ALEX HORTIN
HW1

1:Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.

-John copies Mary's homework.
This is confidentiality and availability. Confidentiality due to her lacking the ability to keep her resources s hidden

-Paul crashes Linda's system.
Availability and integrity. She made it available and he compromised the integrity.

-Carol changes the amount of Angelo's check from $100 to $1,000.
This is integrity since the original amount was changed and availability since Angelo's check is available to change.

-Gina forges Roger's signature on a deed.
Gina changed the integrity of the document, but it was also available for her to do so.

-Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.
Integrity since assuming they once used the domain she compromised the route (legally).

-Jonah obtains Peter's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number.
Availability, Integrity, and Confidentiality. Availability because he could do it, Confidentiality because he had enough data to validate himself as peter, and Integrity because the origin of the requests was not who the bank thought it was.

-Henry spoofs Julie's IP address to gain access to her computer.
I would be interested to know how spoofing an IP address would enable access to her computer...but this would be integrity, and confidentiality. Integrity since her IP was comprimised and confidentiality since she failed to keep her IP a secret from the haxors.

3:The aphorism "security through obscurity" suggests that hiding information provides some level of security. Give an example of a situation in which hiding information does not add appreciably to the security of a system. Then give an example of a situation in which it does.

Linux is a system that is entirely open source so it can be viewed by black and white hat hackers alike with different intentions. It relies on the many eyes idea that many eyes will help identify and fix faults.

A system that might need information hiding would be early cryptography, before algorithms like RSA. Take for example the systems used it WWII. Information needed to be hidden or else the whole cpytography field would be comprimised. You could also say that the User Name/Password model relies on hiding info.

5:Show that the three security services confidentiality, integrity, and availability are sufficient to deal with the threats of disclosure, disruption, deception, and usurpation.

Disclosure should be dealt with by making sure that information is confidential and the integrity of your system to prevent snooping. Also making a system not physically available or virtually available would be a good idea to prevent installation of snooping software

Disruption (modification of data) can be prevented in much the same way, assuring that proper policies are laid out, and the same can be said for deception and usupation. Since there is never a truly secure system (mathematically proven in class) confidentiality, integrity, and availability must all be tied within the policies of that system to minimize risk of exposure.

7:For each of the following statements, give an example of a situation in which the statement is true.

-Prevention is more important than detection and recovery.
Prevention is most important in a case where you have a critical system such as an airplane guidance program. Detection and recovery might not be a viable option as the plane is hurtling toward the ground after a hacker attack on a guidance system and passengers are screaming and crying as they realize that in a few moments they will be consumed by fiery the inferno.
-Detection is more important than prevention and recovery.
Detection would be important in a system like a linux server, where you need to assume for the most part it is secure and cannot prevent every attack, but you need to be able to detect when a user logs in from a non valid IP address for example with a legit user name.
-Recovery is more important than prevention and detection.
Recovery would be after a system attack has occurred and you lose valuble data you will want to recover it.

8:Is it possible to design and implement a system in which no assumptions about trust are made? Why or why not?

It might be possible, but assumptions about trust is one thing that underlines all aspects of security. SO the system would have no real security. It is impossibe to have a secure system without some assumptions about the integrity of the system. Without policies and mechanisms that implement those policies the system would be fairly worthless for anything more than trivial tasks since anyone could destroy it at any time.

9:Policy restricts the use of electronic mail on a particular system to faculty and staff. Students cannot send or receive electronic mail on that host. Classify the following

mechanisms as secure, precise, or broad.

-The electronic mail sending and receiving programs are disabled.
precise

-As each letter is sent or received, the system looks up the sender (or recipient) in a database. If that party is listed as faculty or staff, the mail is processed. Otherwise, it is rejected. (Assume that the database entries are correct.)
secure

-The electronic mail sending programs ask the user if he or she is a student. If so, the mail is refused. The electronic mail receiving programs are disabled.
broad

20:For many years, industries and financial institutions hired people who broke into their systems once those people were released from prison. Now, such a conviction tends to prevent such people from being hired. Why you think attitudes on this issue changed? Do you think they changed for the better or for the worse?

Well back then I feel like that most of people who were doing it were simply hackers that were curious about the layout of the system. It was just to learn more about computer systems, and they rarely had malicious intent. Now it seems like most of the computer crimes are done with the intent not to learn, but to exploit some vulnerable resource for profit. The motivations have changed, and there are also a lot of people that break into systems that have been setup for that very reason. So between hiring a convict or hiring another guy when both have the same skillset, I think I would go with the clean guy. I think this is for the better since you dont want to trust people with a hacking history to help improve your security system.