8/26/2022

UNIT - II

THREATS & PROGRAM SECURITY

by

Mr. Ajay Kumar Badhan

Assistant Professor

M.TECH[CST], B.TECH [CSE]

Email: ajay.27337@lpu.co.in

Personal Blog: https://ajaykumarbadhan.wordpress.com/

Preferred Text Book

- **Information System Security Wiley Publications by Nina Godole, Wiley**
- **Computer Security: The Complete Reference Roberta: Tata Mcgraw Gill by Bragg, Mcgraw Hill Edition**

CONTENT

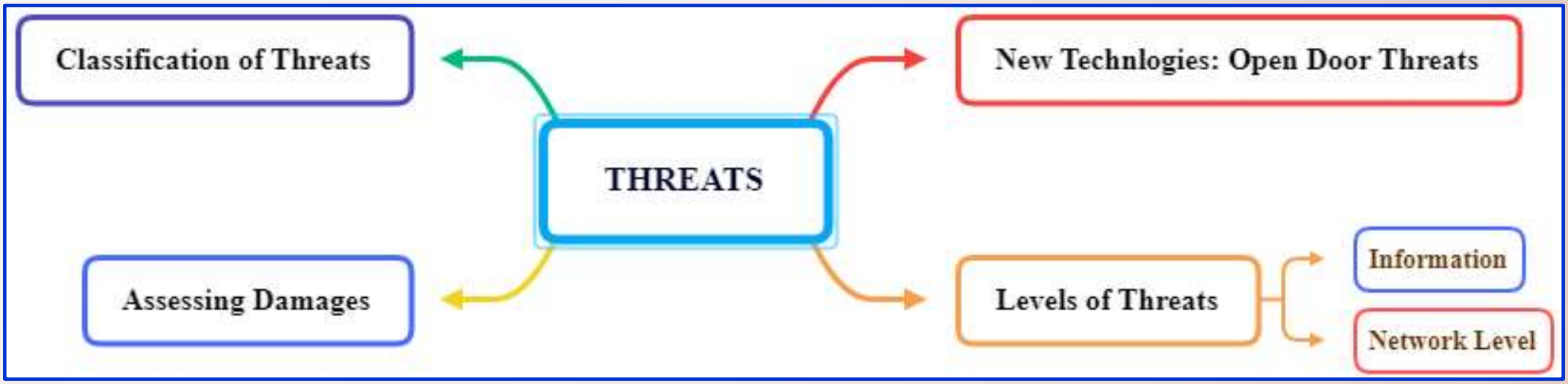
THREATS

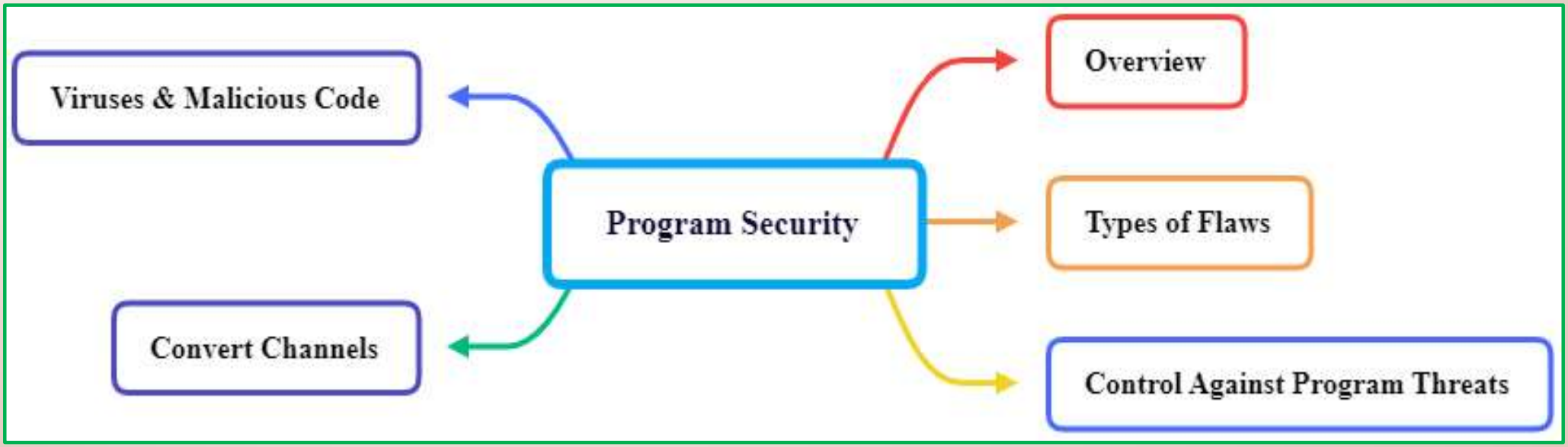
- New Technologies
- Levels of Threats
  - ✓ Information
  - ✓ Network Level
- Classification of Threats
- Assessing Damages
- Privacy Threat

PROGRAM SECURITY

- Overview
- Types of Flaws
- Viruses & Other malicious code
- Control against Program threats
- Covert Channels

CONTENT - GRAPHICAL PRESENTATION





INTRODUCTION TO THREAT

Threat

1. In computer security, a threat is a possible danger that might exploit a vulnerability to **breach** security and therefore cause possible harm.
2. A threat can be either:
   - "**intentional**" (i.e. hacking: an individual cracker or a criminal organization) or
   - "**accidental**" (e.g. the possibility of a computer malfunctioning, or
   - the possibility of a **natural disaster** such as an **earthquake**, a **fire**, or a **tornado**) or
   - otherwise a circumstance, capability, action, or event.

New Technologies Open Door to Threats

1. All organizations have IS that use integrated technologies such as networks of computers, company intranet, and internet access to communicate and transfer information for rapid business decisions, thereby opening the organization to the external world like never before.
2. In these circumstances threats from outside the organization must be addressed because damages can result in great consequences for the organization.

INTRODUCTION TO THREAT

Different Terms

1. **Threat** ⇒ Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

   (***A threat is what we're trying to protect against***)

2. **Vulnerability** ⇒ Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.

   (***A vulnerability is a weakness or gap in our protection efforts***)

3. **Risk** ⇒ The potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability.

   (***Risk is the intersection of assets, threats, and vulnerabilities***)

4. **Asset** ⇒ It is any data, device, or other components of the environment that supports information-related activities. It includes **hardware**, **software**, and **confidential information**.

5. **Counter Measures** ⇒ Set of actions implemented to prevent threats

INTRODUCTION TO THREAT

Information Level Threats

1. Threat that involves the dissemination of information in such a way that organizations, their operations, and their reputations may be affected.
2. Dissemination may be active in case of sending an e-mail or it may be passive as in case of setting up websites.

Network Level Threats

1. In order to make the threat effective, potential attackers require network access to corporate computer systems or to networks used by corporate computer systems.
2. Other security issues involved when data are transmitted over the network are
   - confidentiality,
   - authentication,
   - integrity, and
   - non-repudiation.

INTRODUCTION TO THREAT

Examples: Information Level Threat

1. SQL Injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements (also commonly referred to as a malicious *payload*) that control a web application's database server.
2. Since an SQL Injection vulnerability could possibly affect any website or web application that makes use of an SQL-based database, the vulnerability is one of the oldest, most prevalent and most dangerous of web application vulnerabilities.

Example: Network Level Threats

1. DOS (Denial of Services) attack (flooding accounts with large quantities of e-mail is a network-based attack)
2. **DOS attack:** Services provided by the server to the fake user(attacker) rather than the authorized user.

INTRODUCTION TO THREAT

Four Source of Risk

1. **Human Error**
   - disclosure of confidential information.
2. **Computer Abuse or Crime**
   - when a person intends to be malicious and starts to steal information from sites.
   - It is defined as any illegal act in which a computer is used as the primary tool.
   - It is unethical use of a computer.
3. **Natural & Political Disaster**
   - This can happen in the form of natural calamities and wars.
4. **Failure of Hardware & Software**
   - server malfunctioning, software errors etc.

INTRODUCTION TO THREAT

Terms in Threat

1. Impersonation

- an act of pretending to be another person for the purpose of entertainment or fraud
- The impersonator enjoys the privileges of a legitimate(Legal) user by gaining access to a system by identifying oneself as another person after having defeated the identification and authentication controls employed by the system.

2. Trojan Horse

- Concealing with an authorized program a set of instructions that will cause unauthorized actions.

3. Logic Bombs

- A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met
- Unauthorized instructions which stay dormant until a specific event occurs, at which time they bring into effect an unauthorized act.

4. Computer Virus

- Segment of code that are able to perform malicious acts and insert copies of themselves into other programs in the system.

INTRODUCTION TO THREAT

Terms in Threat

5. **Dial Diddling**
   - Changing data before or during input, often to change the contents of database.
6. **DOS**
   - Rendering the system unusable by legitimate user.
7. **Salami Technique**
   - A salami attack is a small attack that can be repeated many times very efficiently.
   - Diverting small amount of money from a large number of accounts maintained by the system.
8. **Spoofing**
   - Configuring a computer system to masquerade(pretend) as another system over the network in order to gain unauthorized access to the recourses of the system.
9. **Data Leakage**
   - There are variety of methods for obtaining data stored in the system.

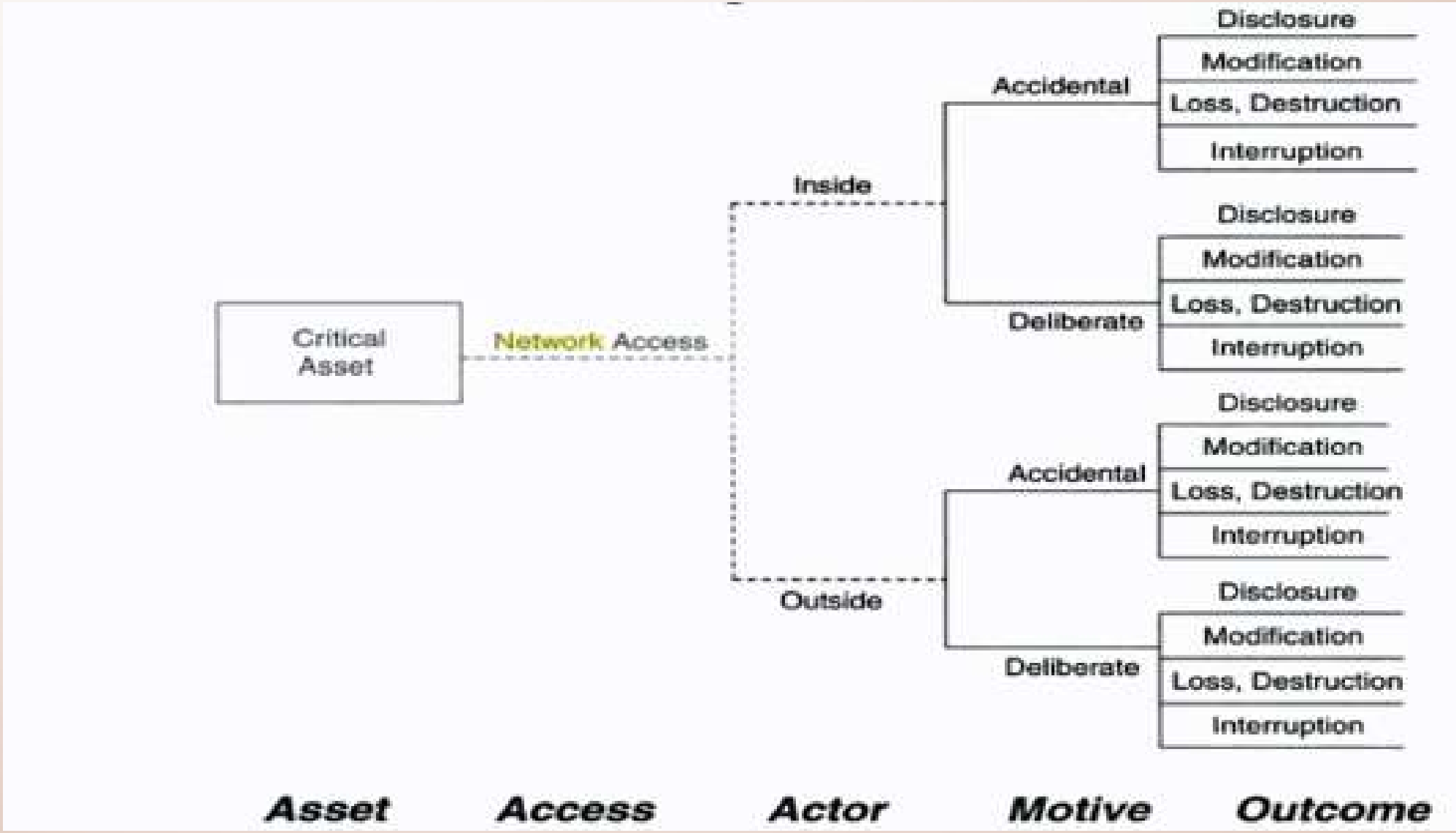
INTRODUCTION TO THREAT

Threat Profile ⇒ Four things to be considered while evaluating threat

1. **Asset**
   - Something of value to the organization.
2. **Actor/Attacker**
   - who or what may violate the security requirements(CIA)
3. **Motive**
   - indication of whether the actor's intentions are deliberate or accidental.
4. **Access**
   - how the asset will be accessed by the actor.
9. **Outcome**
   - the immediate result of violating the security requirements of an asset.

INTRODUCTION TO THREAT

Generic Threat Profile



INTRODUCTION TO THREAT

Asset Types ⇒ Logical or Physical

1. **Information**
   - document data or intellectual property used to meet the mission of an organization.
2. **Software**
   - software applications and services that process ,store or transmit information.
3. **Hardware**
   - IT physical devices considering their replacement costs.
4. **People**
   - People in organization that possess skills, competencies, knowledge and experience that are difficult to replace.
9. **Systems**
   - IS that process and store information.

INTRODUCTION TO THREAT

Accessing Costs of Threats ⇒ The cost of threats is calculated based on following factors:

1. **Productivity**
   - Number of employees affected
   - Number of hours wasted
   - Cost per hour /per employee
2. **Revenue**
   - Direct Financial Loss
   - Future Financial Loss
3. **Financial Performance**
   - Credit Rating and Stock price
4. **Other Expenses**
   - Overtime Costs
   - Travel Expenses
   - Third Party Costs
   - Equipment Rental Costs
5. **Hidden Costs**
   - Difficult to calculate
   - Cost of Damaged Reputation
   - Loss of faith by customers, bankers or vendors

INTRODUCTION TO THREAT

Impact of Threat on Information System

1. Impact can be financial, in form of immediate costs and losses of assets.
2. For example the cost of downtime per hour caused by a DOS attack can be computed by measuring the loss of:
   - **Productivity** ⇒ (no. of employees impacted)*(hours wasted)* (burdened hourly rate)
   - **Revenue** ⇒ direct loss and lost future revenue.
   - **Financial performance** ⇒ credit rating and stock price.
   - **Other expenses** ⇒ equipment rental overtime costs, extra shipping costs, travel expenses etc.

INTRODUCTION TO THREAT

Protecting Information System Security

1. **Preventive Controls:** Prevent an error or an attack from taking effect.
2. **Detective Controls:** Detect a violation. These controls exist to detect and report when errors , omissions and unauthorized use or entry occur.
3. **Corrective control:** Detect and correct an exceptional situation. These controls are designed to correct errors, omissions and unauthorized users and intruders once they are detected.

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Deviations in quality of service from service providers	Power and WAN service issues
9. Forces of nature	Fire, flood, earthquake, lightning
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

INTRODUCTION TO THREAT

Some Examples of INFOSEC Threats

1. **Hacktivism:** The practice of gaining unauthorized access to a computer system and carrying out various disruptive actions as a mean of achieving political & social goals.
   - Hacktivism is the act of misusing a computer system or network for a socially or politically motivated reason. Individuals who perform hacktivism are known as hacktivists.
   - Hacktivism is meant to call the public's attention to something the hacktivist believes is an important issue or cause, such as freedom of information or human rights.
   - It can also be a way for the hacktivists to express their opposition to something by, for instance, displaying messages or images on the website of an organization they believe is doing something wrong.
2. **Advanced Persistent Threat (APT):** It is a prolonged and targeted cyber attack in which an intruder gains access to a network and remains undetected for an extended period of time.
   - The intention of an APT attack is usually to monitor network activity and steal data rather than to cause damage to the network or organization

INTRODUCTION TO THREAT

Some Examples of INFOSEC Threats

1. **Whaling Attack:** A whaling attack, also known as whaling phishing attack.
   - It is a specific type of **Phishing** attack that targets high-profile employees, such as the CEO or CFO, in order to steal sensitive information from a company, as those that hold higher positions within the company typically have complete access to sensitive data.
   - In many whaling phishing attacks, the attacker's goal is to manipulate the victim into authorizing high-value wire transfers to the attacker.
2. **Advanced Persistent Threat (APT):** It is a prolonged and targeted cyber attack in which an intruder gains access to a network and remains undetected for an extended period of time.
   - The intention of an APT attack is usually to monitor network activity and steal data rather than to cause damage to the network or organization