MIT 6.858 - Computer Systems Security "Lecture 1 - Introduction"

Lecture 1 - Introduction

This course is about building secure computer systems. Security is a property or behaviour of a system that is achieved despite attacks from adversaries. This property could be data confidentiality, data integrity, access control, etc.

There are three main aspects to building secure systems -

1. Policy - The plans and/or rules you will implement to make sure that your system is secure. For example, require users to enable 2FA.
2. Threat model - Assumptions about what the attacker can and cannot do. For example, the attacker can try to guess passwords, but cannot try to physically break into the server room (this assumption is fine in most cases).
3. Mechanism - The specific software and hardware techniques you will use to achieve security.

Building secure systems is hard, because security is a *negative goal*. For example, if our goal is to make sure that only the author of a file can access that file, implementing access control is a positive goal - only one code path is needed to check if the accessing user is the owner, and if yes, access is granted. However, to make sure that *no one else* accesses the file, we may need many checks, techniques, etc. to make sure that no one else is granted access to that file. We must make sure that there is no way in our system for a user that is not the owner to pretend to be the owner.

This is a very hard task, and there is no guarantee that we will get it right the very first time. There is also no guarantee that we have thought of and considered all the possible attack vectors for a system. Therefore, we must constantly be vigilant and iterate. We must be vigilant not just of our system, but open source databases of documented security vulnerabilities, such as cve.mitre.org.

Perfect security is not possible. However, perfect security is not required, either. We just have to make sure that the cost to an attacker is higher than the potential reward they may gain from breaking into our system. Also, implementing some

security techniques can ensure that some types of attacks are completely nullified.

The rest of the lecture presents examples on security failures to highlight the ways in which a security engineer must think. They are very interesting and fun reads, you can find them here.