## IT5504/ IT5479 Information Security

**Lab 1 Introduction to Security**

**Due date and time**

This Lab tutorial is carried out in the session in week 1 of the course.

**Purpose**

This exercise develops your understanding of what we mean by security and fundamental concepts around the exercises of 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 are the key topics covered in the introduction to security?

**Security Fundamentals, Mobile Security, Security, Internet Security**

1. Define the fundamental concepts of assets, threats, and protection in the context of security.

**Assets: Any information or related equipment that has a value to an agency or organisation. This includes equipment, facilities, patents, intellectual property, software and hardware.**

**Threats: An act that threatens the security, hackers, spyware, exploitation etc. There are three types such as Intentional (Malware, Phishing, Illegally accessing someone’s account). Unintentional – threats that are human errors such as forgetting to install firewall**

**Natural – Natural disasters that can damage data**

**Protection: Safety such as antivirus software, 2FA, added security to ensure less risk. Protection deals with internal threats, prevents unauthorized access to resources and information.**

1. How would you define information and assets in the context of security?

**Information are facts such as details of a persons medical history and assets would be something of value such as visa details, bitcoin, physical assets like cars, houses.**

1. What is the definition of information assurance?

**The process of processing, storing, and transmitting the right information to the right people at the right time.**

1. Define information security and explain its significance in modern-day contexts.

**Combination of cyber security, information governance, risk management and information assurance. Today’s world many people are online, exchanging personal information so security is required everywhere from transactions to filling out forms online.**

1. Is security a trade-off? Discuss the concept of balancing security measures with other factors.

**Security trade off is basically what the cost of security is to you such as protecting your home contents requires an installation of a burger security system. So hardware installation will take up space and time in your home. The trade off will be modified home and costs. Another example could be installing security software in your computer, the trade off could be that some websites may not work given high risk etc.**

1. Explain the CIA model and its relevance to information security.

**Confidentiality – Assures that information is accessible only by authorized individuals.**

**Integrity – Quality of something being unmodified or complete. Assuring data has not been tampered with and can be trusted.**

**Availability – Indicates that network, systems, and applications are up and operating. Assuring authorized users have timely, trustworthy access to resources when required.**

**Authentication and non-repudiation the proof of origin and integrity of data.**

1. Define the terms cipher and decrypt in the context of cryptography.

**Cipher: Method of hiding words, text with encryption by replacing original letters with other letters.**

**Decrypt: Process of transforming encrypted data back into its original form.**

1. Why is studying security important in today's digital landscape?

**To keep the high volume of personal data etc online secure and protected. Technology is vastly growing so our online presence is frequent and we can better manage our privacy online with heighted security and protection.**

1. Discuss the importance of security in protecting sensitive information and preventing unauthorized access or data breaches.

**The importance of security in protecting sensitive information and preventing unauthorized access or data breaches is very important. Many large organizations would not be able to operate if personal data was not secure or backed up. Protecting sensitive information means you are at low risk of having your personal details compromised to unauthorized people etc. If this was not protected you could lose money, or records you need.**

**Activity 2)**

**Discussion Questions**

**Mini Case 1: Financial Institution Data Breach**

Scenario: A prominent financial institution experiences a major data breach, compromising the personal and financial information of millions of its customers.

Case Description: This case highlights the importance of security in the financial sector and the consequences of inadequate measures. The data breach resulted in severe financial losses for both the affected customers and the institution itself. The compromised information led to identity theft, fraudulent transactions, and damage to the institution's reputation.

Discussion Points:

Analyze the potential security vulnerabilities that could have led to the data breach.

* Weak or outdated security measures, such as lack of encryption or inadequate access controls.
* Insufficient employee training on security protocols and best practices.
* Negligence in applying software patches and updates, leaving systems vulnerable to known exploits.
* Inadequate network segmentation, allowing unauthorized access to sensitive data.
* Lack of robust intrusion detection and prevention systems to identify and respond to potential threats.
* Social engineering attacks targeting employees to gain unauthorized access to the system.
* Inadequate incident response and monitoring capabilities to detect and mitigate security incidents promptly.

Discuss the impact of the breach on the affected customers and the financial institution.

Customers:

* Increased risk of identity theft, fraud, and financial loss.
* Loss of trust and confidence in the financial institution's ability to protect their personal and financial information.
* Potential long-term consequences, such as damaged credit scores and ongoing financial repercussions.
* Emotional distress and the need to invest time and resources in rectifying the consequences of the breach.

Financial Institution:

* Financial losses due to legal liabilities, regulatory fines, and compensation to affected customers.
* Damage to the institution's reputation, leading to decreased customer loyalty and potential loss of business.
* Increased scrutiny from regulatory bodies and potential restrictions on business operations.
* Cost of implementing enhanced security measures, conducting forensic investigations, and restoring systems.
* Potential legal consequences, including class-action lawsuits and settlements.

It is important to note that the specific impact and vulnerabilities may vary depending on the nature of the data breach and the security measures in place prior to the incident.

**Shows multiple different factors that could have led to the data breach. Insufficient employee training could be a situation where an employee hadn’t followed correct protocol when identifying a customer. This leads to identify theft, loss of money etc. A loss of trust and confidence by customers for the organisation.**

**Mini Case 2: Ransomware Attack on Healthcare Organization**

Scenario: A healthcare organization falls victim to a ransomware attack, resulting in the encryption and inaccessibility of critical patient records and systems.

Case Description: This case highlights the criticality of security in the healthcare sector and the potential risks associated with cyberattacks. The ransomware attack disrupted patient care, compromised sensitive medical records, and posed a significant threat to patient safety.

Discussion Points:

Analyze the impact of the ransomware attack on the healthcare organization's operations and patient care.

* Disruption of critical systems and infrastructure, leading to the inability to access patient records, medical equipment, and communication channels.
* Delayed or compromised patient care, as healthcare providers may not have immediate access to vital information and treatment history.
* Increased risks to patient safety, as timely access to medical data is essential for accurate diagnoses and appropriate treatment.
* Operational chaos and resource strain as the organization focuses on incident response, system recovery, and ensuring patient safety.
* Potential cancellation or rescheduling of appointments, surgeries, and procedures, causing inconvenience and potential harm to patients.
* Long-term consequences, such as damaged reputation and loss of public trust in the organization's ability to protect patient data and provide reliable care.

Discuss the potential motivations and methods employed by attackers in targeting healthcare organizations.

Motivations:

* Financial gain through ransom payments or the sale of stolen patient data on the black market.
* Political or ideological motives, such as disrupting healthcare systems for political leverage or causing harm to specific individuals or groups.
* Espionage or gathering sensitive medical research or intellectual property.
* Exploiting the critical nature of healthcare services to extort organizations for ransom.

Methods:

* Phishing attacks targeting employees to gain access to network credentials or deliver malicious payloads.
* Exploiting vulnerabilities in outdated or unpatched software and systems.
* Supply chain attacks through compromised third-party vendors or healthcare equipment.
* Social engineering tactics to manipulate employees into granting unauthorized access or divulging sensitive information.
* Ransomware attacks using malicious software to encrypt critical systems and demand ransom for decryption keys.

The motivations and methods of attackers may vary, and healthcare organizations must be vigilant in implementing robust security measures to protect patient data and mitigate the risk of cyberattacks.

**Backing up data would be important in this situation. With increased risks to cyber attacks it is crucial to have storage back up and adequate security measures to prevent this from happening in future. This tells us no security is 100%**

**Activity 3)**

**Practical Question 1: File Integrity Check**

a) Visit <http://onlinemd5.com/> and generate an MD5 hash for a text file named "mydocument.txt" that you created on your computer.

b) Now, make a small change to the contents of "mydocument.txt" by adding or deleting a sentence.

c) Generate a new MD5 hash for the modified file using http://onlinemd5.com/.

d) Compare the original MD5 hash with the new MD5 hash.

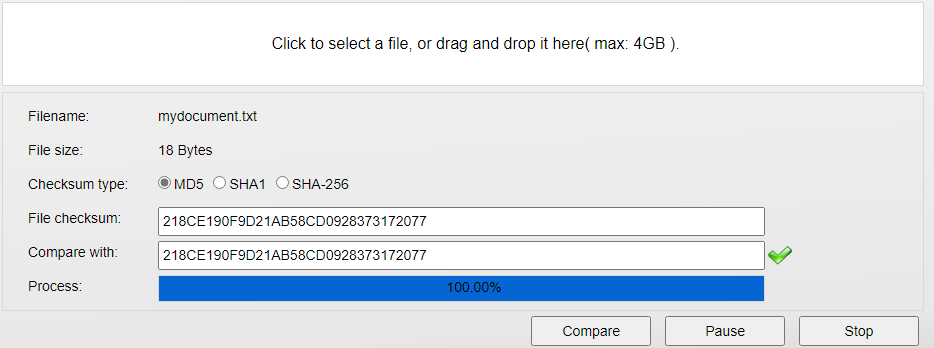
e) What do you observe? Does the MD5 hash change when you modify the file? What does this indicate about the file's integrity?

**Checks to match contents and appears to generate MD5 hash**

**Tick indicates the contents of mydocument.txt and “hello talofa lava” (218CE190F9D21AB58CD0928373172077) contain the same text.**

**A screenshot of a computer

Description automatically generated**



A screenshot of a computer

Description automatically generated

**Practical Question 2: Comparing MD5 Hashes**

1. Generate an MD5 hash for the text "Hello, World!" using <http://onlinemd5.com/>.

A screenshot of a computer

Description automatically generated

b) Ask a friend to generate an MD5 hash for the same text on their computer using the same website.

c) Compare the MD5 hashes you both obtained. Do they match? What does this tell you about the consistency of MD5 hashes for the same input?

**They do match, indicates high consistency of MD5 hashes**

d) Now, change a single character in the text (e.g., "Hello, Worlx!").

A screenshot of a computer

Description automatically generated

e) Generate new MD5 hashes for the modified text on both your and your friend's computers.

**Generates different MD5 string hash**

f) Do the MD5 hashes match this time? What does this indicate about the sensitivity of MD5 hashes to even small changes in input data?

**Shows data consistency.**

These practical questions allow you to experiment with generating MD5 hashes using <http://onlinemd5.com/> and understand the concepts of file integrity checks and comparing MD5 hashes for data consistency.