CSCI/CSIS 631
Fall 2019
Homework 1
Solutions

The answer to Problem No. 1:

a) John copying Mary's homework is a **violation of confidentiality**. John should not see Mary's homework because to copy homework is cheating.

b) Paul crashing Linda's system is a **violation of availability**. Linda's system is no longer available to her, or anyone else.

c) Carol changing the amount of Angelo's check from $100 to $1000 is a **violation of integrity (specifically, data integrity)**. The amount written on the check has been changed.

d) Gina forging Roger's signature on a deed is a **violation of integrity (specifically, the integrity of origin)**. The deed appears to have come from Roger, when in fact it came from Gina.

e) Rhonda registering the domain name "AddisonWesley.com" and refusing to let the publishing house buy or use that domain name is a **violation of availability**. The name "Addison-Wesley" is not available to anyone, including the owner of that name, except Rhonda.

f) Jonah is obtaining Peter's credit card number, and having the credit card company cancel the card and replace it with another bearing a different account, is a **violation of integrity (specifically, the integrity of origin)**. The request appears to come from Peter (else the credit card company would not have honored it), but in reality, came from Jonah.

g) Henry spoofing Julie's IP address to gain access to her computer is a **violation of integrity (specifically, the integrity of origin)**. The messages from Henry appear to come from Julie's IP address, when in fact they do not.

The answer to Problem No. 2:

a) An example of when **prevention is more important** than detection and recovery is the nuclear command and control system. By the time an intrusion is detected and recovered from, an attacker could have launched nuclear weapons.

b) An example of when **detection is more important** than prevention and recovery is in the protection of medical records from unauthorized emergency room personnel. If someone is brought into an emergency room, there may not be time to secure the patient's permission to access his medical records. But if the records are accessed illicitly, the security personnel should detect it.

c) An example of when **recovery is more important** than prevention and detection is on a banking computer that maintains account balances. The bank must be able to recover the balance of all accounts to ensure it provides accurate service to its customers. Prevention and detection, while important, are not so important as keeping the balances accurate.

The answer to Problem No. 3:

a) The mechanism is **secure** because students cannot send or receive electronic mail on the system. It is not precise, as faculty cannot send or receive electronic mail on the system, and the security policy says they are allowed to.

b) This mechanism is **precise** because any mail from or to students is discarded. (You can argue this is broad because students can execute the "send mail" command, but the mail will never leave the machine. The word "send" is somewhat ambiguous.)

c) This mechanism is **broad** because a student can claim to be a faculty member when answering the question.