**Please answer the following questions and upload your answers om a file.**

**1. Consider the availability of various items related to a smart phone (data, voice, apps, and other services). What would be different ways to attack the availability of the phone? (10 points)**

There are many different ways someone could attack the availability of smart phones. They could corrupt data on the device by installing malware. They can send a bunch of traffic to the phone, so it slows down and uses more power. This could be accomplished by a ddos attack.

**2. What would be ideal ways to defend against availability attacks you described in question number 1. (10 points)**

For the data corruption they could have antivirus software installed on their phone. Another solution would be to have a backup of their data somewhere other than the phone. To stop/ prevent a ddos attack they can block numbers or email addresses that are trying to flood them with traffic. If the attack is happening in the moment, they can turn of wifi and data and then block the numbers or addresses they need to.

**3. A company requires employees to set 20-digit passwords, with letters, special characters, numbers, and asks them to change it every 2 weeks. What is the advantage and disadvantage of such a password policy? (5 points)**

The passwords would be very strong because they are long and are not simply designed. You wouldn’t really have to worry about them being brute forced. On the other hand, long passwords are hard to remember, so the employees will probably have to write them down somewhere. Because they need their passwords to log into their computers, the employees will probably store the passwords somewhere physically next to their computers. Now all malicious actor would have to do is read the password.

**4. In the movie "Gattaca", the central character works in a company that authenticates employees into the office by taking a DNA sample from blood every morning. What is the advantage and disadvantage of such an approach towards authentication? (5 points)**

The advantage is that DNA from blood would be a very strong biometric, which for all practical purposes, would be impossible to forge. The disadvantage is that it would take a while to check the DNA from the blood of employees every day. The time it takes to input a user name and password is far smaller than the time it would take to give blood and have it tested to match specific DNA sequences.

**5. Design a strong authentication system for the following scenario:  
You are authenticating users of a library. The users all have smartphones. They are authenticated either in person at the library building, or over the Internet.**

**What type or types of authentication factor(s) will you choose here?  
Explain the reasons behind your design decision. What are the advantages and disadvantages of the mechanism you chose? (20 points)**

**I’d have the following authentication methods available:**

For both physical and virtual authentication into the library system I would require two-factor authentication. Two factor authentication is much more secure than just utilizing one authentication factor for admission into a system. In my system, users would have the option to choose 1 authentication factor from option A and one from option B.

**Option A**

* **Scanned face ID**
* **Scanned fingerprint ID**
* **Username and password**

**Option B**

* **Email message code**
* **Text message code**
* **Phone call (accept and press 1 to authenticate)**
* **Physical library card**

Option A is based on biometrics via fingerprint or face ID. There is also the standard username and password option. Option B is meant to assess some type of physical identification. I specifically differentiated option A and option B because I wanted to provide different mediums to access. In any given scenario a criminal would have to have some type of physical authentication in tandem with biometrics or the traditional username password.