## IT5504/ IT5479 Information Security

**Lab 3 Personal Security**

**Due date and time**

This Lab tutorial is carried out in the session in week 3 of the course.

**Purpose**

This lab exercise helps in gaining a better understanding of our perception of personal security.

**Preparation**

Lecture notes, online research, journal articles and appropriate relevant resources.

**Submission**

Submit your answers to this exercise in a word document and upload it to the Moodle dropbox provided.

**Activity 1)**

**Review Questions**

*(Briefly answer the following review questions)*

1. What is the simple definition of privacy, and why is it important in information security and the digital era? **Privacy is the right of being apart from interference or intrusion. The ability to have freedom without feeling any intrusion or disturbance. Privacy is important in information security and the digital era because of the volume of personal information that is collected. Privacy helps keep personal information confidential.**
2. How can hardware be protected using anti-malware measures? **Anti-malware uses three strategies to protect systems from malicious software: signature based detection, behaviour based detection and sand-boxing. Signature based uses a set of known software components and their digital signature to identify new malicious software. Behaviour based malware detection helps computer security professionals more quickly identify, block and eradicate malware by using an active approach to malware analysis. Sandboxing used to isolate potentially malicious files from the rest of the system. Sandboxing filters out malicious files.**
3. Why is patching significant in maintaining the security of software and systems? **Patching is significant in maintaining the security of software and systems because it helps protect against vulnerabilities and security risks.**
4. What is the definition of personal data, and why is its protection crucial? **Personal data could be important information about yourself such as date of birth, address, health, income etc. Protection is crucial because you do not want to have your privacy invaded or personal data used by non-authorized people. It is crucial to add layers of security to your personal information.**
5. What are the potential threats and challenges related to IoT security? **Potential threats and challenges related to IoT security are privacy and personal information due to lack of encryption (not properly securing private information), firmware updates missing, AI based attacks, weak passcodes or inconsistent security standards etc**
6. Why are regular backups essential for personal security and data protection? **Regular backups are essential because there are common events that happen that could lose your important files from inevitable data loss situations. These could be a result from malware infection where you can have data stolen, damaged or systems destroyed. So regular back ups will protect this.**
7. What is the difference between encryption and backups, and how do they contribute to personal security? **Encryption helps convert important information into a code which proves difficult for anyone to access or read if they do not have access. Back ups is a saved copy of whole data stored somewhere safe such as in the computer, external hard drive or cloud storage.**
8. What information is typically collected about individuals, and how is it collected in today's digital landscape? **Information such as preferences are being collected about individuals. This is by tracing “likes” on particular products which many large organizations thrive of. Companies would gather this data, on wide range of metrics and use to generate ideas to bring to consumer market.**
9. How can individuals safeguard their personal data from unauthorized collection and misuse? **Strong passwords can help safeguard individuals personal data, applying 2FA two factor authentication, updating software regularly, intrusion detection software etc.**
10. What are some best practices for maintaining personal security and protecting sensitive information in the digital age? **Avoid using public wifi, back up data, encryption, antivirus software, regular updating, keeping a low profile such as private etc. These practices can help maintain personal security and protect sensitive information in the digital age.**

The above review questions cover a range of topics related to personal security and aim to explore different dimensions of securing personal information and maintaining privacy in today's digital landscape.

**Activity 2)**

**Discussion Questions**

**Mini Case 1: Privacy and Personal Data Protection**

Scenario: Sarah is an avid social media user who recently discovered that her personal data was being collected and shared without her consent. She is concerned about her privacy and wants to understand the importance of privacy and the protection of personal data.

Discussion: Sarah's case highlights the significance of privacy and the protection of personal data in the digital era. Privacy ensures that individuals have control over their personal information, allowing them to maintain their autonomy and safeguard their sensitive data. In this case, Sarah's experience serves as a reminder that individuals should be aware of the information collected about them, how it is collected, and take measures to protect their personal data from unauthorized access or misuse.

**Why is privacy important in the digital era, and how does it relate to the protection of personal data?**

*(This question prompts a discussion on the significance of privacy in the context of digital technologies, emphasizing the importance of individuals having control over their personal information and the potential risks associated with unauthorized access or misuse of personal data.)*

**Privacy is important in the digital era because of not only how much we consume but importantly sharing personal information about ourselves with the frequent use of social media. We use the internet for banking that hold savings etc, doctors appointments with important health information or family/personal memories such as photos that hold sentimental value. In this case study, Sarahs personal data was being collected without consent. Having control over your personal information can mean reading the terms and conditions of any social platforms or websites you sign up to, using safe browsing methods such as private mode, encryptors and researching websites for legitimacy and identifying differences between what appears to be genuine or not. These all relate to the protection of personal data.**

**Mini Case 2: IoT Security and Threats**

Scenario: John recently installed a smart home automation system that connects various devices, such as his security cameras, thermostat, and lights, to the Internet. He wants to understand the potential threats related to IoT security.

Discussion: John's case highlights the importance of considering security in IoT devices. IoT devices, when connected to the internet, can be vulnerable to security breaches, such as unauthorized access or control, data leaks, or even becoming part of a botnet. It is crucial for individuals to understand the potential threats and take necessary precautions, such as ensuring strong passwords, regularly updating firmware, and implementing network segmentation to enhance the security of their IoT devices and protect their privacy within their homes.

**What are some potential threats to IoT security, and how can individuals protect themselves from these threats?**

*(This question encourages you to explore the various security risks associated with IoT devices, such as unauthorized access or control, data breaches. It also prompts to consider proactive measures that individuals can take to enhance the security of their IoT devices and safeguard their privacy within their homes.)*

**Some** **potential threats to IoT security are lack of security updates which leaves room for vulnerabilities in devices that could lead to an attack such as malware infecting the devices. Regular security updates will repair patches etc that reduces the chances of threats etc. Another potential and common threat is weak default passwords. These days, hackers would have identified all the common default passwords in the world on one database accessing many IoT devices such as video cameras, routers, ipads etc. To better protect yourself is creating strong passwords, 2FA and storing these passwords in safe managers.**