Cybersecurity Study Guide

***List of topics***

* Concepts of C.I.A, Threats, and Attacks (Slide set 1)
  + Security Goals = C.I.A or **Confidentiality, Integrity, Availability**
    - **C** = Avoidance of the unauthorized disclosure of information
    - **I**  = the property that information has not been altered in an unauthorized way
    - **A** = the property that information is accessible and modifiable in a timely fashion by those authorized to do so.
  + Tool for **Confidentiality**
    - ***Encryption*** the transformation of information using a secret, called an encryption key.
    - ***Access Control*.** Rules and policies that limit access to confidential information to those people and/or system with a **“need to know.”**
    - ***Authorization:*** the determination if a person or system is allowed access to resources, based on an access control policy.
    - ***Authentication***: determination of the identity or role that someone has. This determination can be done in several different ways, but it is usually based on a combination of
      * + – something the person has (like a smart card or a radio key fob storing secret keys),
        + – something the person knows (like a password),
        + – something the person is (like a human with a fingerprint).
  + Tools for **Integrity**
    - ***Backups:*** the periodic archiving of data.

* + - ***Checksums:*** the computation of a function that maps the contents of a file to a numerical value. A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value.
    - ***Data correcting codes:*** methods for storing data in such a way that small changes can be easily detected and automatically corrected.
  + Tool for integrity
    - ***Physical protections:*** infrastructure meant to keep information available even in the event of physical challenges.
    - ***Computational redundancies:*** computers and storage devices that serve as fallbacks in the case of failures.
* ***Threats and Attacks***
  + **Eavesdropping:** the interception of information intended for someone else during its transmission over a communication channel.
  + **Alteration:** unauthorized modification of information.
    - Example: the man-in-the-middle attack, where a network stream is intercepted, modified, and retransmitted
  + **Denial-of-service:** the interruption or degradation of a data service or information access.
    - – Example: email spam, to the degree that it is meant to simply fill up a mail queue and slow down an email server.
  + ***Masquerading:*** the fabrication of information that is purported to be from someone who is not actually the author.
  + ***Repudiation:*** the denial of a commitment or data receipt.
    - This involves an attempt to back out of a contract or a protocol that requires the different parties to provide receipts acknowledging that data has been received.
  + ***Correlation and traceback:*** the integration of multiple data sources and information flows to determine the source of a particular data stream or piece of information.
* ***Authorization*** 
  + ***Access Control*** 
    - ***Access Control Matrices*** 
      * **A table that defines permissions**.
        + Each row of this table is associated with a subject, which is a user, group, or system that can perform actions.
        + Each column of the table is associated with an object, which is a file, directory, document, device, resource, or any other entity for which we want to define access rights.
        + Each cell of the table is then filled with the access rights for the associated combination of subject and object.
        + Access rights can include actions such as reading, writing, copying, executing, deleting, and annotating.
        + An empty cell means that no access rights are granted.

***Access Control List***

* + It defines, for each object, o, a list, L, called o’s access control list, which enumerates all the subjects that have access rights for o and, for each such subject, s, gives the access rights that s has for object o
    - ***Capabilities***
      * Takes a subject centered approach to access control. It defines, for each subject s, the list of the objects for which s has nonempty access control rights, together with the specific rights for each such object.
* ***Malware***
  + ***Insider Attacks*** 
    - An insider attack is a security breach that is caused or facilitated by someone who is a part of the very organization that controls or builds the asset that should be protected.
    - In the case of malware, an insider attack refers to a security hole that is created in a software system by one of its programmers.
  + ***BackDoors***
    - **A backdoor**, which is also sometimes called a **trapdoor**, is a hidden feature or command in a program that allows a user to perform actions he or she would not normally be allowed to do
    - When used in a normal way, this program performs completely as expected and advertised.
    - But if the hidden feature is activated, the program does something unexpected, often in violation of security policies, such as performing a privilege escalation. – Benign example: Easter Eggs in DVDs and software.
  + ***Logic Bombs***
    - A logic bomb is a program that performs a malicious action as a result of a certain logic condition. •
    - The classic example of a logic bomb is a programmer coding up the software for the payroll system who puts in code that makes the program crash should it ever process two consecutive payrolls without paying him.
    - Another classic example combines a logic bomb with a backdoor, where a programmer puts in a logic bomb that will crash the program on a certain date.
* ***Computer Viruses***
  + A computer virus is computer code that can replicate itself by modifying other files or programs to insert code that is capable of further replication.

***Virus Phases***

* + Dormant phase. During this phase, the virus just exists—the virus is laying low and avoiding detection.
  + Propagation phase. During this phase, the virus is replicating itself, infecting new files on new systems.
  + Triggering phase. In this phase, some logical condition causes the virus to move from a dormant or propagation phase to perform its intended action.
  + Action phase. In this phase, the virus performs the malicious action that it was designed to perform, called payload.
    - This action could include something seemingly innocent, like displaying a silly picture on a computer’s screen, or something quite malicious, such as deleting all essential files on the hard drive.
  + ***Infection Types***
    - **Overwriting** – Destroys original code
    - **Pre-pending** – Keeps original code, possibly compressed
    - **Infection of libraries** – Allows virus to be memory resident – E.g., kernel32.dll
    - **Macro viruses** – Infects MS Office documents – Often installs in main document template.