Cryptography and Network Security (Lecture 6:Threat modeling and Security architectures)

Maniteja Tallapally

10-Sep-2020

1 Introduction

Security for a given system is never absolute. There is always a weak-link in the system that an attacker can exploit to get in to the system. Accepting this fact, it is rational to design our system defences enough to face the level of threat that is most common to the kind of system we are trying to protect. This is Convenient to user and also cost efficient. This risk-based approach is security design is called "Threat modelling". Threat modelling follows by analysing the following questions:

- What do we intend to protect? (system model)
- Who is the attacker or the threat? (threat model)
- What are the security requirements? (Security Goals)
- What security approaches can be effective? (Solution)

2 System model

System modelling consists of understanding the system architecture, listing assets and assigning value to the assets.
Here, assets are any files/data that the attacker might be seeking for their selfish purposes. Assigning values to assets help in sorting the system's priorities in the matter of what assets must be protected the most in an event of attack.This minimizes the losses(financial/aesthetic), still providing a convenient user experience without placing security on each and every other detail(asset) in the system.
The algorithm that evaluate the assets must consider the below two attributes:

• The operating value of the assets (can be cost, can be man hours)

• The impact if the asset if breached (Ex: if an admin password is breached by the attacker, he can then sweep the entire system with no effort)

3 Threat modelling

Threat modelling deals by identifying potential hackers, enumerate their resources, estimate the no. of attacks and probability of attack. Doing this gives us an idea of what we are dealing with, how vulnerable the system is to such threats and what measures must we take to keep the system secure.

3.1 Adversary attributes

Measuring an adversary is important if we intend to beat their wits in an impending attack. We should design our system so that an attacker of such level cannot penetrate in to the system. The attributes used to evaluate an adversary are:

• Attacker action: Passive (eavesdropping), Active(man-in-the-middle attack)

• Attacker capability: Script kiddies to nation states (decides how resilient your solution should be)

• Attacker access: External (can only observe the system), Internal (inside the system, e.g., compromised user account)

3.2 Schema for modelling adversaries

Below are the named categories of adversaries a system might face, sorted in decreasing level of capability, resources, malicious intent etc.

• Foreign intelligence (including government-funded agencies)

• cyber-terrorists or politically-motivated adversaries

• industrial espionage agents (perhaps funded by competitors)

• organized crime syndicate

• lesser criminals and crackers (i.e., individuals who break into computers)

• malicious insiders (including disgruntled employees)

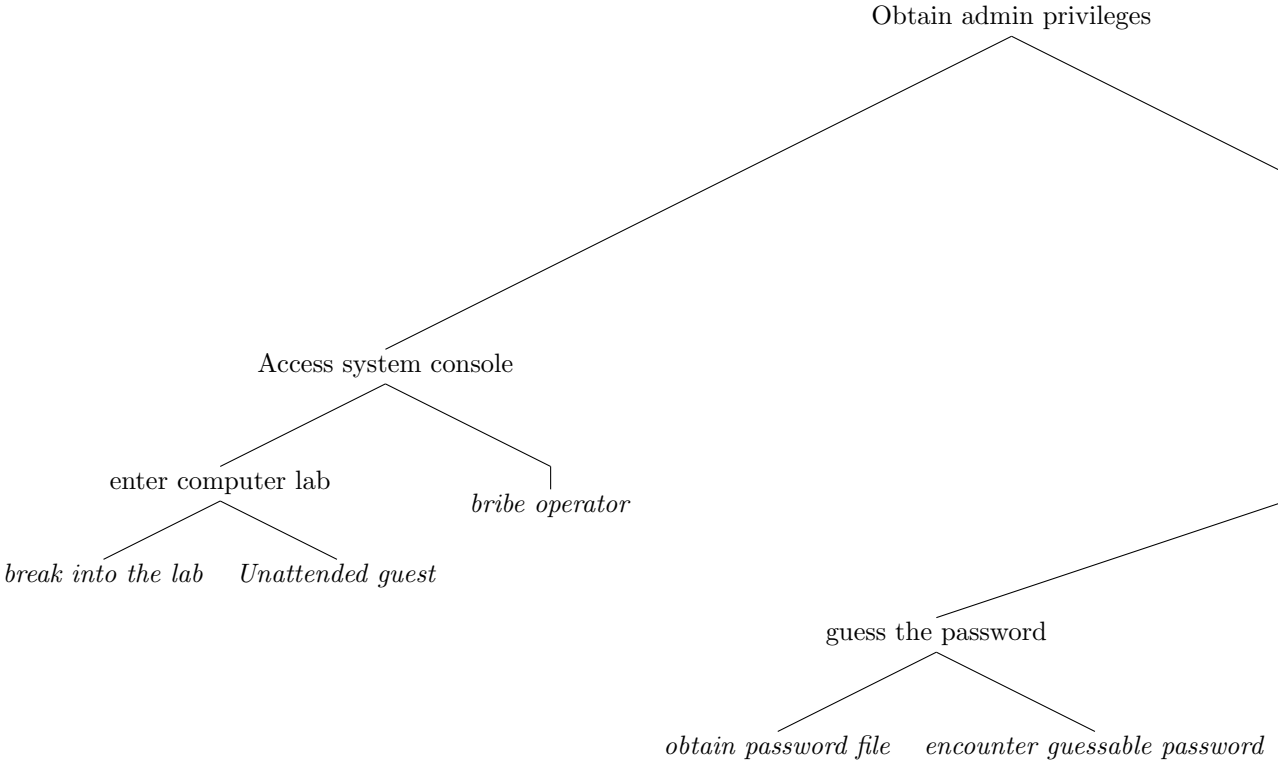
• non-malicious employees (often security-unaware)

3.3 Modelling approaches

Once we know the possible threat/adversary, based on their skill set and intentions, it is easy to guess the target assets and how the attacks on them might be planned. Understanding the attack strategy helps us to prepare our defences strategy. Following are the approaches used to analyse the attacks:

3.3.1 Attack tree

Attack tree is a B-tree representation of all possible ways an asset might be attacked. Here is an example:



4 Conclusion