COM-301 Computer Security
Exercise sheet: Basic concepts

September 27, 2023

Note: Some of these exercises could have multiple acceptable answers. The answers we provide are just one example. If you have another answer and would like to check, use the forum or send us an email or ask us during the exercise sessions or ask for student hours.

1. Write a security policy for protecting examination results kept on a computer system considering Confidentiality, Integrity, and Availability. Define the assets and principals.
   Your policy should at least consider the access requirements of students, lecturers, and school administrators.

2. Are these threats, harms or vulnerabilities? Justify.
   Note that some of these could be classified in more than one category. How they are classified would influence the threat model and associated security policy if you were to design a system.

   (a) Thieves can enter into a lab to steal equipment
   (b) Credit card numbers are stolen
   (c) Users choose weak passwords
   (d) The backup system stops working
   (e) A hacker can install malware
   (f) A botnet sends many packets to a server
   (g) The students can see the exam questions before the test
   (h) The cryptographic keys are 56 bits (hint: `https://en.wikipedia.org/wiki/Data_Encryption_Standard#History_of_DES`)

3. Why is testing hopelessly inadequate for showing the absence of bugs?

4. Is this a security problem? (justify)

   (a) I need to send a wireless signal in an environment where there may be obstacles (walls, rain,...)

(b) I need to keep my valuable laptop in my car to go shopping

(c) I need to build a boat that floats under adverse conditions (storm)

(d) I need to store the secret final exam on a server open to the internet

(e) I need to make sure I am talking with my lawyer over the phone

(f) I inadvertently added an infinite loop and took down my server

5. An ad company wants to record how many times its users open the game Sandy Clash. A privacy-conscious user installs an app that opens Sandy Clash a random number of times taken from a uniform distribution between 0 and 2 (i.e., 0 times with probability 1/3, 1 time with probability 1/3, and 2 times with probability 1/3).

   The ad company, which detects the use of the privacy-preserving app receives the following uses ion a week: [3,5,1,2,4,3,4].

   Should the ad company believe that on average the user has opened the app Mean([3,5,1,2,4,3,4])=3.14? If not, what should the ad company do?

6. Are the following compositions of security mechanisms defense in depth or weakest link?

   (a) The PIN/PUK authentication system for SIM cards. If you forget your PIN you can use a PUK to unblock the phone that comes written in a paper when you buy the SIM card.

   (b) A biometric lock that checks whether fingerprint or face recognition are successful.

   (c) Two doors after each other in which the first one opens with a fingerprint and the second one opens with face recognition.

   (d) A biometric lock that requires both fingerprint and face recognition to be successful.

   (e) A door closed with three different types of locks

   (f) Two doors after each other that require two keys. The first can be opened with K1 or K2, and the second door with K2 or K3.

   (g) A password recovery system in which in order to receive your password you need two of your friends to reveal a secret number.