CENG 374E - INTRODUCTION TO COMPUTER SECURITY

Prof. Dr. Şeref SAĞIROĞLU
Gazi University
Engineering Faculty
Computer Engineering Department
Maltepe/Ankara

SS@gazi.edu.tr
https://avesis.gazi.edu.tr/ss

Threat Classification and Attack Types

Summary of Lecture

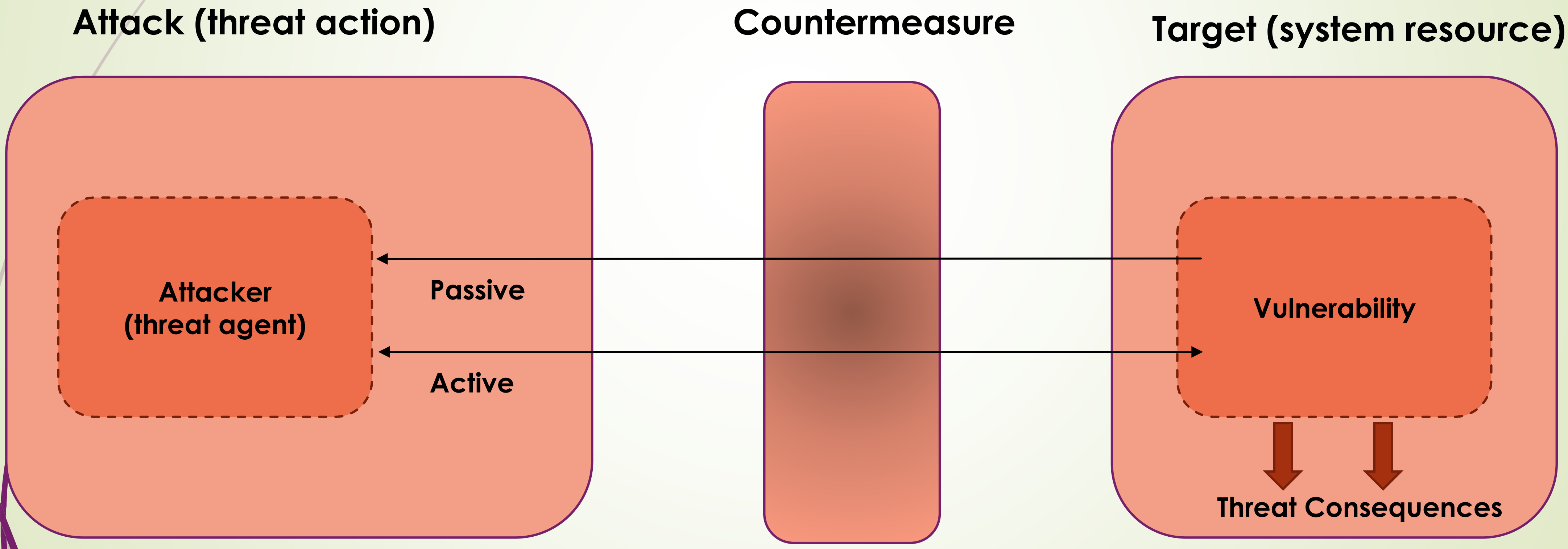
Computer security

- becoming more and more important
- attack surface increasing
- vulnerabilities, attacks, threats drastically increasing
- more difficult and harder to handle and protect.
- shortage of security experts.

Summary of Lecture

- Information Security Attributes (goals or properties)
  - Confidentiality Integrity Availability
- Risk Management Concepts
  - Value-appropriate protection, Risk assessment
  - Threat, Vulnerability, Attack, Risk, Countermeasure
  - Defense-in-depth

Summary of Lecture



(Adapted from RFC 2828)

Today

- Classifying threats
- Types of attacks

Types of Cyber Attacks

01 Denial of service (DDoS)

02 Malware Attack

03 Man in the Middle

04 Phishing

05 Eavesdropping

06 SQL injection

07 Password Attack

08 Social Engineering

intercepting
communication
between the people

Threat Classification

STRIDE model identifies six threat categories

- **Spoofing of Identity**
- **Tampering**
- **Repudiation**
- **Information disclosure**
- **Denial of service**
- **Elevation of privilege**

(Microsoft proposal)

Spoofing of Identity

Acting as someone / something else

- IP address spoofing
- Email address spoofing
- Phishing

…

Tampering

Changing something without authorization

- **Threatens integrity**
- Data tampering is one of the biggest security challenges facing applications, programs, and organizations.
- It's the **malicious modification, editing, or manipulation of data in transit that corrupts the data or underlying programming code**.

Repudiation

Denying the validity of a statement or contract

- **Countermeasure: Digital certificates and trusted third parties**

Information Disclosure

Release of secure information to an untrusted environment

- **Threatens confidentiality and privacy**
- **Human errors combined with malicious actors**
  - iCloud leaks
  - Adobe user records leak
  - Target credit cards leak

Denial of Service

Making a resource unavailable to its intended users

- **Threatens availability**
- **Easy and common**

Elevation of Privilege

Making yourself authorized

- **Vertical: taking on higher privileges**
  - Accessing student information system as department head
- **Horizontal: taking the privileges of someone else at the same level**
  - Accessing your classmate’s bank account, student account etc.

Threat Components

Threat agent: source of threat

Threat action: assault on security

Threat consequence: result of threat action

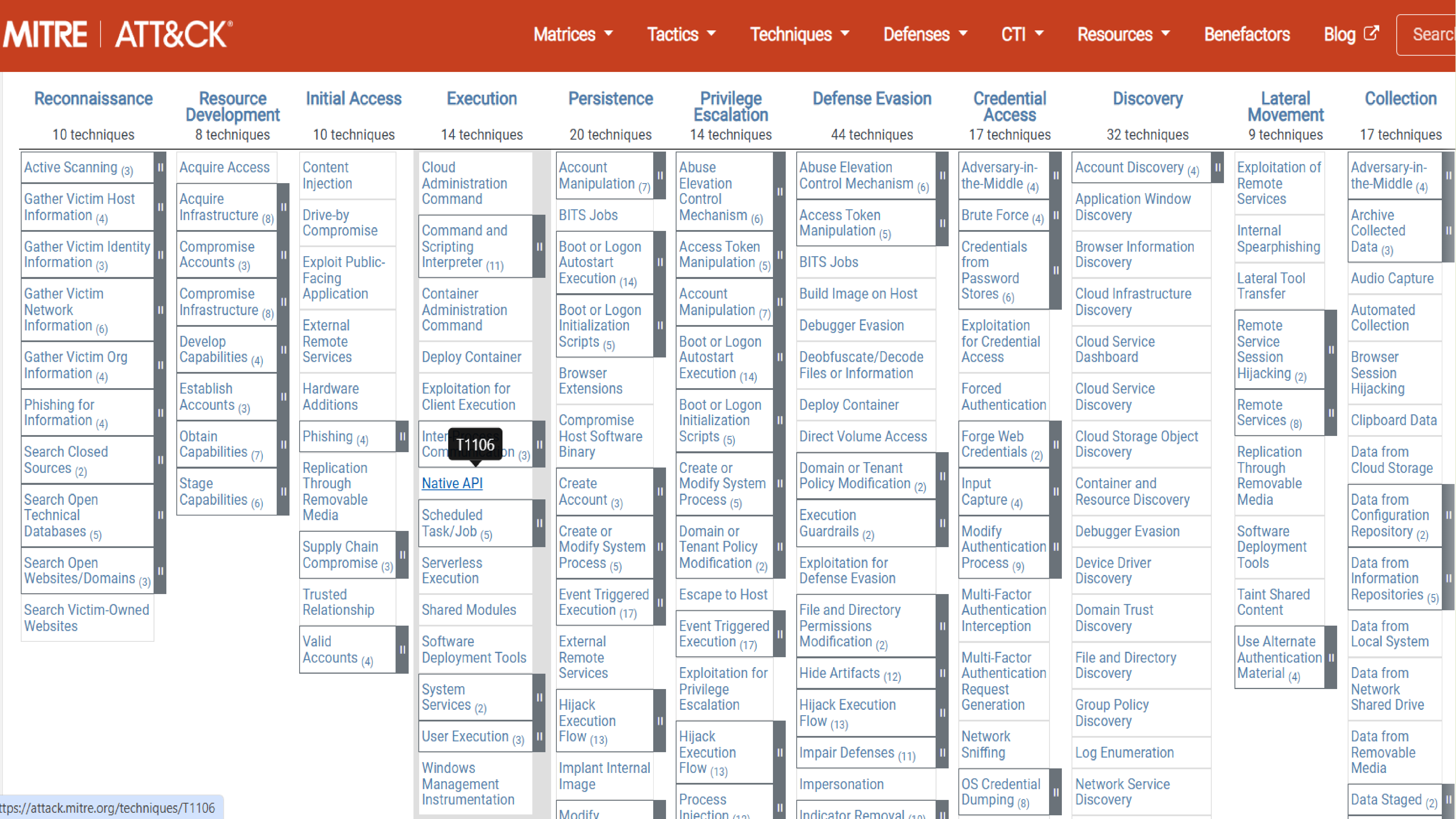
- Disclosure → loss of confidentiality
- Deception
- Disruption → loss of availability
- Usurpation

Usurpation: **Unauthorized control of some part of a system**.
This includes theft of service or theft of data as well as any misuse of the system such as tampering or actions that result in the violation of system privileges.

Types of Attacks

MITRE ATT&CK Framework

- a comprehensive, **publicly available** framework
- catalogues adversary **tactics, techniques, and procedures** based on real-world observations
- organizes attacker behavior into **14 core tactical categories (+1=15)**
  - with each tactic broken down into numerous specific techniques and sub-techniques
  - helping organizations to **better understand, detect, and defend against cyber threats**.



MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Blog Searc

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 44 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (11)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3) T1106	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Escape to Host	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (17)	Event Triggered Execution (17)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (5)
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (2)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System
			Software Deployment Tools	Hijack Execution Flow (13)	Hijack Execution Flow (13)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive
			System Services (2)	Implant Internal Image	Process Injection (12)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	File and Directory Discovery		Data from Removable Media
			User Execution (3)	Modify		Hide Artifacts (12)		Group Policy Discovery		Data Staged (2)
			Windows Management Instrumentation			Hijack Execution Flow (13)		Log Enumeration		
						Impair Defenses (11)		Network Service Discovery		
						Impersonation				
						Indicator Removal (10)				

ttps://attack.mitre.org/techniques/T1106

Types of Attacks (MITRE ATTACK Framework)

- Phishing Attacks
- Malware Attacks
- Denial-of-Service (DoS/DDoS) Attacks
- Man-in-the-Middle (MitM) Attacks
- Web-Based Attacks (e.g., SQL Injection & Cross-Site Scripting)
- Zero-Day Exploits
- Insider Threats
- Advanced Persistent Threats (APTs)
- IoT and Supply Chain Attacks
- Credential Stuffing & Brute Force Attacks
- Cryptojacking
- Supply Chain Attacks
- Deepfake & AI-Driven Attacks
- Advanced Social Engineering (Beyond Phishing)
- DNS Tunneling & Network Protocol Attacks

Types of Attack (MITRE ATTACK Framework)

- **Phishing Attacks**
  - uses deceptive emails, texts, or websites to trick users into revealing sensitive data.
  - modern variants like spear phishing and whaling employ highly targeted social engineering to increase success rates.

- **Malware Attacks**
  - encompasses harmful software
    - such as viruses, worms, Trojans, and ransomware—that infiltrates systems to damage or steal data.
  - ransomware, a prominent form, encrypts victims’ files and demands payment for restoration.

Types of Attack (MITRE ATTACK Framework)

- **Denial-of-Service (DoS/DDoS) Attacks**
  - DoS attacks flood a target system with excessive requests, rendering services unavailable to legitimate users.
  - Distributed DoS (DDoS) amplifies this effect by launching coordinated attacks from multiple compromised devices.

- **Man-in-the-Middle (MitM) Attacks**
  - an adversary intercepts and potentially alters communications between two parties without their knowledge.
  - This type of attack is especially dangerous on unsecured networks where data is transmitted in clear text.

Types of Attack (MITRE ATTACK Framework)

- **Web-Based Attacks (SQL Injection&Cross-Site Scripting)**
  - XSS attacks exploit vulnerabilities in web applications to manipulate databases
  - inject malicious code into user sessions.
  - SQL injections can extract or corrupt data, while XSS hijacks user interactions on compromised pages.
- **Zero-Day Exploits**
  - Zero-day attacks take advantage of previously unknown vulnerabilities before patches are released.
  - Their unpredictable nature makes them particularly perilous, as defenses aren’t yet prepared to counter them.

Types of Attack (MITRE ATTACK Framework)

- **Insider Threats**
  - Insider threats arise when individuals with authorized access abuse their privileges—either maliciously or accidentally—to compromise data or systems.
  - They're especially hard to detect because insiders often bypass traditional security controls.
- **Advanced Persistent Threats (APTs)**
  - APTs are prolonged, covert cyber intrusions aimed at stealing sensitive information over time.
  - They typically involve multiple stages—from reconnaissance to lateral movement—and use sophisticated, stealthy techniques to avoid detection.

Types of Attack (MITRE ATTACK Framework)

- **IoT and Supply Chain Attacks**
  - IoT attacks target the expanding network of connected devices that often have weak security
  - supply chain attacks compromise third-party vendors to infiltrate larger organizations.
  - Both methods exploit nontraditional entry points outside the core IT infrastructure.

Types of Attack (MITRE ATTACK Framework)

Many experts combine both technical attack vectors and human-centric methods into comprehensive frameworks more

- **Credential Stuffing & Brute Force Attacks**
  - Attackers use automated tools to try millions of username–password combinations until they find a match.
  - These methods succeed largely due to poor password hygiene.
- **Cryptojacking**
  - In cryptojacking, malware surreptitiously uses a victim’s computing power to mine cryptocurrencies without their knowledge.
  - This not only slows down systems and degrades hardware but also generates illicit revenue for attackers.

Types of Attack (MITRE ATTACK Framework)

- **Supply Chain Attacks**
  - target vulnerabilities in third-party vendors, software updates, or partner systems to compromise a primary target’s infrastructure.
  - exploits trusted relationships
  - can infiltrate well-defended organizations and often remain undetected for long periods.
- **Deepfake & AI-Driven Attacks**
  - Use advanced AI techniques
  - attackers create hyper-realistic audio, video, or text impersonations to mislead individuals into taking harmful actions.
  - Such attacks can manipulate public opinion, facilitate fraud, or even impersonate executives in corporate email scams.

Types of Attack (MITRE ATTACK Framework)

- **Advanced Social Engineering (Beyond Phishing)**
  - This category includes tactics like vishing or smishing—each manipulating human behavior to bypass technical defenses.
  - Despite robust technological controls, these attacks succeed by exploiting human trust
  - can be mitigated only through continuous training and awareness.
- **DNS Tunneling & Network Protocol Attacks**
  - DNS tunneling hides malicious data within standard DNS queries and responses to bypass firewall and intrusion detection systems.
  - Such techniques allow attackers to establish covert communication channels, often used in data exfiltration or to maintain persistent access to compromised networks.

Types of Attacks

Passive: "Listening"

- Example: Wiretapping

Active: "Changing"

- Example: Buffer overflow

Example: Buffer Overflow

- Overwriting adjacent memory
- Violates memory safety
- This can be turned into attacks.

Example: Stack Buffer Overflow

The attacker can overwrite

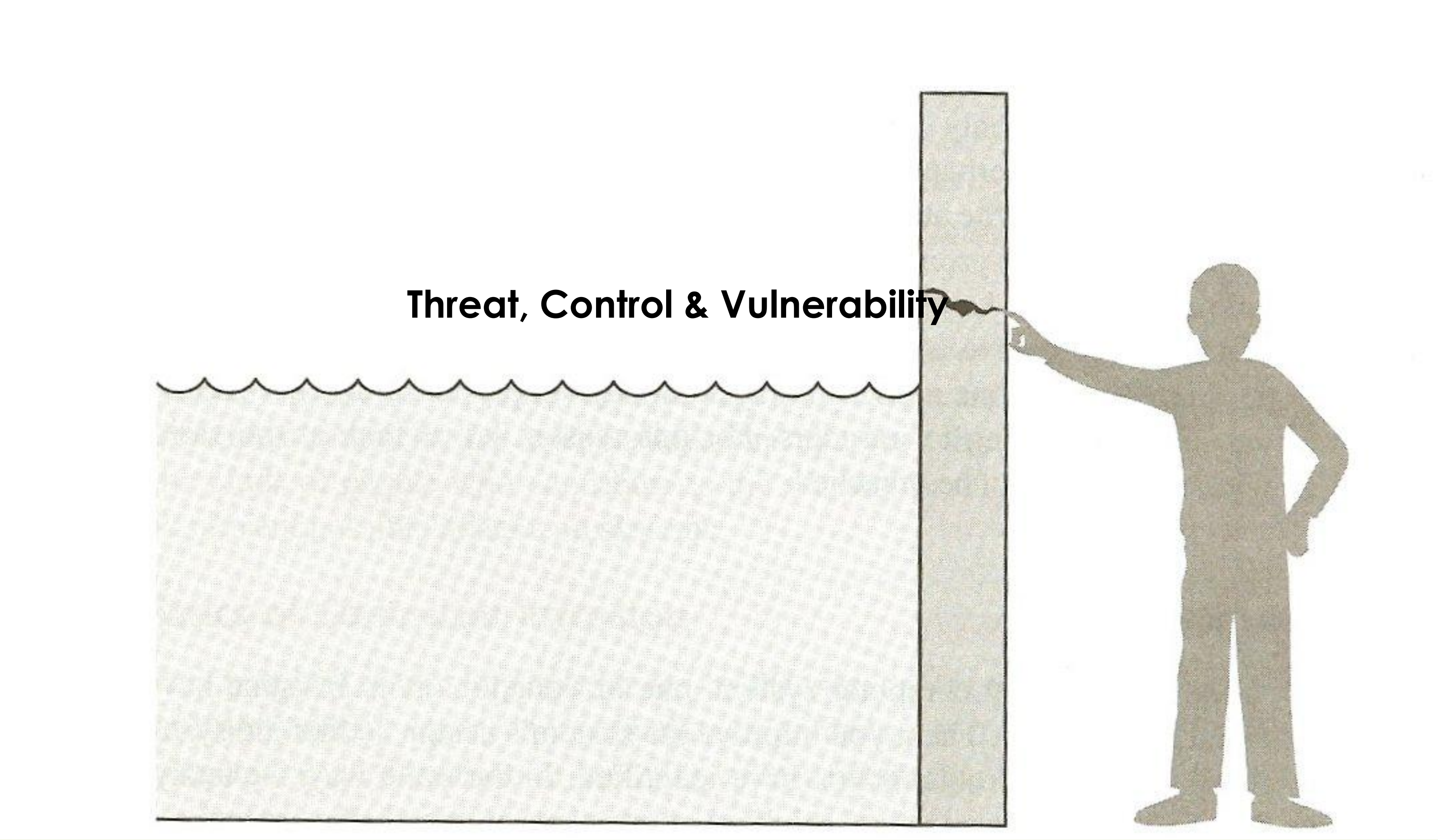
- Local variable
- Return address in a stack frame
- Function pointer
- Parameter of a different stack frame

and then execute malicious code.

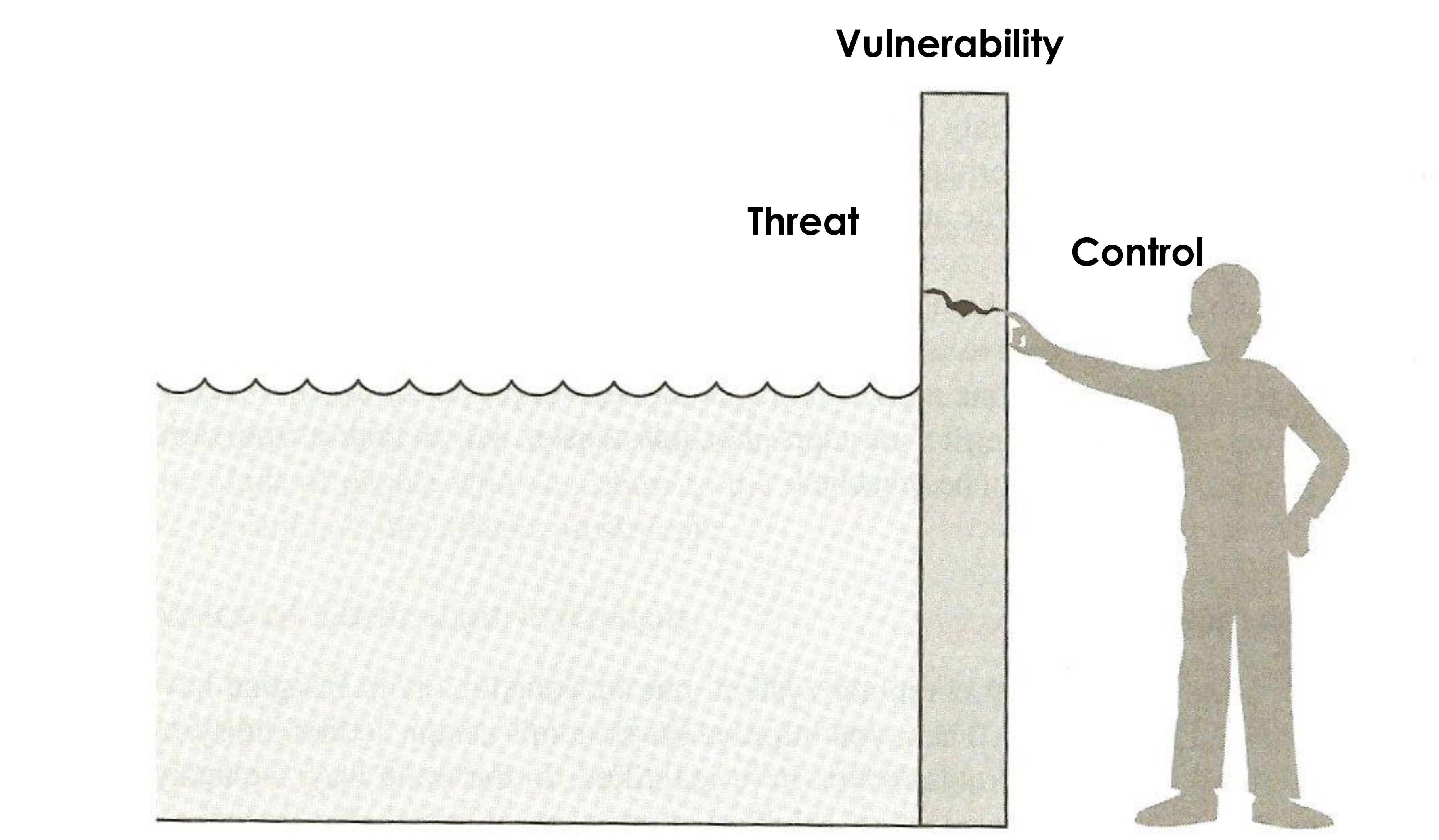
Threats Terms

- Threat
  - Set of circumstances that has the potential to cause loss or harm
  - a potential violation of security.
- Vulnerability
  - Weakness in the system that could be exploited to cause loss or harm
- Attack
  - When an entity exploits a vulnerability on system
- Control
  - A means to prevent a vulnerability from being exploited

Example (Threat, Control & Vulnerability)



Example (Threat, Control & Vulnerability)



Classes of Threats

- Disclosure
  - Unauthorized access to information
- Deception
  - Acceptance of false data
- Disruption
  - Interruption or prevention of correct operation
- Usurpation
  - Unauthorized control of some part of a system

Some Common Threats

- Snooping
  - Unauthorized interception of information
- Modification or alteration
  - Unauthorized change of information
- Masquerading or spoofing
  - An impersonation of one entity by another
- Repudiation of origin
  - A false denial that an entity sent or created something.

More Common Threats

- Denial of receipt
  - A false denial that an entity received some information.
- Delay
  - A temporary inhibition of service
- Denial of Service
  - A long-term inhibition of service

Q&A