UTHM

Universiti Tun Hussein Onn Malaysia

BIE 33003

SOFTWARE ENGINEERING SECURITY

SEM II 2024/2025

LAB 1 : SECURITY CONCEPT AND REQUIREMENTS

LECTURE :PUAN RUHAYA BINTI AB.AZIZ

SECTION 4

NAME	MATRIC NUMBER
NURALYANA MAISARA BINTI NOORISHAM	AI220222
SITI NUR SYUHADAH BINTI ARIFIN	AI220044
NURUL NABILAH BINTI SUHUD	AI220050
NURUL SYAZANA BINTI ABDU GHANI	AI220059

Labsheet 1: Security Concept and Requirements

Instructors:	Ruhaya Binti Ab. Aziz
Duration:	4 hours (2 weeks)
Laboratory:	MKP
Tools/Software:	Lab computer, CASE tools: Microsoft Word, Project etc.
References:	i. Lecture note. ii. Stallings, W. & Brown, L. 2019. *Computer Security: Principles and Practice*. England; Pearson Education Limited. iii. Any online/offline related sources.
Report	1. Report is done **by group**. 2. The report must be submitted on **week 3 (4/4/2025)**. **3. Submit a softcopy of report to the assignment folder in Author.**

Tutorial Questions (Self Assessment)

1) Describe three key fundamental goals of software engineering security?

The fundamental key principles of software engineering security are confidentiality, availability, and integrity. The confidentiality principles ensure that private information remains undisclosed. Next, the availability principles ensure the data availability to be used when it is needed to make decisions. Lastly, the integrity principles ensure that the data can be trusted to be accurate and it has not been inappropriately modified.

2) Compare vulnerabilities, threats and attacks.

Vulnerabilities are flaws in a system that can be exploited by threats and cause harm. Threats are capabilities and potential events that can exploit the vulnerabilities of the system. Attacks are actual actions that happen that harm the system.

3) Compare authentication to authorization.

Authentication is a method of verifying the credibility of a person by their username, password, facial recognition or fingerprints. Authorization is a method that grants permission to the person to access the assets and actions they are allowed to.

4) Why are the forms of non-repudiations discussed important to information assurance?

The form of non-repudiation is a guarantee of security with a special force on transactions and data exchange over the Internet. The importance of this form is to ensure accountability and trust to prove the authenticity and integrity of transactions or communications, making it impossible for parties to deny their involvement.

Case Study (Group Assessment)

Task: You can form a group of 3 or 4 people and do it during a lab session. Discuss with your instructor. Read each of the questions carefully then, answer it.

1. Consider UTHM MPP Voting system as the case study. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirements.

Confidentiality	Requirements: Ensure that the voter data remains private. Importance: **High**, by implementing secure mechanisms, Google Authenticator, only registered students are allowed to vote in the UTHM MPP Voting system.
Integrity	Requirements: Ensure that votes cannot be altered, deleted, or tampered with once cast. Importance: **Very high**, to ensure the accuracy and fairness of the election results, so that votes cannot be tampered with or altered once the student clicks submit after choosing 3 candidates from the nominees list of MPP candidates.
Availability	Requirements: Ensure the system is accessible to all eligible voters during the voting period. Importance: **High**, the list of MPP candidates shows from the start of the voting season until the end of the season.

2. Consider Food Panda: Food delivery and Grocery system. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirements.

Confidentiality	The personal data like phone number, address, payment info is not shared with the restaurant or rider in full detail unless necessary for fulfilling the order.
Integrity	End-to-end encryption and digital signatures to ensure the transactions are secure and unaltered, maintaining the trust of their customers.
Availability	Implement scalable architecture and disaster recovery plans to handle high traffic volumes and maintain service continuity during peak hour periods or in the event of technical issues.

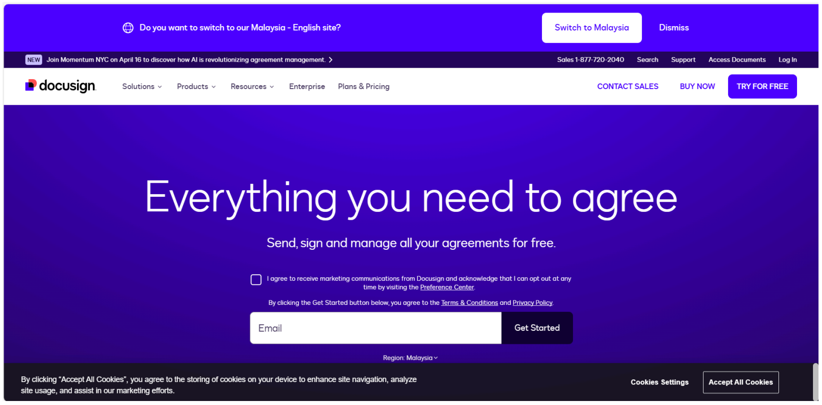
3. Consider Patient Management System for Hospital Sultanah Nora Ismail. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirements.

Confidentiality	**Requirement:** Ensure that only authorized personnel can access a patient's medical records such as doctors, nurse and admin staff. **High Importance:** Patient data includes personal information, medical history, and treatment plans, which must remain private under laws such as Malaysia's PDPA (Personal Data Protection Act). Unauthorized disclosure can lead to **privacy breaches**, legal issues, and loss of trust.
Integrity	**Requirement:** Ensure that patient diagnosis and treatment records cannot be modified or deleted by unauthorized users. **High Importance:** Incorrect or altered information can lead to misdiagnosis, improper treatment, or even patient harm. Audit logs and checksums should be used to detect unauthorized changes.
Availability	**Requirement:** Ensure that the Patient Management System is accessible 24/7, especially for emergency departments **Medium to High Importance**: While less critical than integrity or confidentiality in some cases, unavailable systems can delay treatment, hinder operations, or cause administrative chaos. Measures such as failover systems, backup servers, and disaster recovery plans are important.

4. Consider different websites used to display pages for various organizations.

   a. Give an example of a web page for which non-repudiation is the most important requirement.

   Docusign (online e-signature platform) - Docusign | #1 in Electronic Signature and Intelligent Agreement Management



Do you want to switch to our Malaysia - English site?

NEW Join Momentum NYC on April 16 to discover how AI is revolutionizing agreement management.

Everything you need to agree

Send, sign and manage all your agreements for free.

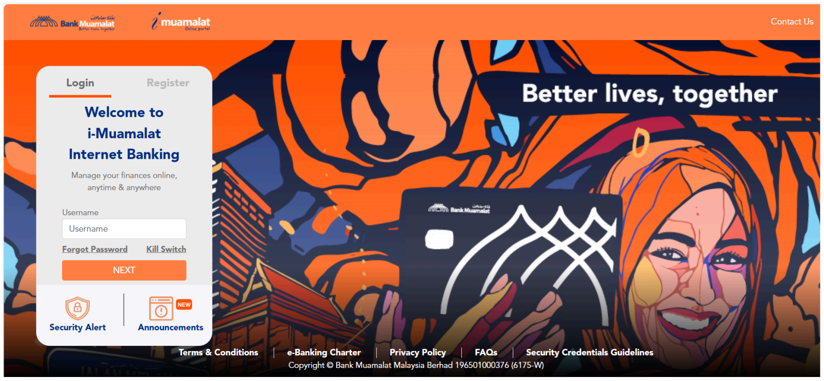
□ I agree to receive marketing communications from Docusign and acknowledge that I can opt out at any time by visiting the Preference Center.

By clicking the Get Started button below, you agree to the Terms & Conditions and Privacy Policy.

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

   b. Give an example of a web page for which authentication is the most important requirement.

   i-Muamalat (online banking portal) - i-Muamalat



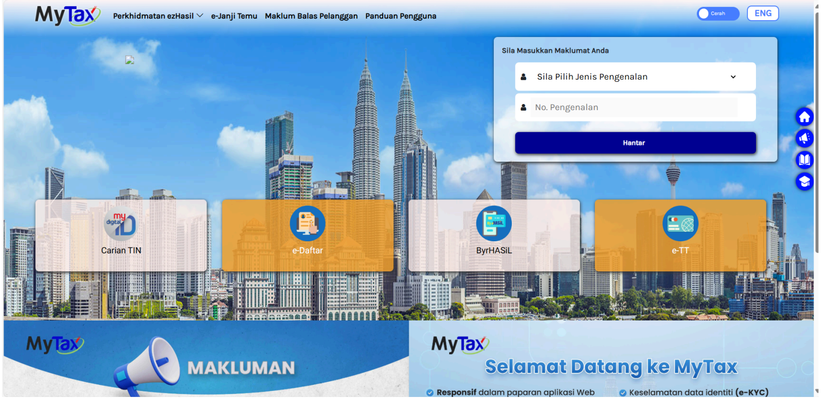
Welcome to i-Muamalat Internet Banking

Manage your finances online, anytime & anywhere

Copyright © Bank Muamalat Malaysia Berhad 196501000376 (6175-W)

   c. Give an example of a web page for which accessibility is the most important requirement.

   MyTax (government services portal) - MyTax



Selamat Datang ke MyTax

✓ **Responsif** dalam paparan aplikasi Web ✓ Keselamatan data identiti **(e-KYC)**

5. For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity respectively. Justify your answers.

   a. A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the entire information system.

- Real-time sensor data

Confidentiality	Low. While the sensor is responsible for monitoring accurate data for the distribution of electric power, it has a low impact towards its confidentiality. If the data is exposed, it could provide insight into operational conditions, but it would not typically lead to a direct security breach or compromise of sensitive information.
Availability	High. If the sensor is unavailable, operators would not be able to monitor the system accurately. This could lead to system malfunctions and downtime.
Integrity	High. The sensor is responsible to detect most of the accurate data, if it has less integrity, it would affect the accuracy and the quality of the data, where operators could mislead to inaccurate decision-making. In other words, it could lead to system failure and power outage.

- Routine administrative information

Confidentiality	Moderate. While it is important, the information exposure can be considered as less harmful than real-time sensor data. Unauthorized access could lead to any information exposed. However, it would not directly

	affect the physical infrastructure the same way the real-time sensor data might.
Availability	Moderate. It is important for day-to-day management in the form of reports, logs and user data. However, its unavailability can still be considered as less critical for immediate stability and operation needs.
Integrity	Moderate. The information integrity is important but less critical than the integrity of real-time sensor data. If administrative data is altered or corrupted, it could create confusion or disrupt administrative decision-making, but it would generally not have the same immediate or catastrophic consequences as the loss of integrity in real-time data.

b. An information system used for large acquisition in a contracting organization for government agency in Malaysia contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the entire information system.

- Pre-solicitation phase contract

Confidentiality	High. The pre-solicitation phase contract information contains sensitive details about upcoming government contracts, including drafts, negotiation terms, and potential bidders. If this information is disclosed prematurely, it could lead to competitive disadvantage, manipulation of the bidding process, or even legal and financial repercussions.
Availability	Moderate. While it's important that the pre-solicitation phase contract information is available to the authorized personnel involved in the procurement process, its availability is less critical than its confidentiality. If the information is temporarily unavailable (e.g., due to a technical issue or server downtime), the procurement process may be delayed, but the consequences would typically not be as severe as a breach of confidentiality
Integrity	High. The integrity of the pre-solicitation phase contract information is critical. If this data is altered or tampered with (e.g., by changing contract terms or bidder details), it could lead to unfair bidding practices, legal challenges, or even fraud.

- Routine administrative information

Confidentiality	Moderate. Routine administrative information includes general organizational data, such as internal memos, employee records, and procurement procedures. While some of this data could be sensitive, it typically does not hold the same level of confidentiality as the pre-solicitation phase contract information.
Availability	High. Routine administrative information needs to be available to ensure smooth organizational functioning. If the system or specific data related to internal operations (e.g., employee scheduling, meeting records) is unavailable, it could disrupt normal activities.
Integrity	Moderate. The integrity of routine administrative information is important to ensure that internal processes, such as scheduling or employee management, are accurate and function as intended. However, tampering with this type of data would typically have less serious consequences than tampering with sensitive contract information.

6. Give examples of different threat attacks on confidentiality, authentication, integrity, and availability.

	Confidentiality	Authentication	Integrity	Availability
Hardware	-	-keylogging (Done by hardware keyloggers) -Human negligence (leave computer unlocked, losing devices theft)	Physical Tampering (replacing secure chips with compromised ones).	Hard Disk Failure - A critical server's hard drive crashes due to wear and tear. - Users cannot access the system or data until the hardware is replaced and restored from backup.
Software	An unauthorized copy of software is made.	-Brute Force Attack(gain illegal access to a system by entering large numbers of randomly generated or pregenerated combinations of	Supply Chain Attacks (malicious code is injected into third-party libraries or dependencies).	Software bug or crash - A newly installed update contains a bug that causes the application to crash repeatedly.

		usernames and password until they find one that work)		- This prevents users from accessing the system or completing tasks.
Data	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	sql injection(uses malicious SQL code input in an unexpected way to manipulate and access a database)	Unauthorized Modifications (attackers alter stored data, compromising its accuracy and trustworthiness).	Ransomware - A ransomware attack encrypts all user data and denies access unless a ransom is paid. The data is there, but completely unusable, resulting in system downtime.
Communication Lines	Messages are read. The traffic pattern of messages is observed.	Man-in-the-middle(intercepts info over a network)	Eavesdropping (unauthorized listening to communication lines to extract sensitive information).	Network Outage - A construction crew accidentally cuts an underground fiber optic cable, disrupting internet access to an entire building. - Users cannot connect to online services, causing a halt in operations.

-END OF LAB EXERCISE 1-