CSE409 – FALL 2010
Lecture 1

*Http://www.cs.sunysb.edu/~rob/teaching/cse509-fa10*

Professor: Rob Johnson
(rob+509r@cs.sunysb.edu) <- REVIEWS ONLY

**COURSE STRUCTURE**

- Reading/Reviews
- Midterm and Final
- Project (2-3 people)
- HW's

**NOTES**

Extra Credit

mostly short answer midterms. NO multiple choice/(true/false) questions.
What is computer security?

- something that cannot be bypassed (ideally).
- Not vulnerable to external or internal threat. (Threat Model)
- Trust boundaries: Trusted Computing Base (TCB). --- Want small TCB.
- Consequences and (Mitigations???)
  - What are you priority.
  - What property is being protected.

Security Goals:

- **Availability**
  - people who should have access can actually have it.
  - Deial of Service (DoS)
    - network bandwidth exhaustion
    - man-in-the-middle attack?
    - crash system via bad input.
    - account locking
    - CPU time
    - RAM
    - Disk
- **Secrecy**
  - password
  - encryption key
  - financial info
  - SSN
  - cookies
  - contacts
  - business cards
  - source code
  - national security
  - trade secrets
  - credit card #
  - annonimity
    - hide who is talking to whom
  - authentication
    - identify users or other remote parties
    - verify property account
- **Integrity**
  - data only modified in authorized ways
  - DB contents
  - source code
  - modifying messages in transit
  - C:\Program Files\Caphyon\Advanced Installer 7.7\bin\x86\advinst.exe
• **Security** is the study of computing in the presence of an **adversary**.
  
  ○ Security vs. Reliability
    ▪ attackers adapt to defenses
    ▪ attackers do not follow a known probability distribution
  
  • **Threat Model**
    ○ Defines power and limits of attacker
      ▪ computation (can vary from 1 to $10^6$ CPU’s or more)
      ▪ access (insider – remote / outsider - local)
      ▪ bandwith, connectivity, etc
      ▪ time
      ▪ knowledge of defenses (everything except explicitly dented secrets : password, encryption keys, random numbers)
        • cryptosystem
        • logging rules
        • public keys
        • network layout
        • O.S.
        • F.S.
        • Browser
        • partial knowledge of data
        • user info
        • trap doors
        • time
        • source code