## IT5504/ IT5479 Information Security

**Lab 4 Identification and Authentication**

**Due date and time**

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

**Purpose**

This lab exercise enables us with a better understanding of concepts associated with Identification and Authentication in 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. **Definition & Importance:** What is the difference between Identification and Authentication? Why are these concepts essential in ensuring information security in the digital era?

**The difference between identification and authentication is identification is the act of identifying the user and authentication is proof of the user’s identity. These concepts are essential in ensuring information security in the digital era in a three step process. Step one identification establishes user identity based on information they provide. This can be email address, username etc. Step two would be verification confirming who the user is using a trusted source such as drivers license or passport. Step three as we discussed being authentication by confirming the user’s identity and verify they have permissions to access system or service.**

1. **Dynamic Biometrics & Real-Life Example:** Explain the concept of dynamic biometrics, specifically voice dynamics. Provide a real-life example of how voice dynamics can be used for authentication in a practical scenario.

**Voice biometrics technology verifies the identity of a speaker. Dynamic biometrics are based on behavioural characteristics that can vary sample to sample they can include handwritten signatures, voiceprints, keystroke dynamics, face and finger movements.**

**A real life example of voice dynamics for authentication could be when ringing IRD and they use voice id which has captured your voice when saying your name and date of birth. The system recognises the similarities/matching voice and tone to authenticate you (as week as answering the correct personal information).**

1. **Potential Problems with Three Basic Authentication Techniques:** Discuss the three basic authentication techniques - something you know, something you have, and something you are. Identify and explain potential security issues or vulnerabilities associated with each technique.

**Something you know – is knowledge based, such as knowing your PIN code or password**

**Password or pin numbers can be easily guessed if not strong or long enough**

**Something you have – is property based, having a key tag, card swipe an authorized device**

**Potentially losing the key card or swipe could end up in the wrong hands allowing unauthorized access**

**Something you are – is biologically based, a fingerprint or face recognition – the vulnerability here is someone being able to copy your fingerprint or realistic face to pass the recognitions.**

1. **Example of Multi-Factor Authentication (MFA):** Give a simple use case of Multi-Factor Authentication (MFA) in action. Describe the different factors involved in the MFA process and how it enhances security compared to single-factor authentication.

**Examples of MFA in action could be when changing a password. Multi factor authentication is where the security level increases using tow or more factors (a minimum of three) Enter old password, enter the code sent to mobile phone, click verify link to email and enter the code generated from the authentication generator.**

1. **Differences between Two-Step Verification and MFA:** What is the difference between Two-Step Verification and Multi-Factor Authentication (MFA)? Are they the same, or do they have distinct characteristics?

**Difference between two step verification and MFA is 2-step have two factors of security level (enter code sent via text and verify link via email) and MFA would be the same but have an extra factor of security or more – example is the 2-step and an added layer such as code from authentication generator.**

1. **Standard vs. Mutual Authentication:** Compare and contrast Standard Authentication with Mutual Authentication. How do these two approaches differ in ensuring secure communication between entities?

**Standard Authentication would be for the user entering the user ID and a password. Mutual authentication is also known as two way authentication where two side of the communications channel to authenticate each other’s identities instead of just one as per the standard authentication.**

1. **Password as the Most Common Authentication Technique:** Discuss why passwords are still the most commonly used authentication technique despite their vulnerabilities. What makes them susceptible to attacks?

**Passwords are still the most commonly used authentication techniques because it is a unique user requirement where they inputs a chosen password which makes the user feel more comfortable and in control. Passwords are susceptible to attacks because they can be guessed if not strong with mix of characters and symbols.**

1. **Proper Use of Passwords:** What are some best practices for using passwords securely? Provide a list of recommendations on how to create strong and memorable passwords.

**Best practises of using passwords securely is never using easily guessed passwords such as 1234 or your name etc. Some best practices are a combination of symbols and alphabets and of at least 10 characters. A list of recommendations on how to create strong and memorable passwords is using passphrases, or words in dictionary, there are alternatives such as downloading the password manager which helps create strong passwords and stores this for you. There are various ones to use online. You can use password strength checkers which gives you and indication of how strong your created password is.**

1. **Common Password Cracking Techniques:** Explain at least three common password cracking techniques employed by hackers to breach accounts. Discuss the importance of using strong and unique passwords to mitigate these risks.

**Phishing: A fraudulent practice used by hackers in sending emails pretending to be someone else in attempt to lure an individual to revealing their passwords or personal information when clicking on the links – that contains malware.**

**Malware: Malicious software containing programs or code that is harmful to systems that can lead to leaking passwords**

**Social engineering: An increasing common attack where hackers pretend to be a legitimate person tricking other social media platform users into asking for support that leads to giving passwords/personal information.**

1. **Importance of Regularly Updating Passwords:** Why is it crucial to update passwords regularly? How often should users change their passwords, and what are the potential consequences of not doing so?

**It is crucial to update passwords regularly because it reduces risk that they will have frequent access. If you lose or change computers it is possible for someone to access your passwords. It is recommended to change passwords every few months and the potential consequences are clear – this may result in unauthorised access to your passwords or the system it is protected by.**

The above review questions cover a range of topics related to identification and authentication, biometrics, various authentication techniques, password security, and the importance of securing digital information in the modern era. They should provide us with a comprehensive understanding of these concepts and encourage meaningful discussions on information security best practices.

**Activity 2)**

**Discussion Questions**

**Mini Case 1: Online Banking Authentication**

John, a young professional, uses online banking to manage his finances. He accesses his bank account through a mobile app and typically logs in using a username and password (single-factor authentication). Recently, his bank implemented a new security measure, requiring customers to set up Multi-Factor Authentication (MFA) for added protection. Now, in addition to his password, John needs to provide a one-time passcode sent to his mobile phone for each login attempt.

**Discussion Points:**

* How does the implementation of Multi-Factor Authentication enhance the security of John's online banking account?

**MFA will add layers to the security of the online banking account which increases security a lot. Instead of user password, you will have code generator and even email to confirm your access.**

* What are the possible risks or vulnerabilities associated with relying solely on a username and password for online banking?

**It is easily guessed by hackers who are able to manipulate the system by various ways through phishing, malware, or in putting all easily guessed passwords. One layer of security as just being password will not suffice.**

* Have any of you experienced MFA in your own online accounts? If so, how do you feel about using it for added security?

**Yes – most online banking require MFA – these are great and makes me feel well protected as a user and online customer.**

**Mini Case 2: Workplace Mutual Authentication**

At a technology company, employees often need to access sensitive data on the company's internal network. To ensure secure communication, the company implements Mutual Authentication for remote access. Employees use a smart card (something they have) and enter a PIN (something they know) to log in. Additionally, the company's servers verify their identity before establishing a connection.

**Discussion Points:**

* How does Mutual Authentication benefit the company's security compared to traditional single-factor authentication methods?

**It is a complete verification with the added layers where two sides of communications channel verify each other’s identity. This benefits company security as the process of verifying both parties reaches mutual secure confidence. A single factor authentication is where only channel is being verified.**

* In what situations would Mutual Authentication be particularly crucial for an organization?

**IOT devices that need to connect to a remote server, mutual authentication will help data received is accurate from a legitimate source and reducing chances of an attacker compromising connections. Other mutual authentication is Uber where you check the license plate matches your request, and driver checks your name and both can confirm the destination and fare.**

* Have any of you encountered Mutual Authentication in your workplaces or other environments? Do you think it is an effective security measure?

**I have while using Uber – making sure the car that has pulled over is the correct one as I approach it. Matching the plate number and the driver saying my name as I enter. Mutual authentication is used in online banking – making sure all credentials match, and secure websites. It is an effective security measure to keep data safe and private.**

***Reflection and Personal Experiences:***

*After discussing the mini cases, I would encourage you to reflect on your own experiences with authentication methods in your daily lives, whether it's using passwords for online accounts, two-factor authentication for social media, or smart cards for accessing certain facilities. Briefly share your thoughts on the effectiveness of these methods, any concerns you might have about your personal data security, and how these examples relate to the broader importance of secure authentication in the digital era. (share your thoughts in bullet points and briefly discuss it)*

**I have always used 2FA, and smart cards to increase personal security. It helps reduce the risk a lot and there has been times where a password was compromised however thanks to 2FA the intruder did not get the verification email to bypass. This happens quite often with phone numbers so it is ideal to use an alternative.**