1. Define the term *computer security.*

* The protection of computer system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resource (that includes hardware, software, firmware, information/data, and telecommunications) from theft or from being information corrupted.

1. What is the difference between passive and active security threats?

* An active security threat attempts to modify the data stream from the system resources or affect their operation, but the passive security threat attempts to eavesdrop data being transmitted, to learn or make use of information from the system but with no harm to the system sources. Basically, passive does not involve breaking security, only observation of the resource information, but active employs some sort of methods to break into the system and manipulate or harm the resources.

1. Explain the difference between an attack surface and an attack tree.

* An attack surface consists of the reachable and exploitable vulnerabilities in a system, and an attack tree is a branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities. Basically, an attack surface is a form of methods that the attacker potentially can use to try to circumvent some sort of security, and an attack tree provides all the potential security breach scenarios that can be attacked by the adversaries from the system perspective.

1. Consider automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement.

* Confidentiality would include actual debit card with associated pin number to identify that the person accessing the account service is not a threat to harm the resources. Confidentiality will be placed as low priority, because the main point of the ATM is to access with convenience, without having to wait in lines; which only requires physical card and pin to access the account services on ATM. Much of confidential security will fail to meet the convenience of use by the customers.
* Integrity would come in important role during transactions, accurate amount of money is being deposited or withdrawn from the ones’ account. Integrity will be placed as moderate priority, because bookkeeping correct transaction is essential to both the customers and the bank. If ATM gives the customer one million that he/she did not have in first place, it could end up with major law suits back and forth.
* Availability would include ATM being accessible by the customers without much of hassles, being available in many places and accessible by all people regardless of which bank they’re from. Availability will be placed as high priority, because the more people access the ATM the more beneficial for the bank, since they get to have save money by replacing actual teller.

1. Repeat question #4 for a telephone switching system that routes calls through a switching network based on the telephone number requested by the caller.

* Confidentiality would include massages being only exchanged between the two originally requested person and the caller. Confidentiality will be placed as low priority, because unlike written letters, the main purpose of the telephone is to communicate quickly without having to wait for days to get reply; there are other mediums to have secure conversations.
* Integrity would include communication being successfully held without any interruptions or call disconnected. Integrity will be placed as high priority, because with the original purpose in mind and message being disconnected at the middle of conversation will potentially bring negative effects towards the providers.
* Availability would include telephone being located at understandable distance for each people to communicate when needed; each office desk if the person requires to use most of the time, but otherwise, every other household having one would be appropriate. Availability will be placed as moderate priority, because everyone has cellphone now a day as their major medium for communication, and usage of telephones are more practiced in offices and homes, which in number it is lot less than individual people carrying cellphones.

1. List and briefly define the fundamental security design principles.
   * Economy of mechanism – the design of security measures embodied in both hardware and software should be as simple and small as possible.
   * File-safe default – the access decisions should be based on permission rather than exclusion.
   * Complete mediation – every access must be checked against the access control mechanism.
   * Open design – the design of a security mechanism should be open rather than secret.
   * Separation of privilege – a practice in which multiple privilege attributes are required to achieve access to a restricted resource.
   * Least privilege – every process and every user of the system should operate using the least set of privileges necessary to perform the task.
   * Least common mechanism – the design should minimize the functions shared by different users, providing mutual security.
   * Psychological acceptability – the security mechanisms should not interfere unduly with the work of users, while at the same time meeting the needs of those who authorize access.
   * Isolation – a principle that applies in three contexts; public access system being isolate logically and physically, processes and files of individual users being isolated, and security mechanisms being isolated.
   * Encapsulation – a specific form of isolation based on object-oriented functionality.
   * Modularity – in the context of security refers both to the development of security functions as separate, protected modules and to the use of a modular architecture for mechanism design and implementation.
   * Layering – use of multiple overlapping protection approaches addressing the people, technology, and operational aspects of information systems.
   * Least astonishment – a program or user interface should always respond in the way that is least likely to astonish the user.
2. Consider a desktop publishing system used to produce documents for various organizations.
3. Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.

* When a pharmaceutical company publish report related to their discovery to cure to any cancer cells, the desktop publishing system should prioritize the confidentiality of the data.

1. Give an example of a type of publication in which data integrity is the most important requirement.

* When a financing company publishes annual customer’s investment earnings reports for their investors, the system should prioritize the integrity to ensure that the saved documents are preserved accurately throughout the document’s lifecycle.

1. Give an example in which system availability is the most important requirement.

* When a newspaper company or magazine company publishes their papers, then the system should prioritize the availability to allow as many editors to use the system.

1. For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, integrity, and availability, respectively. Justify your answers.
2. An organization managing public information on its Web server.

* When an organization manages public information on their Web server, then the loss of confidentiality would be low, because it is on their own server and the server will have well enough security within their own boundary that can protect from minor breach.
* There are potential threats that can possibly manipulate the public information on their web server, so loss of integrity would be high, since web server is open to all.
* When many number of employees from organization requires the public information, and pulls up the data all at the same time, the loss of availability would be moderate; there only exists bit of bottleneck.

1. A law enforcement organization managing extremely sensitive investigative information.

* When law enforcement organization manages extremely sensitive investigation information, the loss of confidentiality would be high because when the information has leaked, then there will be quite of damage to everyone who is involved in that case.
* I believe that the loss of integrity is high, because when these information gets modified, it will bring unjust result of the investigation, which will also result an innocent victim.
* Loss of availability is low because extremely sensitive investigation information will probably have made in hard copies, and only associated investigators or lawyers will be handling these documents.

1. A financial organization managing routine administrative information (not privacy-related information).

* Since the financial organization manages routine administrative information that is not privacy related information, then the loss of confidentiality would be low.
* Since the information does not involve any privacy related information, impact of loss of integrity would be low.
* The impact on loss of availability would be low when a financial organization manages routine administrative information that is not privacy involved, because I’m sure only few people will maintain these documents.

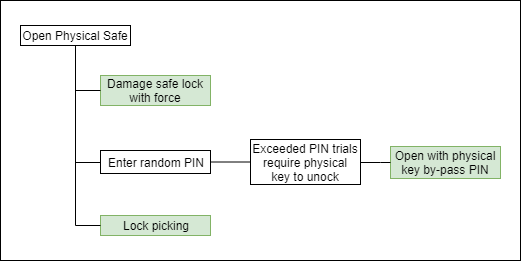
1. An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information, and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

* In case of information system that involves sensitive data, the loss of confidentiality would be high, because if they are not highly value of their private data, then no other contracts will be given in the future that no other company would like to have business with them.
* In case of information system that deals with sensitive data, the loss of integrity would be moderate, because if information of a contract was manipulated by unauthorized person, then they won’t be able to avoid the damages that will be taken by the company, but they can have quick fixes regards.
* In case of information system that involves with sensitive data, the loss of availability would be low, because for example of contract files, it would have already been in a safe place with duplicates have made in advance; no other copies are not needed.
* For routine administrative information that does not involve sensitive information, the loss of confidentiality would be low, because it won’t have much of effect to the company since it’s not confidential data that are being handled.
* The loss of integrity would be low, because they are not dealing with sensitive privacy related information, so manipulated data or incorrect information won’t hurt them as such.
* The loss of availability would be low, because limited amount of people will have access to this routine administrative information.

1. A power plant contains a SCADA (Supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

* For a power plant using the SCADA system that contains real-time sensor data, the loss of confidentiality would be very low or it may not even affect them since the data doesn’t have significant privacy values to them.
* For a power plant using the SCADA system that contains real-time sensor data, the loss of integrity would be high, because if these real-time data do not produce correct values when power plant is in critical situation where there is potential damage within the power plant, then the people who are overseeing the data monitor won’t be able to react to the current situation, and end up in bad situation.
* For a power plant using the SCADA system that contains real-time sensor data, the loss of availability would be high, because these data would be critical to have constant flow in data inputs to the monitor to observe the current operations, and these data will also be distributed to other departments where they would use it to calculate other experiments or future analysis reports.
* For routine administrative information, the loss of confidentiality would be low, because these are just non-privacy related information.
* For routine administrative information, the loss of integrity would be low, because these are non-privacy related information.
* For routine administrative information, the loss of availability would be low, because limited amount of people will use them to follow procedures.

1. Develop an attack tree for gaining access to the contents of a physical safe.



1. Consider the following general code for allowing access to a resource:

DWORD dwRet = IsAccessAllowed(…);  
if (dwRet == ERROR\_ACCESS\_DENIED) {  
*// Security check failed.  
// Inform user that access is denied.*} else {  
*// Security check OK.*}

1. Explain the security flaw in this program.

- The security flaw in this program is that it does not follow the design principle of fail-safe default. According to Stallings and Brown, fail-safe default means that the access decision should be based on permission rather than exclusion. That is, the default situation is lack of access, and the protection scheme identifies conditions under which access is permitted. In this program, default statement allows the access, then it does not provide condition to protect an uncertain error possibly can occur.

1. Rewrite the code to avoid the flaw (Hint: Consider the design principle of fail-safe defaults).

DWORD dwRet = IsAccessAllowed(…);  
if (dwRet == NO\_ERROR\_OCCURED) {  
*// Security check success.  
// Some task.*} else {  
*// Security check failed.  
// Inform user that access denied.*}