Name: Ronit Singh **CDAD-UH 1037** **Date:** 10 October, 2021

CYBERWARFARE

Week 7 Reading Summary

The first reading *"Introduction to Information Security"* by Cengage Learning, introduces the concept of securing information from adversaries or malicious actors in the cyber domain. It begins with a story based on an IT help desk specialist in a company that has been attacked by hackers through phishing and impersonation using email as an attack vector. The employees and technicians are startled and worried. This intends to show the frustration and damage that can happen due to employees' carelessness of clicking on a malicious link. The reading also goes over the history of cybersecurity and how information security evolved separately from it due to the pressing need to protect the rapidly increasing customer information in companies and organizations. *"Data is often the most valuable asset possessed by an organization and it is the main target of intentional attacks."* (page 17). Going back to the history, the reading also mentions the "ARPANET" or "Advanced Research Projects Agency Network" which aimed at linking various computers for resource sharing. This was the beginning of networking and later what would lead to the greatest invention of mankind i.e. the internet. However, security, in the early stages, was mainly focussed on the physical aspects. As the network grew, the need to secure stored information and information in transit grew with it. Thus, giving birth to "information security" as a separate field under cybersecurity. There's also a mention about the "CIA Triad" that stands for "Confidentiality, Integrity, and Availability" which are the key pillars of security. However, according to the author, these have become outdated with the continuous changing environment and threat landscape. As mentioned, *"The threats to the confidentiality, integrity, and availability of information have evolved into a vast collection of events, including accidental or intentional damage, destruction, theft, unintended or unauthorized modification, or other misuse from human or nonhuman threats."* (page 8). The reading outlines various components of the Information System such as Software, Hardware, Data, People, Procedures, and Networks. The 'software' component is considered the most vulnerable among them, while 'people' component the easiest vulnerability because of humans' manipulative and helpful nature. According to the reading, security as well as the ease of access to information should be balanced. It's because both have a direct relationship, that is to say, as security implementations increase, the ease of access decreases due to more security checks and vice-versa. Hence, companies should weigh their risk appetite and work on mitigating risks rather than focusing and spending more resources on completely securing the company and thereby increasing the difficulty and time-consumption of access.

The second reading *"An Introduction to Cryptography"* by PGP Corporation, is about cryptography and its evolution and role in protecting information from being viewed by unauthorized users. It introduces the readers to basic cryptographic terminologies such as cipher, ciphertext, plaintext, encryption, decryption, and public and private keys. According to the article, *"The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key"* (page 10). The article states that conventional cryptography, even though faster, is not reliable in today's world. As mentioned, *"the persistent problem with conventional encryption is key distribution: how do you get the key to the recipient without someone intercepting it?"* (page 12). This is the main issue that the

'public key cryptography' aims to address. This improvisation of conventional cryptography is widely used due to its reliability in the sense that only the user with the right private key (undisclosed and unshared) can decrypt the information. Even though the public key is not hidden, it's still useless without a private key. However, this is slower as compared to the conventional method (symmetric key cryptography having a common key to encrypt as well as decrypt). The article mentions that the conventional method is 1000 times faster. This is where the PGP (Pretty Good Privacy), a hybrid cryptosystem, comes into play. It *"combines some of the best features of both conventional and public key cryptography"* (page 13). Hence, making cryptography faster and more reliable at the same time. The article dives deep into the concept of 'Digital Signatures' as well. It states that, "A digital certificate consists of three things: a public key, certificate information ("Identity" information about the user, such as name, user ID, and so on.), and one or more digital signatures" (page 18). It is mainly used in verifying the integrity and authenticity of information being transmitted. It can also be used for non-repudiation purposes so as to prevent the user from denying that the information has been sent from his/her end. The article also goes over various technical aspects of digital certificates and different types of trust models.

What surprised me?

The term **"salami theft"** was unknown to me. The article states that *"In information security, salami theft occurs when an employee steals a few pieces of information at a time, knowing that taking more would be noticed—but eventually the employee gets something complete or usable."* (page 13). This is a very effective tactic, I believe. I connected this concept to malware and thought that some malwares (like Pegasus, I assume) might use little computer resources, but continuously, so as to be unnoticed and hide from antivirus softwares.

Moreover, I came across a new terminology i.e. *passphrase*, as a new effective method other than 'password managers' to prevent dictionary attacks. It is *"a longer version of a password"*, *"typically composed of multiple words"*, and *"contains a combination of upper and lowercase letters, numeric and punctuation characters"* (page 31). The main important use of a passphrase is in PGP that uses a passphrase to encrypt the private key on the machine, which makes it extremely difficult to decrypt by any normal means.

Questions?

1. Are hash functions more helpful, effective and reliable in encrypting or keeping a check on integrity of information? Which one?
2. Is it important to focus more on the managerial aspect or technical aspect in implementing SDLC? Can a technical team, by themselves, lead and implement the security procedures without any help from the superiors (as in startups)?