QUEZON CITY UNIVERSITY

COLLEGE OF COMPUTER STUDIES

IAS101 – FUNDAMENTAL OF INFORMATION ASSURANCE AND SECURITY 1

LABORATORY ACTIVITY 1

NAME: Guiyab, Angelica G. (Group 1)

STUDENT NO: 20-1854

YEAR/SECTION: 3rd Yr./SBIT3G

DATE: 1/25/2023

SCORE	PERCENTAGE

INSTRUCTIONS:

Conduct some independent research using scholarly or practitioner resources that will answer the following statements below.

Exercises:

1. Describe one multi-factor authentication method you have experienced and discuss the pros and cons of using multi-factor authentication.

   The Multi-Factor Authentication system requires a user to login using a combination of two or more credentials to prove their identity. It is a comprehensive approach to data and application security. One of the examples is the One-Time Password (OTP) that is commonly used nowadays. The One-time password (OTP) systems provide a mechanism for logging on to a network or service using a unique password that can only be used once.

   These are the following pros of using OTP as Multi - Factor Authentication:

   - **Security**
     - A single-use password will alter with each attempt to log in, greatly reducing or even eliminating the possibility of account penetration.
   - **Allows you to keep your emails safe**
     - On mobile devices, OTPs are typically sent via SMS. You are therefore not required to have access to your email. As a result, you should refrain from accessing your email account on public computers or when using an insecure Wi-Fi hotspot.
   - **Convenient to use**
     - Most individuals own a mobile phone, and SMS functionality exists on every device. SMS's ubiquity means that one-time passwords are convenient to use.

   These are the following cons of using OTP as Multi - Factor Authentication:

   - **Could get out of sync**
     - There are quite a few problems with electronic codes. Algorithm-based OTP has to deal with being out of sync with the authorization server if the system has to deliver OTP by a certain deadline. Fortunately, this problem is easily circumvented by using a time synchronization system. These systems prevent such problems by keeping time clocks in electronic code.
   - **Can lock you out of your account**
     - If your OTP device is stolen or lost, multiple login attacks by hackers can result in a permanent ban from your account. This can be an annoyance while traveling as contacting an OTP provider may require an international call and can incur high roaming charges. Also, even if your provider doesn't limit the number of login attempts, an attacker could still be able to brute force your account.
   - **May be costly for the providers**
     - For OTP providers, cost can be an issue, especially when providing OTP hardware. Another problem with hardware devices is that they can be stolen, damaged, or lost. In addition, users

will have to face the hassle of recharging once the battery life runs out. The best way to avoid these problems is to send the one-time password via SMS.

2. What are some of the latest advances in encryption technologies?

- **Homomorphic Encryption**
  - A method called homomorphic encryption enables mathematical operations to be carried out directly on encrypted material without the need to first decode it. Therefore, sensitive data may be included into computations without jeopardizing its security.
- **Virtual Private Network (VPN)**
  - It is a service that enables users to remotely share data over public networks while securely gaining access to a private network. It establishes a safe, encrypted "tunnel" between a user's device and a VPN server, assisting in protecting the privacy of the data sent over that connection. VPNs may be used to access content that could be blocked in particular regions while also protecting sensitive information, such as financial and personal data.
- **Point-to-point or Peer-to-peer Encryption**
  - It was founded by the PCI Security Standards Council on July, 2013. It's goal is to protect the data of payments to minimize the risks. Hacking and fraud was prevented by encrypting and decrypting the codes as it is processed.
- **Honey Encryption**
  - It prevents an attack as it displays a fake plaintext if an attacker decrypts a wrong key. It is effective security that serves as a decoy to confuse the attacker.
- **Biometric Cryptography**
  - It refers to authentication or other access system that combines inherence factors with public-key infrastructure (PKI). This technique was created to safely link and retrieve a digital key through the use of a biometric picture, like a fingerprint, face, eye, voice, palm.
- **Two-factor authentication (2FA)**
  - It is used to strengthen access security by requiring two methods that rely on single-factor authentication (SFA), where a user simply used one factor, usually a password. To apply two-factor authentication, a user must provide a password as the first factor and the second factor, the user used is either a security token or a biometric factor like a fingerprint or facial scan.

3. What are some of the password policies you have encountered? Do you have to change passwords every so often? What are the minimum requirements for a password?

- Password requirements are very common on account creation. Every time we need to fill in a form, a password is a must. Some password policies require special characters such as *, @, #, $, &, and so on. These restrictions may be hard for those people who are not that literate on using computers as some of those characters are a bit hard to find on keyboard. Some websites only allow the user to use the same password once because there are prohibitions that the old password must not be the same to the new password as it was not unlimited to change.

- Yes, we do need to change password very often as it adds another layer of security, protection, and potential hackers will have a very difficult situation if they try to access anyone’s accounts. I think this should be a habit for everyone as it prevents you from anyone to hack your account and access your privacy.

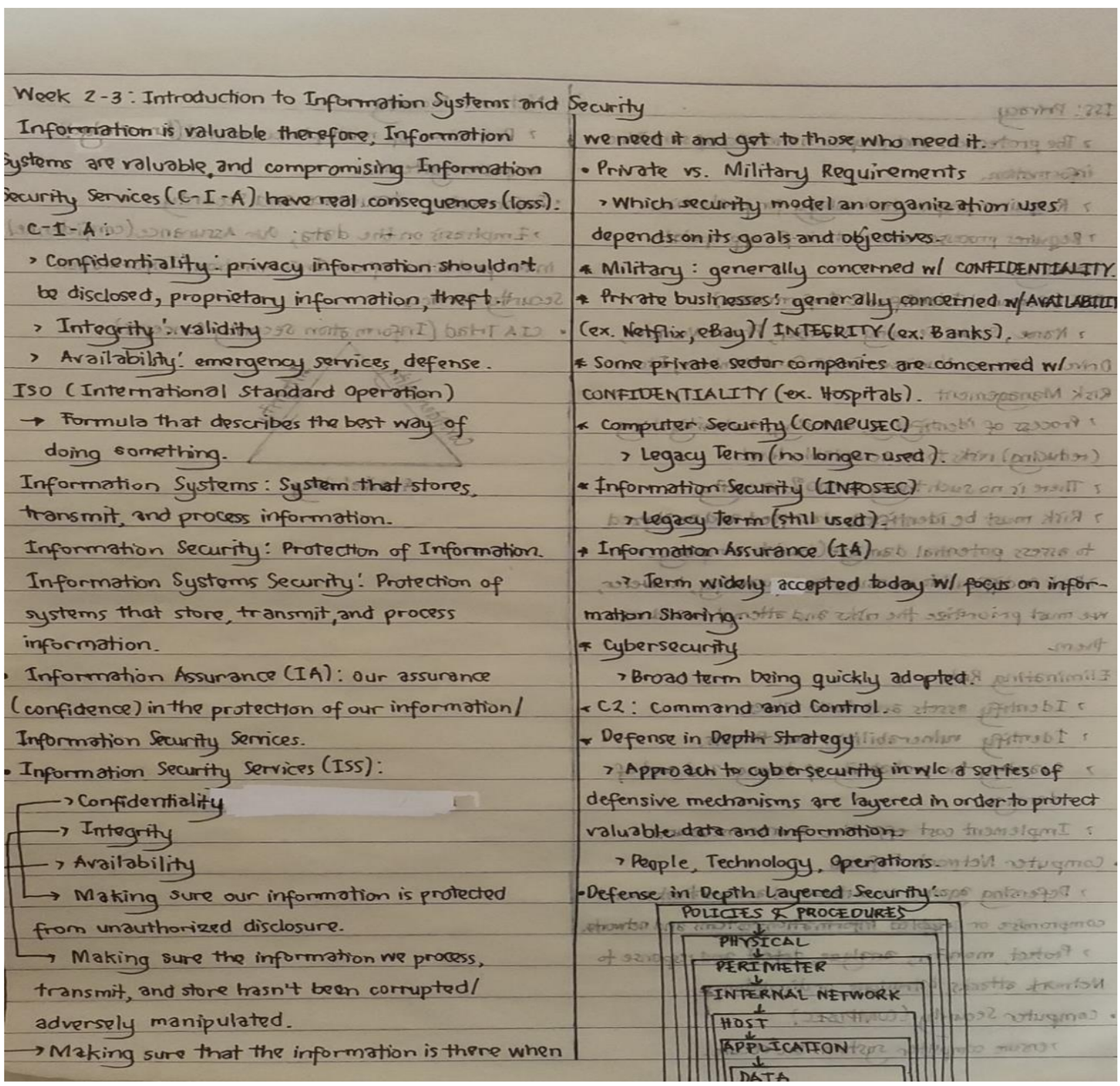
- A strong password is required to be able to reduce the risk of being attacked online. To have a strong password for a person's security, the following characteristics must be implemented:
  - The password must have at least one lowercase and uppercase letter.
  - The password must contain at least one special character such as !, @, #,?,etc.

- It must have a minimum of 12 characters. The longer the character, the harder it is to guess by a machine or a person.
- The password must contain a combination of letters and numbers.

4. How are you doing on keeping your information secure?

- Protect your Web browsing - Companies and websites track everything you do online.
- Update your software and devices - Phone and computer operating systems, Web browsers, popular apps, and even smart-home devices receive frequent updates with new features and security improvements.
- Don't install sketchy software - Every weird app you install on your phone and every browser extension or piece of software you download from a sketchy website represents another potential privacy and security hole.
- Dispose of old IT equipment and records securely - Before you get rid of them, make sure no personal data is left on personal computers, laptops, smartphones or any other devices.
- Don't leave the work unattended - Data breaches can occur when staff and volunteers leave paperwork or laptops unattended.
- Create strong password by out for links and attachments
- Consider additional protections like antivirus, antispyware and firewall
- Back up your data and information's

WEEK 2 - JANUARY 25, 2023 NOTES:



Week 2-3: Introduction to Information Systems and Security

Information is valuable therefore, Information Systems are valuable, and compromising Information Security Services (C-I-A) have real consequences (loss).

C-I-A

› Confidentiality: privacy information shouldn't be disclosed, proprietary information, theft.
› Integrity: validity
› Availability: emergency services, defense.

ISO (International Standard Operation)

→ Formula that describes the best way of doing something.

Information Systems: System that stores, transmit, and process information.

Information Security: Protection of Information.

Information Systems Security: Protection of systems that store, transmit, and process information.

Information Assurance (IA): our assurance (confidence) in the protection of our information/ Information Security Services.

Information Security Services (ISS):

› Confidentiality
› Integrity
› Availability
→ Making sure our information is protected from unauthorized disclosure.
→ Making sure the information we process, transmit, and store hasn't been corrupted/ adversely manipulated.
→ Making sure that the information is there when we need it and get to those who need it.

- Private vs. Military Requirements
  › Which security model an organization uses depends on its goals and objectives.
  * Military: generally concerned w/ CONFIDENTIALITY
  * Private businesses: generally concerned w/ AVAILABILITY (ex. Netflix, eBay)/ INTEGRITY (ex. Banks).
  * Some private sector companies are concerned w/ CONFIDENTIALITY (ex. Hospitals).
  * Computer Security (COMPUSEC)
    › Legacy Term (no longer used).
  * Information Security (INFOSEC)
    › Legacy Term (still used).
  * Information Assurance (IA)
    › Term widely accepted today w/ focus on information sharing.
  * Cybersecurity
    › Broad term being quickly adopted.
  * C2: Command and Control.
  * Defense in Depth Strategy
    › Approach to cybersecurity in w/c a series of defensive mechanisms are layered in order to protect valuable data and information.
    › People, Technology, Operations.

-Defense in Depth Layered Security:

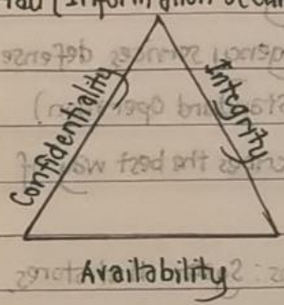
ISS: Privacy

> The protection and proper handling of sensitive information.
> Requires proper technology for protection.
> Requires processes and controls for appropriate handling.

PII (Personal Identifiable Information)

> Name, Social Security Number, Phone Number, Driver's License Number, Credit Card Numbers, Etc.

- Risk Management
  > Process of identifying, assessing, and mitigating (reducing) risks to an acceptable level.
  > There is no such thing as 100% security.
  > Risk must be identified, classified and analyzed to assess potential damage (loss) to company.
  > Risk is difficult to measure and quantify, however, we must prioritize the risks and attempt to address them.
- Eliminating Risk
  > Identify assets and their values.
  > Identify vulnerabilities and threats.
  > Quantify the probability of damage and cost of damage.
  > Implement cost effective countermeasures.
- Computer Network Defense
  > Defensing against unauthorized actions that would compromise or crippled information systems and networks.
  > Protect, monitor, analyze, detect, and response to Network attacks, intrusions, or disruptions.
- Computer Security (COMPUSEC)
  > ensure computer systems are secure.
- Network Security
  > Protection of multiple connected (Networked) computer systems.
- Information Assurance and Security
  > Emphasis on the data; Our Assurance (confidence) in the protection of our Information/Information Security services.
- CIA Triad (Information Security Concepts)



QUEZON CITY UNIVERSITY

COLLEGE OF COMPUTER STUDIES

WEEK 3 – FEBRUARY 01, 2023 NOTES:

Week 3 : INTRODUCTION TO INFORMATION SYSTEMS

7 Domain of a Typical IT Infrastructure

› User Domain : Includes people/employees. Confidentiality-significant asset management.

› Workstation Domain: PC's used by employees either typical desktop PCs, mobile computers, or laptops.

› LAN Domain : All elements used to connect systems & servers together. Internal to the organization.

› LAN - to - WAN Domain: Internal LAN connects to the WAN (Wide Area Network).

› WAN Domain : Any servers that have direct access to ē Internet. Server that has IP address (Internet Protocol).

› Remote Access Domain : Give users access to internal network via external location.

› System/Application Domain: Servers used to host server applications.

→ Assets in ē Workstation Domain have 2 Risks to Address:

1. Theft: organization has significant investment in these systems.

Straight through: switch/ routers are cross.

Bus/ Linear Typology : Coaxial Cable : T-Connector

Modem hub : Star Typology

• Ring Typology : No connector only. T-Connector

• Mesh Typology : Mixed of those typologies mentioned above.

Data on Users Includes:

- Personal & contact data
- Employee reviews
- Salary & bonus data
- Health care choices

2. Updates

› Automated system will often perform 3 steps:

1. Inspect systems for current updates
2. Apply updates
3. Verify ē updates

LAN DOMAIN : Primary hardware components are : hubs, switches, & routers.

› Model, serial number, & location.

› Routers & switches have built-in OS.

LAN to WAN Domain

› WAN is often ē Internet.

- firewalls - primary devices you're connected w/.
  - › single firewall separating ẽ LAN fr. ẽ WAN.
  - › multiple firewalls to create a demilitarized zone (DMZ)/a buffer area.

* Types of Data:

Digital

Analog

Signal/RF/Frequency

Remote Access Domain

- done via VPN (dial-up/virtual private network).
  - Dial-up: client & servers have modems & access to phone lines.
  - VPN: has a public IP address available on ẽ Internet.
  - Client access ẽ Internet, & use tunneling protocols to access ẽ VPN servers.

- System/Application Domain
  - Examples diff. types of application:
    - › E-mail servers: can be single ẽ-mail server. It can also be larger e-mail solution, including both front-end & back-end server configurations.
    - › Database servers: can be Oracle/Microsoft SQL Server. Can be single server/group of servers.
    - › Web Servers: host web sites & serve them to Web clients. Single web server can host single Web site/hundreds.

- WAN: outside ẽ bldg./your area.
- Demilitarized: Private

› Information Security Policy: Policy is ẽ essential foundation of an effective information security program.

→ success of an info. resources protection program depends on ẽ policy generated & attitude of management toward securing info. on automated systems.

* Policy Objectives:
  - reduced risk
  - compliance w/ laws & regulations.
  - assurance of operational continuity, info. integrity, & confidentiality.

REFERENCES:

Fisher, T. (n.d.). Virtual Private Network (VPN). Retrieved from https://www.lifewire.com/virtual-private-network-vpn-4163427'

Indrajit Das and Ria Das, "Mobile Security (OTP) by Cloud Computing," International Journal of Innovations in Engineering and Technology, August 2013 What are one-time passwords and their pros and cons? Retrieved from https://resources.infosecinstitute.com/topic/one-time-passwords-pros-and-cons/

Ir. (2022, July) P2P Encryption: What It Is and Why It's Important To Data Security. Retrieved from https://www.ir.com/guides/p2p-encryption

Knafo, J. (2018, February) Top 10 Password Policies and Best Practices for System Administrators. The Devolutions Blog. Retrieved from https://blog.devolutions.net/2018/02/top-10-password-policies-and-best-practices-for-system-administrators/

Mijin Kim, Byunghee Lee, Seungjoo Kim, and Dongho Won, "Weaknesses and Improvements of a One-time Password Authentication Scheme," International Journal of Future Generation Communication and Networking, December 2009

Muhlenberg College. (2016, May 9). Guidelines for Strong Passwords. Retrieved from https://www.muhlenberg.edu/offices/oit/about/policies_procedures/strong-passwords.html

Omolara, A. E., Jantan, A., & Abiodun, O. I. (2018, December). A comprehensive review of honey encryption scheme. Indonesian Journal of Electrical Engineering and Computer Science. Retrieved from https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=honey+encryption&btnG=#d=gs_qabs&t=1674613962566&u=%23p%3DImUpCOvhbAkJ

Thales. (2020). What does OTP mean? Retrieved from https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/otp?fbclid=IwAR21RhwKZsEe7xmqU1OEESkAwvR0zyn-B0hCDbqfhS40zCuarCU2lVZ8vPo

Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On data banks and privacy homomorphic encryption. Retrieve from https://dl.acm.org/doi/10.1145/359340.359342/

Rosencrance, L. (n.d.). What is Two-Factor Authentication (2FA) and How Does It Work? Retrieved from https://www.techtarget.com/searchsecurity/definition/two-factor authentication#:~:text=Two%2Dfactor%20authentication%20(2FA)%2C%20sometimes%20referred%20to%20as

Tools4ever. (2020). What is an OTP (One-Time Password)? Retrieved from https://www.tools4ever.com/glossary/what-is-otp/#:~:text=The%20foremost%20advantage%20of%20and,are%20virtually%20impossible%20to%20guess.

Virgilio, D. (July 8, 2019). What are one-time passwords and their pros and cons? Retrieved from https://resources.infosecinstitute.com/topic/one-time-passwords-pros-and-cons/

What is Biometric Encryption? | Security Encyclopedia. (n.d.). Retrieved from https://www.hypr.com/security-encyclopedia/biometric-encryption