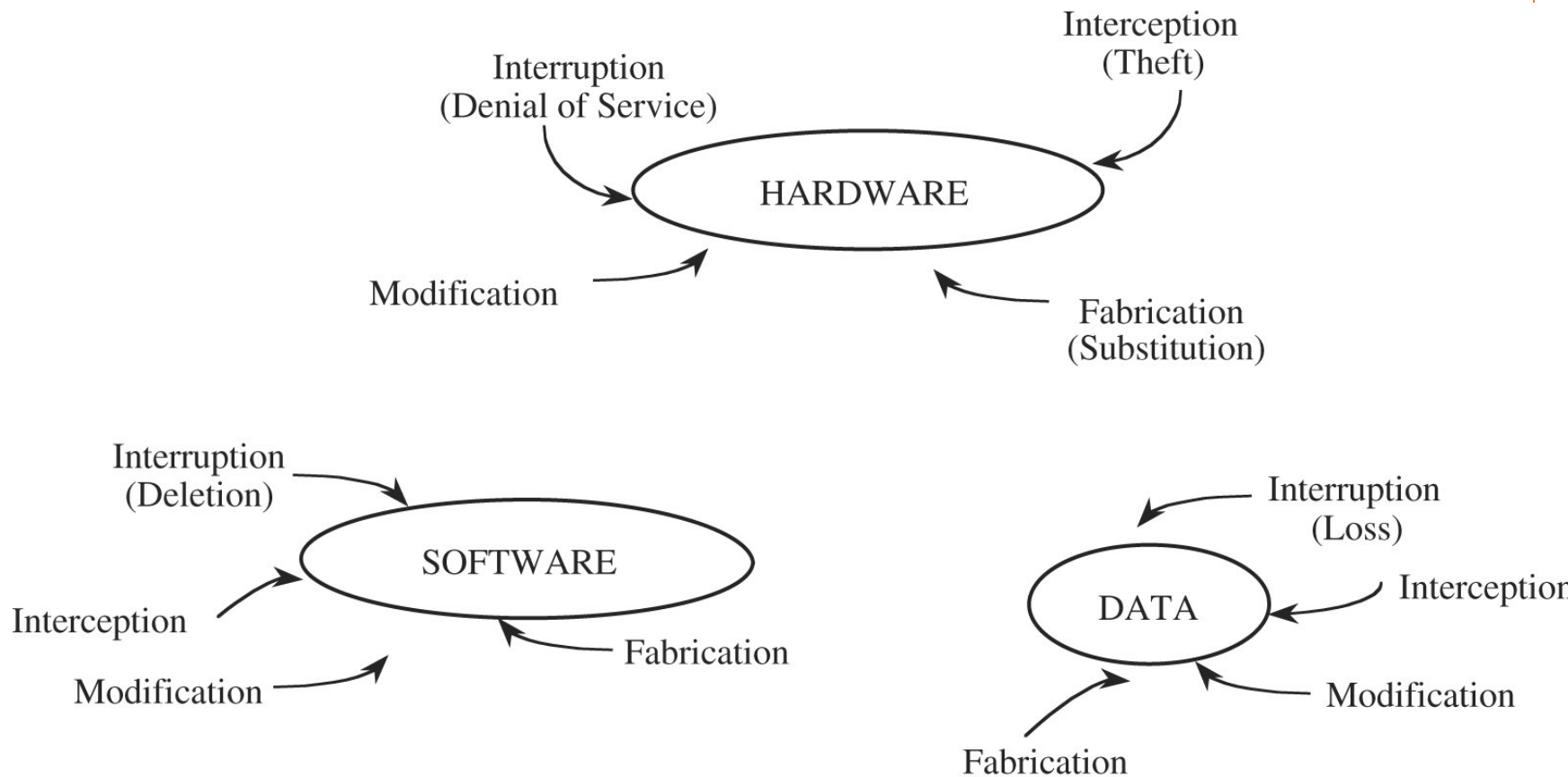


Availability



Secure Data

# Computing system vulnerabilities



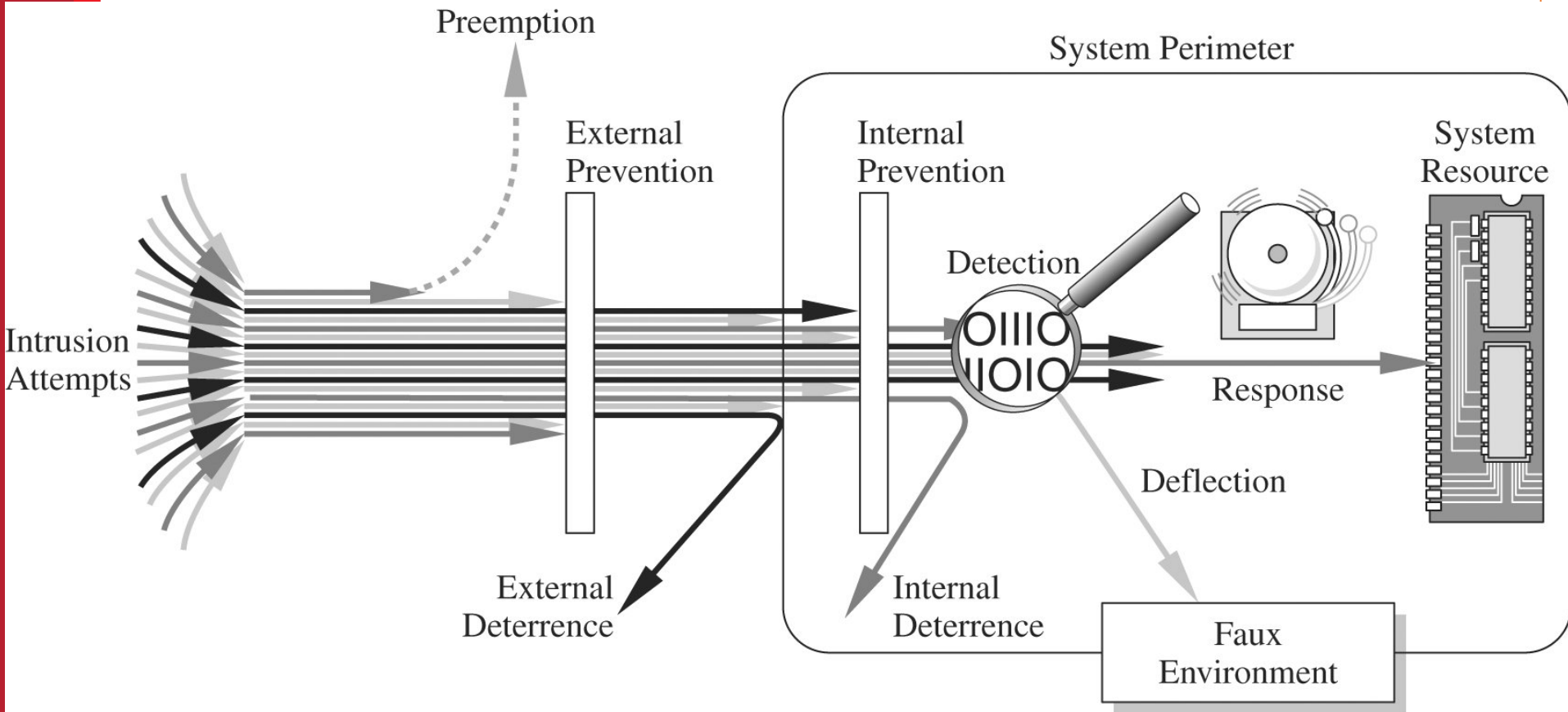
# Methods of Defense

- *Prevent it*, by blocking the attack or closing the vulnerability
- *Deter it*, by making attack harder if not impossible
- *Deflect it*, by making another target more attractive
- *Mitigate it*, by making its impact less severe
- *Detect it*, either as it happens or some time after the fact
- Recover from its effects

# Multiple levels of Defence



# Multiple levels of Defence



Pfleegeer/Pfleegeer Fig. 01-06

# Methods of Defense

- Controls
  - Encryption
  - Hardware Controls
    - Hardware/smart card implementations of encryption
    - Locks or cables limiting access
    - Devices to verify users' identity
    - Firewalls
    - Intrusion detection systems
  - Software Controls
    - Internal program controls,
    - OS and Network system controls
    - Independent control program (anti virus, passwords etc.)
    - Development control
  - Policies and Procedures
    - Time restrictions
    - Geofencing
    - Standard development Environment
    - Non Disclosure Agreement

○ Physical Controls

Ms. Swati Mali

# Reading slides:Computer Criminals

- Amateurs
  - Personal works
- Crackers
  - Trying to access computing facilities for which they are not authorized
  - The perception that nobody is hurt or even endangered by a little stolen machine time
  - Others attack for curiosity, personal gain, or self-satisfaction
- Career Criminals

# Reading slides:Method, Opportunity and Motive

- Method : the skills, knowledge, tools and other things with which to be able to pull off the attack
- Opportunity : the time and access to accomplish the attack
- Motive : a reason to want to perform this attack against this system

DENY ANY OF THESE THREE THINGS AND  
ATTACKS WILL NOT OCCUR



# Reading slides:MOM



**FIGURE 1-11** Method–Opportunity–Motive

# Reading slides:MOM : EVM – breaking

## Method

- **Skills and Knowledge:** Understanding of EVM hardware and software, including operating systems, communication protocols, and cryptographic systems.
- **Tools:** Specialized hardware (e.g., card readers, microcontrollers, or probes), software tools to analyze or reverse-engineer firmware, and pre-designed attack scripts available online.
- **Resources:** Access to programming manuals, technical specifications, and publicly available security research papers on EVMs.
- **Attack Variants:** Techniques like malware injection, side-channel attacks, or exploiting software/firmware vulnerabilities to alter results or compromise integrity.

## Opportunity

- **Access Points:** Physical access during storage, transport, or voting; insider threats from technicians or election staff.
- **System Weaknesses:** Poorly implemented security protocols, use of default settings, lack of tamper-evident features, or absence of robust monitoring mechanisms during elections.
- **Operational Gaps:** Temporary loss of custody during transit, inadequate auditing of results, or lack of rigorous testing for vulnerabilities.
- **Public Accessibility:** In some cases, older or widely used EVM models are studied extensively, making their weaknesses well-known.

## Motive

- **Political:** Altering election outcomes to favor specific candidates or parties.
- **Financial:** Bribes or monetary gains in exchange for compromising election integrity.
- **Ideological:** Disrupting democratic processes to undermine trust in governance or to promote political agendas.
- **Reputation:** Demonstrating technical prowess by hacking high-profile systems like EVMs.
- **Sabotage:** Creating confusion, delaying results, or delegitimizing election outcomes by spreading misinformation about the security of EVMs.

Ms. Swati Mali

# Reading slides:MOM : EVM – breaking

Actor	Method	Opportunity	Motive
<b>Amateur Hackers</b>	- Using publicly available hacking tools.	- Insecure endpoints (voting kiosks, admin panels).	- Gaining recognition or thrill.
	- Exploiting weak or reused passwords.	- Lack of encryption in communication.	- Testing their hacking skills for personal satisfaction.
	- Basic phishing or social engineering techniques.	- Minimal technical safeguards in place.	
<b>Anti-Social Individuals</b>	- Spreading misinformation via fake e-voting portals.	- Overloaded servers.	- Causing disruption and chaos.
	- DDoS attacks to disrupt voting processes.	- Lack of traffic filtering mechanisms.	- Undermining public trust in technology and elections.
	- Tampering with voters' devices.	- High dependence on online systems without backup mechanisms.	

# Reading slides:MOM : EVM – breaking

Actor	Method	Opportunity	Motive
<b>Anti-Democratic Groups</b>	- Altering vote tallies by breaching databases.	- Poorly secured servers and databases.	- Undermining democracy to destabilize the nation.
	- Installing backdoors in e-voting infrastructure.	- Insider access to the election systems.	- Promoting authoritarian control.
	- Manipulating algorithms in vote counting software.	- Lack of robust access control mechanisms.	
<b>Notorious-Studious Hackers</b>	- Creating custom malware to infiltrate systems.	- Lack of regular security audits.	- Gaining fame or infamy.
	- Exploiting zero-day vulnerabilities.	- Use of outdated software/hardware.	- Demonstrating technical superiority.
	- Reverse-engineering voting software to identify flaws.	- Absence of real-time anomaly detection in e-voting systems.	- Selling vulnerabilities to third parties.
<b>Politicians</b>	- Colluding with insiders to manipulate vote records.	- Access to campaign funds and influence over infrastructure.	- Gaining an unfair advantage to win elections.
	- Funding professional hackers to breach systems.	- Exploiting politically aligned insiders.	- Ensuring their political power remains intact.
	- Using legal loopholes to influence voting systems.	- Weak regulatory oversight of election systems.	

# Reading slides:MOM : EVM – breaking

Actor	Method	Opportunity	Motive
<b>Foreign Governments</b>	- Advanced persistent threats (APTs) targeting critical election systems.	- Cross-border jurisdiction limits enforcement.	- Undermining the country's political stability.
	- Spreading propaganda and misinformation campaigns.	- Geopolitical tensions creating vulnerabilities.	- Influencing policies to favor their own geopolitical interests.
		- Lack of robust international cybersecurity coordination.	
<b>Criminal Organizations</b>	- Stealing voter data for identity theft.	- Weak encryption on databases.	- Financial gain through data sales.
	- Selling vote manipulation as a service (election fraud as a business).	- Lack of robust authentication for accessing systems.	- Running election fraud services for profit.
		- High black-market demand for personal and voter information.	
<b>Disgruntled Employees/Insiders</b>	- Leaking sensitive data about voters or systems.	- Direct access to e-voting infrastructure.	- Personal vendetta against employers or the government.
	- Tampering with configurations to enable external breaches.	- Minimal monitoring of employee activity.	- Financial gain from selling information or services.
	- Intentionally bypassing security measures.	- Insufficient background checks or employee screening.	

# Reading slides:

Actor	Method	Opportunity	Motive
<b>Activist Groups (Hacktivists)</b>	- Defacing e-voting portals to spread their message.	- Overreliance on online platforms without redundancy.	- Advocating for their causes.
	- Blocking systems through DDoS.	- Lack of regular penetration testing.	- Exposing perceived flaws in the democratic system.
	- Manipulating results to make a statement.	- Misconfigured public-facing services.	- Drawing attention to their ideologies.
<b>Curious Researchers</b>	- Ethical hacking to identify flaws.	- Access to test environments or real systems due to weak authorization checks.	- Publishing findings to improve security.
	- Testing various attack methods (often with consent).	- Collaboration with system administrators without strict boundaries.	- Building a reputation in cybersecurity circles.

# Reading slides: Effectiveness of Controls

- Awareness of Problem
  - Highlighting Need of security
- Likelihood of Use
  - They must be efficient, easy to use, and appropriate
- Overlapping Controls
  - Use several different controls, layered defense
- Periodic reviews
  - Judging the effectiveness of control is an ongoing task

# Others Exposed Assets

- Networks
  - Network's lack of physical proximity
  - Use of insecure, shared media
  - Inability to identify remote users positively
- Access
  - Computer time
  - Malicious access
  - Denial of service to legitimate user
- Key People



- An attacker secretly intercepts communication between two parties to steal credentials.

- A user receives a fake email asking to update bank details, which leads to credential theft.

- A hacker floods a website with traffic until it becomes unavailable to real users.

- An attacker captures and reuses valid authentication messages to gain unauthorized access.

- An attacker installs spyware to collect sensitive user information without consent.

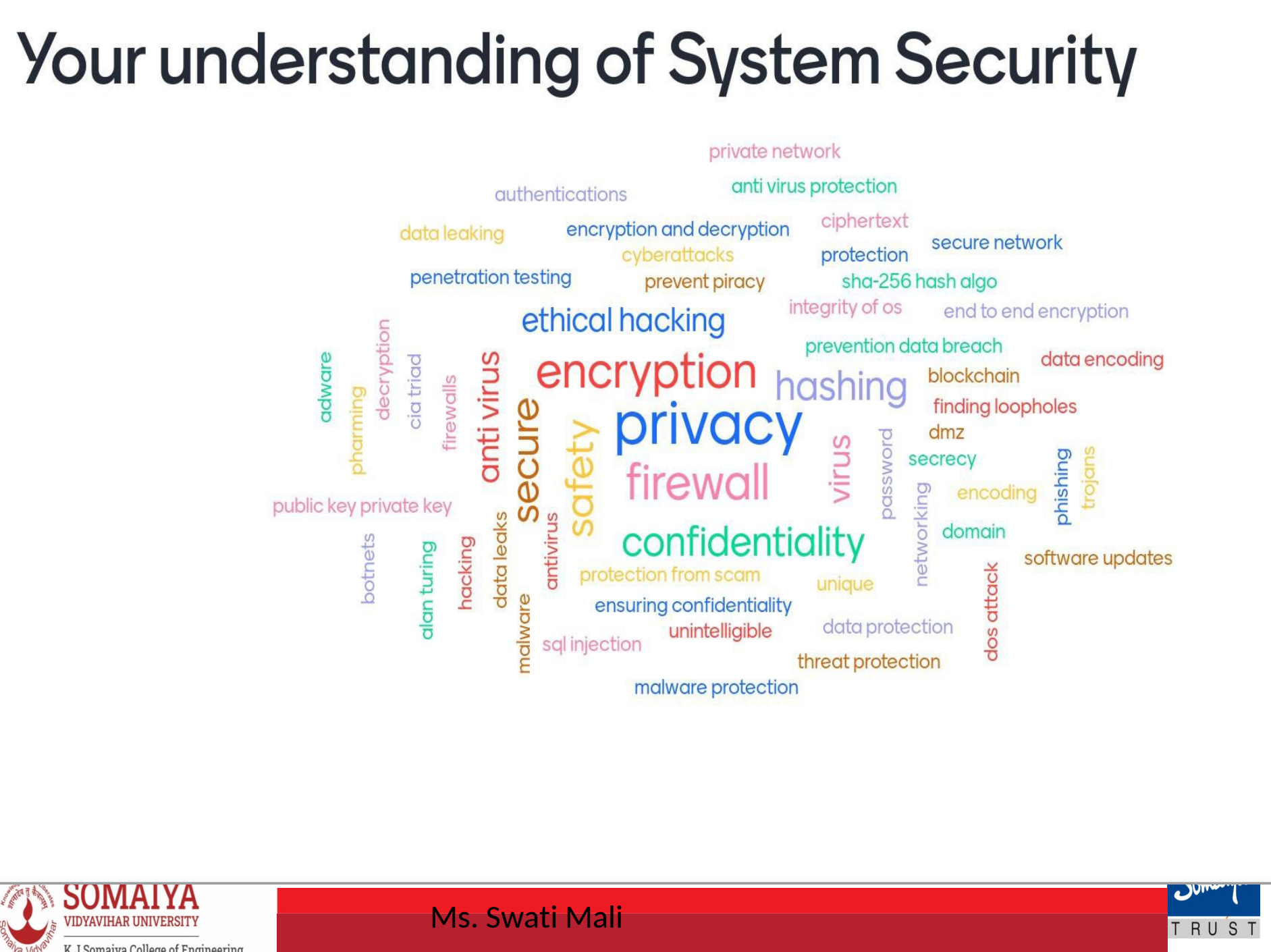
- A hacker modifies data in transit to alter financial transactions.

- An attacker sends thousands of password attempts to crack a user's account.

- A cybercriminal exploits an unknown vulnerability before the vendor can patch it.



- An attacker impersonates a trusted website to steal login credentials.

[illegible]

# Questions?