Midterm Review

CSE 565: Fall 2024
Computer Security

Xiangyu Guo (xiangyug@buffalo.edu)

University at Buffalo

Midterm Exam Policy

Section B

- All relevant info have been announced on Piazza
  - https://piazza.com/class/lzvskuhlm3v35b/post/57
- In-class Exam: **Knox 104**; Please arrive before **2 PM**
- Duration: **1 hr**
- Only thing allowed: Pen, 1 page of A4-size cheatsheet, your UB card
- Sit at your **assigned seat:** https://piazza.com/class_profile/get_resource/lzvskuhlm3v35b/m229jkvo61m1gb

Midterm Exam Policy

Section C

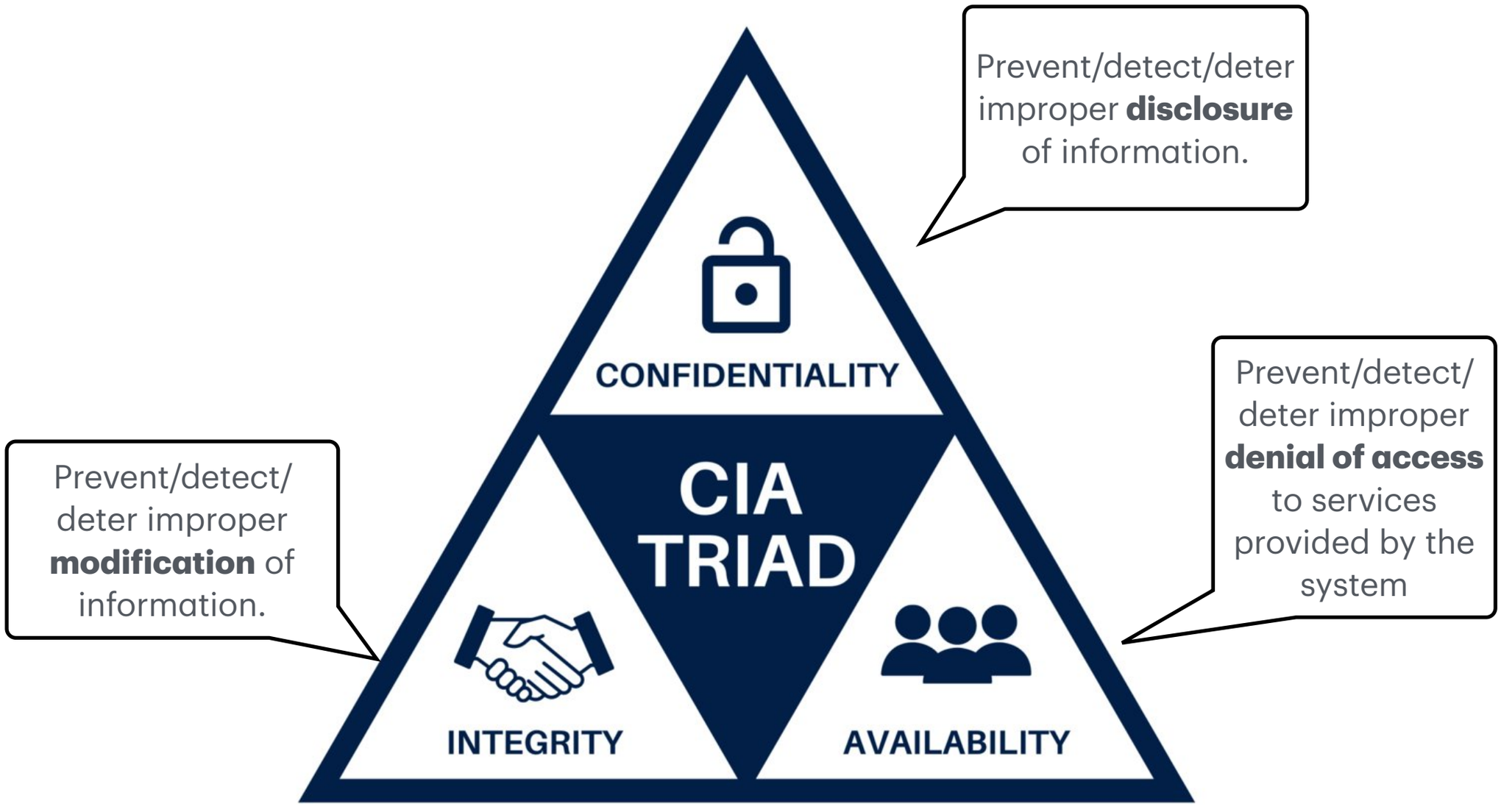
- All relevant info have been announced on Piazza
  - https://piazza.com/class/lzvspclhyvj5ev/post/45
- In-class Exam: **Knox 110**, Please arrive before **5:05 PM**
- Duration: **1 hr**
- Only thing allowed: Pen, 1 page of A4-size cheatsheet, your UB card
- Sit at your **assigned seat:** https://piazza.com/class_profile/get_resource/lzvspclhyvj5ev/m225y18iwyg3rz

Security Objectives

Basic objectives

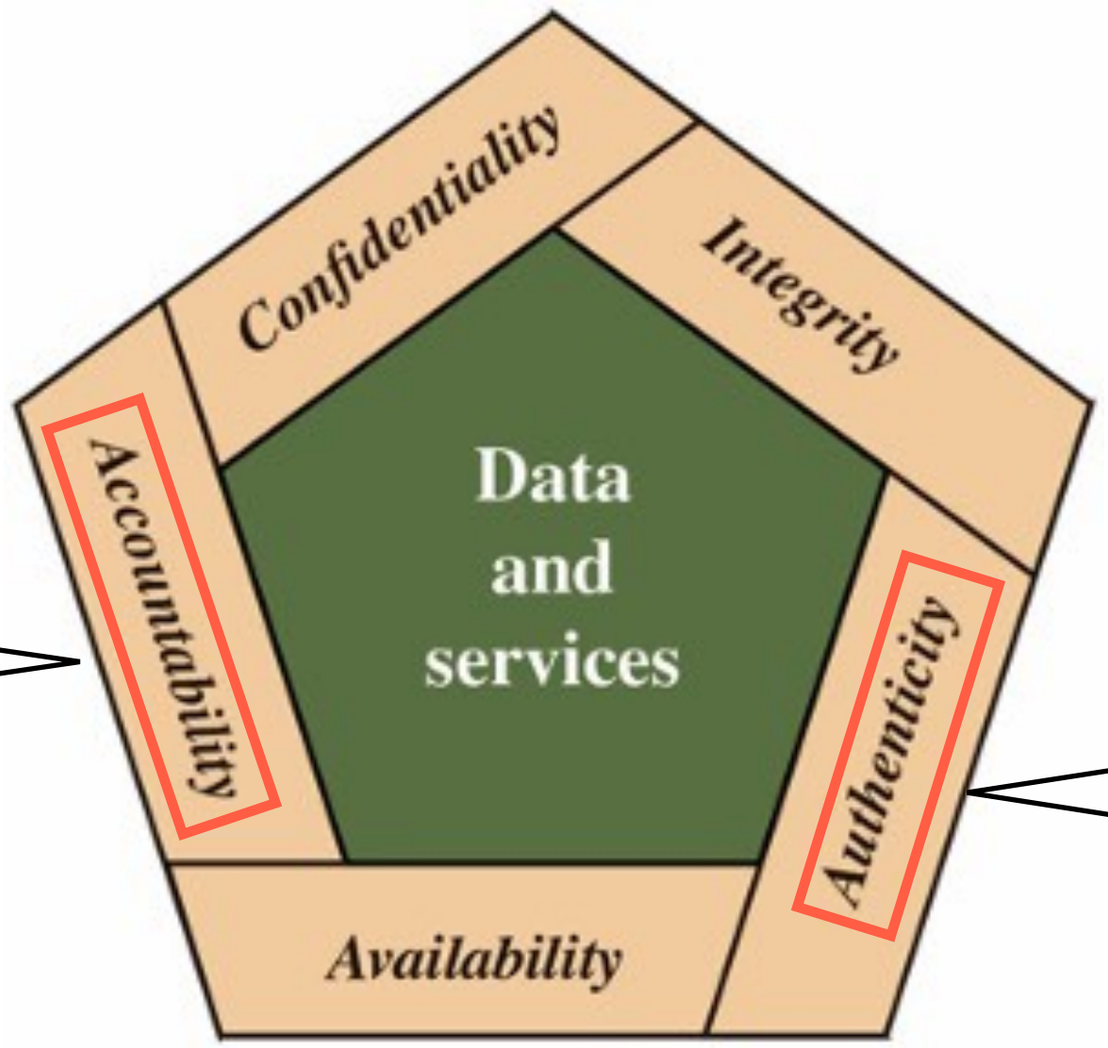
- The “CIA Triad” :
  - What does each letter stands for?
  - What are the two major augmentations (“A” & “A”) to the Triad?

Security Objective: The CIA Triad



Augmenting CIA Triad

Authenticity & Accountability



The assurance that every action can be attributed to the entity **responsible** for it.

The assurance that a message, transaction, or other exchange of information is from the **source** it claims to be from.

Basic objectives

- Examples?
    - Common **tools** for ensuring each objective?
- *Confidentiality?*
- *Integrity?*
- *Availability?*

Basic objectives

- Examples?
    - Common **tools** for ensuring each objective?
        - *Confidentiality?*: Encryption; Authentication; Authorization
        - *Integrity?*: MAC, Digital Signature
        - *Availability?*: Redundancy; Backup;

Basic objectives

- Examples?
    - **Attack** examples against each objective?
    - *Confidentiality?*:
    - *Integrity?*:
    - *Availability?*:

Basic objectives

- Examples?
    - **Attack** examples against each objective?
    - *Confidentiality?*: Eavesdropping; Sniffing;
    - *Integrity?*: Message alteration; Signature forgery;
    - *Availability?*: DDOS

Sample questions

- Q. What does the “C” in the CIA Triad stand for?
  - a) Consistency
  - b) Confidentiality
  - c) Control
  - d) Cryptography

- Answer: b) Confidentiality

Sample questions

- Q. Which of the following is an example of maintaining Confidentiality in information security?
    - a) Encrypting sensitive files to protect them from unauthorized access.
    - b) Ensuring data is accurate and unaltered.
    - c) Keeping the system available for authorized users at all times.
    - d) Creating backups to recover lost data.

- Answer: a) Encrypting sensitive files to protect them from unauthorized access. Confidentiality focuses on restricting access to data to authorized individuals only.

Sample questions

- Q. Which of the following scenarios is an example of an Availability issue?
  - a) An unauthorized user accesses sensitive financial data.
  - b) A server crash causes a website to be offline for several hours.
  - c) A hacker alters data in a customer database.
  - d) A virus encrypts data and demands a ransom.

- Answer: b) A server crash causes a website to be offline for several hours. Availability is compromised when authorized users cannot access the system or data.

Cryptography

Cryptography

- **Major applications**
  - Most important: **Secure communication**
    - Phase I: Channel Establishment - Key exchange; PKC
    - Phase II: Data transmission - symm enc & dec

Cryptography

- **Major applications**
  - How does crypto help to achieve security objectives?
    - Confidentiality: encryption
    - Integrity: MAC
    - Authenticity: MAC; Digital signature
    - Non-repudiation: Digital signature

Cryptography

- **Part I: Symmetric encryption**
  - Kerckhoff's principle: only the key is secret
  - Probability: birthday paradox; birthday attack.

Cryptography

- **Part I: Symmetric encryption**
  - Ciphers
  - Stream cipher: PRG + OTP
  - **Block cipher**:
    - Confusion-Diffusion Paradigm by Shannon.
    - Building block: Feistel Network & SPN

Cryptography

- **Part I: Symmetric encryption**
  - Ciphers
  - Block cipher example: DES & AES
  - **Encryption modes**: how to use block cipher to encrypt msgs
    - ECB vs CBC: error propagation; IV; nounce
    - OFB & CFB
    - CTR: implementing stream cipher using block cipher

Cryptography

- **Part I: Symmetric encryption**
  - **Integrity**
    - MAC: basic construction? MAC Key vs Enc Key?
    - Hash function: basic construction? what does collision-resistant mean?
    - Authentication Encryption
      - How to combine MAC with encryption?

Cryptography

- **Part I: Symmetric encryption**
  - Attacks
    - Insecure instantiation
      - Repeated / predictable IV
      - non-unique nounce
      - Insecure encryption mode: ECB

Cryptography

- **Part I: Symmetric encryption**
  - Attacks
    - Insecure implementation:
      - Padding oracle
      - Timing attack

Cryptography

- **Part II: Asymmetric (Public-Key) Encryption**
  - Major applications
    - Key Exchange: Diffie-Hellman; RSA.
      - Establishing secure channel
    - Signature
      - Integrity & Authenticity & Non-repudiation

Cryptography

- **Part II: Asymmetric (Public-Key) Encryption**
  - Constructions
    - Hard problem: Discrete Log (DH), Factoring (RSA)
    - RSA Trapdoor function
- PKC System
  - PKC only used for exchanging (encrypting) a symm key
  - Actual msg is encrypted using the symm key

Sample Questions

- Q. What is the primary weakness of Electronic Codebook (ECB) mode in block ciphers?
  - a) It requires an initialization vector (IV) for security.
  - b) It can reveal patterns in the plaintext if the same block of data is repeated.
  - c) It encrypts each block using a different key.
  - d) It is slower compared to other block cipher modes.

- Answer: b) It can reveal patterns in the plaintext if the same block of data is repeated. ECB is vulnerable because repeating identical plaintext blocks produces the same ciphertext blocks, allowing patterns to be visible.

Sample Questions

- Q. Which of the following is NOT true about a Message Authentication Code (MAC)?
  - a) A MAC can detect if a message has been altered.
  - b) A MAC ensures that a message was sent by a legitimate sender.
  - c) A MAC can be used to encrypt a message.
  - d) A MAC uses a secret key in its generation process.

- Answer: c) A MAC can be used to encrypt a message. A MAC provides integrity and authentication but does not encrypt the message itself.

Sample Questions

- Q. Which of the following describes the concept of pre-image resistance in hash functions?
  - a) It is difficult to generate the same hash from two different inputs.
  - b) It is difficult to reverse a hash to find the original input.
  - c) It is easy to compute the hash value from the input.
  - d) It is impossible to hash two inputs to the same output.

- Answer: b) It is difficult to reverse a hash to find the original input. Pre-image resistance means it should be computationally infeasible to reverse the hash and obtain the original input.

Sample Questions

- Lab questions
  - Analyzing a given encryption mode
  - Error propagation: impact of corruption of a single ciphertext blocks
  - IV usage
    - Incorrect IV usage leads to attacks: use XOR to cancel out IVs

Authentication

Authentication

- **Purpose**: Authenticate (Identify) Human to a machine
- Major approaches
  - Password-based: Definition? Advantage & Disadvantages?
  - Token-based: Definition?
  - Biometrics-based: Definition?
- Multi-Factor Authentication

Authentication

- **Password-based Authentication**
  - Vulnerability: Simple password; Dictionary attack
  - Countermeasures
    - Salt: what is it?
    - One-Time Password (OTP)
      - HOTP: construction?
      - TOTP: construction? Difference with HOTP? How is this combined/ implemented with token-based authentication?
      - Challenge-Response Protocol

Sample Questions

- Q. What is the main purpose of biometric authentication?
    - a) To verify the identity of a user based on physical or behavioral characteristics.
    - b) To encrypt user data with a unique key.
    - c) To provide access to the system without any form of password.
    - d) To generate a one-time password for login.
- Answer: a) To verify the identity of a user based on physical or behavioral characteristics. Biometric authentication uses fingerprints, facial recognition, or other unique characteristics to authenticate users.

Sample Questions

- Q. Which of the following statements is true about time-based one-time passwords (TOTP)?
  - a) The OTP remains valid indefinitely until used.
  - b) The OTP is generated based on the time and a shared secret key.
  - c) The OTP is regenerated every time the user logs in.
  - d) TOTP can only be used once every 24 hours.
- Answer: b) The OTP is generated based on the time and a shared secret key. TOTP uses the current time and a shared secret key to generate a unique password that is valid for a short period, typically 30 seconds.

Sample Questions

- Q. In a typical challenge-response authentication protocol, what does the server send to the client?
  - a) A username and password.
  - b) A shared secret key.
  - c) A random challenge, such as a nonce or timestamp.
  - d) An encrypted message containing the client's credentials.
- Answer: c) A random challenge, such as a nonce or timestamp. The server sends a random value (challenge), and the client must respond using a function (such as a hash or encryption) involving this challenge.

Access Control

Access Control

- Purpose: authorization for *authenticated* user
- Basic principle: Least privilege; Separation of duty.
- Core concept: Subject, Object, Policy
- Instantiation: Access Control matrix
  - ACL vs Capabilities

Access Control

- Models
  - DAC: Definition? POSIX File Permission;
  - MAC: Definition? Security levels;
  - RBAC: Definition? Design simple RBAC for corporate management.
  - ABAC: Definition?

Sample Questions

- Q. Which of the following describes Discretionary Access Control (DAC)?
  - a) Access is based on predefined roles and the tasks assigned to those roles.
  - b) Access is determined by the system based on policies set by the administrator.
  - c) Access control is based on the identity of users, and the owner of the resource controls permissions.
  - d) Access is granted based on security labels and classifications assigned to the data.

- Answer: c) Access control is based on the identity of users, and the owner of the resource controls permissions. In DAC, the owner of a resource decides who can access it and what they can do.

Sample Questions

- Q. Attribute-Based Access Control (ABAC) differs from Role-Based Access Control (RBAC) in that:
  - a) It uses only the user's identity to grant access.
  - b) It considers a wide range of attributes (e.g., user attributes, resource attributes) to make access decisions.
  - c) It only assigns permissions based on predefined roles.
  - d) It does not allow any flexibility in assigning permissions.

- Answer: b) It considers a wide range of attributes (e.g., user attributes, resource attributes) to make access decisions. ABAC makes access decisions based on a combination of attributes, such as user roles, time of day, resource sensitivity, and more.

Sample Questions

- Q. Which of the following is an example of the *separation of duties* principle in access control?
  - a) A single user is allowed to manage both payroll and audits for the same department.
  - b) A system administrator can modify access control policies without requiring approval.
  - c) No single individual has complete control over all phases of a critical business process.
  - d) All employees are granted read access to all company data.

- Answer: c) No single individual has complete control over all phases of a critical business process. The separation of duties principle prevents a single individual from having excessive control, reducing the risk of fraud or error.

Web Security

Web Security

- Web Architecture
  - Browser/User/Client $\Longleftrightarrow$ Web server : Shell & Database
  - HTTP Protocol
    - Cookies & Sessions: What and How?
  - HTML Basics
  - **Same-Origin Policy**

Web Security

- **Attacks**
  - Cross-Site Request Forgery (CSRF): What, Where, and How?
    - Access cross-origin resource; From user's browser; Cookie automatic attachment.
  - Cross-Site Scripting (XSS): What, Where, and How?
    - Code injection; User's browser; Reflected & Public XSS.
  - (SQL) Injection: What, Where, and How?
    - Query injection; Server (Database); Semantic gap (code mix with data)

Sample Questions

- Q. Cross-Site Request Forgery (CSRF) attacks typically:
  - a) Trick a user into submitting a request to a website where they are authenticated, performing unwanted actions.
  - b) Involve injecting malicious scripts into a website.
  - c) Exploit database queries to retrieve sensitive data.
  - d) Encrypt all data on the target system and demand a ransom.

- Answer: a) Trick a user into submitting a request to a website where they are authenticated, performing unwanted actions. CSRF attacks exploit a user's authenticated session to perform unwanted actions on a website without their consent.

Sample Questions

- Q. Which of the following is a security practice that helps mitigate Cross-Site Scripting (XSS) vulnerabilities?
  - a) Using parameterized queries.
  - b) Encrypting all user data in the database.
  - c) Escaping or sanitizing user input before rendering it on the page.
  - d) Using long, complex passwords for user authentication.

- Answer: c) Escaping or sanitizing user input before rendering it on the page. Sanitizing and escaping user input prevents attackers from injecting malicious scripts into web applications.

Sample Questions

- Lab question about SQL injection
  - Comment-based injection: `username='admin' - - AND pwd=…`
  - UNION-based injection: `username='' UNION SELECT pwd FROM users WHERE username='admin'`
- Boolean-based injection: `username='admin' AND pwd='' OR 1=1`
- Blind injection: When the server does not return the query result
  - still 1 bit of information leak: whether the pwd is correct or not
  - iterative guess of the pwd

Questions?