Tutorial 1

1. Imagine the following scenario.
   (a) You live on your own, and one day when you arrive home you find your door open, and there are dirty footprints on the floor.
      - What may have happened?
      - What is an appropriate response in this case?

   (b) The scene is the same as in part (a), but no dirty footprints on the floor.
      - What may have happened?
      - What is an appropriate response in this case?

   (c) The scene is the same as in part (b), but the door is closed, and when you examine the door lock you find it was forced open.
      - What may have happened?
      - What is an appropriate response in this case?

Broader context: stages of "Protection of Assets":

1. Deterrence - "Don't dare to mess with my system"
2. Prevention - "You can't mess with my system"
3. Detection - "I caught you"
4. Reaction - "I get rid of you"

- In these scenarios, we have **detected** something. In cases a & b as the door was not forced open, so there is a possibility that either the door was not closed or the person who entered the house is someone who has a key. But in case c, it looks like the intruder did not have a key.
- An appropriate reaction would be:
  - Assess the situation (avoid further damage, ensure personal safety)
    - Check if the dirty footprints lead to the outside (in case a)
    - Some people may want to make some noise to ensure that their presence is noticed, which may make the intruder flee
  - Try to establish what happened
    - Check if someone they know has entered the apartment (As the lock is not broken) (in case a, b)
    - Check if any valuables are missing (in case a,b)
    - Call the authorities. (in case a, b & c)
    - Might want to leave the scene untouched to preserve the crime scene (especially in case c)
  - Avoid recurrence of events
    - Check who has keys to your home
    - Use better locks (case c)

2. What is security by obscurity and security via legislation in case of your home?

Security by obscurity: Means hiding the system and consequently its vulnerabilities. A system relying on security through obscurity may have theoretical or actual security vulnerabilities, but its owners or designers believe that if the system

details and flaws are not known, attackers are unlikely to find them. This may help in reducing the likelihood of an attack, but definitely cannot prevent it.

Security via legislation: Laws prescribe allowable user activities and penalties for breaching them.

Security by obscurity in your home.

Prevent any insight

- Close all curtains & window blinds, keep the door closed and locked.
- Turn off all lights

Security via legislation:

- Sign stating "Trespassers will be prosecuted" (and see it through)

3. Define a simple security policy for your home.

In business, a security policy is a document that states in writing how a company plans to protect the company's physical and information technology (IT) assets.

- Only authorised people shall be allowed to have a key / enter alone /…
- Keys are not to be passed on to others
- No dangerous activities to be performed in the home
  (This refers to gas to be turned off when not in use, no fire crackers, etc)

4. What would be a scenario similar to question one in case of your desktop computer (instead of your home)? Explain the scenarios in parts a, b and c.

A locked door represents an authentication mechanism, only people with a key matching the lock can enter the house. In case of your desktop computer, your login screen (where you enter your credentials – username + password) is the door.

In case a, you notice that someone else has logged into your computer and you see obvious things indicating that someone other than you has accessed your desktop. This could be anything, such as opened folders or files moved on your desktop.

In cases b & c, you notice that someone else has used your computer, but you don't see any obvious changes. In these cases you might leave the system untouched and involve an expert to check your system to see if any files are missing or have been tampered with. This can include

- checking the last accessed or modified times on any sensitive files stored on your computer to check if they have been accessed or modified.
- checking the "Recent Files" and also browsing history.
- checking system log files to get any additional information. If you are a technical expert, you may take a memory dump of volatile memory (RAM) and even check print queues.

Additionally think of network attacks.

- In case a, PC may not boot up.
- In case b, Files may be missing.
- In case c, RootKits installed.

5. How would you define security by obscurity and security via legislation in case of your desktop computer?

- The desktop computer should be located in a Physically Secure area.
- All users have to be successfully authenticated before being able to use the computer.

6. Read the court case posted on Blackboard, and discuss the following.
    (a) What did the offender do?
    (b) What was his/her goal, and what did he/she achieve?
    (c) What penalty did the offender get?
    (d) With reference to the lecture slides, what type of adversary is this?

Abuse of privileges for personal gain

- Installed code to bypass the regular system process and disperse cash without recording it
- Goal: monetary gain, partially succeeded (not all money was recovered)
- Prison sentence + supervision after release
- Malicious insider