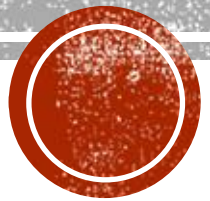
LECTURE 3: UNDERSTAND AND APPLY THREAT MODELING CONCEPTS AND METHODOLOGIES



Learning Outcomes

- By the end of this chapter, students will be able to:
  - Define core threat modeling terminology
  - Explain proactive vs reactive threat modeling
  - Apply STRIDE to identify threats
  - Understand threat modeling in modern systems (cloud, AI, supply chain)
  - Relate threat modeling to risk management and governance

What Is Threat Modeling?

Threat Modeling is a structured security process used to:

Identify potential threats	Analyze how those threats could exploit vulnerabilities	Determine the impact on valuable assets	Define appropriate security controls

Threat Modeling help in preventing security issues *before* they become real attacks.

DICTIONARY

To better understand the main idea of threat modeling, we have to understand some concepts and terminologies

ASSET

- An *asset* is any element that has a value for organization.
  - A **resource**, **process**, product, computing infrastructure, and so forth that an organization has determined must be protected.

THREAT

- The presence of any **potential event** that causes an unwanted impact on the organization
- **ATTACK**
- The presence of any **actual event** that causes an unwanted impact on the organization.

VULNERABILITY

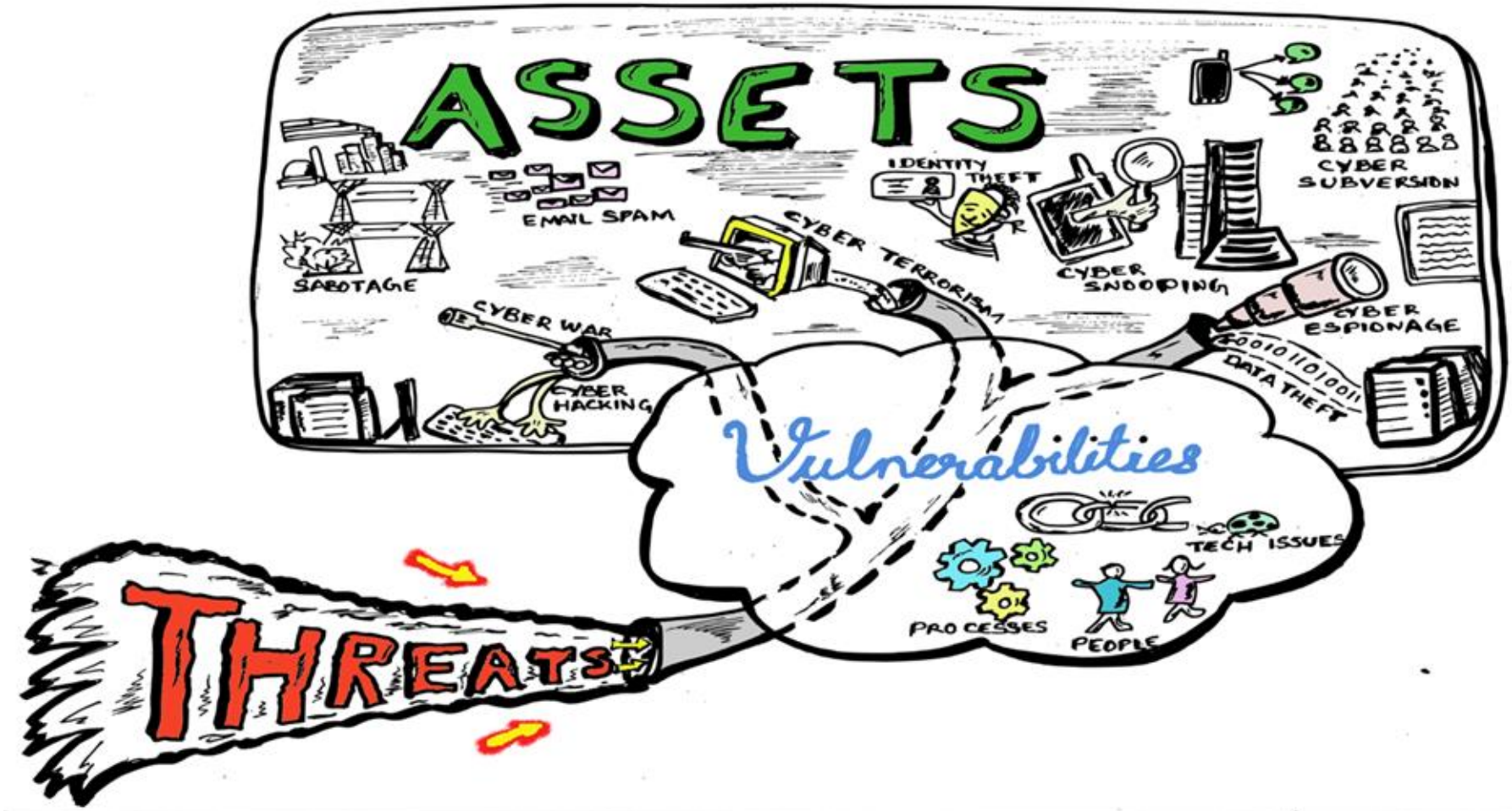
- The absence of safeguard OR a system weakness might be used by threat to cause a damage to the system.

THREAT AGENT

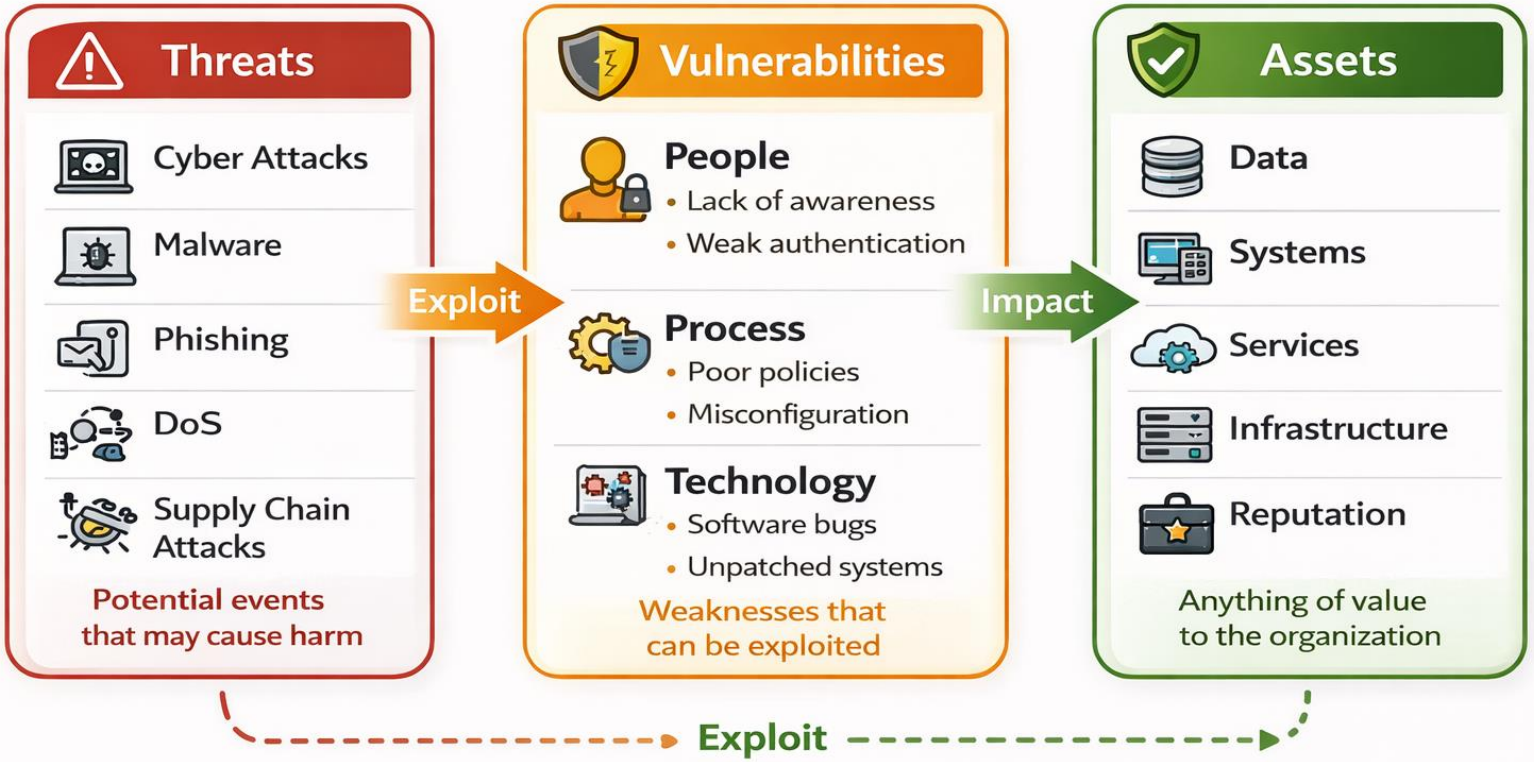
- The entity (a person or process) initiates the threat.

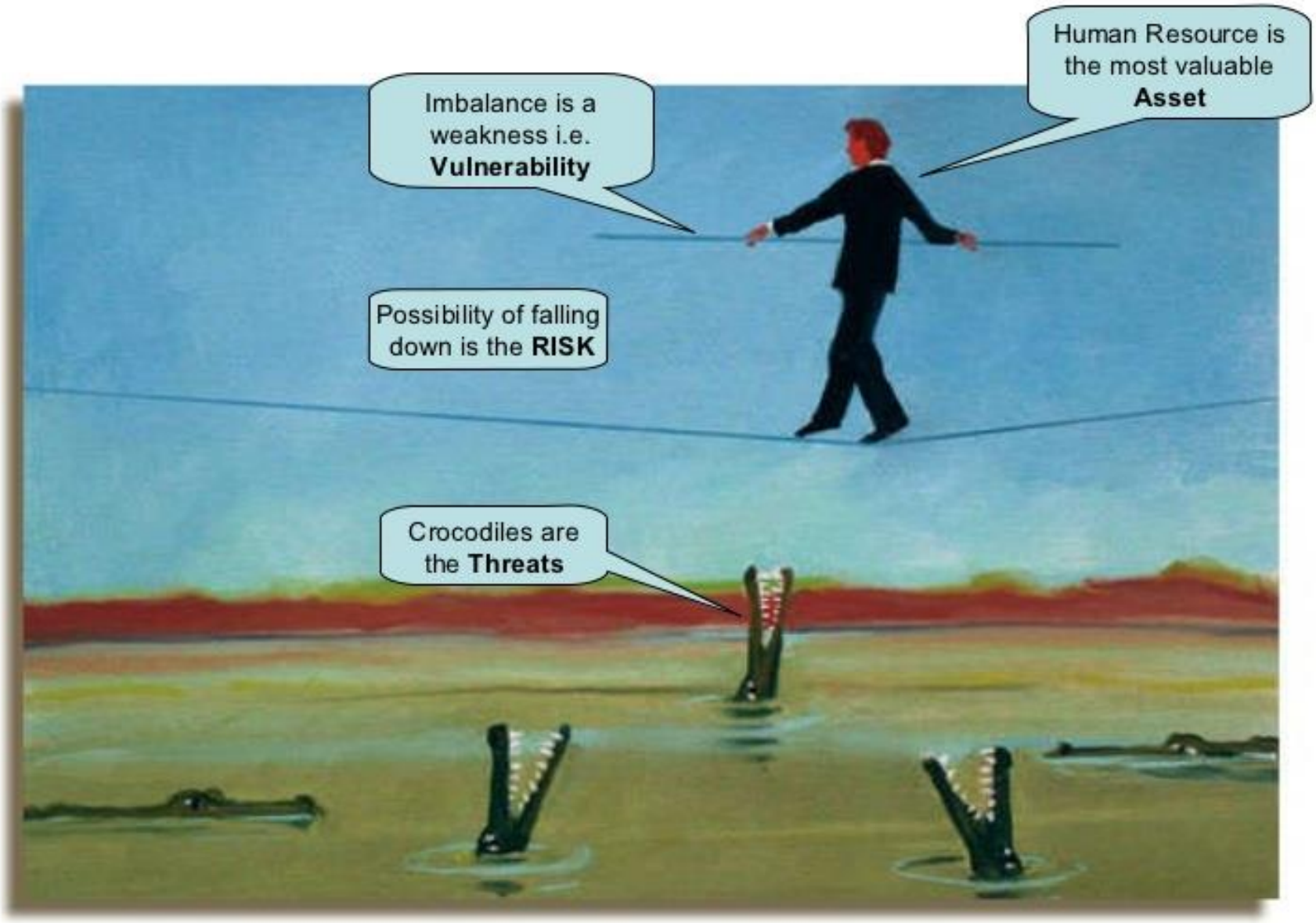
EXPLOIT

- if the vulnerability found by threat agent and threat initiated.


ASSETS
IDENTITY THEFT
CYBER SUBVERSION
EMAIL SPAM
SABOTAGE
CYBER TERRORISM
CYBER SNOOPING
CYBER ESPIONAGE
CYBER WAR
CYBER HACKING
DATA THEFT
Vulnerabilities
TECH ISSUES
PROCESSES
PEOPLE
THREATS

Threat Modeling: Threats, Vulnerabilities, and Assets

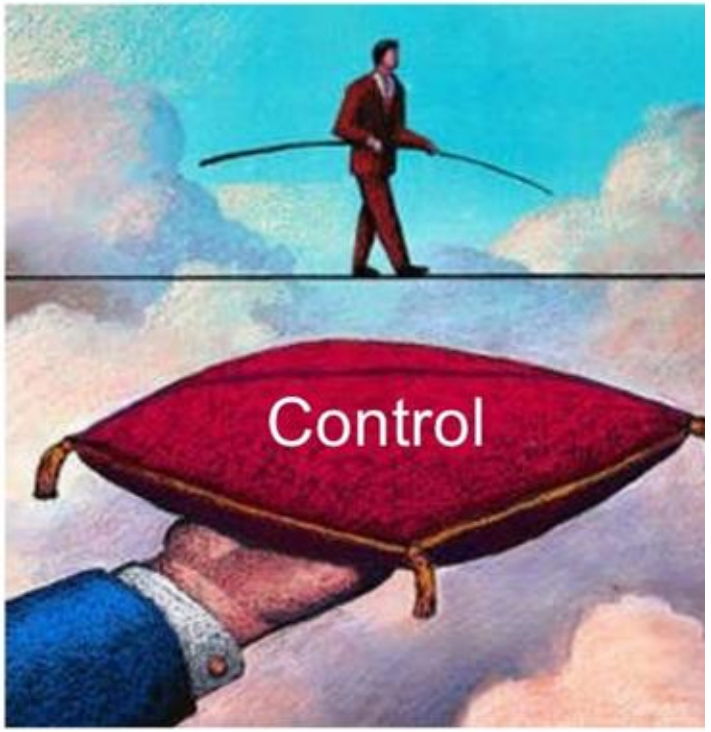



Human Resource is the most valuable **Asset**
Imbalance is a weakness i.e. **Vulnerability**
Possibility of falling down is the **RISK**
Crocodiles are the **Threats**

DICTIONARY

CONTROL/COUNTERMEASURE/SAFEGUARD

- Any step/action to prevent the threat exploiting the vulnerability.
- (OR): Minimize the damage of the exploit



RISK ELEMENTS

- A *risk* is the possibility or likelihood that a threat will exploit a vulnerability resulting in a loss such as harm to an asset.
- **Risk management** attempts to reduce or eliminate vulnerabilities or reduce the impact of potential threats by implementing controls or countermeasures.
- Risk elements are:
  - Threat
  - Vulnerability
  - Asset
  - Damage

When Is Threat Modeling Performed?

- *Threat modeling* can be performed as:
  - Proactively
    - During system design and development
    - So, Security is built in from the start
  - Reactively
    - After deployment or after incidents
    - Based on observed attacks or failures

When Is Threat Modeling Performed?

- ***A PROACTIVE APPROACH*** to threat modeling is known as a **defensive approach**.
  - This method is based on predicting threats and designing in specific defenses during the coding and crafting process, rather than relying on post-deployment updates and patches.
  - During system design and development
    - So, Security is built in from the start
- ***A REACTIVE APPROACH*** to threat modeling takes place after a product has been created and deployed or after an incident.
  - This type of threat modeling is also known as ***the*** **adversarial approach**.

Which approach is the preferred one:
Proactive threat modeling is the preferred and more effective approach.

IDENTIFYING THREATS
Key Approaches

- **Focused on Assets** This method uses asset valuation results and attempts to identify threats to the valuable assets
- **Focused on Attackers** Some organizations are able to identify potential attackers and can identify the threats they represent based on the attacker's goals.
- **Focused on Software** If an organization develops software, it can consider potential threats against the software.

Identifying Threats – Key Approaches

Asset-Focused Approach

- ✓ Start with valuable assets
- ✓ Use asset valuation results
- ✓ Identify threats to critical assets

What can harm our most valuable assets?

What can harm our most valuable assets?

Attacker-Focused Approach

- ✓ Identify potential attackers
- ✓ Analyze attacker goals and motives
- ✓ Predict likely threats

Who would attack us and why?

Who would attack us and why?

Software-Focused Approach

- ✓ Analyze application design
- ✓ Identify abuse and misuse cases
- ✓ Focus on software weaknesses

How can this software be attacked?

How can this software be attacked?

Most organizations use a combination of **all three approaches**.

IDENTIFYING THREATS
Key Approaches

Assets (What you want to protect)

- **Examples:** data, systems, money, reputation, intellectual property.
- **Key question:** *"What is valuable to the organization or individual?"*

Threat Actors / Attackers (Who could harm you)

- **Examples:** hackers, insiders, competitors, nation-states, malware authors.
- **Key question:** *"Who would want to harm these assets and why?"*

Vulnerabilities / Software (How attackers could harm you)

- **Examples:** software bugs, misconfigurations, weak passwords, lack of encryption.
- **Key question:** *"Where are the weaknesses that could be exploited?"*

Other Approaches in Modern Threat Modeling

1- System / Architecture-Focused

- Focuses on system components, their interactions, and trust boundaries.
- Looks at how threats exploit structural weaknesses, not just assets or software bugs.
- Why it matters:
  - Modern systems are distributed (microservices, APIs, cloud services).
  - An attack on a weakly protected service can compromise the entire system.
- Examples:
  - Exposed internal APIs in a cloud app allow data exfiltration.
  - Misconfigured firewall rules between containers lead to lateral movement.
  - IoT network segmentation not enforced, allowing attacker access to critical devices.

Other Approaches in Modern Threat Modeling

2- Data-Focused

- Focuses on **sensitive data**, how it is stored, transmitted, or processed.
- Data breaches are the **most common impact** of modern cyber incidents.
- Protecting assets alone doesn't guarantee data security.
- Examples:
  - Customer personal data stored unencrypted in a cloud database.
  - Logs containing PII sent over unsecured channels.
  - GDPR-regulated data processed by third-party SaaS without proper consent.

Other Approaches in Modern Threat Modeling

3- Supply Chain / Third-Party Focused

- Focuses on vendors, libraries, APIs, and other external dependencies.
- Attackers increasingly exploit **weak links outside the organization**.
- Modern software relies on third-party packages or services.
- Examples:
  - Compromised third-party software update used in corporate software.

Other Approaches in Modern Threat Modeling

4- Environment / Deployment-Focused

- Looks at the environment where the system runs: cloud, on-prem, hybrid, containerized.
- Includes configuration management, patching, and deployment pipelines.
- Misconfigurations are a top attack vector in modern systems.

5- Emerging Technology Focus

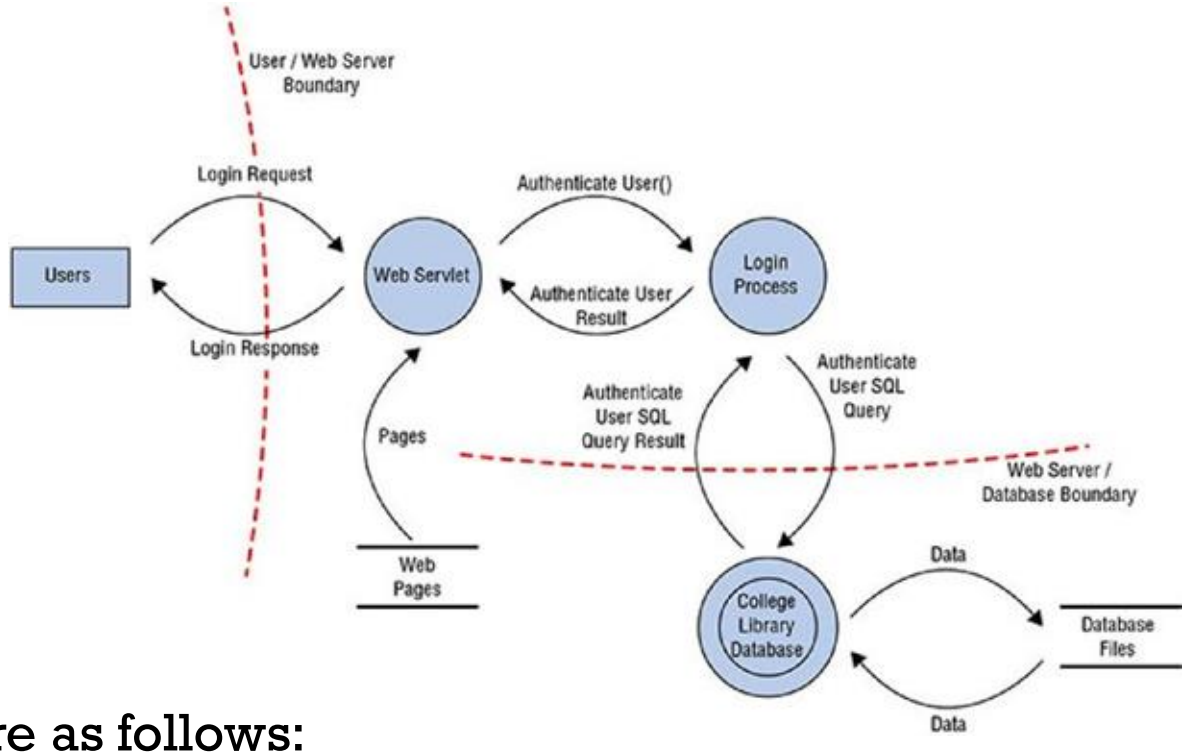
- **AI-Powered Systems:** Automated decision-making (Agentic-AI) can be exploited.
- **IoT / OT Systems:** Sensors, actuators, or industrial control systems can be attacked physically or digitally.

Example:

- A university uses an online learning platform where students can:
  - Submit assignments
  - Take quizzes and exams
  - Access lecture notes and resources
- The platform stores sensitive information such as:
  - Student personal info (ID, email, grades)
  - Faculty login credentials
  - Academic records

Asset	Threat Actor	Vulnerability/Software	Threat Scenario
Student grades	Student	Weak authentication	Student changes their own grade
Exam content	Hacker	SQL injection	Hacker extracts upcoming exam questions
Faculty login	Hacker	Phishing, no MFA	Hacker accesses faculty account to manipulate data
Platform uptime	Insider	Misconfigured permissions	Staff deletes files causing downtime

IDENTIFYING THREATS



The three primary steps are as follows:

1. Identify all of the technologies involved.

2. Identify attacks that could be targeted at each element of the diagram. Keep in mind that all forms of attacks should be considered, including logical/technical, physical, and social.

3. Prevention measures.

Threat Models

- There are several threat models:
  - STRIDE
  - PASTA
  - LINDDUN
  - CVSS
  - Attack Trees
  - Persona non Grata
  - OCTAVE
  - Others

In this course we will cover STRIDE model, Other models will be covered in CYS 403

Think like hackers
Predict the issues
before they happen

STRIDE THREAT MODEL

- In order to assess the security of a system, we must therefore look at all the possible threats.
- The STRIDE model is a useful tool to help us classify threats.
- To categorize a threat, it is often helpful to use a guide or reference to do so, a well-known guide is known as STRIDE.
- STRIDE is a threat categorization scheme developed by Microsoft.

STRIDE THREAT MODEL – CONT.

1. **Spoofing**: gaining access through falsified identity
2. **Tampering**: unauthorized changes or manipulation of data
3. **Repudiation**: Ability to deny having performed an action/activity
4. **Information disclosure**: Revelation or distribution of private, confidential, or controlled information to unauthorized entities
5. **Denial of service (DoS):** Prevent authorized use of a resource. This can be done through connection overloading or traffic flooding
6. **Elevation of privilege:** A limited user account is transformed into an account with greater privileges, powers, and access.

Although STRIDE is typically used to focus on application threats, it is applicable to other situations, such as network threats

Other attacks may be more specific to network, such as sniffing.

STRIDE

Threat	Property Violated	Example	Mitigation Approach/ Countermeasures
Spoofing	Authentication	Pretending to be any of Bill Gates, Paypal.com or ntdll.dll	Digital signatures, Active directory, LDAP Passwords, crypto tunnels
Tampering	Integrity	Modifying a DLL on disk or DVD, or a packet as it traverses the network	Hashing, Digital signatures, ACLs/permissions, crypto tunnels
Repudiation	Non-repudiation	"I didn't send that email," "I didn't modify that file," "I certainly didn't visit that web site, dear!"	Digital Signatures, Customer history risk management, Logging
Information Disclosure	Confidentiality	Allowing someone to read the Windows source code; publishing a list of customers to a web site.	Encryption, Access Control Lists, PGP (for emails), SSL/TLS
Denial of Service	Availability	Crashing Windows or a web site, sending a packet and absorbing seconds of CPU time, or routing packets into a black hole	Load Balancers, more capacity
Elevation of Privilege	Authorization	Allowing a remote internet user to run commands is the classic example, but going from a limited user to admin	Isolation, Input Validation, Firewalls, Sandboxing

STRIDE Example 1: a Web Application

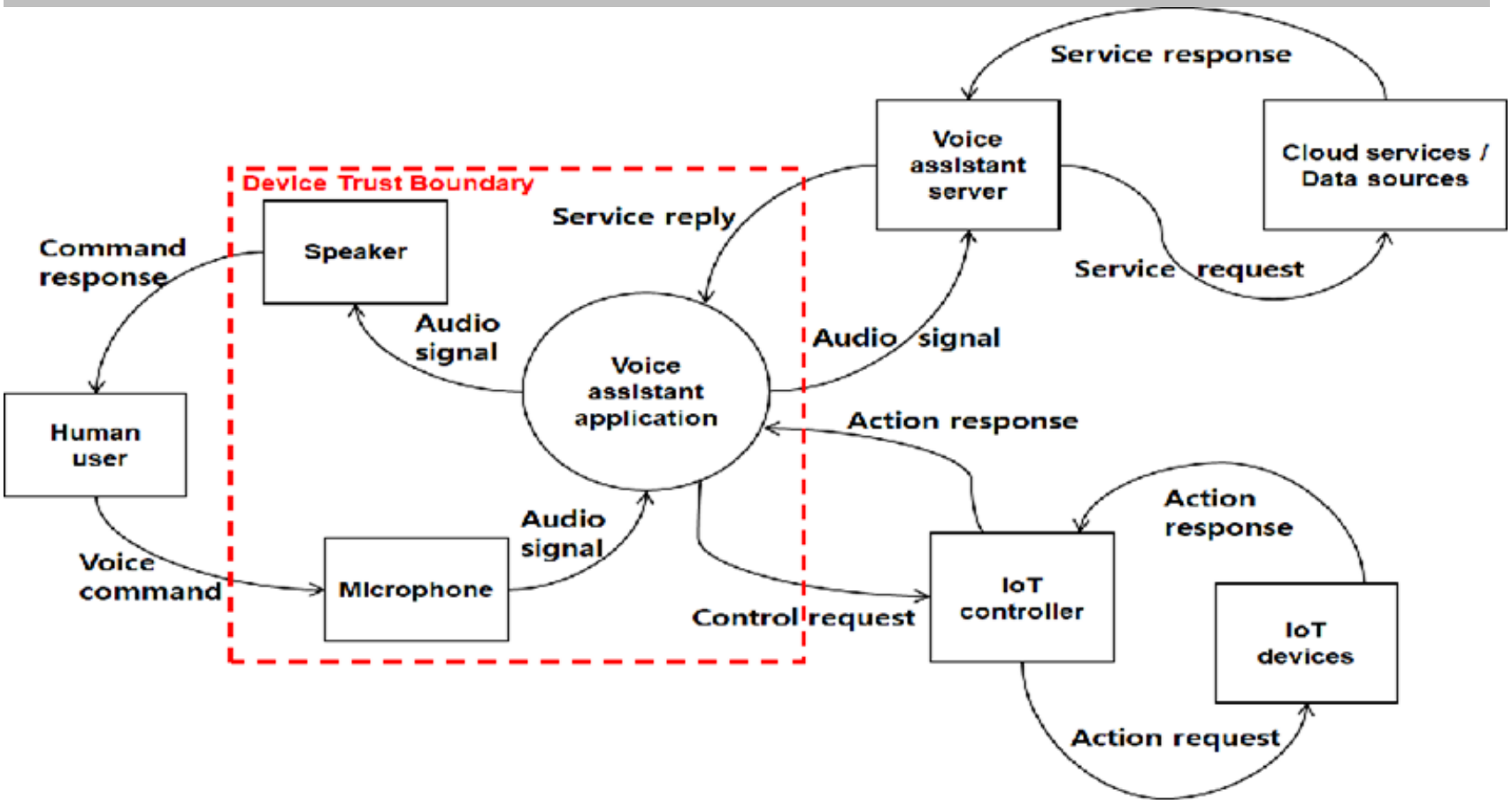
STRIDE	Example Threat
S – Spoofing	An attacker logs in using stolen credentials
T – Tampering	User modifies form data to change prices
R – Repudiation	User performs a transaction and denies it later
I – Information Disclosure	Sensitive user data exposed via API
D – Denial of Service	Flooding the server with requests to crash it
E – Elevation of Privilege	Regular user exploits a bug to become admin

STRIDE Example 2: a mobile app

An online banking app allows users to transfer money, check balances, and update account information.

STRIDE	Example Threat
S – Spoofing	Attacker logs in using stolen credentials
T – Tampering	Modifying transfer amount in transit
R – Repudiation	Denying a fraudulent transfer
I – Information Disclosure	Account balances exposed via API
D – Denial of Service	Flood login page to prevent access
E – Elevation of Privilege	Exploit bug to access admin panel

STRIDE THREAT MODEL EXAMPLE 3



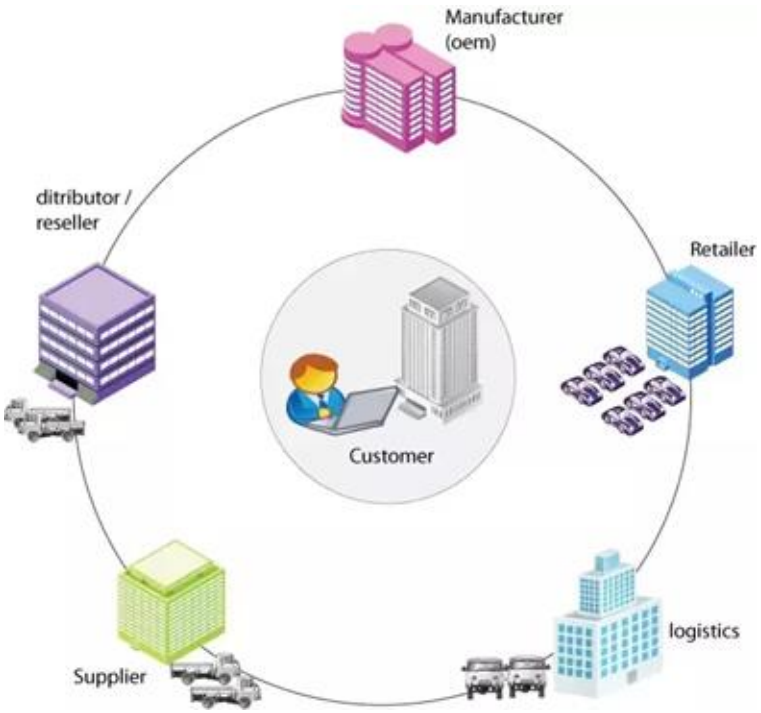
Threat Modeling in the Supply Chain

Modern systems rely on third parties

Threats may originate outside the organization

Trust boundaries extend beyond internal systems

APPLY CYS CONCEPTS TO THE SUPPLY CHAIN



- **A SUPPLY CHAIN IS** A NETWORK BETWEEN A COMPANY AND ITS SUPPLIERS TO PRODUCE AND DISTRIBUTE A SPECIFIC PRODUCT TO THE FINAL BUYER.

- **A *SUPPLY CHAIN*** is the concept that most computers, devices, networks, and systems are not built by a single entity.

APPLY CYS CONCEPTS TO THE SUPPLY CHAIN

- ***A SECURE SUPPLY CHAIN*** is one in which all of the vendors or links in the chain are reliable, trustworthy, reputable organizations that disclose their practices and security requirements to their business partners.
- The goal of a secure supply chain is:
  - to ensure that the finished product is of sufficient quality, meets performance and operational goals, and provides stated security mechanisms, and
  - that at no point in the process was any element counterfeited or subjected to unauthorized or malicious manipulation or sabotage.

APPLY CYS CONCEPTS TO THE SUPPLY CHAIN

- Integrating security assessments **when working with external entities** is just as important as ensuring a product was designed with security in mind.

APPLY CYS CONCEPTS TO THE SUPPLY CHAIN

CYS team should inspect the connected systems throughout:

- **On-Site Assessment** Visit the site of the organization to interview personnel and observe their operating habits.
- **Document Exchange and Review** Investigate the means by which datasets and documentation are exchanged as well as the formal processes by which they perform assessments and reviews.
- **Process/Policy Review** Request copies of their security policies, processes/procedures, and documentation of incidents and responses for review.
- **Third-Party Audit** Having an independent third-party auditor

Thank you