Alex Hortin
Assignment 7

Chapter 12
25 Pts. List and define the eight design principles covered in Chapter 12.

1) Principle of Least Privilege - This principle restricts how privileges are granted. The main idea is that if someone does not need access to a certain resource that they should not have access.

2) Principle of Fail-Safe Defaults This principle restricts how privileges are initialized when a subject or object is created. Unless a person is given specific access to an item it defaults denial of access.

3)Principle of Economy of Mechanism This principle simplifies the design and implementation of security mechanisms. Fewer possibility for errors will exist if the implementation is minimal we talked about this in class on our Friday lecture.

4)Principle of Complete Mediation This principle restricts the caching of information, which often leads to simpler implementations of mechanisms. This is best exemplified in the permissions feature of unix operating system where the OS intervenes and makes sure a user requesting a file has the proper set of permissions to use that file in the intended way.

5) Principle of Open Design The principle of open design states that the security of a mechanism should not depend on the secrecy of its design or implementation. For example RSA's algorithm is totally available online, and it is still extremely secure.

6) Principle of Separation of Privilege This principle is restrictive because it limits access to system entities. The principle of separation of privilege states that a system should not grant permission based on a single condition. For example just because I know my email address for my email does not mean that I am it's owner, I should know it's password and maybe my date of birth.

7) Principle of Least Common Mechanism The principle of least common mechanism states that mechanisms used to access resources should not be shared.

8) Principle of Psychological Acceptability This principle is that there must be a human element to the implementation and configuration of security to make it more natural and effective to administer. The process should be as easy and direct as possible

15 Pts. Question 12.7.
7:Given that the Internet is a shared network, discuss whether preventing denial of service attacks is inherently possible or not possible. Do systems connected to the Internet violate the principle of least common mechanism?

The Internet does suffer denial of service attacks, but some of these attacks could simply mean a website suffered the "slash dot" or "digg" effect of an unexpected influx of traffic they received not expecting it or being properly prepared for it. There are mechanisms in place to prevent attacks like this (Purdue SYN intermediary**), but I could compare unintentional denial of service to the release of**

a large movie in a theatre. A theatre plans it's size for maximizing yearly profits, and every week there is not a new star wars, harry potter, or some other huge movie. The same might go for a small blog that purchases enough bandwidth and servers to support a medium sized market, but if they suddenly publish a large article they might go down just because of interest. For the most part the Internet is successful because people have found a balance of purchasing the resources they need to use.

Chapter 19
15 Pts. List and define the three major types of malicious logic.

Trojan Horse: . A Trojan horse is a program with an overt (documented or known) effect and a covert (undocumented or unexpected) effect.

Computer Virus: A computer virus is a program that inserts itself into one or more files and then performs some (possibly null) action. This can be a type of trojan horse.

Computer Worm: A computer worm is a program that copies itself from one computer to another.

10 Pts. Present an argument for the statement that Trojan horses are worse than viruses.
A trojan horse can worse than a computer virus because a Trojan horse can reside in commonly used documents like photos or excel spreadsheets and will operate usually as intended while also making the user vulnerable, yet since the file operated as intended they will have no idea.

10 Pts. Present an argument for the statement that viruses are worse than Trojan horses.
A virus is worse than a trojan horse since a virus propagates without help from the user. It will usually infect other files in an attempt to spread from one PC to another.

25 Pts. Compare and contrast Thompson's compiler and the Soviet gas pipeline explosion incident from a malware perspective. (Give at least two similarities and two differences).

The First similarity that I see is that both cases of malware could be used to injure and kill people, though it doesn't seem any were. The pipeline explosion was pure luck that no one was injured, while the C compiler could be used to inject backdoors into all kinds of critical software that may be used in all kinds of life and death situations (ie. login controll for shuttle doors)

The second similarity that I notice between these two pieces of malware is that they could both be considered Trojan horses. They both have an intended purpose, and than another covert action.

That leads to the first difference which is that Thompson's compiler could be considered a virus since it will inject itself into any new copies of that compiler.

Another Difference I noticed is that the C compiler example still remains effective even in most open source environments while the Pipeline explosion would be much easier to detect if the software was open source.