Computer Security: Task 3.2C

Name of Student

Institutional Affiliation

**Question 1:**

**Principles of Authentication**

The CIA triad is a reference to information security initiatives. This triad is sometimes called CIA triangle. Protection of information affects the way IT is used. Communication systems in businesses and homes are now commonly used. These actions should safeguard valuable data such as company confidential information and individual users' personal or financial information. CIA triads are used by information security teams to establish security measures. The CIA safety triangle illustrates the basic objectives to be incorporated into information security initiatives. The CIA triad provides a tool or guide to secure IT systems and networks and their associated technical properties (Chapple, 2020). In order to reduce vulnerabilities to security and leverage the capabilities that support the CIA modules, a CIA triad implementation in enterprises often needs frequent monitoring and upgrading of specific IT systems.

Confidentiality

The protection of data against unauthorised access is confidentiality. This purpose of the CIA triad illustrates the need to protect knowledge. Confidentiality includes steps to ensure access to information is permitted only to approved persons. For example, if approved users have access to a computer file, confidentiality would be maintained, although unauthorised individuals have no access to the computer file (Velazquez, 2020). The CIA Security Triangle's confidentiality applies to information security because the security of information needs control over access to protected information.

Integrity

The triad objective of honesty of the CIA is to provide reliable and consistent information if permitted modifications do not occur. Due to careless access and use, mistakes in the information system or unauthorised access and use, information can have changed. The credibility of the CIA triad remains unchanged if the information is processed, distributed and used without alteration to the information. Integrity concerns security of information, since proper protection results in reliable and consistent information. In some cases of financial details, the CIA triad honesty target is more critical than the other objectives. Any modification of financial documents leads to problems in information quality, continuity and value. For example, the privacy of financial reports is of greater importance to banks, with confidentiality being second priority. ATM receipts are left untouched and hanging around after the money is removed by certain account holders or depositors. This indicates that secrecy is not the top priority. Instead, honesty is the most significant objective in the banking system's information security.

Availability

The CIA's triad objective is to provide information where and when it is rightly needed. In the CIA triad, main concern is that if approved users have access to it, they should be accessible. The availability of all elements of the information system is ensured when it operates properly. Problems with the information system may prevent access to information, thereby rendering it impossible to access information. When government produced online press releases are involved, the CIA triad availability target is more critical than other objectives. Public consumption media are normally available. The details contained in them should be accessible to the public in order to be accurate. Confidentiality is also not a problem. The only second priority is integrity. In this CIA triad, governments ensure that their websites and networks have limited or negligible downtime in order to ensure that information is available in press releases. Backups also ensure public information is accessible.

**Question 2:**

Challenges with Password based Authentication:

1. Easy passwords can be cracked

End-user actions, including selecting simple to remember passwords, introduces most of the vulnerabilities in password. For a hacker you can quickly crack or guess these passwords. Surveys indicate that the word password, personal family names, names of animals and dictionary terms are frequent passwords.

Hackers can use a variety of tricks to try to get online passwords. The most popular technique, however, is the brute force assault which uses automated tools to perform dirty work. In this case, cyber criminals are given access through a data breach to some account information. Most web pages, at least safe ones, do not store your passwords in simple text but use some kind of encryption algorithm to save your passwords. In this case the hackers will learn the names, email addresses, street addresses, telephone numbers and other information for each account that has been compromised (Boulgouris, Plataniotis, & Micheli-Tzanakou, 2019). The one missing element is the password.

2. Random passwords can’t be remembered

A random password should not and should not be familiar with information, meaning and content. Only by using it repeatedly can it be understood. As repetition is a poor way of recalling, however, users sometimes disregard pseudo-random passwords entirely.

Users usually need a set of password guidelines to stick to in order to improve the strength of passwords selected by users. Users write their passwords in accordance with the relevant guidelines. In other words, it does not include the username and should have at least 8 characters, including at least one or one number or upper-case letter (Das, 2020). There are different password guidelines used by organisations and they should be written effectively to give the organisations adequate levels of safety

3. Remembering Multiple Passwords

The more you know a person's password, the more likely you are to remember that another password. The possibility of interfering with identical passwords also increases with several passwords. This applies in particular to systems not commonly used. With the expanded growth of online services, we must note the same amount of account data. Many of us want to simply reuse a popular password, but that can be extremely risky. With the same password for different providers, the chance of an account breach is even greater. An assailant can compromise your financial, email or social media accounts by simply failing to provide protection for any of these services (Wayman, 2019).

4. Problems with passwords that needs to be continuously changed

In order to keep the device robust from different attacks, computer systems need regular password amendments. Users need to think of new passwords that are consistent with, but easy to remember, all organisations’ specifications. However, system-based password policies cannot insure the privacy of passwords.

**Question 3:**

Mobile applications receive the most popular and likely most significant value from biometrics by identifying and cybersecurity. Passwords and pins have historically been the key way to protect such applications. Biometrics have enhanced the credibility of mobile apps and diminished their cyber security risks as a result of both the alarmingly sophisticated attacks of hackers.

In this way, biometric safety has grown into the fingerprint identification, face recognition, voice recognition or even finger vein recognition of specific features in applications or apps. Multifactor authentication multi-modal security systems (combining two ways of biometric identification) further increased the degree of protection provided and became highly secure methods in the prevention of data breaches and attacks.

a. Fingerprint scanning

Authentication by fingerprint is the act of verifying the identity of one or more individuals on the basis of their fingerprints. For decades the term has been used in a range of practises, including digital identification, criminal enforcement, financial services and border security.

Authentication or scanning by fingerprint is a type of biometric technology that allows users to access online services with fingerprint photos (Wayman, 2019). The biometric scan is typically based on native sensing technology for mobile and other devices since all this has but obsolete applications, biometric algorithms from a third parties. Several fingerprint scan solutions are designed to ensure that a user's fingerprint model is protected on a user's computer in a decentralised form, such as FIDO. Here, the fingerprint scan for a user is checked locally, a token is forwarded to the provider of services and access is enabled.

Other solutions for fingerprint scanning are architected according to an old centralised scheme that stores user models to the service provider and matches a library with biometrics of other users.

b. Iris scanning

Iris detection or iris scanning is the technique used to take a high-contrast image of an iris by using visible and near-infrared light. This is a type of biometrics in the same category as face and fingerprint (Boulgouris, Plataniotis, & Micheli-Tzanakou, 2019).

The iris scan tests in irises the peculiar patterns, the colourful circles in the eyes of the citizens. By lighting the iris with invisible infrared light, biometric iris scanners are able to collect special patterns not apparent to the naked eye (Chapple, 2020). Iris scanners detect eyelashes, eyelids, specular reflection and exclude them, which usually obscure parts of the iris. The end result is a pixel pack that only contains the iris. The pattern of the lines and colours of the eye is then analysed so that a bit of a pattern is extracted that encodes the information in the iris. This bit pattern is digitalized and compared to templates stored in a verification database (one-on-one template matching) or ID (one-to-many template matching).

Iris and fingerprint accuracy are higher compared with other biometric characteristics, and both are more reliable and simpler. These characteristics improve the performance of iris and fingerprint recognition in today's society. The method begins with the collection of iris and fingerprint images, which are pre-processed for noise removal. The characteristics are then extracted and matched such that correlation is found between the two characteristics. The matching ratings provided by each recognizer are given to the decision module, which determines whether an individual is genuine or impostor.

# **References**

Boulgouris, N. V., Plataniotis, K. N., & Micheli-Tzanakou, E. (2019). *Biometrics: Theory, Methods, and Applications.* John Wiley & Sons.

Chapple, M. (2020). *Access Control, Authentication, and Public Key Infrastructure.* Jones & Bartlett Learning.

Das, R. (2020). *Adopting Biometric Technology: Challenges and Solutions.* CRC Press.

Velazquez, J. (2020). *A Guide to Understanding Identification and Authentication in Trusted Systems.* National Computer Security.

Wayman, J. (2019). *Using Biometric Identification Technologies.* CRC Press.