Waterford Institute *of* Technology

INTRODUCTION TO COMPUTER SECURITY

SAMITHA SOMATHILAKA

Department of Computing & Mathematics, WIT

LEARNING OBJECTIVES

Upon successful completion of this chapter, you will be able to:

- Identify the information security triad
- Identify and understand the high-level concepts surrounding information security tools
- Concepts of cloud security

GOOD SECURITY MEANS…..

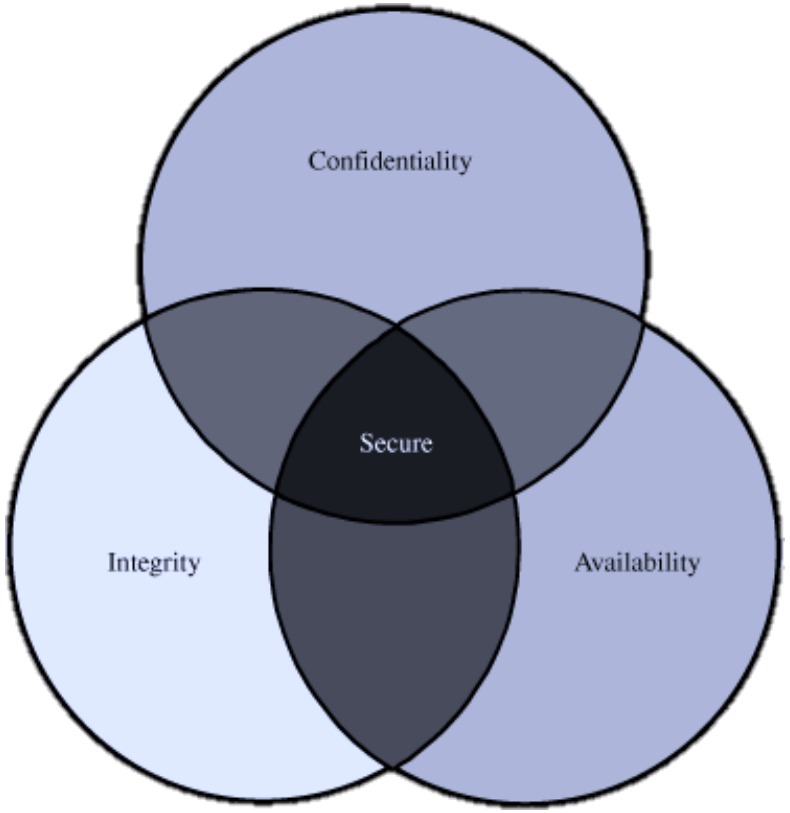
- **10%** of security safeguards are technical
- **90%** of security safeguards rely on the computer user (“YOU”) to adhere to good computing practices

Example: The lock on the door is the 10%. You remembering to lock the lock, checking to see if the door is closed, keeping control of the keys, etc. is the 90%. You need both parts for effective security.

WHAT IS COMPUTER SECURITY

These are the three goals in computing Security.

- Confidentiality
- Integrity
- Availability



3 PILLARS OF SECURITY

- **Confidentiality**
  - restrict access to authorized individuals
- **Integrity**
  - data has not been altered in an unauthorized manner
- **Availability**
  - information can be accessed and modified by authorized individuals in an appropriate timeframe

TOOLS FOR INFORMATION SECURITY

- Authentication
- Access Control
- Encryption
- Backup
- Firewalls
- Virtual Private Networks (VPN)
- Physical Security
- Security Policies

AUTHENTICATION

- Authentication is the act of proving an assertion, such as the identity of a computer system user. In contrast with identification, the act of indicating a person or thing's identity, authentication is the process of verifying that identity.

SINGLE FACTOR AUTHENTICATION

- As the weakest level of authentication, only a single component from one of the three categories of factors is used to authenticate an individual's identity.
- This type of authentication is not recommended for financial or personally relevant transactions that warrant a higher level of security.

TWO FACTOR AUTHENTICATION

- When elements representing two factors are required for authentication, the term two-factor authentication is applied — e.g. a bankcard (something the user has) and a PIN (something the user knows).
- Business networks may require users to provide a password (knowledge factor) and a pseudorandom number from a security token

MULTI FACTOR AUTHENTICATION

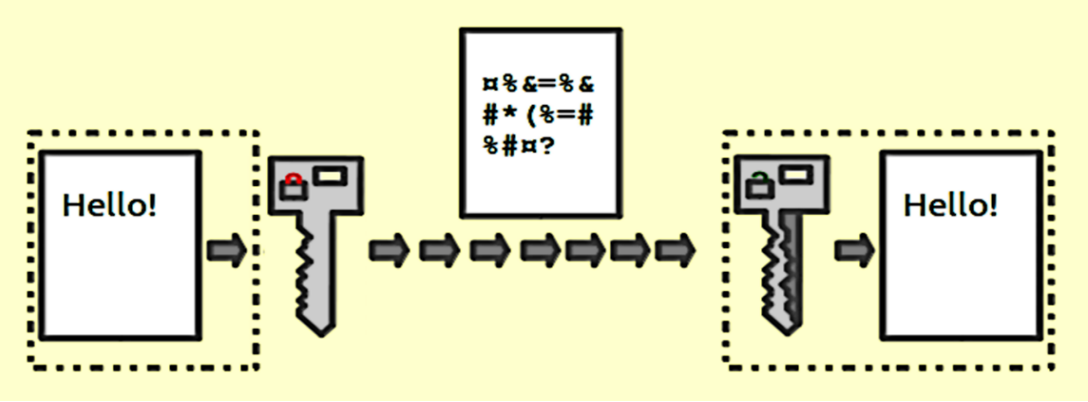
- Instead of using two factors as used in 2FA, multiple authentication factors are used to enhance security. This enhances the security of a transaction in comparison to the 2FA authentication process.

ACCESS CONTROL

- Once authenticated – only provide access to information necessary to perform their job duties to read, modify, add, and/or delete information by:
- Access control list (ACL) created for each resource (information)
- List of users that can read, write, delete or add information

ENCRYPTION

- An algorithm (program) encodes or scrambles information during transmission or storage
- Decoded/unscrambled by only authorized individuals to read it



FIREWALLS

- Can be a piece of hardware and/or software
- Inspects and stops packets of information that don’t apply to a strict set of rules
  - Inbound and outbound
- Hardware firewalls are connected to the network

FIREWALLS

- Software firewalls run on the operating system and intercepts packets as they arrive to a computer
- Can implement multiple firewalls to allow segments of the network to be partially secured to conduct business

VIRTUAL PRIVATE NETWORKS (VPN)

- Some systems can be made private using an internal network to limit access to them
  - Can’t be accessed remotely and are more secure
  - Requires specific connections such as being onsite

VPN

- VPN allows users to remotely access these systems over a public network like the Internet
  - Bypasses the firewall
  - Encrypts the communication or the data exchanged

PHYSICAL SECURITY

- Protection of the actual equipment
  - Hardware
  - Networking components

SECURITY POLICIES

- Guidelines for users use of the information resources
- Embraces general beliefs, goals, objectives, and acceptable procedures
- Security policies focus on confidentiality, integrity, and availability
- Includes applicable government or industry regulations

BACKUP

Important information should be backed up and store in a separate location

- Very useful in the event that the primary computer systems become unavailable

A good backup plan requires:

- Understanding of the organizational information resources
- Regular backups of all data
- Offsite storage of backups
- Test of the data restoration

SUMMARY

- Identified the information security triad
- Identified and understand the high-level concepts surrounding information security tools
- Understanding some basic concepts of computer security which is important for cloud security.