CS 537 Notes, Section #30: Security Abuses

In general, protecting a computer system is extremely difficult. There is no completely secure computer system in existence. Some common problems:

- Abuse of valid privileges.
- Imposter.
- Trojan Horse.
- Listener.
- Spoiler.
- Send weird escape sequences to terminals that cause commands to be echoed back from the terminal.

Once the system has been penetrated, it may be impossible to secure it again: hooks could have been left around for the imposter to regain control.

It is not always possible to tell when the system has been penetrated, since the villain can clean up all traces behind himself.

If we can never be sure that there are no bugs, then we can never be sure that the system is secure, since bugs could provide loopholes in the protection mechanisms.

How are computers different from humans when it comes to security?

- Computer memory is volatile, humans do not forget.
- We are much more trusting of computers than of people: privileges are given away freely in huge doses: any program you run could conceivably modify any of your files.
- Computer programs are very poorly understood.
