Scribe: Cryptography and Network Security (Class.2.A)

Prashant Shishodia

10-Sep-2020

Introduction

While designing a system, a set of **Design Principles for security** must be followed to secure the system. We'll discuss about these design principles later in this text.

Basic Security Analysis, on the other hand aims at securing the system from external attacks, and minimising the impact that an attack will have on the system by modelling the system, threats and the adversaries. We'll also discuss about how to model them and the basic security goals we should satisfy for a system to be "secure enough".

System Modelling

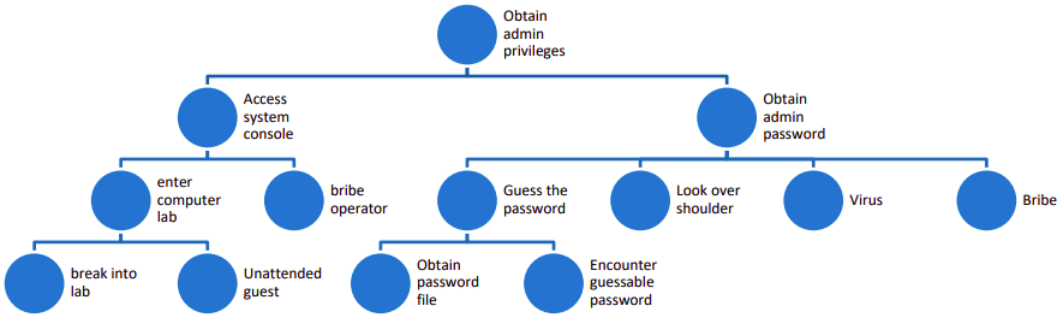
System Modelling consists of precisely defining the assets in the system, their values, and the impact it will have on the system, if that asset is breached.

Threat Modelling

Threat modelling consists of identifying potential attackers, and their expected resources, the estimated number of attacks and the probability of an attack happening. Unlike System modelling where we know everything about out system, we're still in shade during Threat Modelling, and need to make assumptions about attackers and their resources (using past experiences).

The different approaches generally used for Threat Modelling are:

- Architectural diagrams: Data flow and user diagrams
- Attack Trees: Tree for all possible choices to breach the system, at each step.



- Checklists: Listing all possible attacks and building security against them.
- Stride: Keeping track of the major attacks, spoofing, tampering, repudiation, information disclosure, denial of Service, and escalation of privilege

0.1 Adversary Modelling

We consider the three factors, namely, **attacker action**, **capabilities** and his **access** to the system. The adversaries can range from Foreign intelligence to malicious insiders, to even employees unaware of security measures.

Security Goals

The final goal of security analysis is to secure the system, satisfying the basic security requirements - Confidentiality, Integrity, Authencity, Availability, Auditability, Access Control, Privacy and Plausible Deniability.

Designing Systems

Apart from using cryptogtraphy for encryption and hashes, the system should also be resilient to attack, which can be done by keeping updated copies of system. Mechanism for detecting attacks and recovering from them in minimal time should be one of the most important things to be considered, while designing a system.
Securing the system against each and every attack is expensive and inconvenient, thus identifying like attackers and the consequences reduces the cost, still making us aware when the system might not be secure, we then have a choice to finalize the system if that vulnerability doesn't have too big of an impact.

Basic Principles

Over time, people have realized that what is more vulnerable to attack than the other. Some of the basic attacks can be reduced by using the following principles.

- Make defaults safe (eg, use https by default)
- Make the desing open (more eyeballs, better security)
- Principle of Least privilege (never use root account)
- Least Surprise
- Never trust the input: Verify
- Isolation: compartmentalize resources, eg, firewalls
- KISS (Keep-it-simple-stupid)

Conclusion

A system can almost never be made fully secure, but with the help of system, adversary and threat modelling we can minimize the impact an attack will have on them system. Apart from the modelling, basic security measures should also be taken while designing the system, and later on to reduce the probability of a successful attack.