Elijah Andrushenko

CPTS 427

Computer Security

PS1

1.

(1) Settings – Tamper – One could change the settings and change the web host client – This is a serious threat since unwanted users may have a lot of power and can break the entire system.

(2) Settings – Denial of Service – A user can change the deny you of making changes to client. – This threat is important since it would not allow you to make fixes and changes.

(3) Updates – Denial of Service – Not allow updates to be sent back to the file system. – This threat is important since no updates means you are able to respond effectively to what is being sent.

(4) File System – Tamper – Unwanted users accessing the file system – Users can have control of the File System and do something unwanted.

(5) User – Spoofing – Unauthorized access – This is dangerous because unwanted users will have access to information they should not be allowed to see.

(6) Command – Spoofing – Sending incorrect information to the host client – This is dangerous as the command may be malicious in intent and could break the system.

(7) Host Web Client – Denial of Service – Shut down the web client – This is very dangerous as the entire system would not work without the host web client.

(8) Remote Web Server – Denial of Service – Shut down the web server – This is also dangerous due to the fact that the client would not be available without the server.

(9) Host Web Client – Tamper – Make changes to the client – Malicious activity can take place if the Client can be tampered with.

(10) File System – Information Disclosure – Unwanted users viewing the file system - This is a big threat since it removes privacy of the information stored in the web client.

2.

(A) The backdoor would be removed if outside users didn’t have such strong privileges before logging in. Inspection of the source C compiler would identify this.

(B) The backdoor would be removed if untrusted code was no longer used which is almost impossible. Checking the compiler, handler, assembler, loader, and hardware microcode would be a way to identify this but it is difficult.

3.

•Confidentiality – Medium

-Hiding this information is not of utmost importance, but it would be best if an outsider did not know the location of the planes easily.

•Integrity – High

-Any changes or information exchanges made need to be reported by someone very trusted. If anybody can easily access this, sabotage to the flight plans or air traffic could be a catastrophe.

•Availability – High

-Monitoring the location of planes must be known at all times. Not knowing the location of even one plane at any time is dangerous. Even when all planes are not flying, it is important to know if a plane is where it is supposed to be, an example would someone stealing a plane and taking off, knowing if that was happening as soon as possible would be useful.

4.

A) The principle that is violated here would **Least Common Mechanism** since only one person is managing the systems for storing files, while the principle states multiple users should have minimal privileges the problem here is that one user has too much power over the systems.

B) The principle that is violated in this scenario would be **Open Design** because they are trying to hide everything with DRM, which doesn’t allow you to see anything inside while still allowing you to use it.

C) The principle being violated here would be **Least Privilege** due to the fact that the lowest tier user can do things that can be harmful giving them too much power.

D) **Psychological Acceptability** is being violated here since mechanisms are not designed for ease of use making it difficult for trusted users to complete tasks.

E) The principle that is being violated here would be **Separation of privilege** since only one key is being used to unlock all his sites. This principle states that multiple keys or privileges need to be used for authentication.