Scribe: Cryptography and Network Security (Class.1.A)

Akash Tiwari

9-Sep-2020

1 Security threats,vulnerability: risk and security controls

This lecture analyses the following problem - Given a System, How do you go about identifying the threats, vulnerabilities and devising counter-measures to them? In this lecture, we focus on-

- Section 2 - Defining computer security
- Section 3 - Properties of a secure system(CIA model)
- Section 4 - Security policies of system
- Section 5 - Security violations, threats and vulnerabilities
- Section 6 - Risk analysis.

2 Computer Security: Definition

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

3 CIA model

CIA stands for -

- Confidentiality - Access of information should be limited to authorized parties. eg- access control, encryption.
- Integrity - Information or data should be modified ONLY by authorized parties. eg-Parity bits, Check-sums, Error correction Code.

- Availability - Information and system should remain accessible for authorized use. eg- Protection against DDOS.

Some additional properties are needed for proper functioning of the CIA model-

- Authorization - System and data should be accessed by intended entities only.
- Authentication - Verification whether an entity is genuine or not. eg- passwords
- Accountability - holding entities responsible for past actions. eg-Logs.

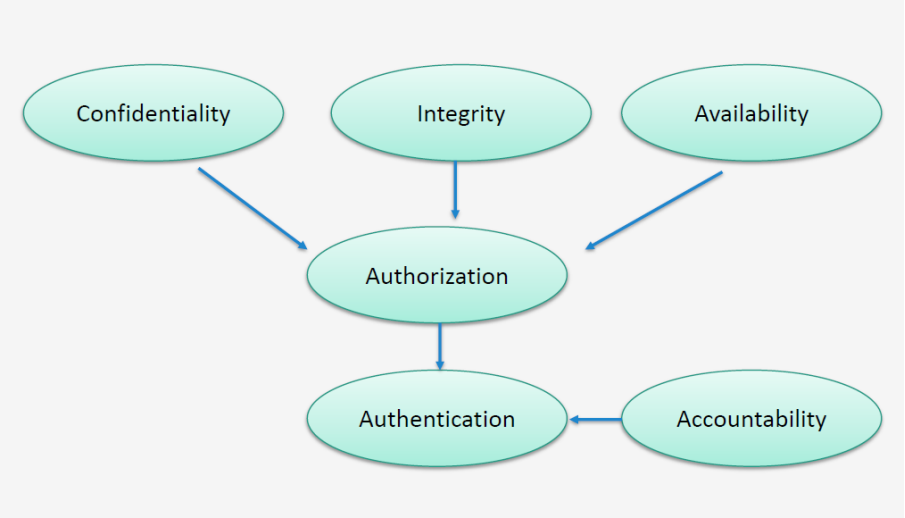

Figure 1: Summary of CIA model.

4 Security Policies in a System

The security policy of the system decides the access of resources for various entities. If some unauthorized modification or access is made then this policy is said to be violated.Here we define-

- Threats - Entities violating the Security policy.
- Attack Vector- The steps followed for an attack.

5 Security threats and vulnerabilities in practice

Some misuses and vulnerabilities in brief-

- External misuse- Non-technical, breach of confidentiality to access data. eg-visual spying, deception.
- Hardware misuse- Accessing or changing data/configuration. Passive - No modification of system eg-Key-loggers,eavesdropping.Active- Modify system too. eg-Trojans.
- Masquerading- Pretending/impersonating an authorised party to gain access(Breaks Authentication) eg-Spoofing.
- Setting up Subsequent misuse-malicious programs that are triggered by some event later(Time,action) eg-worms, ransomware.
- Bypassing Intended Control- activities that bypass the security measures to gain access to information. eg- trapdoor, cracking passwords.

These misuses can be classified into 4 categories-

- Active misuse- modification of data.
- Passive misuse- Collection of data without changing anything in the system.
- Inactive misuse- Misuse because of user. eg- setting an easily guessable password.
- Indirect misuse- breaking keys and using the key to listen to encrypted data subsequently.

6 Risk analysis

Developers who devise counter-measures also have limited resources. So we need to prioritise the different areas that need protection. This priority(risk) is set up by protecting the most important and most vulnerable resources. We calculate the risk as-

$$Riskduetoanattack =$$
$$P(anattackwillhappen) * P(vulnerabilityexists) * P(valueofthetargetedasset)$$

7 Conclusion

In this lecture, we learnt the aspects of a secure system that is the extended CIA model.We then learned about the security policies to prevent unauthorized accesses and then looked at different kind of vulnerabilities and misuse. At the end we discussed on how to assign priority and do the risk assessment.