**SHOUZAB KHAN  
SKHAN6**

**COMPUTER SECURITY**

**1.** How is Computer Security different from other computer science areas? What specific aspect of computer security makes it different from other areas and difficult to solve with technology completely? Write your answer based on the module 1 slides. Justify your answer.

**Answer:** Computer Security is basically all about the security of the computer; it means how a computer can be protected through various unauthorized access, protection of systems, protection of data, and other different types of attacks. It doesn’t mean that computer security is limited to the security of computers but to everything where the computer is used. For example, in cars, phones, and many more gadgets.

If we talk about the differences between Computer Security and other computer science areas, there are many differences. Computer Security mainly depends on the involvement of the human, unlike other computer science areas. Computer Security all depends on the decision of the human. All the attacks like phishing, Social Engineering, password breaches, and human is the reason behind all these attacks. In every other Computer Science technology can be a technical problem, but in computer security, Security is not the technical problem.

**2.** Alice has a document containing confidential information. Alice wants to ensure the confidentiality of the document. Name two techniques to ensure confidentiality of the document and explain how each will do so. Please write your answer based on the module 1 slides.

**Answer:** If Alice has documents that contain confidential information which he has to protect from unauthorized access. He has two methods to ensure confidentiality, which are Encryption and Access Control.

In Encryption, you convert the plain text into cipher text using a specific mathematical process and key. Only an authorized person can reverse the cipher text into plain text through the key. That is called decryption. So, if Alice encrypts the Document, it will become cipher text, and no one will be able to understand it till it is decrypted through the key which only Alice knows.

In Access Control, you have to change the settings and permission for who can view the document and who cannot view the document. And what are the actions that can be performed. These all are done in the Access Control. By Access Control, Alice can restrict the documents only to authorized users who want to read them or do anything.

**3.** Name two authentication factors that you use at UAB for online and in-person authentication. What type of authentication factors are they?

**Answer:** The two authentication factors we use at UAB online are the ‘DUO MOBILE’ and in-person; we use our own ‘ONE CARD.’

The ONE CARD is a biometric type.

The DUO MOBILE is a token type.

**4.** Consider the threat model of a house. What are the potential entry points through which an attacker can physically and/or virtually attack the assets inside the house?

**Answer:** If we consider a threat model of a house, there can be several potential entry points through which the attacker can attack the house.

The attacker can attack both the assets, physical and virtual.

An attacker can have physical entry points like the front door, back door, windows, and roof.

And if we talk about Virtual entry points through which an attacker can attack the house's assets, it can be the Wi-Fi router, the cameras, Emails, and any security system installed in the house.

5. Suppose that Dr. Hasan has sent you a document by email. He wants to make sure that you can verify the integrity of the email. Name two integrity verification techniques that Dr. Hasan can use to ensure you can verify the integrity of the letter.

**Answer:** If Dr. Hasan has sent me the documents by email and he wants me to ensure the integrity of the documents. Dr. Hasan can use two integrity verification techniques to ensure you can verify the integrity of the letter by hashes and Digital Signatures. These two techniques are used to verify the authenticity of the documents so that they are not tempered or changed.

6. **For the threat model, please write a document with the following sections: (a) Assets (sort based on importance, highest to lowest), (b) entry points (c) attacker model. (d) vulnerabilities (sorted from the most severe to the least severe, and then classified using the STRIDE model) and (e) mitigation strategies.**

(CS 636 students) Write a threat model for a smartwatch (e.g., an Apple Watch).

**Answer:**

**ASSETS:**

**User data:** A smart watch's most important asset is the user's personal information.

**Heath Data:** Nowadays, all smartwatch keeps users' health data like heartbeat, blood pressure, and much more.

**Location:** Location can also be an important asset for a user, stored in the smartwatch.

**ENTRY POINT:**

**Bluetooth:** Connecting with any other device uses Bluetooth, which can be an entry point for the attacker.

**Mobile Application:** Mobile applications can also be the entry point for attackers.

**Physical Access to Hardware:** Direct physical access to hardware can also be an entry point for the attacker.

**Attacker Model:**

**Developers:** Developers of other applications can be potential Attackers for getting the user data.

**Physical attacker:** A physical attacker with physical access to the watch can be the attacker.

**Vulnerabilities:**

**S** Spoofing Identity: The Attacker May get the smartwatch access and users' private data.

**T** Tampering with data: The attacker may tamper with the data of the user's health and breach privacy.

**R** Repudiation:

**I** Information Disclosure: The attacker may get unauthorized access to the user's personal data.

**D** Denial of service: The attacker can deny services like location sharing, step counting, or heart rate counting.

**E** Elevation of privilege: The attacker may get the Privilege over the user to use the smartwatch and can handle it.

**Mitigation Strategies:**

**Data Encryption:**

**Privacy Setting:**

**Authorization:**

**Security Updates:**