INFO 310
Fall 2016

Week 4 – Lecture 1

HOUSEKEEPING

- Attendance

- Study Session

Quiz – Study Guide

- Define encryption
- Knowledge of basic vocabulary and definitions
- Explain difference between symmetric and asymmetric encryption, as well as advantages & disadvantages
- Knowledge of different ciphers and algorithms (high level)
- Basic knowledge of key size and why/how it matters, symmetric vs. asymmetric key size differences
- Key players of Public Key Cryptography
- Describe how OpenPGP / public key encryption works

Quiz – Study Guide Cont'd

- Knowledge of the Web of Trust
- Knowledge of the components of PKI
- Explain what hashing does, what its characteristics are
- Knowledge of Access Control Models and how they differ
- Knowledge of definitions of terms (Access Control as defined in class)
- Authentication & Authorization mechanisms
- Describe what makes a good password

Quiz – Study Guide Cont'd

- Knowledge of different types of password attacks
- Knowledge of different types of authentication (besides password)
- Describe what 2-Factor Auth is (including technical implementations), how it works (high level), what its purpose is
- Knowledge of different types of biometrics
- Pros and cons of biometrics

Quiz – Study Guide Cont'd

- Reading: Anderson, pages
  - **31-39 (2.4 - 2.4.4.2)**
  - **129-155 (5.1 - 5.4.2)**
  - **160-182 (5.5 - 5.8)**
  - **239-252 (8.1 - 8.4)**
  - **275-292 (9.1 - 9.3)**