COM-301 Computer Security
Exercise sheet: Basic concepts

September 22, 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.

   Solution:

   This is one of the very open questions. This answer is a possible one. Other answers can be correct. If you want a correction, just send it via email/forum.

   - Principals: students, lecturers, school administrators
   - Assets: examination grades
   - Properties:
     - Students must be able to read their own grades, not others', to keep integrity they cannot write
     - Lecturers must be able to read and write all grades for their own courses (i.e., cannot read/write on other lecturers' courses)
     - Administrators must be able to read all courses to generate final reports. It could be argued that they also need to write (e.g., to fix grades)

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`)

Solution:
In green, the answer we were thinking about when writing the question. In blue, valid alternatives heard in class. (More alternatives may be also correct. If yours is not there and you want to check, use email/forum.) In red, wrong answers.

(a) Threat: This sentence expresses something that can happen to the system: who can attack it and with what goal. It is a feared event.
Harm: This sentence describes the result of the thieves exploiting a vulnerability, entering the lab and stealing material. In other words, it can be seen as the result of an attack.

(b) Harm: This sentence expresses the result of an attack (e.g., exfiltration of data, for instance using malware)
Threat: This sentence describes a feared event, that the credit cards numbers are stolen and the thieves can use them to commit fraud.

(c) Vulnerability: This opens the door for an exploit (guessing the password is easier)
Harm: While this sentence establishes a fact, the fact that users have weak passwords in and by itself, is not a harm yet. It only becomes a fact if an adversary exploits the vulnerability.

(d) Harm: The sentence describes damage that happened on a system as a result of an attack (e.g., denial of service on the backup server).
Vulnerability: The sentence describes a situation, when the backup is down, that can be exploited by an adversary to delete or modify files in the system without the possibility to recover them.

(e) Threat: The sentence describes a feared event – who might attack the system and how would this attack be performed.

(f) Threat: The sentence describes a feared event. Who might attack the system and how would this attack be performed.

(g) Harm: The sentence describes a damage made to the system as a result of an attack (e.g., students steal the professor's office keys)
Threat: The sentence describes a feared event, that the students may have access to the exam questions.

(h) Vulnerability: The sentence describes a weakness of the cryptographic algorithm DES, namely that it uses a small key: 56 bits. Such small space can nowadays be brute forced (i.e., it is possible to find the key by trying all the possibilities via exhaustive search) rendering the encryption useless.

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

   Solution:
   "Showing absence of bugs" implies that one is able to prove that there is NO bug in a program. However, it is hard, and arguably impossible, to test for all possible failure conditions. Also, many problems are caused by combinations of bugs. Thus, even when one finds a problem it may not be possible to identify all the bugs that cause the error.

   As a side note (and as it is dictated by the economy of mechanism principle), the more complex a system is, the more difficult it is to identify 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

   Solution:

   (a) No. The environment is not adversarial, does not act purposefully to break the system.

   (b) Yes. In this scenario there is an adversary that wants to actively and purposely steal my laptop.

   (c) No. The sea and the storm are not adversarial. They do not happen at the worse moment and their goal is not to sink the ship.

   (d) Yes. In this scenario there can be an adversary that purposely will try to use the fact that the server is connected to the internet to try to steal the exam

   (e) Yes. In this scenario there can be an adversary that tries to impersonate my lawyer to, on purpose, try to extract confidential information from the conversation.

(f) No. This is a bug, the attack is not intended, it is not adversarial and not a security problem.
Yes. This is a bug, as such it creates a vulnerability that could be exploited by an adversary to harm my system on purpose.

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?

   Solution:
   If the company knows there is a privacy-preserving mechanism, as an strategic adversary, it should take the use of the mechanism into account. That is, it should compute the average number of fake accesses and subtract it from the observed values.

   More concretely, given the mechanism, the ad company can know that on average each day the privacy-preserving app makes 1 fake access to Sandy Clash (1.0/3*0 + 1.0/3*1 + 1.0/3*2). Thus, it should consider that on average the user has accessed the app 2.14 times.

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.

   Solution:

(a) Weakest link: knowledge of PIN or PUK breaks the system.

(b) Weakest link: knowledge of fingerprint or face breaks the system.

(c) Defense in depth: you need both fingerprint and face to succeed.

(d) Defense in depth: you need both fingerprint and face to succeed.

(e) Defense in depth: as long as one lock holds, the door is closed

(f) Weakest link: if K2 is stolen, the door can be open.

(g) Weakest link: if the password or your two friends fail your account
Defense in depth: as long as one friend stays loyal, the password is safe.