Brett Tomita

016336357

CECS 378 Assignment 1

1. Computer Security are measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.
2. Passive attacks are in the nature of eavesdropping on, or monitoring transmissions. Active attacks involve some modification of the data stream or the creation of a false stream.
3. An attack surface consists of the reachable and exploitable vulnerabilities in a system. An attack tree is a branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities.
4. An example of availability is the number of ATMs, or how easy it is to get to one. This is a high priority because it saves the bank money by reducing labor costs, as well as making it more convenient for customers. An example of integrity is having frequent validations to make sure transactions are legitimate. This would be medium priority. An example of confidentiality is bank account/ATM security. This would be low priority, since mistakes can be fixed.
5. An example of availability is number of open connections. This would be high priority. Confidentiality would be user privacy. This would be medium priority. An example of integrity would be making sure callers get connected to the right people. This would be low priority.
6. **Economy of mechanism** means the design of security measures embodied in both hardware and software should be as simple and small as possible. **Fail-safe default** means access decisions should be based on permission rather than exclusion. **Complete mediation** means every access must be checked against the access. **Open design** means 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** means every process and every user of the system should operate using the least set of privileges necessary to perform the task. **Least common mechanism** means the design should minimize the functions shared by different users, providing mutual security. **Psychological acceptability** implies the security mechanisms should not interfere unduly with the work of users, and at the same time meet the needs of those who authorize access. **Isolation** is a principle that says components should be isolated from other critical components that it doesn’t depend on. **Encapsulation** is when data objects are stored in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the protected subsystem and the procedures may be called only at designated domain entry points. **Modularity** 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** refers to the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems. **Least astonishment** means a program or user interface should always respond in the way that is least likely to astonish the user.
7. a. A publishing system being used by a government organization like the FBI, CIA, NSA, etc. would require the confidentiality of stored data to be the most important requirement.

b. A publishing system being used by an organization that requires information to be accurate, such as a hospital or law enforcement organization, would require data integrity to be the most important requirement.

c. A publishing system being used by an organization that heavily relies on publishing, such as a news organization, would require availability to be the most important requirement.

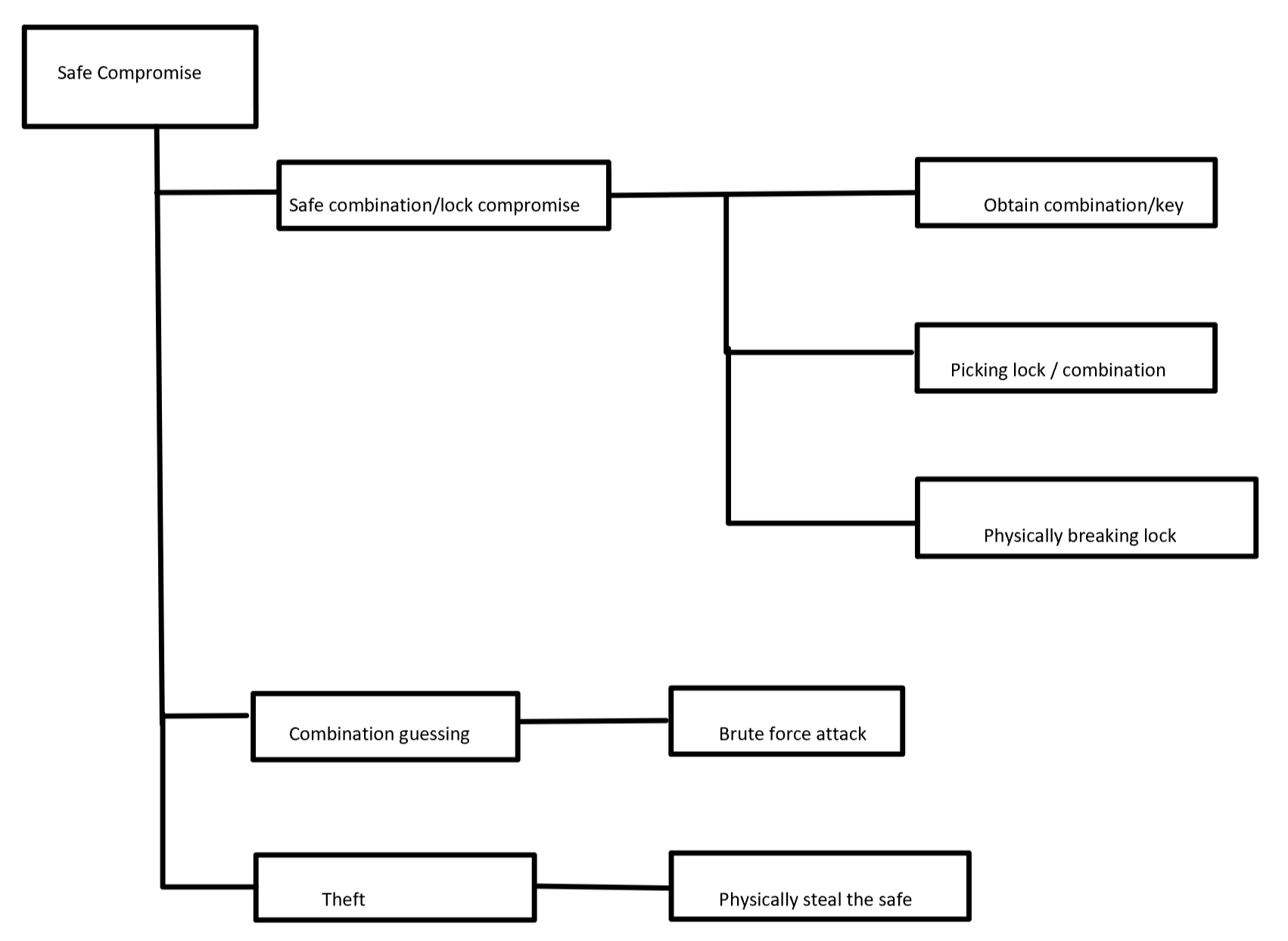
1. a. High = Availability; their purpose is to provide public information, so it is very important that the public can easily access it. Medium = Integrity; They should want the information they provide to be accurate since it will be used by the public. Low = Confidentiality; since it is intended for anyone to use, confidentiality should not be a major concern.

b. High = Confidentiality; keeping their information secret it vital for an investigation. Medium = integrity; They need to have accurate information in order to bring the right people to justice. Low = availability; not too many people should have access to the information.

c. High = Integrity; in order for the organization to work effectively, administrative information must be managed accurately. Medium = Availability; A routine system should be available and dependable. Low = Confidentiality; if private and sensitive information is not being handled, confidentiality is not a main concern.

d. The sensitive information would require confidentiality to be the highest priority due to the organization depending on it to function. Integrity would be medium priority since the information must be accurate, and availability would be least priority since not too many people should have access to it. For the routine administrative information system: High = Integrity; in order for the organization to work effectively, administrative information must be managed accurately. Medium = Availability; A routine system should be available and dependable. Low = Confidentiality; if private and sensitive information is not being handled, confidentiality is not a main concern. As a whole, Integrity would be the most important, since the accuracy of all information considered is very important for the organization to succeed. Confidentiality would be medium priority because making sure people outside the organization’s business don’t have their information. Availability would be lowest priority since only certain people within the organization would need access to the system.

e. Real time sensor data would require integrity to be the highest priority since the purpose of real time sensors are to accurately report current information. Availability should be medium priority since the data is useless if it can’t be used immediately. Confidentiality should be lowest priority for just information sent by the real time sensors. For the routine administrative information system: High = Integrity; in order for the organization to work effectively, administrative information must be managed accurately. Medium = Availability; A routine system should be available and dependable. Low = Confidentiality; if private and sensitive information is not being handled, confidentiality is not a main concern. As a whole, the system should have availability to be the highest priority, since having access to all of the system’s information is crucial for overall operations. Integrity should have medium priority since it is also important for the information being processed by the system to be accurate. Confidentiality should be the lowest priority since it is not as important for overall operations.

1. 
2. a. if dwRet is assigned some other value besides ERROR\_ACCESS\_DENIED that indicates an error or no permission, the security check will still pass.

b. DWORD dwRet = IsAccessAllowed(…);

if(dwRet == ACCESS\_GRANTED){

// Security check OK

}

else{

// Security check fail

}