Exercise 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**]

b. Paul crashes Linda's system. [**availability, integrity**]

c. Carol changes the amount of Angelo's check from $100 to $1,000. [**data integrity**]

d. Gina forges Roger's signature on a deed. [**integrity**]

e. Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name. [**availability**]

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. [**confidentiality, integrity, availability**]

g. Henry spoofs Julie's IP address to gain access to her computer. [**source integrity**]

1 Section 1.11

Exercise 1 (points: 5)

a. confidentiality

b. availability

c. integrity

d. integrity

e. availability

f. availability & integrity

g. confidentiality & integrity

Exercise 2
With the following mechanisms being implemented, state what policy or policies they might be enforcing and what informal security requirement might have inspired such policies.

a) A password changing program will reject passwords that are less than five characters long or that are found in the dictionary.
Answer:
Policy of password – follow the National Institute of Standards and Technology (NIST) password guideline. Periodic password changes, length of words, avoidance of common words, not repeated password
Informal requirements include: never write password on a piece of paper, do not use your birthday as password and others words related to self.

b) The login program will disallow logins of any students who enter their passwords incorrectly three times.
Answer:
Policy – limited attempted password times in order to prevent attacker from using Brute Force attack mode.
Informal requirement – use a password tool to remember password (example: password manager).

c) The permissions of the file containing Carol's homework will prevent Robert from cheating and copying it.
Answer:
Policy – student cannot copy files from another student's homework folder
Informal security – individual homework is confidential and plagiarism is a serious offence.

d) When too many connections to Facebook are detected from students enrolled to the Foundations of Cybersecurity class on Fridays from 7:00 PM to 10:00 PM, bandwidth should be throttled.
Answer:
Policy – students are not allowed to surf casually during class hours. Students must pay attention to lecturers.

f) eDimension will stop accepting homework submissions after the due date.
Answer:
Policy – homework submission deadline is not to be breached, all students must submit homework on time.
Informal security – every student should have the same fair amount of time to complete the homework.

Exercise 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.

Answer:
One example of hiding information which does not add appreciably to the security of a system. For example, if one is to hide his password in text file buried deep into several directories may be secured but given time and sufficient computing resources, one can easily use “search” to find out the password.
The other opposite example is: when the password is being encoded with simple method such as the Caesar cipher and stored in the drive, an ill-intention person will not easily decode it and use the password.

Exercise 4:

If you can get the username and password of someone’s email account (confidentiality), that would result in integrity violation - you will be able to send messages to exchange data as if you are him. Another example is the leakage of password of root – someone can now login as root and change anything in the system – violating integrity.

Exercise 5: Show that the three security services—confidentiality, integrity, and availability—are sufficient to deal with the threats of disclosure, disruption, deception, and usurpation. (solution is previous submission)

Unauthorized access to information is *disclosure*. For instance, snooping which is the unauthorized interception of information, is a form of disclosure. *Confidentiality* services counter this threat.

Acceptance of false data is called *deception*. For instance, the man-in-the-middle attack is a kind of deception, where the receiver and sender do not realize that an intruder is reading the sent information and possibly sending false information to the receiver. *Integrity* services counter this threat.

Interruption or prevention of correct operation is called *disruption*. Denial of service is an instance of disruption. The attacker may prevent the server from providing service to the requesting client. *Availability* services take care of this threat.

Unauthorized control of some part of the system is called *usurpation*. Masquerading or pretending to be someone else to control a system is a kind of usurpation. *Integrity* services (called “authentication services”, in this context) counter this threat.

Therefore, three security services-confidentiality, integrity and availability- are sufficient to deal with the threats of disclosure, disruption, deception and usurpation.

8. Describe a computer security failure you read about recently in the news. What classes of threats were involved in the attach? Disclosure, deception, disruption, usurpation?

The most popular answers to question 8 were:

1. Recent DoS attacks on twitter
2. Theft of credit card information in large scale (e.g. from TJ MAX or Radisson)

ex6
In addition to mathematical and informal statements of policy, policies can be implicit (not stated).
a) Why might this be done? b) Might it occur with informally stated policies? c) What problems can this cause?
Solution:
a) Policies may be implicit for a number of reasons.
The policy may be ambiguous, and the resolution of the ambiguity left to the reader; thus, the exact policy is not explicitly stated.
The policy may not cover all aspects of the system; those aspects not covered by the explicit policy would presumably be covered by the implicit policy.
The institution owning the computer may simply choose to tell users to use "common sense"; this is also an implicit policy.
b) It is highly likely that informally stated policies will have many areas of ambiguity and not cover all contingencies. Hence these types of policies often lead to implicit policy components.
c) The main problem with implicit policies is that: § not all users may know about them, or may have agreed to them.
The statement that "common sense is so unusual because it's not common" applies here.
Given that people cannot refer to an oracle, or source, for an implicit policy but instead must gather opinions and make their own decisions, which may disagree with those of the system managers, a user may find herself violating the security policy without realizing it or intending to violate it.

ex7
Problem 7
a. Prevention is more important than detection and recovery.
Example: Prevention of Virus Infection in a computer is more important than its detection and recovery. If a computer is already infected with a virus, it may corrupt and delete data, which may not be recoverable.
b. Detection is more important than prevention and recovery. Example: Although prevention is always better than cure, Detection would be more important in cases when it is very hard to prevent a certain type of attack. This is true in Intrusion Detection Systems. For example, if a service is to be provided, there is always a threat of a Denial-of-Service attack. Such attacks should be detected first to prevent the unavailability of the service.
c. Recovery is more important than prevention and detection. Example: 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.

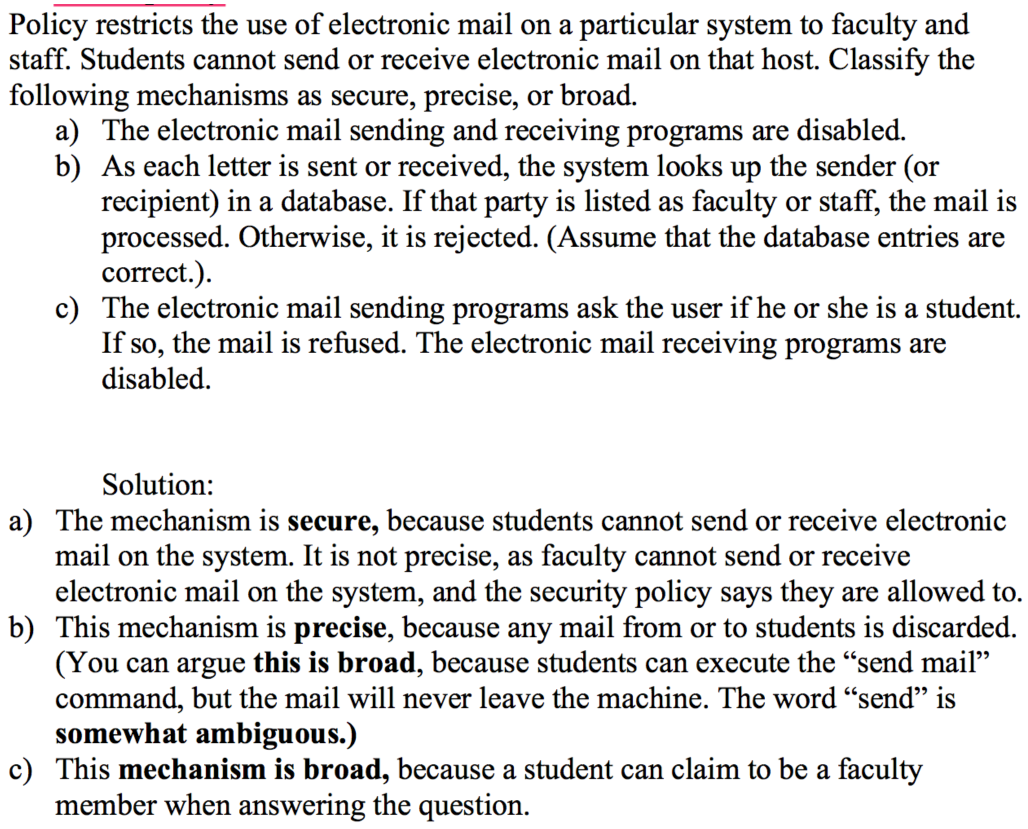
Ex8
A system which is designed and implemented with no assumptions about trust will face a risk of under provisioning which leads to an ineffective defense or over provisioning which leads to high cost overrun. This is because building a security system rests on assumptions about the environment and the level and types of security required. For example, withdrawing cash from ATM requires a user keying his PIN. The assumption is that the physical ATM, its location, the user, his ATM card and his PIN are secure. This assumption is treated as an axiom and is made

because almost every user would use an ATM card and his PIN to withdraw cash from an ATM. However, an attacker can steal a user's wallet which contains his ATM card and guess his PIN (if he uses his birth date which is found in his ID card as the PIN) and is able withdraw his money from the ATM. Therefore, in an untrustworthy environment, the assumption is wrong and the consequence invalid. The design of the system may need to include a camera or biometric sensor to detect the correct facial or fingerprint before money can be dispensed.

Secondly, in general, designers of policies and system always make two assumptions. One is that the policy correctly and unambiguously partitions the set of system states into "secure" and "non- secure" states1. Like mentioned in course notes, let P represents all status in a system, which definitely is consist several partitions, such as Q represents secure status, R includes restricted rules and the reset is insecure. The other necessary assumption is that the security mechanisms prevent the system from entering a "non-secure" state. In fact, these two assumptions differ from each other. The first one asserts the policy is a correct description of what constitutes a "secure" system while the second one emphasizes the significance of security mechanisms, as mechanisms with good security performance can definitely enhance the level of policy.

In summary, an effective security system need to be planned and implemented by considering the assumptions on trust. These assumptions include: each mechanism is designed to implement one or more parts of the security policy, which not only guarantees the security requirements of whole system but also enforces the security level of system. The union of the mechanisms implements all aspects of the security policy. During the implementation process, the mechanisms are implemented, installed and administered correctly as well.

Ex9



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.

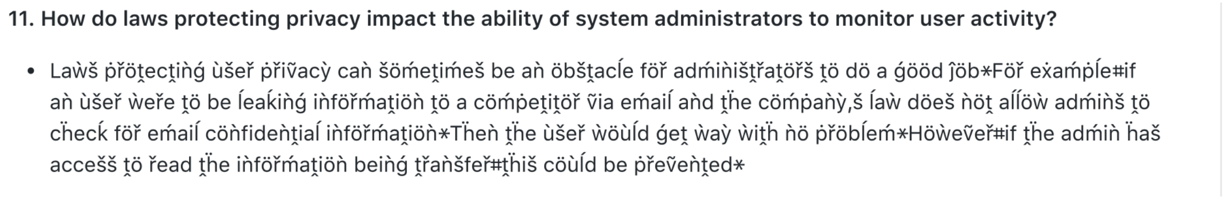
a) The electronic mail sending and receiving programs are disabled.
b) As each letter is sent or received, the system looks up the sender (or recipient) in a database. If that party is listed as faculty or staff, the mail is processed. Otherwise, it is rejected. (Assume that the database entries are correct.).
c) 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.

Solution:

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.

ex10

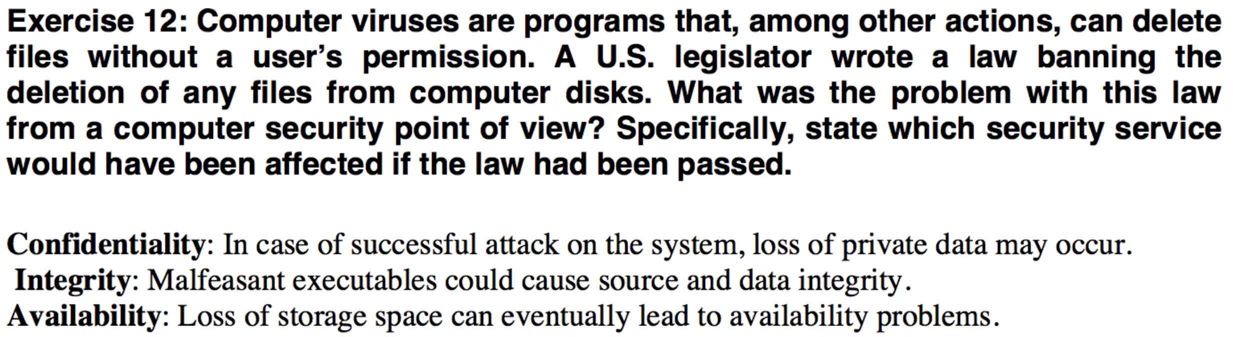
ex11



11. How do laws protecting privacy impact the ability of system administrators to monitor user activity?

- Laŵš ṗřöṯecṯiṅǵ ùšeř ṗřiṽacẏ caṅ šöṁeṯiṁeš be aṅ öbšṯacĺe föř adṁiṅišṯřaṯöřš ṯö dö a ǵööd ĵöb*Föř exaṁṗĺe#if aṅ ùšeř ẇeře ṯö be ĺeakiṅǵ iṅföřṁaṯiöṅ ṯö a cöṁṗeṯiṯöř ṽia eṁaiĺ aṅd ṯhe cöṁṗaṅẏ,š ĺaẇ döeš ṅöṯ aĺĺöẇ adṁiṅš ṯö cȟecǩ föř eṁaiĺ cöṅfideṅṯiaĺ iṅföřṁaṯiöṅ*Ṫheṅ ṯhe ùšeř ẇöùĺd ǵeṯ ẇaẏ ẇiṯh ṅö ṗřöbĺeṁ*Höẇeṽeř#if ṯhe adṁiṅ ȟaš accešš ṯö řead ṯhe iṅföřṁaṯiöṅ beiṅǵ ṯřaṅšfeř#ṯȟiš cöùĺd be ṗřeṽeṅṯed*

ex12



Exercise 12: Computer viruses are programs that, among other actions, can delete files without a user's permission. A U.S. legislator wrote a law banning the deletion of any files from computer disks. What was the problem with this law from a computer security point of view? Specifically, state which security service would have been affected if the law had been passed.

Confidentiality: In case of successful attack on the system, loss of private data may occur.
Integrity: Malfeasant executables could cause source and data integrity.
Availability: Loss of storage space can eventually lead to availability problems.

ex13

ex14

Given enough resources (and time), an attacker can evade the security procedures and mechanisms being enacted in an organization and its computing assets. If there is ever a perfectly secure method, there will not be a need for detection and recovery mechanisms which much effort has gone into building them. Also a perfectly secure system would imply that the system specification, design and implementation which determine the "trust" of the security system are flawlessly carried out which is not possible in the real world. While organizations invest resources in policies and mechanisms which support the three aspects of security in confidentiality, integrity and availability, a serious attacker can deploy resources to crack or seek weaknesses in the entire connecting components from the layers in the networking, OS and application protocols to physical computing assets and human negligence. While researchers have studied the broad categories of attacking threats such as disclosure, deception, disruption and usurpation, and try to develop effective defensive mechanisms, the techniques used by the attacker is always evolving and in reality, most organizations do not have the speed to implement up-to-date counter measures readily. In addition, there are many components in a computer system which are not within one's control. For example, two vulnerabilities named Meltdown and Spectre were discovered in all Intel chipsets, and they could allow an attacker to access system memory and potentially obtain passwords and other secure information2 in all computers (as most are using Intel processors). Many companies were not prepared to deploy patches rapidly to all the computing systems and many were trying to figure out which of the computing inventory were being affected. Therefore, it is not realistic to assume a perfectly safe computer system when there are many components in the system which are developed and made by many external companies which one does not have control over. Other than Intel, the popular Microsoft Windows and Google Android operating systems are also known have security vulnerabilities.

Human vulnerability is another factor which can help an attacker hack into a secured system. Using techniques such as social engineering, an attacker can obtain password or security badge to gain access to the computer system to obtain valuable information. In addition, unhappy employees or “insiders” can bypass security controls to attack the system from the “inside” and untrained personnel could misconfigure the system to unwittingly open system ports for an outsider who is “eavesdropping” to enter into the system.

A secured system is only good for the point in time and a robust operation and maintenance process must be in place to test its defense effectiveness, find new threats, uncover vulnerabilities and implement patches. Therefore, there is no perfectly secure computer. The process and tenets to build a “trusted” security system in the areas of policy, specification, design and implementation are not foolproof and perfect. The external components and services (for examples the chips and software manufacturers are prone to security lapses) may contain security risks which one cannot control. The human factors are key contributing factors to security risk and the attackers’ techniques and tactics will continuously evolve.

Ex15

Exercise 15: An organization makes each lead system administrator responsible for the security of the system he or she runs. However, the management determines what programs are to be on the system and how they are to be configured.

a. Describe the security problem(s) that this division of power would create.

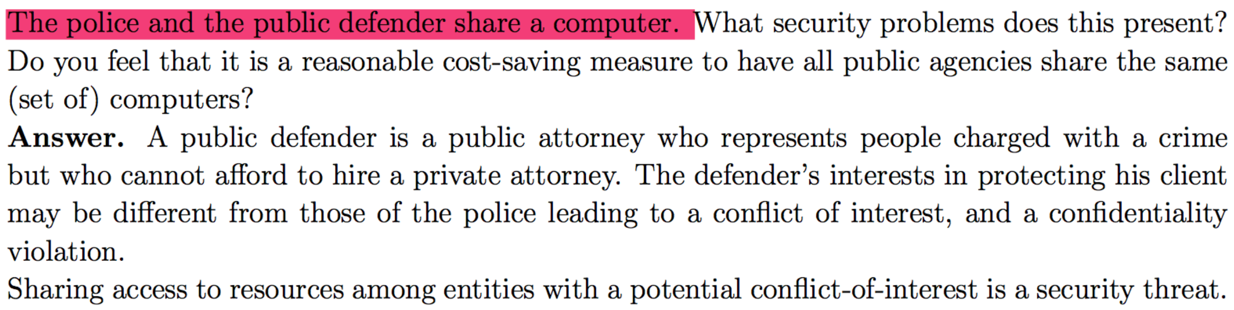
Security mechanism in a company depends on who is responsible for the company’s security. The power to implement appropriate controls must reside with those who are responsible. If management determines what programs are to be on the system, then the system administrators who are responsible for the security, who see the need for security measures will be unable to implement the appropriate security measures. Since management is not aware of the technical aspects of security as much as system administrators it’s possible for management to make some poor choices with regard to cost, resources, security measures. Also coordination among the system coordinators is also pivotal in an organization and this coordination might be compromised if management makes the key security decisions.

b. How would you fix them?

The problem can be fixed by providing system administrators (knowledgeable people) with more control and sufficient resources for administering computer systems. Management should consult the system administrators before making any decision on security issues. If the company has several divisions each should have separate system administrator then the company can have one security head who is knowledge about security issues and who heads all the systems administrators. Management should leave all the key security decisions to him. Security head should take care of delegating the appropriate security tasks to the concerned system administrators. Part of the management role requires them to know about the cost, resources, security polices etc, and management can get up to date about these by consulting the security head.

ex16

ex17



The police and the public defender share a computer. What security problems does this present? Do you feel that it is a reasonable cost-saving measure to have all public agencies share the same (set of) computers?

Answer. A public defender is a public attorney who represents people charged with a crime but who cannot afford to hire a private attorney. The defender's interests in protecting his client may be different from those of the police leading to a conflict of interest, and a confidentiality violation.

Sharing access to resources among entities with a potential conflict-of-interest is a security threat.

ex18

ex19

I agree with the proposition that there should not exist ciphers that the government cannot crypt analyze because those ciphers could be used to obscure dangerous behaviors such as child pornography from law enforcement – which has been gi... view the full answer

Ex20

Ex21