Week 4 – Task 4.2 C

1. Question 1
   a. What are the four principles of authentication? Briefly discuss each of them. (up to 400 words)
      - An essential of information security is authentication, which makes sure that before allowing access to resources, the identities of persons, devices, or systems are confirmed. The four primary tenets of verification are;

✓ **Something you know :**
The user's knowledge is necessary for this principle to work. A password or PIN is the most popular type. This method's security is contingent upon the confidentiality and intricacy of the data. This approach's strengths include its simplicity in terms of execution and comprehension, as well as its ease of changing information in the event that it is compromised. However, because users frequently select weak or simple passwords, it has flaws including vulnerability to phishing, guessing, and social engineering attacks.

✓ **Something you have :**
According to this theory, identity is confirmed using an item the user is in possession of. Smart cards, security tokens, and cell phones that are used to get one-time passwords (OTPs) are a few examples. The advantages of this approach include its capacity to provide an extra degree of security on top of knowledge-based authentication and the difficulty with which attackers can breach the system short of physically stealing the object. The potential for goods to be misplaced, stolen, or damaged, as well as the expense and administrative difficulties involved in organizing and delivering tangible tokens are the limitations.

- ✓ **Something you are:**
  This concept depends on the user’s distinct bodily traits, such as voice, facial, or retinal or iris patterns, fingerprints, or retinal patterns. This method’s advantages include its high level of security, ease of usage (because users don’t need to carry a tangible item or memorize anything), and difficulty in forging or sharing. Nevertheless, shortcomings include the possibility of biometric systems being faked, privacy issues with regard to the usage and storage of biometric data, and the likelihood of biometric recognition errors including false positives and false negatives.

- ✓ **Something You do :**
  According to this theory people can be distinguished from one another by their distinctive behavioral patterns, which could include usage patterns, stride, or typing rhythm. The ability to provide continuous authentication during a session, which adds an extra layer of protection that is challenging for attackers to precisely recreate, is one of this method’s features. However, it can be impacted by changes in user behavior. Brought on by stress, injury, or other circumstances. It also requires sophisticated equipment to effectively capture and evaluate behavioral patterns.

b. Give 4 arguments as to why password-based authentication is problematic. (up to 400 words)

- Despite being commonly used, password-based authentication has a number of flaws that affect both security and user experience. The following four main arguments draw attention to these issues:

  - ✓ **Attack-Susceptibility:**
    Password are susceptible to a number of attacks, including dictionary attacks, phishing, brute force attacks, and social engineering. Brute force and dictionary attacks involve the use of software by attackers to repeatedly guess passwords until they discover the right one. Phishing is the practice of using phone emails or websites to deceive consumers into disclosing their passwords. Social engineering uses psychological tricks on people to obtain private data. These attack methods highlight the intrinsic fragility of passwords, especially those that are short and/ or used for serval accounts.

  - ✓ **User Conduct and Password Administration:**
    Password security is seriously undermined by human factors. People frequently select simple, easy-to-remember passwords like “password,” “qwerty,” or “123456” Additionally, they frequently reuse passwords on many platforms in an efforts to reduce the mental strain of having to remember numerous strong password. This behavior raises the possibility of a security breach because it can result in the compromise of one account and the illegal access of other accounts. Furthermore, even while changing passwords on a regular basis is a suggested security practice, users frequently acquire predictable patterns as a result, further weakening security.

- ✓ **Difficulties in coming up with Robust Passwords:**

  It is naturally difficult to come up with a strong, memorable password that is hard for hackers to figure out or guess. Generally speaking, long passwords with a combination of capital and lowercase letters, digits, and special characters are considered strong passwords. But because they are difficult to remember, people frequently write down or save these passwords in unsafe places like sticky notes or unencrypted files. The security advantages of using a strong password are compromised by this behavior.

- ✓ **User Experience and Scalability:**
  Users are burdened more and more as service and applications that require password multiply. Password fatigue results from having to deal with so many passwords. Users' overall experience may be impacted by annoyance and inconvenience. Additionally, firms incur higher support expenses and administrative overhead as a results of having to reset passwords owing to forgetting them Complicated password policies and the requirement for frequently passwords changes can increase user annoyance and encourage non- compliance with security protocols.

- In conclusion, even though passwords are still widely used for authentication, there are still a number of problems with them, including scalability concerns, user error, password creation and memory difficulties, and vulnerability to different types of assaults. In order to strengthen security and improve the user experience, these considerations emphasize the need for more user- friendly and safe authentication techniques, including multi-factor authentication (MFA) or password less alternative.

c. Upon graduation, you become a security consultant for a prestigious firm. Your client is the Australian government. They are seeking expert advice about adoption of biometric technology for the mobile app of "my.gov.au". The mobile app allows access and management of your Medicare and Tax. Hence, a large number of users are expected to rely on the mobile app upon introduction to the market. Referring to the 4 requirements offered by Jain and et al., and challenges discussed in Section 29.6, which 2 biometric technologies you think are the best candidate for adoption in the app? Support your answer with arguments (up to 500 words)

- Biometric technology provides safe and practical user authentication, which is essential for app like the myGov mobile app that handle sensitive data like Medicare and Tax. The two biometric technologies that seem to have the greatest chance of being adopted are face recognition and fingerprint recognition. These decisions are based on the four criteria for biometric systems proposed by Jain et al.(universality, distinctiveness, permanence, and collectability), as well as some insights from Section 29.6 regarding biometric problems.

- **Jain et al.'s Biometric Requirements**
  - ✓ **Distinctiveness:**
    Even with identical twins, there is extremely little chance that two fingerprints will ever be exactly alike. When precisely mapped utilizing algorithms, facial traits provide high uniqueness, essentially allowing for individual identification.
  - ✓ **Permanence:**
    Fingerprints are a stable biometric characteristic that don't really over the course of a person's life. Although ageing and other causes might cause changes in facial features, contemporary facial recognition algorithms are resilient enough to accommodate these changes.
  - ✓ **Collectability:**
    The majority of contemporary smartphones have sensors that make it simple to gather fingerprints, making this a speedy and dependable means of authentication. Smartphones come equipped with front-facing cameras which may be used to take facial photographs. This makes the process of gathering facial images simple and unobtrusive.
  - ✓ **Universality**:
    Since almost everyone has a fingerprint and they may be taken from a large population, fingerprints are considered universal. Faces are Omnipresent and identifiable to a wide range of people.

- **Difficulties and Things to Think about from section 29.6**

  - ✓ **Privacy Concerns:**
    Data from fingerprints is regarded as extremely sensitive. To preserve user privacy, secure storage and appropriate encryption are crucial. Faces are very recognizable, which raises privacy concerns. It is essential to make sure that facial data is safety preserved and is only utilized for authentication.

  - ✓ **Security and spoofing:**
    Even though fingerprint sensors are generally safe, lifted prints can be used to fake them. This risk can be reduced by using advanced sensors that can detect liveness. When using images or videos foe facial recognition, there is a risk of spoofing. Nonetheless, 3D sensing and liveness detection technologies greatly lessen these weakness.

  - ✓ **Cost of implementation and technical viability:**
    Economical since fingerprint sensors are widely used in contemporary devices. It is technically possible to implement and integrate it easily with the myGov app. slightly more expensive implementation because of the sophisticated software and camera specifications. Still it's a viable alternative given how common facial recognition technology is in gadgets like iPhone

  - ✓ **User Acceptance:**
    Because fingerprints sensors are widely used in smartphones and fingerprints identification is simple to use, users generally accept it favorably. Because it is non-contact and simple to use, facial recognition technology has also gained popularity, albeit user acceptability may be impacted by privacy concerns.

- For the myGov mobile app, fingerprints and facial recognition both satisfy the requirements of universality, uniqueness, permanence, and collectability. They provide a harmonious blend of technical viability, user-friendliness, and security. While facial recognition gives a noncontact option that keeps up with modern technology advances, fingerprint recognition offer a more developed approach. By implementing these technologies, the myGov app will be more user-friendly and secure, providing safe access to sensitive personal data.

2. Question 2
    a. Reflection point – how difficult or easy did you find reading through the content of chapters. Did you use any of the tips suggested in useful guides in page 2? Share a few words of your experience when working through questions as a note-to-self.
        - Going through the chapters in the textbook was difficult yet educational at the same time. Through the use of AAA principles, they provided a comprehensive overview of the fundamentals of cyber security, which is necessary to understand the field's larger context. I used various recommended techniques, such skimming and creating concept maps, to establish a suitable hierarchy and structure so that I could comprehend the content.