27&28. SECURITY INTRO & AUTH

- **Attacks Happen example（P13）**
- **HOW TO SHOP FOR FREE ONLINE example（P19.20）**
- **Other Attacks（P21）**
- **Security: Real World VS. Computer（P22-23）**
- **Why is Security So Hard（P24-27）**
- **Fault Tolerant Fails Here(P28)**
  - **Much Harder to Reason about Security(P29)**

2 Steps towards Building a More Secure System

Be clear about goals: "**policy**"

Be clear about assumptions: "**threat model**"

- **Policy: Goals(P31)**
- **Threat Model: Assumptions(P32-34)**
  - **What does a threat model look like**
  - **Unrealistic / incomplete threat models**
  - **important to have a threat model**
  - **Overly-ambitious threat models not always a good thing**

GUARD MODEL

- **Guard Model of Security: Complete mediation(P6-7)**

- **Designing the Guard(P8)**
- **Example: Unix FS(P9)**
- **Example: Web Server(P10)**
- **Example: Firewall(P11)**
- 可能出问题的原因(P12)
  - **Bypassing Complete Mediation**
    - **Example: SQL Injection**
    - **Example: Paymaxx.com (2005)**

AUTHENTICATION: PASSWORD

- **Authentication的三种方式（P18）**
- **Authentication: Password（P19）**
  - **Timing Attack: Guess One Character at a Time（P20-23）**
  - solution：**Idea: Store Hash of Password（P24-27）**
- **Store Hash of Password的相关改进：Salting（P31-32）**
- **Bootstrap Authentication（P33）**
  - **Session Cookies: Strawman（P34-35）**
- **Phishing Attacks（P36）**
- **Key Problem of Password：once you send a password to the server, it can impersonate you（P37）**
  - **Technique 1: challenge-response scheme（P38-39）**
  - **Tech 2: use passwords to authenticate the server（P40-41）**
  - **Tech 3: turn offline into online attack（P42-44）**
  - **Tech 4: Specific password（P45）**
  - **Tech 5: one-time passwords（P46-47）**
  - **Tech 6: bind authentication and request authorization（P49）**
  - **Tech 7: FIDO: Replace the Password（P50）**

- **Three Bindings（lec29 P4)**
- **Bootstrapping: 在初始化和修改密码时的相关问题(P5)**