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

7.2 Access Control Continued

7.2.0.1 Role-based access control (RBAC)

- In a company, objects that a user can access often do not depend on the identity of the user.
- RBAC involves an administrator assigning a role to a user which grants access certain rights to a rolw
- RBAC Extensions
  - Hierarchical roles
  - Multiple Roles
  - Separation of Duty - Rights for a task are split across multiple roles

7.3 User Authentication

- Computer systems often have to identify and authenticate users before authorizing them
- **Identification** is determining who you are
- **Authentication** is proving the individuals identity

7.3.1 Authentication Factors

- Factors the user knows (PIN, Password, etc)
- Factors the user has (Card, Badge, etc)
- Factors impacting who the user is (Biometrics, etc)
- Factors impacting the users context (Location, time, device proximity, etc)

7.3.1.1 Combination of Authentication Factors

- Different classes of authentication factors can be combined for more solid authentication
- User multiple factors from the same class might not provide better authentication

7.3.1.2 Passwords

- Probably oldest authentication mechanism used in computer systems
- Many usability problems, such as
  - Entering passwords is inconvenient
  - Password composition/change rules
  - Forgotten passwords may not be recoverable
  - If password is shared among many people, password update becomes difficult
- Security Problems
  - If password is disclosed to unauthorized individual
  - Shoulder surfing
  - Keystroke logging
  - Interface illusions / Phishing
  - Passwords could be reused across sites
  - Passwords can be guessed