Cybersecurity Notes

Table of contents

Anish Goyal Schepens Period 1 01/23/2023

Overview

Secrecy

- Only the people that should have access can have access

Integrity

- The information cannot be manipulated. The data has not been compromised and remains unchaiged

Availability

- The information is available to the people that need it when they want it.

Authentication

- Who I confirm who you are
- Word that usually goes with it: authorization
  - Authorization is how I figure out what you have access to given your identity
- Three types of authentication
  1. What you know
     - Based on knowledge that only the user should know
     - Dongle, key, password
     - No physical interaction, could just be the passing of information that leads to this being compromised
  2. What you have
     - A physical thing you hold (a card)
  3. What you are
     - Biometrics
     - Hardest to change and attack
     - Can't be changed

Attack vectors

Threat/Attack vectors

- How someone can attack a system. The media or method that hackers use to attack a system

Brute force attack

- Not smart at all
- Trying every possible combination of a password until you get it right
- Can be done with a computer or a human
- A dictionary or a random string generator
- Typically goes in order
- Some computers lock you out after a certain number of attempts
- If hackers take over a botnet, they can use that to brute force attack
- Increasing the length of the password makes it harder to brute force attack
- Certain cites enforce a password complexity policy such that you have to have a certain number of characters, a certain number of numbers, a certain number of special characters, etc so that it is harder to brute force

Authentication

Two factor authentication

- When you have to provide two pieces of information to authenticate
- The first is something you know (password)
- The second is something you have (a dongle)

Access control

- Controlling what you have access to once you are authenticated
- Authenticated users may not be authorized to access certain things

Permissions

- Read
  - Can read the file
  - Can see the contents of the file
- Write
  - Can change the contents of the file
  - Can delete the file
- Execute
  - Can run the file
  - Can run the program

Malware

Overview

- Malicious software
- Security vulnerabilities in software manifest themselves due to the way the software is written
- Most security errors come from implementation errors
  - The more code you have, the more likely you are to have a security vulnerability
- Malware can be used to steal information, destroy information, or disrupt the normal operation of a computer system
- It is best to have a secure kernel than have a less secure user space

Independent Verification & Validation

- Independent verification is when a third party verifies that the software is secure
- Open sourced projects have a lot of people looking at the code, thus making it more secure
- The more eyes on the code, the better
- Penetration testers are white hat hackers that try to break into systems to find vulnerabilities

Isolation

- When a programmer writes code that anticipates their systems being compromised to minimize the damage
  - Sandboxing is when you allocate a certain amount of memory to a program and it can't access anything outside of that memory
  - This makes it so that it is difficult for the program to do any damage to the system

Virtual machines

- A virtual machine is a computer that runs on top of another computer
- Has its own operating system, virtual memory, and CPU
- The virtual machine is isolated from the host computer
  - This makes it so that if the virtual machine is compromised, it doesn't affect the host computer