**Spring 2021**

**CS-452 Handout 1** Name: RJ Andaya

**Relevant Slides:** Introduction **Chapter:** Chapter 1

Please note: handouts *will not* be collected and graded. However, *you are expected to complete them.* The material on the handouts is a fair game for exams, quizzes, and assignments. It is in your best interest to use handouts during lectures. The instructor will be happy to assist you.

1. What is the C.I.A. triad? Explain.

Confidentiality: Only authorized people or systems can access the data or resource

Integrity: Assurance that the information is authentic and complete

* Data Integrity: The assurance that data received is exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay)
* Origin Integrity: The source of the data is trustworthy
* System Integrity: The assurance that the system performs its intended function without inadvertent or deliberate unauthorized manipulation of the system

1. What is ITU-T? What is OSI? What is ITU-X.800?

ITU-T: International Telecommunication Union, Telecommunication Standardization Sector

OSI: Open Systems Interconnection – an effort to standardize networking

ITU-X.800: Security Architecture for OSI.

1. What three aspects of data security does ITU-X.800 consider?

Security attacks

Security mechanisms

Security services

1. What is the difference between an active and a passive attack?

Active Attack: Attempts to alter system resources or affect their operation

Passive Attack: Attempts to learn or make use of the information from the system but does not affect system resources

1. Why are passive attacks difficult to detect?

Because passive attacks do not involve any alteration of the data

1. What security services does X.800 consider?

Authentication: Assurance that the communication entity is the one claimed

Access Control: Prevention of unauthorized use of a resource

Data Confidentiality: Protection of data from unauthorized disclosure

Data Integrity: Assurance that data received is sent from an authorized entity

Nonrepudiation: Protection against denial by one of the parties in a communication

1. What security mechanisms does X.800 consider?

Encipherment: the use of mathematical algorithms to transform data into a form that is not readily intelligible

Digital Signatures: Data appended to a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery

Access Control: A variety of mechanisms that enforces access rights to resources

Data Integrity: A variety of mechanisms used to assure the integrity of a data unit or stream of data units

Authentication Exchange: A mechanism intended to ensure the identity of an entity by means of information exchange

Traffic Padding: The insertion of bits into gaps in a data stream to frustrate traffic analysis

1. Describe the relationship between X.800 security services and mechanisms.

The security services are provided by a system to give a specific type of protection of system resource. These are complimented by security mechanism that are features designed to detect, prevent, and/or recover from a security attack

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Mechanism | | | | | | | |
| Service | Encipherment | Digital Signature | Access Control | Data Integrity | Authentication Exchange | Traffic Padding | Routing Control | Notarization |
| Peer Entity Authentication | Y | Y |  |  | Y |  |  |  |
| Data Origin Authentication | Y | Y |  |  |  |  |  |  |
| Access Control |  |  | Y |  |  |  |  |  |
| Confidentiality | Y |  |  |  |  |  | Y |  |
| Traffic Flow Confidentiality | Y |  |  |  |  | Y | Y |  |
| Data Integrity | Y | Y |  | Y |  |  |  |  |
| Non-Repudiation |  | Y |  | Y |  |  |  | Y |
| Availability |  |  |  | Y | Y |  |  |  |

1. Describe the basic model for network security

A basic model for network security requires a suitable algorithm for security transformation. Next, generate secret information keys by the algorithm. Finally, develop methods to share and distribute the secret information

1. What is the difference between OSI and TCP/IP models?

OSI refers to Open Systems Interconnection. While TCP refers to Transmission Control Protocol. The OSI model operates in a vertical structure, while the TCP/IP model operates in a horizontal structure. The OSI model has seven layers compared to TCP/IP’s five layers

1. Encryption services in the presentation layer of the OSI model, would likely be implemented in the layer of the TCP/IP model.

Application layer of the TCP/IP Model

1. What is FIPS-140 standard?

Federal Information Processing Standard. FIPS-140 is the US Government standard for securing cryptographic models used in systems that process sensitive but unclassified data

1. Explain how the U.S. government/military classify data. To what type of data does FIPS-140 apply?

The US Government has a pyramid structure for classifying data. At the tip of the pyramid is top-secret data. Next layer is secret data, confidential data, sensitive but unclassified data, unclassified data. FIPS-140 applies to sensitive but unclassified data, so this can include payroll data, tax ID, purchasing information, etc

1. What is the current version of the FIPS-140 standard?

FIPS-140-2: Issued in 2001 and will be discontinued in September 2006. FIPS-140-3 is also the current version

1. Does compliance with FIPS-140 guarantee the security of the module in question? Explain.

Compliance with FIPS-140 does not guarantee that the model is secure. This means some functionality may not be there and some individual services may not be compatible. In addition, other issues include maintenance, relevance, and marketing

1. What 11 areas does FIPS-140 apply to?

Cryptographic module specification

Cryptographic module ports and interfaces

Roles, services and authentication

Finite state model

Physical security

Operational environment

Cryptographic key management

Electromagnetic Interference (EMI)/Electromagnetic Compatibility(EMC)

Self-tests

Design assurance

Mitigation of attacks

1. What are the levels of FIPS-140? What level is the least/most secure.

Level 1: All components must be production grade; must not have serious security issues

Level 2: Adds a requirement that tampering attempts must leave evidence; module must implement authentication based on user roles

Level 3: Adds a requirement that the module must be tamper resistant; must be able to authenticate users based on user identity; imposes additional requirements on module interface security

Level 4: Adds stricter physical security requirements; requires resistance against attacks targeting the device environment

Level 1 is least secure; Level 4 is most secure

1. I am shopping for a cryptographically protected drive that is resistant to physical tampering. What FIPS-140 compliance level should I be looking for?

FIPS-140 Level 3

1. I now need a cryptographic device that has very strict physical security specifications. What would be the best FIPS-140 category for this?

FIPS-140 Level 4

**Additional Practice Questions to Test Your Understanding**

1. **Deloitte/U.S. Army Interview Question:** What is the CIA triad of cyber security, and describe the meaning of each?

The CIA triad stands for Confidentiality, Integrity, and Availability. Confidentiality refers to the idea that only authorized people are allowed to access sensitive information. Integrity refers to the assurance that the information is legitimate. Finally, availability refers to the ability to use the information by individuals.

1. **Interview Question:** What is the goal of information security within the organization?
2. **Security+ Certificate Question:** This is the model designed for guiding the policies of Information security within a company, firm or organization. What is “this” referred to here? a. Confidentiality
   1. Non-repudiation
   2. **CIA Triad**
   3. Authenticity
3. **Security+ Certificate Question:** CIA triad is also known as
   1. NIC (Non-repudiation, Integrity, Confidentiality)
   2. **AIC (Availability, Integrity, Confidentiality)**
   3. AIN (Availability, Integrity, Non-repudiation)
   4. AIC (Authenticity, Integrity, Confidentiality)
4. **CISSP Certificate Practice Question:** Which of the following is a principle of the CIA Triad that means authorized subjects are granted timely and uninterrupted access to objects? a. Identification
   1. **Availability**
   2. Encryption
   3. Layering
5. **CISSP Certificate Practice Question:** What does the last “D” in the DAD triad stand for?

Destruction. The direct opposite to availability in the CIA triad

1. **CISSP Certificate Practice Question:** Which of the following is not considered a violation of confidentiality?
   1. Stealing Passwords
   2. Eavesdropping
   3. **Hardware Destruction**
   4. Social Engineering
2. **CISSP Certificate Practice Question:** Which of the following is not true?
   1. Violations of confidentiality include human error
   2. Violations of confidentiality include management oversight
   3. **Violations of confidentiality are limited to direct intentional attacks**
   4. Violations of confidentiality can occur when a transmission is not properly encrypted
3. **Interview Question:** Why should you care about the OSI Reference Model?

The OSI Reference Model provides a baseline for the coordination of standards. In addition, this model is useful for new standards as they are developed, and for thinking about existing standards

1. **Interview Question:** Which OSI layer controls application to application communication?

Application layer