Module 1: Assignment 1

Thembelihle W. Shongwe

Ira A. Fulton Schools of Engineering, Arizona State University

IFT 520: Advanced Information Systems Security

Professor Upakar Bhatta

August 21, 2023

1. **List and define the principal security objectives.**

The five principal security objectives as below:

- Confidentiality – systems and data are only disclosed to authorized party.
- Integrity – systems and data are secured and free of unauthorized modifications in storage and in transit.
- Non-repudiation – also known as accountability and a subset of integrity, it is defined by the ability to accurately trace and record activities on systems and data housed in them.
- Authenticity – another subset of integrity. The goal is to verify, trust and validate a user on a system. For messages/data, the source and recipient need to have a level of trust in the message and transmission method used.
- Availability – systems and data are accessible to authorized parties as and when needed.

2. **Describe the uses of data encryption.**

Data encryption is used to secure electronically transmitted data, using the main security objectives – more emphasis on integrity. Through encryption algorithms, the authenticity of a data source is verified, data integrity during transmission checked, and delivery is accounted for.

3. **What are the essential ingredients of a symmetric cipher?**

- plaintext and ciphertext
- algorithm for encryption and decryption.
- a secret key shared between the sender and recipient to encrypt/decrypt plaintext/ciphertext.

4. **What are the two basic functions used in encryption algorithms?**

Encryption algorithms transform data in order to hide its content from unauthorized parties, thus ensuring confidentiality. The second function is to ensure accountability of the data at source, in transit and upon delivery.

5. How many keys are required for two people to communicate via a symmetric cipher?

Just one key is required for people to communication through a symmetric cipher.

6. Describe the two general approaches to attacking a cipher.

a. Brute force – dedicating resources to try multiple combinations of secret keys to decrypt ciphertext.
b. Crypto-analysis – studying characteristics of the algorithm used and exploiting it using known vulnerabilities.

7. What are the principal ingredients of a public-key cryptosystem?

Public-key cryptosystem is asymmetric encryption. The principal ingredients are:

- Plaintext and ciphertext
- Encryption algorithm
- Two unique keys (public and private) that interchangeably encrypt or decrypt data.
- The corresponding private key is needed if data is encrypted with a public key.
- Decryption algorithm

8. List and briefly define three uses of a public-key cryptosystem.

- Key exchange – secure sharing of secret keys between two or more parties.
- Digital signatures – to electronically sign documents. Recipients can also check integrity and source of data if they have a corresponding key.
- User authentication – remote access to applications can be configured using asymmetric encryption to authenticate users though their public keys. Corresponding private keys will be stored in a secure repository.

9. What is the difference between a private key and a secret key?

A private key is used in asymmetric encryption while a public key is used for symmetric encryption. Private keys need corresponding public keys to encrypt or decrypt data, depending on the encryption algorithm used. Secret keys are identical and shared between the parties using an encryption algorithm.

10. What is a message authentication code?

MAC is a single-key encryption algorithm that is used to verify the origin and integrity of data transferred over a network. It accompanies the data transferred so that a recipient can re-check the data integrity using the MAC. If the data has not been modified from source, the MAC will not change (Fortinet, 2023).

11. What is a digital signature?

A digital signature is an electronic signature of a data object that is generated through asymmetric encryption. The signer uses their private key to generate the signature and any party with the public key can verify the source of the data object.

12. Describe the use of public-key certificates and certificate authorities?

Public-key certificates are used to validate an entity's public key and verify their identity. These certificates a designed to make the distribution of public-keys quicker, reliable, and authentic. Certificate authorities (CAs) are trusted third party providers who accept unique public-keys from entities and create certificates that digitally bind public-key to respective entities. For authentication, entities can valid each other's public-keys using certificates issued by CAs.

References

Stallings, W. (2019). *Information privacy engineering and privacy by design: Understanding privacy threats, technology, and regulations based on standards and best practices* (1st ed.). Pearson Education, Inc.

What is a message authentication code (Mac)? Fortinet. Retrieved August 21, 2023, from https://www.fortinet.com/resources/cyberglossary/message-authentication-code