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

Lecture 7: September 20, 2018

Lecturer: Ian Goldberg *Notes By: Harsh Mistry*

7.1 Operating Systems Continued

7.1.1 User Authentication Continued

7.1.1.1 Graphical Passwords

- Graphical passwords are an alternative to text based passwords
- There are multiple techniques such as
  - User choosing a picture to login
  - User choosing a set of places in a picture

7.1.1.2 Server Authentication

- With the help of a password, system authenticates user (client)
- But user should also authenticate system (server) else might end up with attacker

7.1.1.3 Biometrics

- Biometrics have been hailed as a way to get rid of the problems with password and token-based authentication
- Unfortunately, they have their own problems
- Biometrics are based on the concept of using physical characteristics
- If observed trait is sufficiently close to previously stored trait, the system must accept the user
- Biometrics can't be changed if compromised
- Biometrics work well for local authentication, but are less suited for remote authentication or for identification.
- With local authentication, a guard can ensure that the person is indeed the individual and not someone trying to fool the system
- Authentication of biometrics is ensuring a captured trait correspond to a particular stored trait.
- Identification is ensuring a capture trait corresponds to any of the stored traits
- False positives can make biometrics-based identification useless

7.1.2 Security Policies and Models

7.1.2.1 Trusted Operating Systems

- Trusting an entity means that if this entity misbehaves, the security of the system fails.
- We trust an OS if we have confidence that is provides security services
- Trusted operating systems typically builds on four factors
  - Policy : A set of rules outlining what is secured and why
  - Model : A model that implements the policy and that can be used for reasoning about the policy
  - Design : A specification of how the OS implements the model
  - Trust: Assurance that the OS is implemented according to design
- Trusted software means it does what its expected and **Nothing More!**
  - Functional correctness : Software works correctly
  - Enforcement of integrity : Wrong inputs don't impact correctness of data
  - Limit Privilege : Access rights are minimized and not passed to others
  - Appropriate confidence level : Software has been rated as required by environment
- Trust can change over time

7.1.2.2 Security Policies

- Many OS security policies have their roots in military security policies
- Each object has a sensitivity level
- Each object might also be assigned to one or more compartments