Week 2 Lecture 1

Pravesh Jain

9th September 2020

1 Introduction

The idea of this weeks class was understanding security, and what to expect when we say that we need to make our system secure. We looked at two slightly different definitions for security.

1. ISO/IEC , 1998

"The protection of data and resources from accidental and malicious acts, usually by taking appropriate actions ...These acts many be modification, destruction, access, disclosure or acquisition if not authorized."

2. Ross Anderson

"Building Systems to remain dependable in face of malice, error or mischance."

The idea here is to make system resilient in face of possible, error, mischance, or actions to disrupt the system. We need to ensure that our data and it's access is safe, even if there are other problems surrounding the system.
For understanding how to ensure safety of data/access, we will use CIA Properties of Secure System

2 CIA(Confidentiality, Integrity and Availability)

Confidentiality: We need to ensure that documents are only accessible to authorised parties. In a simple terms, data should only be accessible to people who have permission to view it. There are methods to ensure it. *Access Control, Encryption and Procedural Means*

Access Control is the final goal we want to implement. It can be done via following methods.
1. Encryption: Encryption means to modify the data in such a way that only a person with the same key as the sending party can re change it back into it's original state.

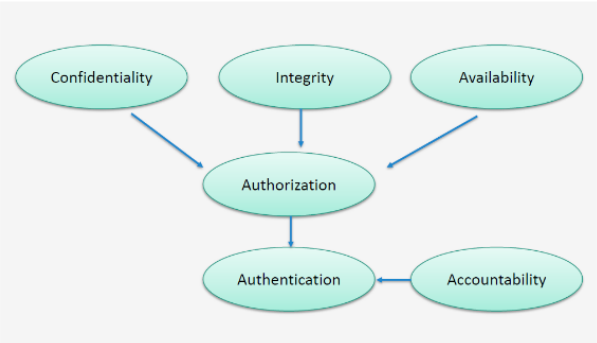

Figure 1: Summary Of CIA Model

2. Procedural Means: The physical means (such as passing Laws against accessing certain information) which we can use to make certain parts of data accessible to certain people alone. It can also involve transferring data physically instead of over a network to ensure it's safety.

Integrity : We need to ensure that the data we receive is unaltered and is presented to the authorised users in it's original form. There are various methods that we presently use such as Error Correction Code, Cryptographic Hashes or/and check-sums.

Availability: One of the most common method of disruption of a secure system is to deny it's service even to the authorised parties. We need to ensure that our data is always accessible to the authorised user, and is not deleted/made unavailable to them. For this we use protection against DDOS (Distributed Denial of Service) attack.

As we can see, CIA models lays a special stress on authorisation of users. Next we will understand, how we ensure this correct authorisation.

1. **Authorization**: Ensuring that the system and data are only available to intended entities.

2. **Authentication**: Ensuring that the entity that is granted the authorization is genuine with respect to expectation arising to the context. For example, my twitter account should only be accessible to me, and it's twitters' responsibility to ensure that I am the person who is accessing my account. This is done using Passwords, Cryptographic Keys, etc

3. **Accountability**: Ensuring that actions on the systems are mapped with the entities that are performing it. This leads to understanding the end point where the system has been compromised. With accountability, we can trace

back an error to a cause, and fix it from there. Examples include, block-chain, append-only logs, etc.

3 Security Policies in a System

Security Policies in a nutshell help us identify who allowed to access what. Helps us to identify if there are any violations of the policies we set. Violations of a security policy means unauthorised changes to the system.
Here we define the following:

Threat: Entities performing actions that can give them unauthorized access to the system, thus, violating our security policies.

Attack-Vector: Steps/Algorithms by which a threats violates our system security.

Control And Counter Measures: Prevent/Detect unauthorized access to systems.

4 Security Violations/ Threats / Vulnerabilities in Practice

The following is the list of possible violations for a system.
External Misuse: Non technical in nature. Example: physical scavenging, visual spying, deception.
Hardware Misuse: Accessing the data
Passive: Doesn't change the system. Includes Logical Scavenging, Eavesdropping
Active: Changes/Breaks the system. Includes Trojan Horse, introducing faults.
Masquerading: Pretending/Impersonating an authorized entity to access the data. Sometimes indistinguishable from legitimate activity.
Setting Up Subsequent Misuse: Malicious Programs that are triggered by later event (Time, Action). Ex: Worms, Ransomware
Bypassing Intended Control: Activities that bypass our security measure to gain information from a system. Ex: Trapdoors, Cracking Passwords, etc

The above misuses can be classified into more categories:
1. Active Misuse: Actively changing data, ex DOS attack.
2. Passive Misuse: Browsing and Analysing Data, without changing the system.
3. Inactive Misuse: Unintentional Misuse. Include mistakes from user's side. Ex: Giving phone for repair, without repairing the data
4. Indirect Misuse: Breaking cryptographic keys and then use it for listening to

encrypted communications

5 Basic Risk Analysis

Understanding the most important and most vulnerable part of system, helps us understand where to divert our resources for protection at. If we know what data an attacker will most likely try to gain access to, we can provide it an additional layer of security. The following equation can give us approximate idea of Risk of an attack.

Risk Due to attack = Probability That an attack will happen * Probability that the vulnerability exits * Value of the target asset (tangible + intangible)

6 Conclusion

In this lecture we focused on identifying how to make a system more secure. We understood important aspects of secure system using the CIA model of security. Also, we understood the important part involved in making a system secure using CIA model. Understanding where is to divert our resources while ensuring security is also an essential part. We learned how to analyse vulnerability of different parts of a system.