CAN 304
Computer Systems Security

Lecture 1. Introduction

Week 1: 2024-02-27, 14:00-15:50, Tuesday

Jie Zhang
Department of Communications and Networking
Email: jie.zhang01@xjtlu.edu.cn
Office: EE522

Outline

- Description of class
- Introduction to computer systems security

1. Description of class

Objectives

- Demonstrate understanding of a range of problems in computer security, and the available solutions and tradeoffs;
- Effectively describe and analyze secure methods for the transmission and storage of data.

Topics to be covered

- Fundamentals of cryptography
  - Symmetric and asymmetric cryptography
- Security protocols
- User authentication
- Access control
- Attacks and defenses
  - Malicious software, DoS attacks, Intrusion detection, Firewall & intrusion prevention
- Advanced topics
  - Cloud, IoT and edge security, blockchain, etc.
  - Update every year

Classes

- Lectures
  - 14:00-15:50, Tuesday Week 1 to 13 (skipping Week 7)
  - (11+1) * 2 hours
    - Introduce and explain main topics
    - Review
- Labs
  - 18:00-18:50, Thursday Week 3 to 13 (skipping Week 7)
  - (9+1) * 1 hour
    - Cryptography and security related experiments
    - Presentation of coursework

Resources

- Documents online (Learning Mall)
  - Module notices
  - Lecture and lab materials
  - Coursework information and submission links

Sources of help

- Email me directly
  - jie.zhang01@xjtlu.edu.cn
- Office hours
  - 14:00-16:00PM, Thursday
  - EE522
  - Appointment by e-mail

Assessment

- Coursework: group project – 20%
  - 5-6 students / group
  - Written report + code + oral presentation
- Final exam – 80%

Reading materials

- References
  - Computer Security: Principles and Practice
    - *By William Stallings and Lawrie Brown*
  - Introduction to Modern Cryptography
    - *By Jonathan Katz and Yehuda Lindell*
- Papers and Web pages

2. Introduction to computer systems security

Learning objectives

- Learn about definitions and terms related to computer security.
- Understand confidentiality, integrity, and availability.

2.1 Overview

Computer security concepts

- Definition
  - The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

NIST95

- Three key objectives: CIA
  - Confidentiality
  - Integrity
  - Availability

Three key objectives

- Confidentiality
  - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity
  - Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.
- Availability
  - Ensuring timely and reliable access to and use of information.

Three key objectives

- Examples:
  - Which of CIA is violated in the following cases?
    - The e-bridge system is out of service.
    - Your Academic Records stored in the server are leaked to an attacker.
    - Your final exam marks stored in the server are changed by an attacker.

Other objectives

- Authenticity
  - Verifying users are who they say they are. (users' authenticity)
  - Messages' authenticity: integrity

- Accountability
  - Ensuring actions of an entity to be traced uniquely to that entity.
  - Supports nonrepudiation, deterrence, intrusion detection and prevention, etc.

Terminology

- Computer security deals with
  - computer-related assets that are subject to a variety of threats and for which various measures are taken to protect those assets

- What assets do we need to protect?
- How are those assets threatened?
- What can we do to counter those threats?

Terminology

- System Resource (Asset)
  - **Hardware**: Including computer systems and other data processing, data storage, and data communications devices
  - **Software**: Including the operating system, system utilities, and applications.
  - **Data**: Including files and databases, as well as security-related data, such as password files.
  - **Communication facilities and networks**: Local and wide area network communication links, bridges, routers, and so on.

What assets do we need to protect?

Terminology

- Security Policy
  - A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

- Examples:
  - “Only authorized user may access this file.”

Terminology

- Vulnerability
  - A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

- Examples:
  - Missing security camera and security guard at the entrance of EE building
  - A weakness in a firewall that can lead to malicious hackers getting into a computer network

Terminology

- Exploit
  - An actual incident of taking advantage of a vulnerability.
  - Term also refers to the code or methodology used to take advantage of a vulnerability.

- Threat
  - A potential for violation of security, which exists when there is a circumstance, capability, action, or event, that could breach security and cause harm.

Terminology

- Vulnerability vs threat
  - Vulnerabilities are not introduced to a system; rather they are there from the beginning.
  - Threats are introduced to a system like a virus download or a social engineering attack.
  - That is, a threat is a possible danger that might exploit a vulnerability.

Terminology

- Attack
  - A threat that is carried out and, if successful, leads to an undesirable violation of security, or threat consequence.

- Attacker
  - The agent carrying out the attack.

Terminology

- Types of attack:
  - **Active attack**: An attempt to alter system resources or affect their operation.
  - **Passive attack**: An attempt to learn or make use of information from the system that does not affect system resources.

- Are the following attacks active or passive?
  - A denial of service (DoS) attack attempts to tie up a website's resource so that users who need to access the site cannot do so.
  - A timing side-channel attack attempts to leak a secret key by analyzing the time taken to execute cryptographical algorithms.

Terminology

- Types of attacks:
  - **Inside attack**: Initiated by an entity inside the security perimeter (an “insider”). The insider is authorized to access system resources but uses them in a way not approved by those who granted the authorization.
  - **Outside attack**: Initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an “outsider”).

Terminology

- Countermeasure
  - An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

- Examples:
  - Report to website's administrator there is DoS attack
  - Adding randomness to cryptographical algorithms to prevent timing side-channel attack

2.2 More on threats, attacks, and assets:
How are assets threatened?

Four kinds of threat consequences

- Unauthorized disclosure
- Deception
- Disruption
- Usurpation

Threat consequences and attacks

- Unauthorized disclosure
  - A circumstance or event whereby an entity gains access to data for which the entity is not authorized.
  - Which one of CIA is violated?

- Attacks can result in this consequence
  - Exposure
  - Interception
  - Inference
  - Intrusion

Threat consequences and attacks

- Attacks can result in unauthorized disclosure:
  - **Exposure**: Sensitive data are directly released to an unauthorized entity.
  - **Interception**: An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations.
  - **Inference**: An unauthorized entity indirectly accesses sensitive data by reasoning from characteristics or by-products of communications.
  - **Intrusion**: An unauthorized entity gains access to sensitive data by circumventing a system's security protections.

Threat consequences and attacks

- Deception
  - A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.
  - Which one of CIA is violated?

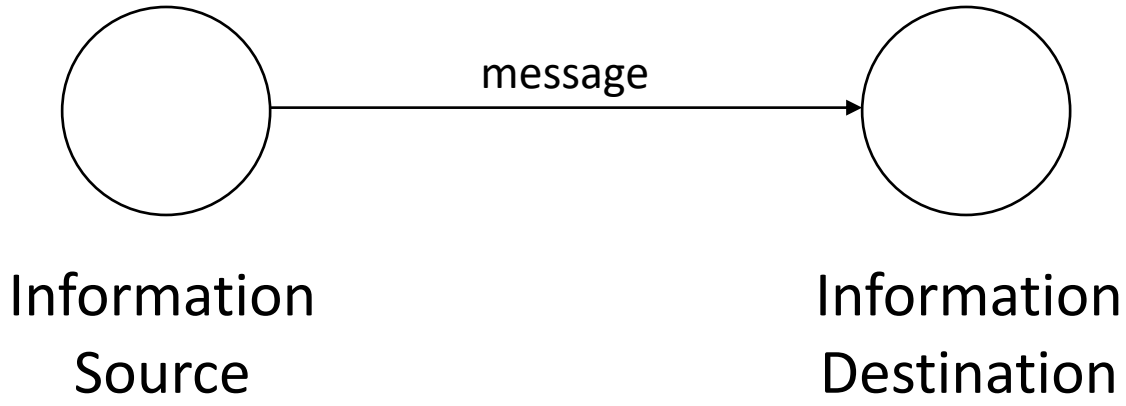
- Attacks can result in this consequences
  - Masquerade
  - Falsification
  - Repudiation

Threat consequences and attacks

- Attacks can result in deception
  - **Masquerade**: An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.
  - **Falsification**: False data deceive an authorized entity.
  - **Repudiation**: An entity deceives another by falsely denying responsibility for an act.

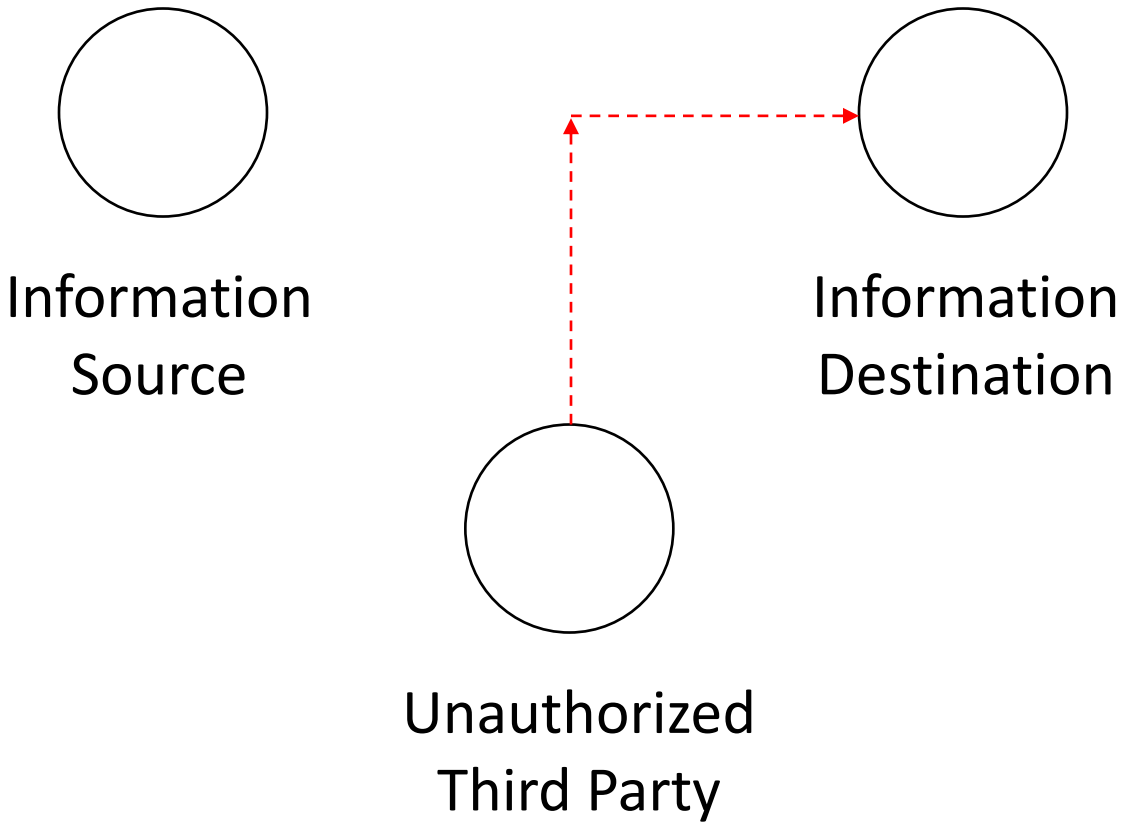
Threat consequences and attacks

- Example:
  - The information source denies the information it sent
  - Repudiation



Threat consequences and attacks

- Example:
  - The destination receives information the source never sent.
  - Falsification



Threat consequences and attacks

- Disruption
  - A circumstance or event that interrupts or prevents the correct operation of system services and functions.
  - Which one of CIA is violated?

- Attacks can result in this consequences
  - Incapacitation
  - Corruption
  - Obstruction

Threat consequences and attacks

- Attacks can result in disruption
  - **Incapacitation**: Prevents or interrupts system operation by disabling a system component.
  - **Corruption**: Undesirably alters system operation by adversely modifying system functions or data.
  - **Obstruction**: A threat action that interrupts delivery of system services by hindering system operation.
- Examples:
  - Malicious software (e.g., viruses) disable a system or some of its services.
  - Malicious software change a system data.

Threat consequences and attacks

- Usurpation
  - A circumstance or event that results in control of system services or functions by an unauthorized entity.
  - Which one of CIA is violated?
- Attacks can result in this consequences
  - **Misappropriation**: An entity assumes unauthorized logical or physical control of a system resource.
    - E.g.: In distributed denial of service (DDoS) attack, malicious software is installed on a number of hosts to be used as platforms to launch traffic at a target host.
  - **Misuse**: Causes a system component to perform a function or service that is detrimental to system security.

Threats to assets

- Hardware
  - Major threat: availability
  - Confidentiality, integrity

- Example:
  - Equipment is stolen or disabled, thus denying service.
  - A laptop/smart phone/tablet storing unencrypted privacy data is stolen.

Threats to assets

- Software
  - Major threat: availability
  - Confidentiality, integrity

- Example:
  - Programs are deleted, denying access to user.
  - A working program is modified by computer viruses, either to cause it to fail during execution or to cause it to do some unintended task.

Threats to assets

- Data
  - A much more widespread problem is data security
  - Availability, confidentiality, integrity

- Example:
  - Files are deleted, denying access to users.
  - An unauthorized read of data is performed.
  - Existing files are modified, or new files are fabricated.

Threats to assets

- Communication lines and networks
  - Network security

- Network security attacks
  - Passive attacks
    - are in the nature of eavesdropping on, or monitoring of, transmissions
  - Active attacks
    - involve some modification of the data stream or the creation of a false stream

Threats to assets

- Passive attacks
  - Release of message contents
    - e.g., a telephone conversation involving sensitive information
  - Traffic analysis
    - e.g., messages are encrypted, but pattern of messages are observed by attacker

- Passive attacks are very difficult to detect because they do not involve any alteration of the data.

Threats to assets

- Active attacks
  - Replay
    - passive capture of a data unit
    - subsequent retransmission to produce an unauthorized effect
  - Masquerade
    - one entity pretends to be a different entity
  - Modification of messages
    - some portion of a legitimate message is altered
    - messages are delayed or blocked
  - Denial of service

2.3 Countermeasures:
What can we do to counter those threats?

Fundamental security design principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privileges
- Least privilege
- Least common mechanism
- Psychological acceptability

Economy of mechanism

- The design of security measures should be economical to develop, use and verify.

- Should add little or no overhead.
- Should do only what needs to be done.
- Generally, try to keep it simple and small.

Fail-safe designs

- Access decisions should be based on permission rather than exclusion
- Default to lack of access
- So if something goes wrong or is forgotten or isn’t done, no security lost.

Complete mediation

- Apply security on every access to a protected object
  - Every access must be checked against the access control mechanism

- Typically, once a user has opened a file, no check is made to see of permissions change.
- To fully implement complete mediation, every time a user reads a field or record in a file, or a data item in a database, the system must exercise access control.

Open design

- The design of a security mechanism should be open rather than secret.
- Assume all potential attackers know everything about the design
  - And completely understand it

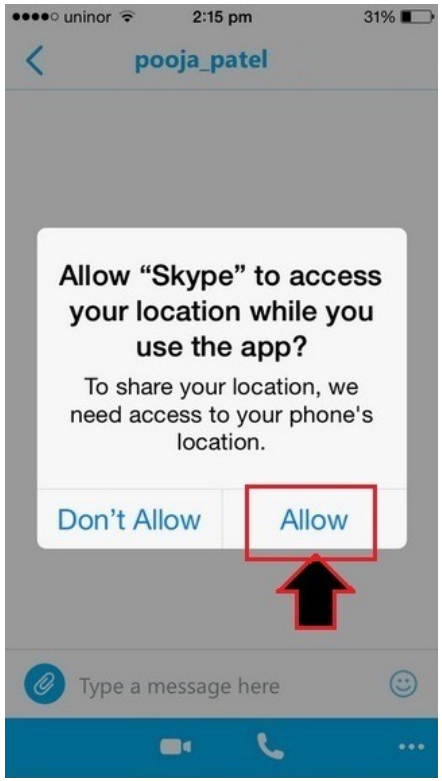
- This doesn't necessarily mean publishing everything important about your security system

Kerckhoffs principle:
A cryptographic system should be secure even if everything about the system, except the key, is public knowledge.

Separation of privileges

- Provide mechanisms that separate the privileges used for one purpose from those used for another.
  - To allow flexibility in security systems
  - To mitigate the potential damage of a computer security attack

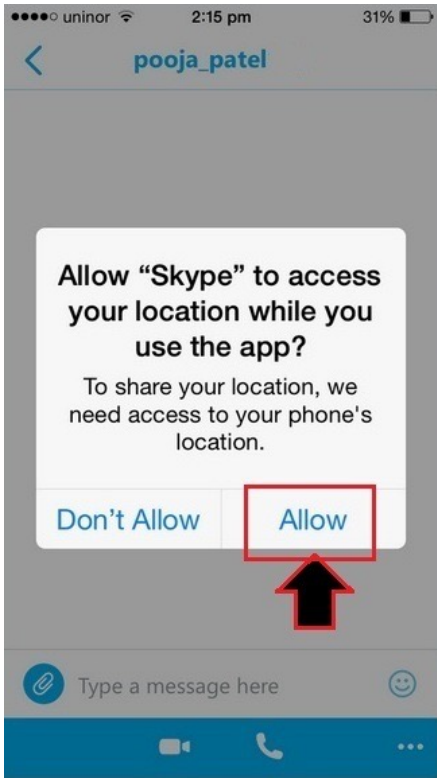
- Example:
  - A program is divided into parts that are limited to the specific privileges they require in order to perform a specific task.
  - TencentMeeting will need access your camera and microphone for video meeting.



Least privilege

- Every process and every user of the system should operate using the least set of privileges necessary to perform the task
- Require another request to perform another type of access

- Example:
  - Don’t give write permission to a file if the program only asked for read
  - Forbid a map application to access your camera.



Least common mechanism

- The design should minimize the functions shared by different users, providing mutual security

- Coupling leads to possible security breaches
- Example:
  - Side-channel attacks based on OS shared memory

Unveiling your keystrokes: A Cache-based Side-channel Attack on Graphics Libraries

Daimeng Wang*, Ajaya Neupane*, Zhiyun Qian*, Nael Abu-Ghazaleh*, Srikanth V. Krishnamurthy*
Edward J. M. Colbert†, and Paul Yu‡
*University of California Riverside. {dwang030, ajaya, zhiyunq, nael, krish}@cs.ucr.edu
†Virginia Tech. ecolbert@vt.edu
‡U.S. Army Research Lab (ARL). paul.l.yu.civ@mail.mil

***Abstract*—Operating systems use shared memory to improve performance. However, as shown in recent studies, attackers can exploit CPU cache side-channels associated with shared memory to extract sensitive information. The attacks that were previously attempted typically only detect the presence of a certain operation and require significant manual analysis to identify and evaluate their effectiveness. Moreover, very few of them target graphics libraries which are commonly used, but difficult to attack. In this paper, we consider the execution time of shared libraries as the side-channel, and showcase a completely automated technique to**

i.e., different virtual pages are mapped to the same physical pages. This creates an opportunity for a malicious process to infer graphics-related activities of a victim process.

Our intuition of the attack is that the performance of graphics rendering is critical for user experience across a wide range of applications. Consequently, graphics libraries often optimize their execution logic for high performance. For example, when handling simpler graphical content, graphics libraries usually execute a different set of procedures than

Psychological acceptability

- Mechanism must be simple to use
- Simple enough that people will use it without thinking about it
- Must rarely or never prevent permissible accesses

Computer security strategy

- A comprehensive security strategy involves three aspects:
  - Specification/policy:
    - What is the security scheme supposed to do?
  - Implementation/mechanisms:
    - How does it do it?
  - Correctness/assurance:
    - Does it really work?

Security policies

- Security policies describe how a secure system should behave.
- Policy says what should happen, not how you achieve that.

- Example
  - Informal security policies
    - "Users should only be able to access their own files, in most cases."
    - "System executables should only be altered by system administrators."

Security policies

- In developing a security policy, a security manager needs to consider the following factors:
  - The value of the assets being protected
  - The vulnerabilities of the system
  - Potential threats and the likelihood of attacks

- Trade-offs
  - Ease of use versus security
  - Cost of security versus cost of failure and recovery

Security implementation

- Security implementation involves four complementary courses of action:
  - Prevention
    - encrypting the data, authenticate via password, etc.
  - Detection
    - intrusion detection, detection of DoS attack
  - Response
    - halt the attack and prevent further damage
  - Recovery
    - backup system

Assurance and evaluation

- Assurance deals with the questions:
  - Does the security system design meet its requirements?
  - Does the security system implementation meet its specifications?
- Assurance is expressed as a degree of confidence, not in terms of a formal proof that a design or implementation is correct.

- Evaluation is the process of examining a computer product or system with respect to certain criteria. Evaluation involves testing and may also involve formal analytic or mathematical techniques.

Tools for security

- Cryptographic tools
  - Encryption, message authentication code, digital signature, etc.
- Access control
- User authentication
- Intrusion detection/prevention, firewall

Cryptographic tools

- Encryption
  - Algorithms to hide the content of data or communications
  - Only those knowing a secret can decrypt the protection
  - One of the most important tools in computer security
- Message authentication code
- Digital signature

Access controls & user authentication

- Access control
  - Only let authorized parties access the system

- User authentication
  - Methods of ensuring that someone is who they say they are
  - Vital for access control, but also vital for many other purposes
  - Both cryptographic methods and non-cryptographic methods

Intrusion detection

- A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

- IDS: Intrusion detection system

Firewall & Intrusion prevention

- Firewall
  - A machine to protect a network from malicious external attacks.
  - Typically sits between a LAN/WAN and the Internet.
  - Runs special software to regulate network traffic.

- Intrusion prevention system (IPS)
  - Also known as intrusion detection and prevention system (IDPS)
  - An extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity

Appendix: related standards/specifications

- National Institute of Standards and Technology (NIST)
  - Federal Information Processing Standards (FIPS)
- Internet Society (ISOC)
  - Internet Engineering Task Force (IETF)
- International Organization for Standardization (ISO)

Summary

- Key objectives of security: CIA
- What assets do we need to protect?
  - Hardware, software, data, and communication facilities and networks
- How are those assets threatened?
  - Threat consequences and attacks
  - Threats to assets
- What can we do to counter those threats?
  - Security design principles
  - Security strategy
  - Tools