Rayan Hassan 4511021
ECE 1155 - Homework 1

(1) • Vulnerability is weakness in a system (ex: if you don't have a password to your account)

• Threat is any even that can potentially violate security and cause harm (ex: weak password or phishing attacks)

• Control is the processes that you have to protect from any vulnerabilities they prevent attacks or just detect them.

(2) Yes I use ESET NOD32 Antivirus which protects my laptop from all types of malware (viruses, ransomware, worms and spyware).

(3) Attackers might want to take your credit card information, or steal your identity. Attackers can be thieves or a large group of people / hackers specialized in that.

(4) Passive threats are those who don't affect the system resources.
(ex: if you're monitoring internet traffic but just to see how things are, like what websites people visit)

Active ~~attack~~ threats is when you try to change system resources or affect their operation.
(ex: if you steal someone's identity or modify their information)

(5) a) C: Confidentiality = data only for people allowed to see it (legitimate users)

example of control method to achieve it
→ Face ID when opening a phone or authentification.

I: integrity: don't change or destroy documents if you can't / not allowed to

ex. of control to do that: signature agreeing to that term

A: Availability = system should be available when needed

ex of controls: keeping hardware up to date or monitoring bandwidth usage.

b) i) Integrity

ii) Confidentiality

iii) Availability

c) for example if you log in with your teacher's identity to their account (confidentiality) and change the grades of the class (integrity).

(6) Here we use a pin to access our own account which is why it is confidential

When we deposit for example 100 $, and the system says that we only deposited 50 $ (so balance shows 50 $ instead of 100 $) that's an example of integrity breaking

Also we want the ATM to give us the amount of money we want to withdraw ~~some money~~ → availability

(7) Key principles are: Economy of mechanism, open design, fail-safe defaults, complete ~~medi to~~ mediation, seperation of privilege, least privilege and physchological acceptability.

- Least privileges = every process or user should operate with the bare minimum privileges necessary.
  (ex: the mail ~~man~~ man doesn't need to know ~~what the~~ what is in the mail, he just needs the addresses).

- fail safe concept: access decisions should based on permission. Make denying access default until access is explicitly given. (ex: to access your phone, you need a password, if you don't get the password right it doesn't let you in. After a certain time if you still put it wrong, it blocks).

(8) I agree with this, I litterally used this as an example in question (7) before reading this ~~the~~ question! The reason is that a situation

where a hacker tries many combinations to access your account. In this case, if the account is disabled after 3 fails he has no more attempts to try all the other possible combinations. which is good as it prevents attacks. Even if you're the real person trying to login but fail to do so after 3 times, it gets block. So here the default is to deny access until you get it right so it's fail-safe default.

(9) • In summary, the paragraph talk about ethics. First, the difference between laws and ethics is highlighted. A law is undisputable, in the sense that you can't escape it, even if you think that you're being falsly accused. Ethics are subjective; two people might have different opinions as to whether a artain situation or action is right or wrong. Then we proceed to say that ethics ~~have~~ are not the same as religion. Also, ethics are not universal since people have different perceptions of it. In science, ethics is not as supported since scientists want clear, unambiguous answers. which is why it is rejected.

However, ethics are inevitable since in many situations there are no clear answers as they can be perceived differently from different people. Then the author goes on to give examples of ethical principles, like the teleological theory or egoism.

- The issue in software vulnerability reporting is whether you should/can report vulnerabilities that were not there, or report some but not all vulnerabilities to use the additional ones for future leverage against the client. In this case it depends on what your basing your judgement on, potential for good or potential for harm.