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**
     - i. Confidentiality
   - b. **Paul crashes Linda's system.**
     - i. Potentially integrity and availability:
       1. Integrity: It is possible Paul crashed Linda's system by removing/editing/adding files to Linda's system.
       2. Availability: If Linda was hosting some media from her system (such as a website) a crash would result in users not being able to access the media she was hosting from the system.
   - c. **Carol changes the amount of Angelo's check from $100 to $1,000.**
     - i. Integrity
     - ii. Availability: Carol changing the check amount could cause Angelo to overdraw his account, preventing him from accessing his funds, thus lowering the availability to his checking account.
   - d. **Gina forges Roger's signature on a deed.**
     - i. Confidentiality: This is a violation of confidentiality because forging Roger's name restricts access control. Gina now has access to all the housing information which she should not have access to.
     - ii. Integrity: The data (the deed) has encountered an unauthorized change. The deed was not supposed to have Roger's name on it.
   - e. **Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name.**
     - i. Availability: In this scenario, Rhonda has not breached the integrity or confidentiality of any party. Instead, she has breached the availability of this website to a company by refusing to sell or outsource its use.
   - f. **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.**
     - i. Integrity: Peter's credit card now longer contains the original data (CC #, security pin, expiration, etc).
     - ii. Availability: Peter can no longer use his credit card.
     - iii. Confidentiality
   - g. **A program used to submit homework will turn itself off just after the due date**
     - i. Availability: Program might not be available for students to use, even if they are a minute late submitting an assignment.
2. Give an example of a situation in which a compromise of confidentiality leads to a compromise in integrity
   - a. **A file containing nuclear launch codes is encrypted with a key. This key is then stolen by a hacker, thus compromising confidentiality. The hacker then modifies the launch codes to random gibberish, the integrity of the data is now compromised as it is not what it should be.**
3. 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**

        i. Someone steals the login info for an admin of a large. They then delete every table from that server. To recover this lost data from the server it would be time consuming/difficult if even possible. The hacker also has access to sensitive data. It would be far easier to deal with preventing this attack than dealing with the aftermath (Cloning data from backup HDDs, changing permissions etc). Also, by the time the hack has been detected, damage is already done, which is why it is important to prevent the attack before it even happens.

    b. **Detection is more important than prevention and recovery**

        i. Detecting if an email is spam or not. Prevention is not as important as detection because it's almost impossible to prevent spam mail from being sent, trying to prevent spam mail from being sent is nearly impossible. Recovery is not as important as detection because there is almost no recovery necessary after being sent a spam email (maybe just deleting it). Thus detection is the most important to be able to detect which email is spam, and then move it to the spam folder.

    c. **Recovery is more important than prevention and detection.**

        i. In a hard disk crash, recovery of the users files and other information is more important. All Hard disks are probable to crash after some time, so it is hard to prevent such crashes, but a recovery plan should be put in force before hand by using RAID arrays and weekly backups.

4. <u>Explain the difference between a threat and a vulnerability</u>

    a. A threat is something that we want to protect against, e.g someone stealing all the money from your bank account. A vulnerability is a way that a hacker could act upon a threat. As per the previous threat example, the vulnerability could be someone obtaining your bank account password.

5. <u>For two of the following, list some threats:</u>

    a. **Uber eats** (food delivery: customer orders on uber eats web page, the restaurant makes the food, uber eats driver picks up the food and delivers food to the customer, customer gets changed and restaurant gets paid)

    b. **Photo sharing**

        i. Someone steals your photos

        ii. Someone steals your identity

    c. **Home automation system that allows you to control things in your home via your mobile phone**

        i. Someone obtains the ability to control things in your home from their cell phone, not yours.

        ii. Someone could use the automation system to break into your cell phone and obtain sensitive information.

6. <u>What is the difference between a security policy and a security mechanism? Explain the difference between technical and procedural security mechanisms. Give an example</u>.

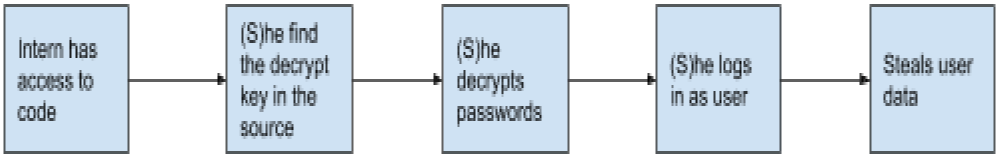
    a. A security policy is a statement of what is, and what is not, allowed. While a security mechanism is the tool, method or procedure used to enforce a policy.

    b. A technical security mechanism uses some piece of technology to enforce the policy within the system, e.g, an access control matrix. A procedural security mechanism enforces a security policy from outside the system. E.g not allowing an untrusted piece of hardware to be used in the system (such as not allowing an untrusted USB drive) .

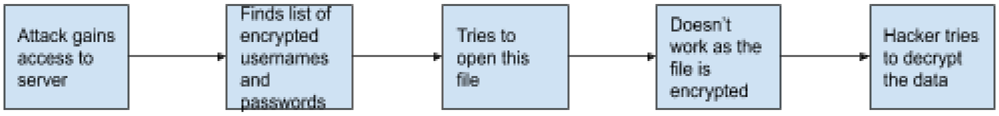
7. Policy: Check the workstation policy (see link on class web page)
    a. **Background: This is for a HIPPA compliant workstation. E.g., a workstation with health records, where we seek a high degree of privacy.**
    b. **How are violations detected**
        i. There are 3 main ways HIPPA violations are detected:
            1. Investigations into a data breach by OCR (or state attorneys general)
            2. Investigations into complaints about covered entities and business associates
            3. HIPAA compliance audits
    c. **Go through each appropriate measures listed in section 3.3 and tag them as**
        i. Enforceable with a security mechanism yes/no
            1. If yes, how?
            2. Who must take the action, the end user, IT personnel, someone else
            3. Useful for cybersecurity yes/no
        ii. Restricting physical access to workstations to only authorized personnel.
            1. Yes, this is enforceable. This can be done by keeping workstations in an area where only authorized personnel have access to. E.g keeping all workstations in a room which can only be unlocked with a keycard which is owned by authorized personnel. The IT personnel must take this action by making sure the workstations are in a secure area. This is useful for cybersecurity but this security measure is not robust. If an unauthorized personnel was to obtain security credentials of an authorized user, they would have access to the workstation. An unauthorized user could also break into the room where the workstations are being stored.
        iii. Securing workstations (screen lock or logout) prior to leaving the area to prevent unauthorized access.
            1. This is most likely NOT enforceable. The only way this could be enforced is if there is a person watching over the workstations to make sure that everyone logs out. This is not likely to happen as a hospital is unlikely to hire someone to stand in the same place all day and just watch people use computers (which is a potential violation in of itself). This would require the end user to logout, as well as another IT personnel to verify that they logged out. If there was a better way to enforce this, it would be useful for cybersecurity, but since there is no easy way to enforce this policy, it is most likely not useful for cybersecurity.
        iv. Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with <Company Name> Password Policy.
            1. This is enforceable by coding a script which will track the time the PC has been idle and then automatically log the user out. An IT personnel would be needed to write the initial code. After the code is written and

implemented, no other personnel action is required. This is useful for cybersecurity.

8. In the SANS examples of policy, the database access policy states
    a. **Database usernames and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writable.**
    b. **A solution that satisfies this requirement is to store the database username and password in a file where the file is encrypted and the password (or key) that to decrypt that file is stored as plain text in the source code. Explain how this approach will or will not protect access to the database in the scenarios below. Make an attack tree for these attacks.**
        i. The attacker is a software developer intern that is adding some functionality to the software
            1. The approach will not protect access to the database. The passwords are stored in the source code. This means that whoever has access to the source code (as is the case with the intern) then has access to the passwords.


Intern has access to code
(S)he find the decrypt key in the source
(S)he decrypts passwords
(S)he logs in as user
Steals user data

        ii. The attacker is an outside hacker that has gained access to the application server
            1. The approach will protect access to the database. Even though the hacker has access to the application server, he doesn't necessarily have access to the source code (which contains the passwords).


Attack gains access to server
Finds list of encrypted usernames and passwords
Tries to open this file
Doesn't work as the file is encrypted
Hacker tries to decrypt the data

9. Suppose that a web server has a link speed of 1Gbps. And suppose that each machine in a botnet has a link speed of 1Mbps
    a. **How many botnet machines are needed to send data to the web server in order to fill the web server's link capacity?**
        i. 1 Gbps = 10^9 bits/sec
        ii. 1Mbps = 10 ^6 bits/sec
        iii. 10^9 / 10^6 = 10^3 machines needed to fill the server's link capacity.
    b. **If DNS amplification is used, then how many botnet machines are needed to fill the web server's link**
        i. If DNS amplification is used, then the required botnet machines needed is 10^3 / Amplification Factor

10. A company has detected several security issues. One issue is that the data archive system has a backdoor that could allow an employee to gain access to the system. Another issue is that the customer portal web server is running an old version of the Apache Web Server software that has

a known vulnerability that, in special situations, allows an attacker to gain access to the server. Use the ideas of risk to discuss how one can make a decision as to which security issue should be addressed first. Note that there is no definitive answer as to which issue gets a higher priority without more information. So your answer should include some discussion of what could make one issue get higher priority than another.

a. This question essentially boils down to if a hacker and an employee gain access to a system, who is the bigger threat? Now both of the end results are the same, someone has access to the system, what differs in each scenario is which specific person has access. In the first scenario, if there are N employees, then it’s possible that N people have access to the system. In the second scenario, it’s possible that any person (with an internet connection) could break into the system. Thus, the amount of people with potential unauthorized access is the deciding factor over which threat should receive the highest priority. Even if the company is large (say 500 employees) that means there are 500 people who could potentially hack into the system. Contrast this with the second threat. There are undoubtedly more than 500 people with an active internet connection who could hack into the system. This means that the probability an attack comes from someone who isn’t an employee is much higher than an attack coming from one of the 500 employees. Thus the company should protect against the threat from an outside hacker, as that is much more likely.