Introduction and Basic Concepts

System Security (CM0625, CM0631) 2023-24
Università Ca' Foscari Venezia

Riccardo Focardi
www.unive.it/data/persone/5590470
secgroup.dais.unive.it

Università
Ca'Foscari
Venezia

Course Overview

Objectives

System Security
(CM0625, CM0631)

https://www.unive.it/data/course/451588/programma

This course aims at providing:

- basic **concepts** and **techniques** for the development of secure systems
- **skills** and **concepts** for evaluating and increasing the security of applications, systems and devices

Programme

System Security
(CM0625, CM0631)

https://www.unive.it/data/course/451588/programma

1. User authentication
2. Access control
3. Malicious software
4. Database security
5. Intrusion detection
6. Software security
7. Operating system security
8. Trusted computing
9. Security management and risk assessment
10. Hardware security
11. Side-channels
12. Formal methods

Material

System Security
(CM0625, CM0631)

https://www.unive.it/data/course/451588/programma

- **Book:** William Stallings, Lawrie Brown. *Computer Security Principles and Practice (Fourth Edition)*. Pearson Edu. 2018

- *Blended* course of the Ca' Foscari e-learning program:
  - traditional classroom
  - on-line classes
  - tutoring and challenges

- **Slides** and extra material are available in moodle

Assessment

System Security
(CM0625, CM0631)

https://www.unive.it/data/course/451588/programma

- **Written test** (base mark)
- Non-mandatory **assignments** (extra score)
    - *Challenges* on attacking and securing IT systems and applications
    - Bonus score with respect to the the mark of the written test

Basic Concepts

Why is Security so relevant?

Information systems are **pervasive** and extremely **connected.**

Examples:

- IoT
- Industry 4.0
- Critical infrastructures
- Government services
- Financial services (e.g. Banks)
- ...

Attacking information systems is more and more **harmful**!

What is Computer Security?

The National Institute of Standards and Technology (NIST) defines ***Computer Security*** as:

> *“Measures and controls that ensure **confidentiality**, **integrity**, and **availability** of the **information** processed, stored (and communicated) by a computer”*

The so-called “CIA” triad: Confidentiality, Integrity, Availability

NOTE: information system assets including **hardware**, **software**, **firmware** are all involved.

Reference: https://csrc.nist.gov/glossary/term/computer_security

Confidentiality

Definition:

1. **Data confidentiality**: confidential information is not disclosed to unauthorized individuals

2. **Privacy**: individuals control what information related to them may be collected and stored and by/to whom that information may be disclosed

Examples:

- Sensitive data in a database
- On-line payments (e.g. by credit card)

- Personal privacy while browsing the Web

Integrity

Definition:

1. **Data integrity**: information and programs are changed only in a specified and authorized manner

2. **System integrity**: a system performs its intended function, free from unauthorized manipulation

Examples:

- Bank accounts
- Bank transfers

- IoT device firmware should not be altered

Availability

Definition:

- Systems work promptly and services are not denied to authorized users

Examples:

- Cloud services
- E-voting
- Electrical grids (Cyber-physical)
- Remote surgery (QoS)

More properties: Authenticity

Definition:

1. **Identification:** The possibility of correctly identifying an entity

2. **Message Authentication**: Confidence in the validity of a transmission, a message, or message originator

Examples:

- User login
- ATM PINs

- Verified email messages (origin and destination)

More properties: Accountability

Definition:

- The possibility of **tracing** an event to a unique entity

⇒ allows for tracing a **security breach** to a responsible party

Examples:

- Digital signature

- Activity logs
- Forensic analysis

Impact (cf. FIPS 199)

Low

i. effectiveness of primary functions is **noticeably** reduced
ii. **minor** damage to organizational assets
iii. **minor** financial loss
iv. **minor** harm to individuals

Medium

i. effectiveness of primary functions is **significantly** reduced
ii. **significant** damage to organizational assets
iii. **significant** financial loss
iv. **significant** harm to individuals

High

i. **unable** to perform one or more primary functions
ii. **major** damage to organizational assets
iii. **major** financial loss
iv. **severe** or **catastrophic** harm to individuals (e.g. loss of life)

Examples

Patient allergy information:

Inaccurate information could result in **severe harm or death** to a patient, and expose the hospital to massive liability

⇒ high requirement of **integrity**

University web site:

Not a critical component of the university’s information system, but its unavailability would cause **significant troubles** to students and professors

⇒ medium requirement of **availability**

Terminology (1)

System Resource (Asset): A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems

Threat: Any circumstance or event with the potential to adversely impact organizational operations, assets, individuals, other organizations, or the Nation

Vulnerability: Weakness in an information system that could be exploited or triggered by a threat source

Attack: malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information and/or system resources. An attack is a **threat** that is carried out, typically through a **vulnerability**

Terminology (2)

Adversary (threat agent): Who conducts harmful activities

Countermeasure: A device or techniques that reduce the effectiveness of attacks

Risk: A measure of the extent to which an entity is threatened based on impact and likelihood

Security Policy: A set of criteria for the provision of security services: defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data

Classes of attacks

Active attack: An attempt to alter system resources or affect their operation

Passive attack: An attempt to learn information from the system that does not affect system resources

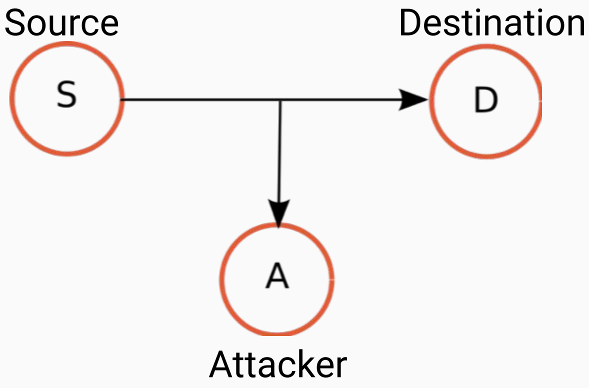
Inside attack: Initiated by an entity inside the security perimeter

Outside attack: Initiated from outside the perimeter, by an unauthorized or illegitimate user of the system

Example 1: Interception

- Attacker gets **unauthorized access** to information
- Breaks **data confidentiality**
- **Passive attack**
- **Example**:
  - S sends a credit card number to D "in the clear"

⇒ Threat consequence: *Unauthorized disclosure*



More examples of attacks on confidentiality

Exposure:

- An **insider** deliberately leaks confidential information
- human, hardware, software error

Inference:

- Traffic analysis
- Inferring information in a database (e.g. aggregate salary of employees s.t. 31<age<32)

Intrusion:

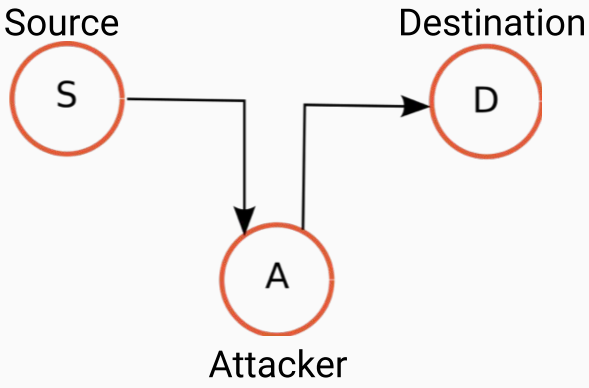
- gaining unauthorized access
- Note: this can be easier for an insider

⇒ Threat consequence: *Unauthorized disclosure*

Example 2: Modification

- Attacker **maliciously modifies** information
- Breaks **data integrity**
- **Active attack**

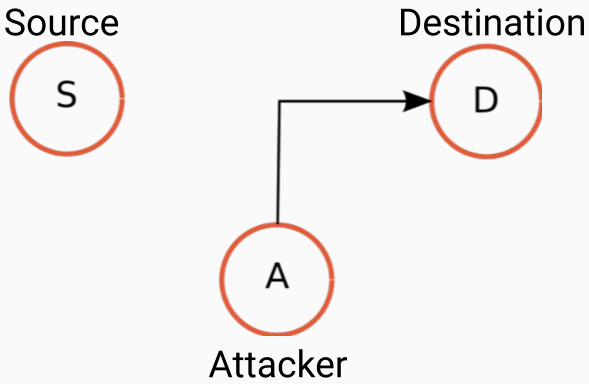
- **Example**:
  - A redirects S bank transfer to herself
  - NOTE: A can be either in the browser or on the network (Man-in-the-middle)



Example 3: Falsification

- Attacker forges new information
- Breaks **authenticity**, **accountability** and **integrity**
- **Active attack**

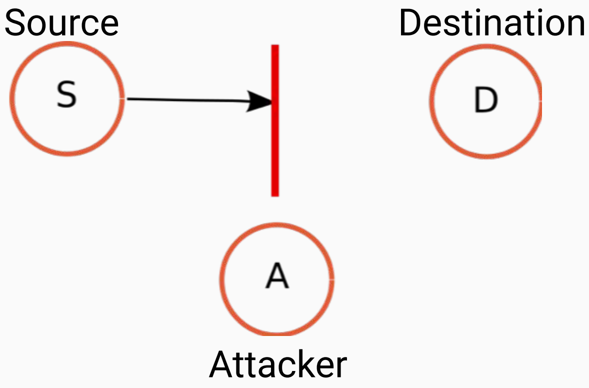
- **Example**:
  - Forging a signature through a crypto vulnerability (e.g. MD5 collisions)
  - Credential theft



Example 4: Interruption

- Attacker interrupts a service
- Breaks **system integrity, availability**
- **Active attack**

- **Examples**:
  - DoS on E-Voting
  - DoS on power grid (e.g., Ukraine recent attacks)



More examples of disruptive attacks

Incapacitation: physical destruction of or damage to system, possibly due to malware

Corruption: modification of system functions. E.g., placing backdoor in the system to provide subsequent access

Misappropriation: malicious software makes unauthorized use of processor and operating system resources.

Attack trees

Attack trees are a formal, methodical way of describing the security of systems, based on varying attacks

Nodes are OR or AND

- OR is possible if one child is possible
- AND is possible if all children are possible

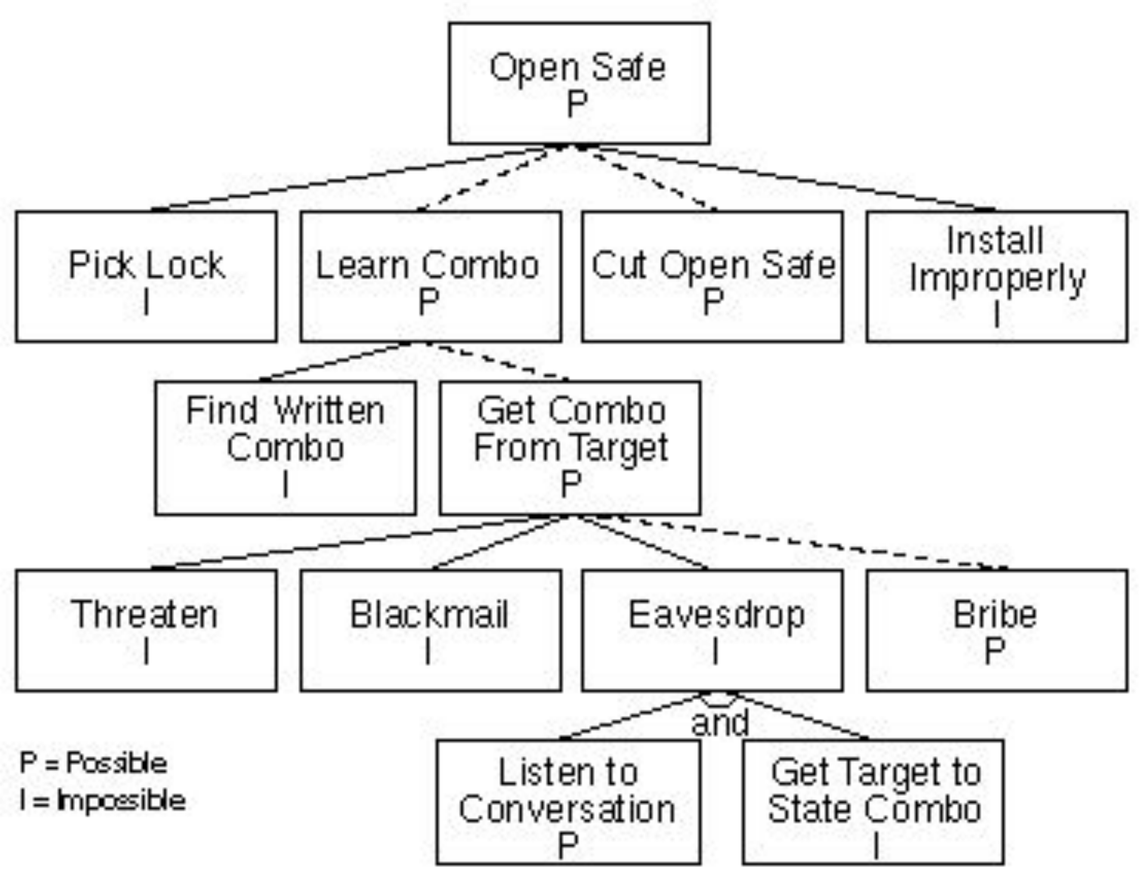


Figure 2: Possible Attacks.From https://www.schneier.com/

Attack trees

Values can be associated to the nodes

- Example: Cost

Values propagate from leaves up (parent gets the cheapest attack)

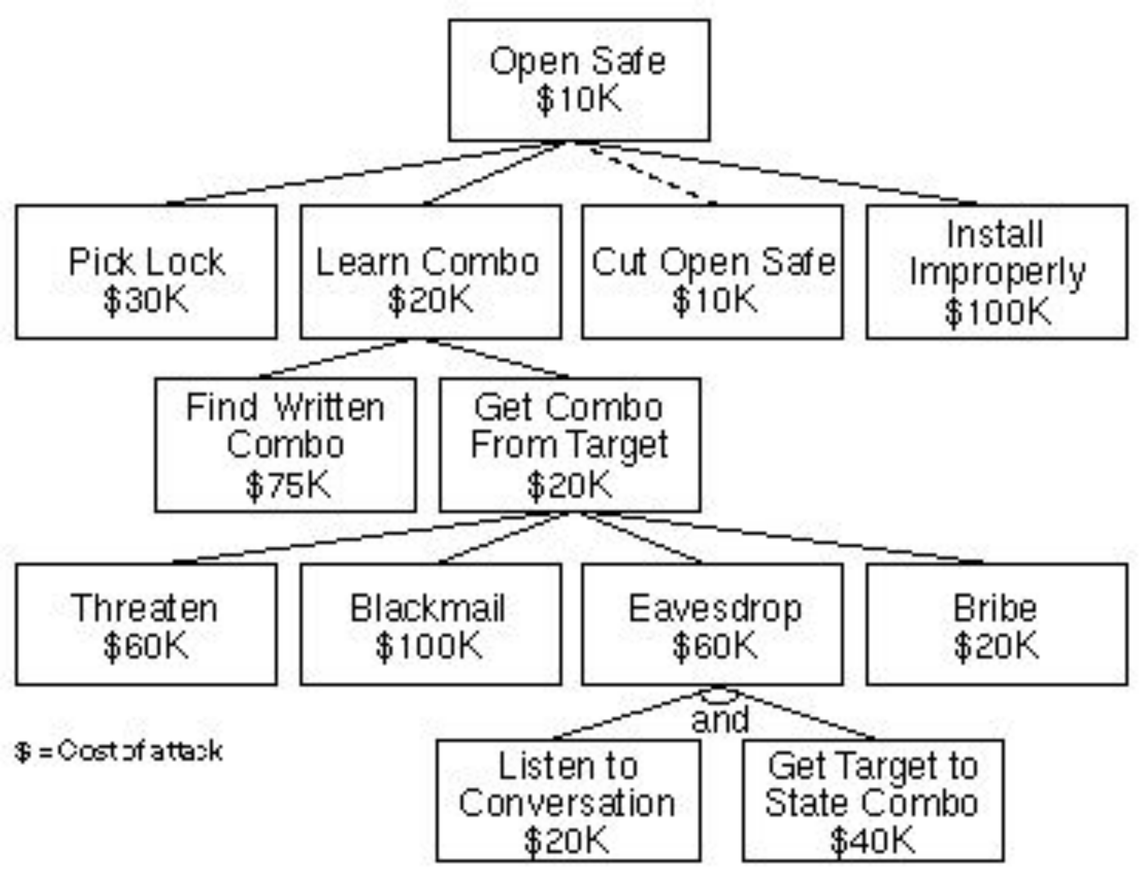


Figure 4: Cost of Attack. From https://www.schneier.com/

Attack trees

Evaluation

- Example : All attacks less that 100K $

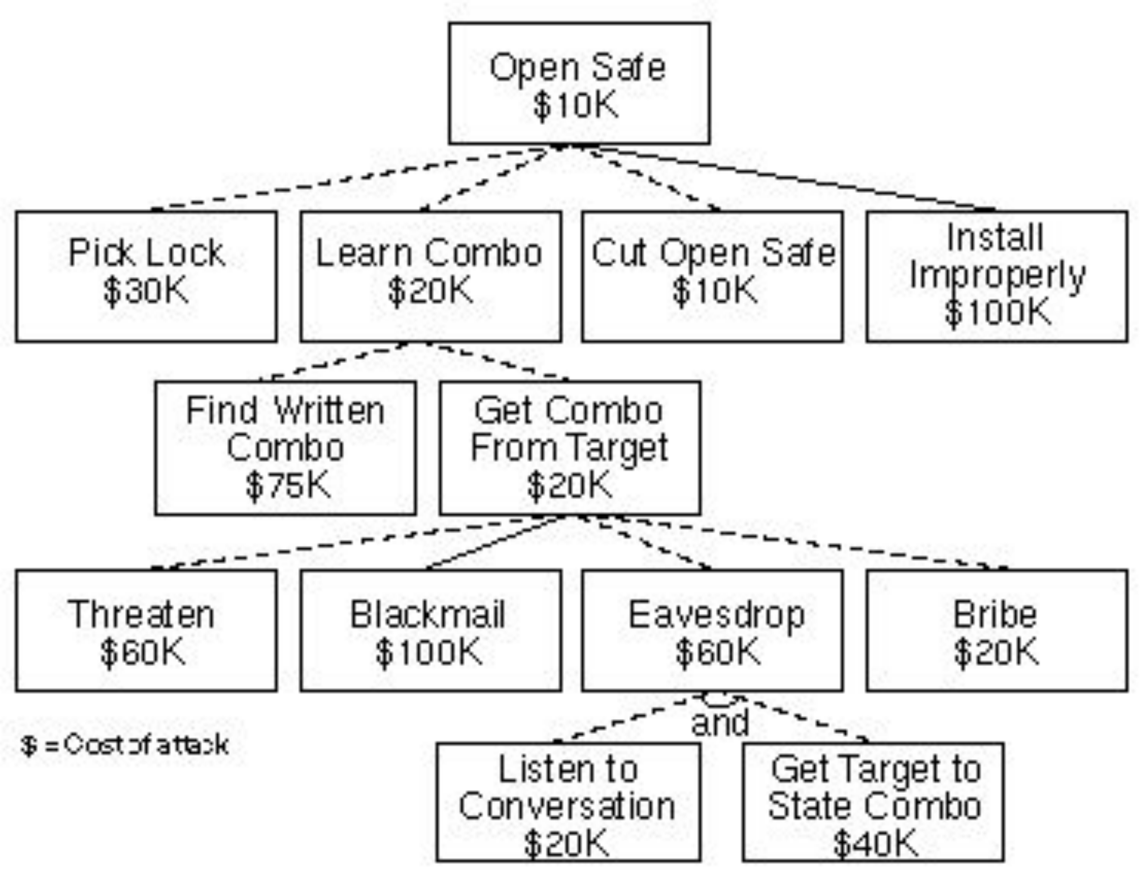


Figure 5: Attacks Less than $100,000. https://www.schneier.com/