Lecture notes for 3.4, 3.5

- Privilege escalation
  - RunAs / setuid explanation
  - Dangers of setuid
  - Combine local user-to-root with remote-to-user attack to get remote-to-root
  - Chroot explanation, chroot jailbreak [draw filesystem tree pictures]

- Directory traversal
  - Connect to discussion of jails [web server root is different from filesystem root]

- Interface spoofing in web browser via javascript
  - Full screen window, fake UI widgets

- Keyloggers, clickloggers

- Timing attacks
  - Against RSA: op for bit 1 in key costlier than op for bit 0 in key
  - With sufficient tests, noise averages out

- Covert channels
  - Piggyback confidential information to open data
  - Low-order bits of image
  - Time delay
  - [Example spam message from Kapil]
  - [Ask students to think of more]

- Software development
  - Identify needs / specify / design / implement / test / deploy
  - Verification: ensure implementation matches specification
    - Combines static analysis with formal methods (model checking)
    - [Give example with kernel pseudo-code / one path sets uid to 0 / property is no prog can elevate privilege]
  - Design for failure
  - Principle of least privilege
  - Confinement / sandboxing / monitoring

- Challenges to code analysis
  - Dynamic (runtime)
    - Only analyze paths of execution
    - Largely black box testing / fuzz testing
  - Static
    - Impossibility results [due to halting problem]
    - [Give halting problem, recast as reachability, almost everything is reachability]
    - White-box analysis
    -