CS 458/658 - Computer Security and Privacy **Fall 2018**

Lecture 1: September 6, 2018

Lecturer: Ian Goldberg *Notes By: Harsh Mistry*

1.1 Introduction to Computer Security and Privacy

- The goal of computer security is to be able to identify security and privacy issues in various aspects of computing. (Programs, operating systems, Networks, Internet applications, Databases)
- The Secondary goal is to be able to use this ability to design systems that are more protective of security and privacy
- In the context of computers, security generally means three things :
  - Confidentiality
  - Integrity
  - Availability
- If CIA is satisfied, that a system is said to be secure
- **Privacy** is "Informational self-determination", which means you get to control information about you

1.1.1 Terminology

- **Assets** - Things we might want to protect
- **Vulnerabilities** - Weaknesses in a system that may be **exploited** in order to cause loss or harm
- **Threats** - A loss or harm that might befall a system
- **Threat Model** - A set of threats we are undertaking to defend against
- **Attack** - An action which exploits a vulnerability to execute a threat
- **Control/Defence** - Removing or reducing a vulnerability

1.1.2 Defence Steps

- **Prevent it**
- **Deter it** - Make the attack harder or more expensive
- **Deflect it** - Make your self less attractive to attackers
- **Detect it** - Notice that attack is occurring or occurred.
- **Recover from it** : Mitigate the effects of the attack

Its also worth noting the **Principle of Easiest Penetration** states a system is only as strong as its weakest link.

1.1.3 Methods of Defence

- Cryptography
- Software controls
- Hardware controls
- Physical controls
- Policies and procedures