

Lecture 2: Threats to Information Security

Classification of Threats and Vulnerabilities



Agenda

01

Basic Concepts: Threat, Attack,

Vulnerability

02

The "Danger Window"

03

Four Main Types of Threats
(Attacks)

04

Threat Classification Criteria

05

Practical Examples of Key Threats

06

Countermeasure Strategies

07

Key Takeaways

Basic Concepts: Terminology



Threat

A potential opportunity to violate information security.

Attack

An active attempt to implement a threat.

Attacker

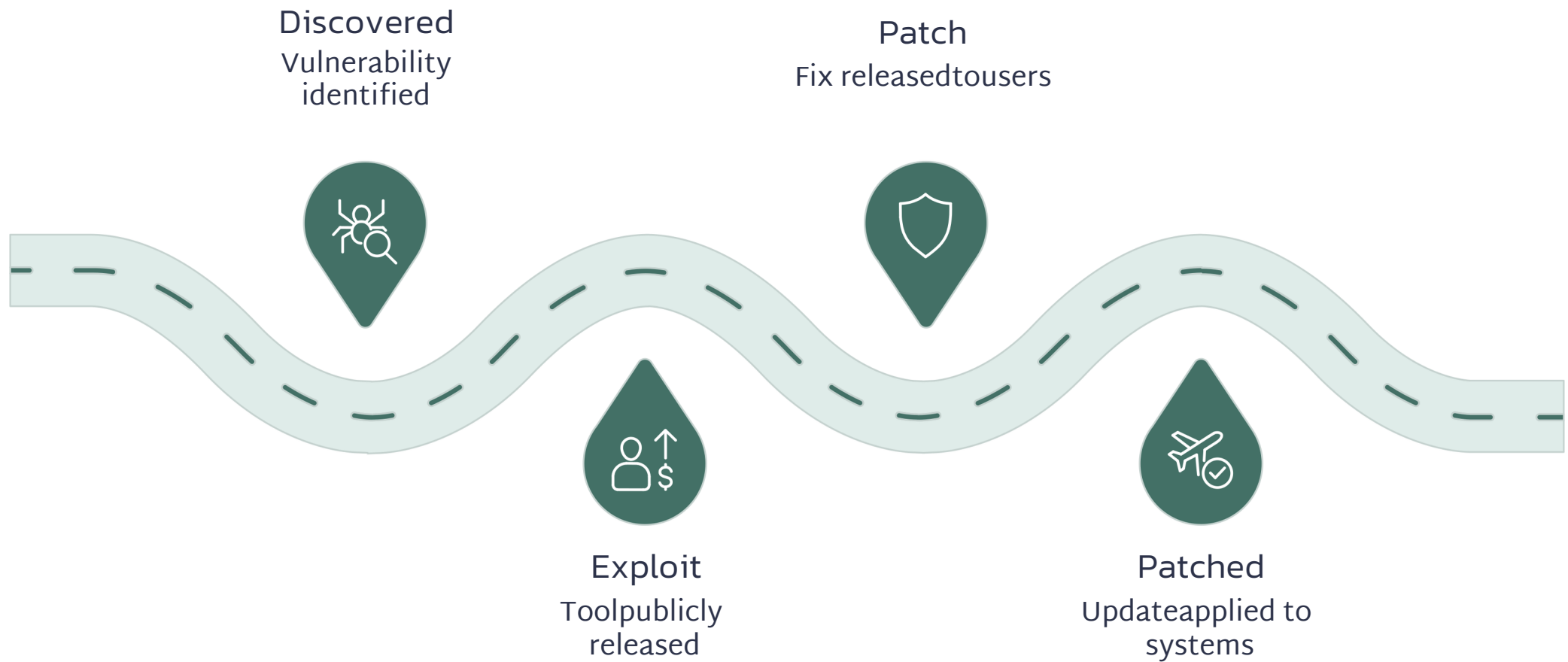
The source making the attempt.

Vulnerability

A weakness in system protection (e.g., software error, poor configuration).

The "Danger Window"

The time interval from a vulnerability's discovery to when it is patched.



Patches require creation, release, and installation, meaning systems are in a constant state of risk.

Four Main Types of Threats

Attacks are classified by their result, directly linking to security components.



Interruption

Attack on Availability: System becomes inaccessible (e.g., DoS, cutting a cable).



Interception

Attack on Confidentiality: Unauthorized party gains access (e.g., eavesdropping, copying files).



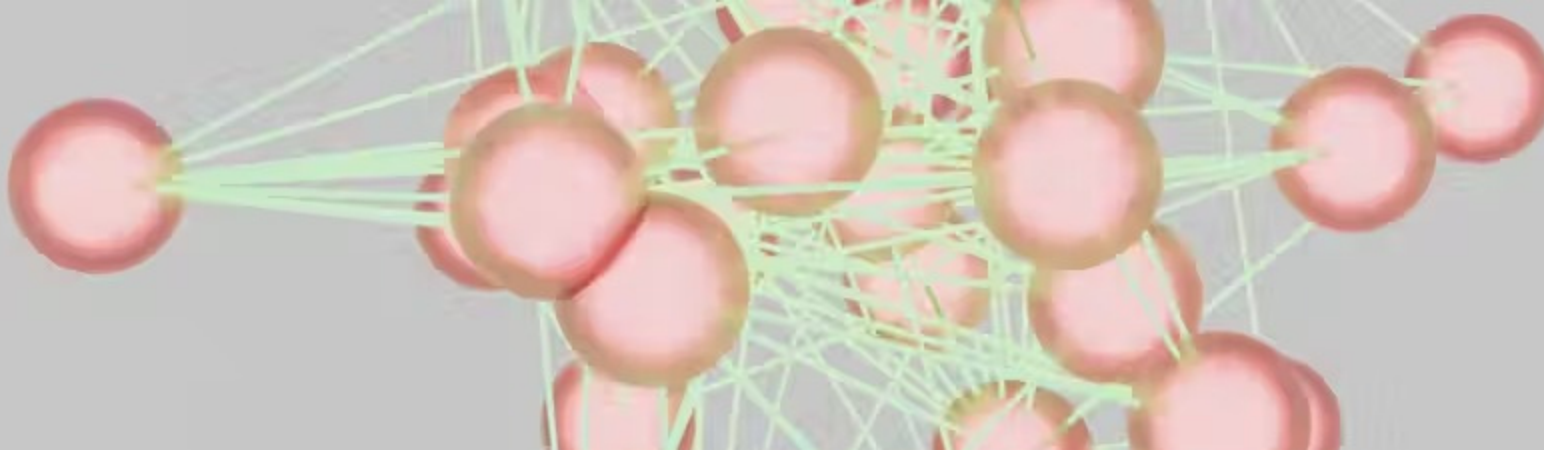
Modification

Attack on Integrity: Unauthorized party tampers with system components (e.g., changing data, altering code).



Counterfeiting

Attack on Authenticity: Unauthorized party introduces fraudulent objects (e.g., fake messages, unauthorized entries).



Threat Classification Criteria

Threats can be categorized in several ways to understand their nature and origin.

1

Aspect of Information Security

Targets Availability, Integrity, or Confidentiality.

2

Components of Information Systems

Targets data, programs, hardware, or infrastructure.

3

Method of Implementation

Accidental or deliberate; natural or man-made.

4

Location of Source

Originates from inside or outside the system.

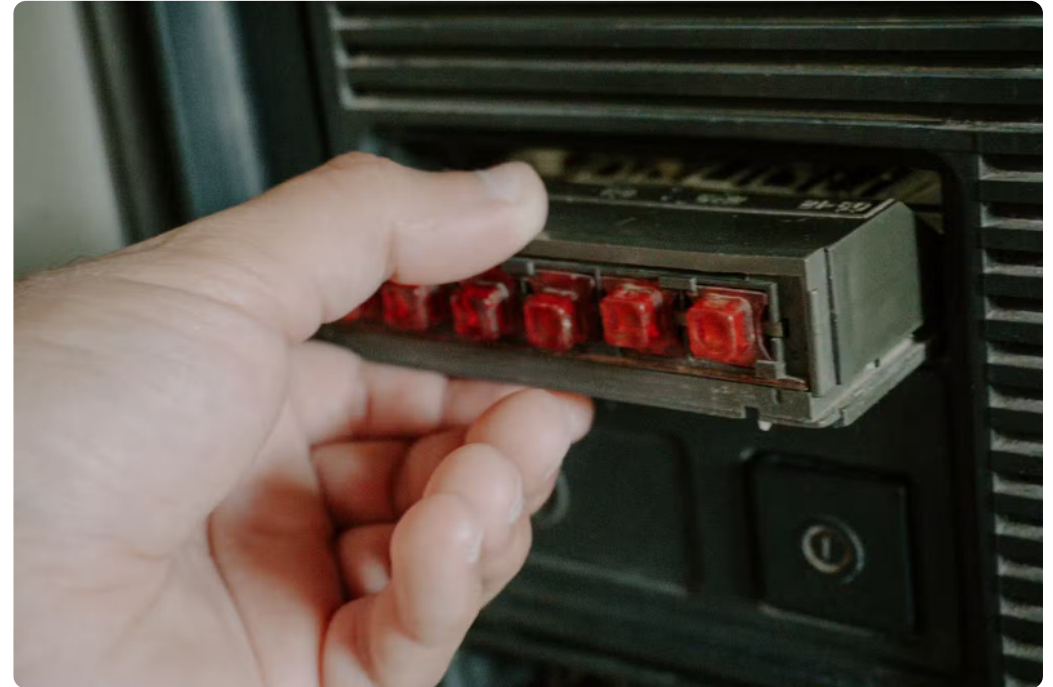
Examples of Key Threats

Accessibility Threats

- Unintentional Errors: Most frequent and damaging.
- Infrastructure Failure: Power outages, communication loss.
- Internal Failure: System deviations, software/hardware issues.
- "Offended" Employees: Deliberate harm from insiders.

Integrity Threats

- Static Integrity: Incorrect data entry or changes.
- Program Integrity: Malware injection.
- Dynamic Integrity: Violation of operation sequence (e.g., data reordering).



Confidentiality Threats

- Non-Technical / Physical: Lost devices, written passwords.
- Data Interception: Unencrypted data transfer.
- Unprotected Backups: Insecure storage of backup media.
- Social Engineering: Deception to gain access (e.g., masquerade).

Countermeasure Strategies

Linking controls directly to specific threats.



Availability

Hardware: UPS, redundant power, mirrored drives.

Organizational: Disaster recovery plans, fire/water detection.



Confidentiality

Hardware: Shielding for electromagnetic radiation.

Software: Cryptography, identification, access controls.

Organizational: Physical access controls, personnel selection.



Integrity

Software: Antivirus, logging, audit tools, access controls.

Hardware: Backup systems, mirrored drives.



Authenticity

Software: User identification, authentication, digital signatures.

Key Takeaways

Threats are Diverse

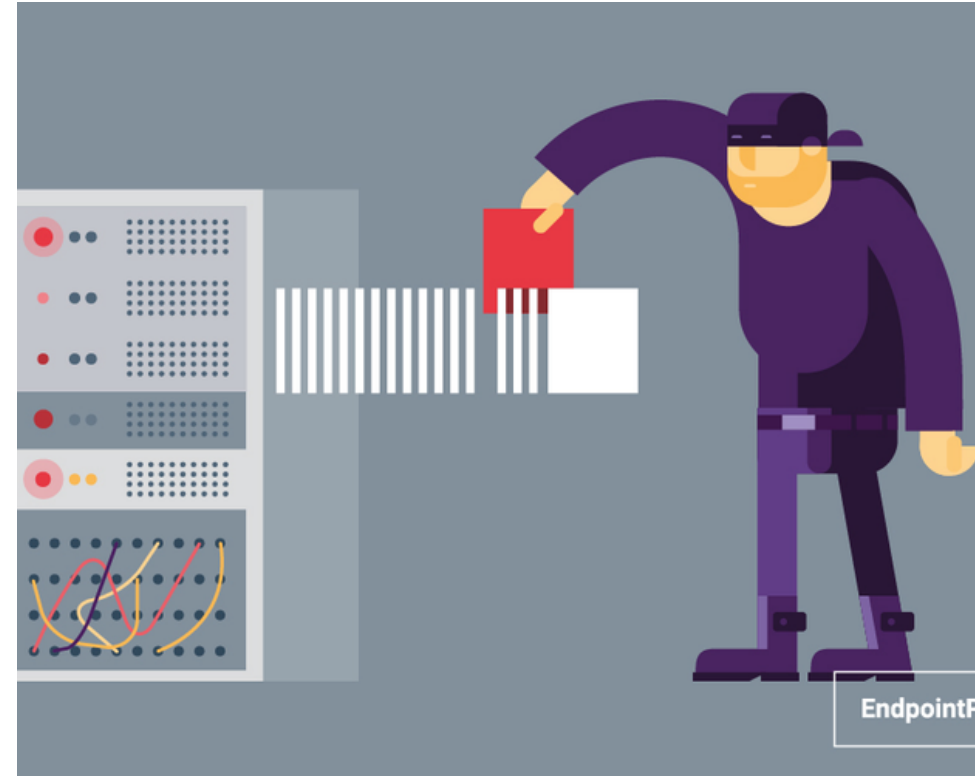
Not just external hackers; unintentional errors and "offended" insiders are significant risks. Threats can also be non-human (e.g., power failure).

Vulnerabilities are Constant

The "danger window" highlights security as an ongoing process, not a one-time product. New vulnerabilities emerge continuously.

Attacks Have Specific Goals

Each attack type (Interruption, Interception, Modification, Counterfeiting) aims to violate a specific component of the CIA Triad.



Control questions:

- What is meant by a threat?
- What is the difference between a threat and an attack?
- Give examples of intruders.
- What is called a danger window?
- Is it possible to completely eliminate the danger window in the information system?
- List the types of threats. What aspect of information security are they aimed at?
- Give an example of random and deliberate threats.
- Give an example of accessibility threats.
- Give an example of privacy threats.
- Give an example of integrity threats.

Further Reading

For deeper insights into information security, consult the following:

- Zegzhda D.P., Ivashko A.M. Fundamentals of security information systems. - M.: - Hot line - Telecom, 2000.
- Partyka T.L., Popov I.I. Information Security. Textbook for students of vocational schools. M.: FORUM: INFRA - M, 2002.

