## IT5504/ IT5479 Information Security

**Lab 2 Security Fundamentals**

**Due date and time**

This Lab tutorial is carried out in the session in week 2 of the course.

**Purpose**

This exercise enables your better understanding of what we mean by fundamentals of security models.

**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 are the key concepts of information security?

**Key concepts to information security are:**

**Fraud Prevention and Detection, System Integrity, Governance and Accountability, Data Security and Privacy.**

1. Define privacy and explain its importance in the context of information security.

Privacy

**Broadly speaking, privacy is the right to be left alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and used.**

1. What is identity management and why is it a critical element in security systems?

**Also known as idM, identity access management ensures that authorized people – and only authorized people – have access to the technology resources they need to perform their job functions. It is a critical element in security systems because it protects data and avoids breaches. Passwords could become compromised, phishing attacks enabled or ransomware.**

1. Explain the CIA triad model and its significance in information security.

**CIA triad model: Confidentiality, Integrity and Availability they are used for finding vulnerabilities and methods for creating solutions. Its significance to information security helps guide security teams to pinpoint the different ways to address each concern (Fortinet).**

1. What is authentication and how does it contribute to ensuring secure access to systems and data? **Authentication is the process of verifying the identity of a user or entity before granting access to a system or resource. Authentication helps prevent unauthorized access, protects sensitive information and ensures only authorized users can use the system.**
2. Define non-repudiation and explain why it is important in security protocols. **Non repudiation ensures that the originator of a message or transaction cannot deny their involvement or the validity of the message, providing undeniable proof of origin and integrity. Non repudiation enhances trust, accountability, and dispute resolution by providing evidence that cannot be disputed or denied, reducing the potential for fraud or false claims.**
3. Discuss the concepts of confidentiality, integrity, and availability in relation to information security. **It’s the act of maintaining the confidentiality, integrity, and availability of information, ensuring that information is not compromised in any way when critical issues arise.**
4. What is encryption and how does it help protect sensitive data? **Encryption is a method of protecting data by turning it into a secret code that can only be unlocked with a secret key or password. Encryption protects data by providing four benefits. Confidentiality, Authentication, Integrity and Non-repudiation.**
5. Describe the three main states of data and explain why securing data in each state is crucial.

**Three main states of data is Data at rest – encrypt inactive data when stored in blob storage, database etc, Data in transit – encrypt data that is flowing between untrusted public or private networks and lastly Data in use – protect/encrypt data that is in use, while in RAM, and during computation. Securing data in each state is crucial because it can be difficult to keep track of all your data. Each information from different state can bring its own kind of vulnerabilities which is why it is crucial to protect data in each state.**

1. Differentiate between symmetric key and asymmetric key encryption algorithms and discuss their respective strengths and weaknesses. **Asymmetric key encryption is a method where there are two mathematically related keys, public key for encryption and a private key for decryption. Strengths are confidentiality and weaknesses could be integrity as unknown what the private key is. Where symmetric key encryption uses a single shared secret key for both encryption and decryption ensuring secure communication between parties. Strengths would be secure communication and weaknesses would be availability having the same key.**

The above questions cover various fundamental elements and concepts of information security, including privacy, identity management, security models, encryption, and data protection. They can serve as a useful exercise to review and reinforce your understanding of the fundamentals of security.

**Activity 2)**

**Discussion Questions**

**Mini Case 1: Non-Repudiation and Legal Disputes**

Scenario: A company engaged in an online transaction with a customer. However, the customer later claims that they did not authorize the transaction, leading to a legal dispute.

Discussion: This case emphasizes the importance of non-repudiation in information security. Non-repudiation ensures that a user cannot deny their involvement in a transaction or action. In this case, if the company had implemented non-repudiation mechanisms such as digital signatures or transaction logs, they would have been able to provide evidence of the customer's authorization, resolving the legal dispute.

Non-repudiation is crucial in situations where there is a need to establish proof of actions or transactions, and it helps ensure trust, accountability, and dispute resolution.

**What is the role of non-repudiation in resolving legal disputes involving online transactions?**

*The role of non-repudiation in resolving legal disputes involving online transactions is to provide evidence that a user cannot deny their involvement or authorization in a transaction. Non-repudiation mechanisms, such as digital signatures or transaction logs, can be used as proof to establish the authenticity and integrity of the transaction. This helps to prevent one party from later denying their participation, reducing disputes and increasing trust in online transactions.*

**How can organizations implement non-repudiation mechanisms to establish proof of user authorization and prevent disputes?**

*Organizations can implement non-repudiation mechanisms by incorporating digital signatures, timestamps, and secure transaction logs. Digital signatures use cryptographic techniques to verify the authenticity and integrity of a digital document or transaction, providing strong evidence of user involvement. Timestamps help establish the time at which a transaction occurred, further reinforcing the chronological order of events. Secure transaction logs record important details and actions during a transaction, serving as an audit trail and providing evidence if disputes arise.*

**Shows how important non-repudiation is important for not only the customer but also the organisation. Companies implementing non-repudiation such as digital signatures, logs etc would prove customers authorisation, increases customer confidence in online transactions and overall reducing transaction disputes online.**

**Mini Case 2: Availability and Denial-of-Service (DoS) Attacks**

Scenario: A popular e-commerce website experienced a Denial-of-Service (DoS) attack, rendering the website unavailable for an extended period of time.

Discussion: This case highlights the importance of availability in information security. Availability ensures that systems, networks, and services are accessible and operational when needed. In this case, the DoS attack disrupted the availability of the e-commerce website, resulting in customer frustration and financial loss.

To protect against such attacks, organizations need to implement measures such as firewalls, intrusion detection systems, and load balancing techniques. These measures help detect and mitigate DoS attacks, ensuring the availability of services to legitimate users.

Maintaining availability is crucial, particularly for critical systems and services. Organizations must proactively assess and enhance their infrastructure and defences to prevent and mitigate disruptions to availability caused by attacks or system failures.

**What is the impact of a Denial-of-Service (DoS) attack on the availability of a website or service?**

*A DoS attack can render a website or service unavailable to legitimate users. By overwhelming the target system with a flood of illegitimate traffic or exploiting vulnerabilities, the attacker can disrupt the normal functioning of the website or service, causing it to become unresponsive or crash. This impacts the availability of the website, leading to customer frustration and potential financial loss for the organization.*

**What measures can organizations implement to mitigate the impact of DoS attacks and ensure availability?**

*Organizations can implement several measures to mitigate the impact of DoS attacks and ensure availability. These include:*

* *Deploying robust firewalls and intrusion detection/prevention systems to filter and block malicious traffic.*
* *Implementing load balancing techniques to distribute traffic across multiple servers, ensuring that no single server is overwhelmed.*
* *Utilizing content delivery networks (CDNs) to cache and deliver website content from multiple geographically distributed servers, improving resilience against attacks.*
* *Employing rate limiting and traffic throttling mechanisms to detect and mitigate suspicious traffic patterns.*
* *Collaborating with Internet Service Providers (ISPs) to leverage their infrastructure and services, such as traffic filtering and traffic diversion during an attack.*

**This case study shows how availability is important in information security. An attack happened which was (DoS) a denial of service which basically put the e-commerce website out of order for sometime leading to obvious frustration and financial loss. Measures were discussed on how to combat these attacks in future such as firewalls, intrusion detection/prevention etc. ISP co-operation with handling the volume of traffic filtering and diversion.**