Paul Baier
HW 1-2
8/31/2019
CSCI 631
Dr. Ghaffari

Problem No. 1: Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.

a) John copies Mary's homework.
Confidentiality - If Mary was unaware that John was copying her homework then her data (homework) was not kept hidden.

Integrity - in the sense that integrity “prevents the improper use of data” (from the Bishop slides). Copying homework could be considered an improper use of Mary’s homework.

b) Paul crashes Linda's system.
Availability - Linda’s system is no longer accessible

c) Carol changes the amount of Angelo's check from $100 to $1000.
Integrity - specifically data integrity because the data (amount) does not represent the truth.

d) Gina forges Roger's signature on a deed.
Integrity - specifically origin integrity because the source of the data (signature) is in question. Did the signature come from Roger?

e) Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.
Availability - Addison Wesley is not able to use a desired resource (although, this sounds more like savvy business sense rather than a C-I-A issue).

f) Jonah obtains Peter's credit card number, and has the credit card company cancel the card and replace it with another bearing a different account.
Confidentiality - Jonah was able to obtain data (the credit card) that should otherwise be hidden or inaccessible to him.

Integrity - in one case the origin integrity of the communication with the credit card company was violated because Jonah was representing himself as Peter. Then the data integrity of the new credit card is also compromised because of the false account.

g) Henry spoofs Julie's IP address to gain access to her computer.
Integrity - Henry is claiming to be someone he is not by spoofing Julie’s IP.

Confidentiality - Julie’s files are no longer hidden once Henry gains access to her computer.

Problem No. 2: For each of the following statements, give an example of a situation in which the statement is true.

a) Prevention is more important than detection and recovery.
In a case where an attacker would want to access a medical device like a heart pump or dialysis machine it would be more important to prevent them from accessing it than detecting or recovering from an attack.

b) Detection is more important than prevention and recovery.
In a case where an attacker is copying someone else's work it is important to know that the violation occurred but is not easily prevented and little needs to be done for recovery.

c) Recovery is more important than prevention and detection.
An example is if a broadcast is being rebroadcast illegally. The most important thing is to take the illegal rebroadcast down once it is detected.

Another arguable example is a case where someone's bank account is cleaned out by an attacker. Of course ideally we would like to prevent this from ever happening and without detecting it we could never recover the stolen money, but ultimately I think the person would be most satisfied by recovering the stolen money.

Problem No. 3: 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.

Possible states:

P: Set of all possible states:
- Only faculty and staff can send/receive emails
- Nobody can send/receive emails
- Everybody can send/receive emails

Q: Set of secure states:
- faculty and staff can send/receive emails
- students cannot send/receive emails

R: Set of states restricted by the security mechanism
a) Nobody can send emails
b) Students cannot send/receive emails
c) Students may lie and send emails and nobody can receive emails

Non-secure: Faculty, staff, and students can send/receive emails
Anyone can send/receive emails

a) The electronic mail sending and receiving programs are disabled.
This would be considered secure because the set of states restricted by the security mechanism, that nobody can send or receive emails, is a subset of the set of secure states that only faculty and staff can send or receive . It is not precise because there are secure states, that faculty and staff can send and receive emails, that are not represented in the set of states restricted by the security mechanism.

b) As each letter is sent or received, the system looks up the sender (or recipient) in a database. If the party is listed as faculty or staff, the mail is processed. Otherwise, it is rejected. (Assume that the database entries are correct.)
This is precise because the security mechanism in this case allows for only faculty and staff to send/receive emails which is the same as the set of secure states.

c) The electronic mail sending program asks the user if he or she is a student. If so, the mail is refused. The electronic mail receiving programs are disabled.
This is broad because there are states within this security mechanism, like if a student lies about their role, that is not in the set of secure states.