Kenny Ta

Assignment 1

1. Computer security is the “measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.”

2. The difference between a passive and active security threat is that any active attack would attempt to alter system resources or affect the operation but the passive one does not affect system resources.

3. Attack surfaces consist of reachable and exploitable vulnerabilities in a system and some examples include open ports on outward facing web, services available on the inside of firewall, employee with access to sensitive information. While an attack tree is a branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities. The goal is represented at the root node of the tree where the attacker can reach that goal are iteratively and incrementally represented as branches or sub-nodes of the tree.

4. Confidentiality: card and pin, these are very important because without these requirements, we cannot access a user’s information via the ATM.

Integrity: The integrity of the card is pretty skeptic, nowadays we have NFC cards and readers and copiers that can copy contents of a debit card that makes their integrity questionable.

Availability: The time and reliable access to the information on the ATM is on point, anyone can come at anytime of the day, 24 hours access to the ATM, granted they have their card and pin.

5. Confidentiality: phone number, the phone number is pretty important in this case cause without it, the system will not be able to switch the call to the appropriate user. This has more of a breach in confidentiality since anyone can request to switch the phone number therefore they don’t know if it’s anyone fishy.

Integrity: There is not much integrity in this system unless someone floods the calling network with robocalls or automated phone calls. In which would render the switching network to it's max and unable to perform it's assigned tasks.

Availability: The availability of this can be either 24 hr/ day or depends on whether the switch network needs an operator, in that case, would be the timeframe of the operator's work hours.

6. List of fundamental security design principles: Economy of mechanism, Fail-safe default, Complete mediation, Open Design, Separation of privilege, Least privilege, Least common mechanism, Psychological acceptability, Isolation, Encapsulation, Modularity, Layering, Least astonishment.

Economy of mechanism just means that the design should be as simple and small as possible.

Fail-Safe defaults indicate that the access should be based on permissions.

Complete mediation shows that every access must be checked against the access mechanisms in place so to ensure that only the admin/ correctly appointed individual has access to certain functions of the system.

Open design indicates that the design for the security mechanism be open instead of in the dark. This allows for the implementation to be checked by hackers to see if it can be breached before being public.

Separation of privilege is a practice that which allows attributes are required to achieve access to restricted resources. This is like user authentication such as the card and pin example of the ATM machine.

Least privilege means every process and every user of the system should operate on the least privilege to perform the task. It means in hindsight that any user that using this system doesn't need to have admin commands access to use it.

Least common mechanism means the design should minimize the functions shared in thus provides mutual security.

Psychological acceptability implies that the security mechanism should not interfere with the works of the users allowing them to perform their assigned tasks without the security of the system saying “no you can’t do that”.

Isolation indicates that the public access systems be isolated from the data storage to prevent disclosure or tampering of information.

Encapsulation is where protection is provided for the user based on object-oriented functionality.

Modularity is the security refers both to the development of the security functions as separate modules not just in the system’s main functioning modules.

Layering indicates the use of multiple, overlapping protection approaches addressing people, technology, and their operational aspects fo information systems.

Least astonishment means a program or user interface should always respond in a way that won’t surprise the user.

7. A) Confidentiality: as in school transcripts are most important requirement because it should only be available to students parents and employees.

B) Integrity such as hospital’s patient allergy information. The data stored on that document must be accurate and correct.

C) We have a public website as most important for system availability. Having a site down and having people try to access your information is rather embarrassing.

8. A) Low, the information is public so it is fine if it gets lost, not much confidentiality, availability will be affected.

B) High impact level. Law enforcement usually has information sensitives to individuals that are confidential such as fingerprints, social security numbers, licenses, and pictures that if leaked can be used against them.

C) Medium, the administrative information is rather important information if it’s for routine purposes since we know they use this information everyday someone can use it against them in a way if leaked.

D) High, anytime there is sensitive information regarding individuals involved, any risk of losing their information is high impact level.

E) High. Power plants with information on whether or not to shut it off will put people at risk for their accessibility, not their confidentiality and integrity.

9. User credential compromise : monitor a human's actions and observe their passcode to safe.

Injection of Commands: Interpreting the passcode to the physical safe allows the user to access it's content.

User Credential guessing: If the user is unable to pinpoint the exact code, they can try to brute force the combination.

Security policy violation: user can check if the physical safe has any holes / abnormalities that will allow blunt instruments or throwing the case to crack open the case.

Use of known authenticated session: if all fails, one can threaten the user to open the safe for them and gain access to the contents.

10. A) I think the flaw here is that it only checks if it is denied then informs the user. Rather it should be the other way around and assume that the user is denied until it is proven otherwise. The fail-safe design indicates that the default should be lack of access.

B) To rewrite the code, it would look similar to this

```
DWORD dwRet = IsAccessAllowed(…);
if(dwRET == ACCESS_GRANTED)
{ //security checks okay
}
Else
{ //security check failed
// inform user that access is denied
}
```