**SHOUZAB KHAN**

**SKHAN6**

**ASSIGNMENT 3**

**CLOUD SECURITY**

1. Consider the availability of various items related to a smart home (e.g., a home equipped with services like Ring.com or Alexa) (think about the services provided). What would be different ways to attack the availability of the smart home?

**ANSWER:** Smart homes can be attacked in different ways, which can just affect the availability of it:

The attacker just over-floods the network or any specific device in the home with heavy requests from outside to make the server down; this attack is known as Denial of Service (DoS). The Device can also be affected by taking advantage of flaws in different firmware.

The hackers use different malware to seek out smart devices with weak security entry points, this is called botnet. The device that stops the WIFI signals can also interfere with the network of smart devices installed in the home and make them disconnect. Attacks that physically harm equipment or elements of the network infrastructure in an effort to interfere with smart home services.

These threats discussed above can seriously affect the device in any smart home; in order to keep our smart homes safe, we have to take some important security measures.

---------------------------------------------------------------------------------------------------------------------

2. What would be ideal ways to defend against the availability attacks you described in question number 1. (5 points)

**ANSWER:** There can be different ideal ways in which you can defend the attack against availability. You can apply the rate limit technique, in which you can just limit the number of connections coming into your networks to fight against the DoS attack. You should regularly update the software and firmware of the smart devices to be on the safe side and not be affected by botnets. You can also secure your devices somewhere in a safe place to be safe through physical tempering. One should also use wireless intrusion detection systems, which can easily detect the signals that jam the signals, so you can just act accordingly to be safe. The important thing in all these is that you should educate yourself about all of these attacks so you can be safe.

 ---------------------------------------------------------------------------------------------------------------------

3.  Elgoog is a company that takes security seriously. Recently, it updated its password policy. Previously, employees could set an 8-digit password and use it forever. However, to "improve" security, Elgoog introduced a new policy. The new rules are as follows: (i) the password must have 55 digits, (ii) must contain uppercase AND lowercase letters, special characters, and numbers, and (iii) employees must change their passwords every week.

What are the advantages and disadvantages of such a password policy? (5+5=10 points)

**ANSWER:** There are many advantages and disadvantages of every password policy:

**Advantages:**

This password can't be compromised because it contains uppercase AND lowercase letters, special characters, and numbers.

This password can't be guessed because it has 55 digits.

By changing the password so frequently, the users are less likely to reuse the passwords, which reduces the risk of password breaches.

**Disadvantage:**

A password with 55 digits will not be memorable by any user, and the user will forget it more likely.

Users will more likely use the same digit 55 times to remember it, and it will be easily compromised.

By changing the password every week, the users will be finished with a new password by which they will start using easy passwords like name, DOB, etc.

---------------------------------------------------------------------------------------------------------------------

4. One fine morning, AsleT employees come to the office to find that their authentication methods have been updated. Instead of swiping their AsleT card to get into the building, they have to pull a rope. AsleT CEO explained to the employees that he thinks each employee has a different degree of arm muscle strength, and hence, employees can be uniquely authenticated using this approach.  What is the advantage and disadvantage of such an approach toward authentication? (5+5=10 points)

**ANSWER:**

**Advantage:**

If pulling a rope is used for the authentication, it will be unique because the arm muscle strength of every person is different, and that can’t be duplicated very likely. So, it has the property of distinctiveness.

**Disadvantage:**

If pulling a rope is used for the authentication, it won't have permanence; what if the user fell off the stairs and broke his arm, so he will not be able to authenticate the password.

What if one day the user was in high energy and another day he was depressed, and he has no energy for any reason, so he will not be able to authenticate the password.

---------------------------------------------------------------------------------------------------------------------

5. Design a robust authentication system for the following scenario: Dr. Hasan wants to take attendance in his class Cloud Security. However, he also wants to make sure only people actually present in the class can submit the attendance form. He is using a QR code which the students scan to access the attendance form.

What type or types of authentication factor(s) will you choose to make sure that only students present in the class are able to authenticate themselves and submit the attendance form? Explain the reasons behind your design decision. What are the advantages and disadvantages of the mechanism you chose? (5+5+5+5=20 points)

**ANSWER:**

Types of Authentications:

1. Fingerprint

**Reason:**

The reason behind choosing Fingerprint authentication is that every person has a unique fingerprint that can't be repeated or duplicated. Plus, this authentication can’t be compromised just like any other method because any other student can’t put his finger instead of another person.

**Advantage:**

The advantage of the Fingerprint can be that it is unique, permanence, and collectable. The fingerprint can't be compromised or can't be used instead of any other student.

**Disadvantage:**

The disadvantage of the fingerprint can be that if the strength of the class is large, it will take a long time to authenticate each and every one. The deployment of the fingerprint scanner can be expensive for every class. This system is not ideal for online classes. Sometimes, it also accepts false fingerprints, which means that accuracy is not very high. But as compared to other authentication methods, this can be far better.

---------------------------------------------------------------------------------------------------------------------