

## Final Study Guide

This is simply a guide of topics that I consider important for the final. I don't promise to ask you about them all, or about any of these in particular; but I may very well ask you about any of these, as well as anything we discussed in class, in the discussion section, or that is in the readings.

1. Anything from the midterm; see the Midterm Study Guide
2. Mobile computing
  - a. Threats to security
  - b. About Android security: permissions
  - c. Countermeasures: controls, sandboxing
3. Anti-malware software
  - a. How anti-malware programs work
  - b. Malware signatures
  - c. Malware behavioral detectors
  - d. How and when to do an anti-malware scan
  - e. Limitations of anti-malware software
4. Digital rights management
  - a. Types of access controls: DAC, MAC, ORCON
  - b. Digital Millennium Copyright Act (DMCA)
  - c. Approaches: cryptographic, system modification
  - d. Problems with implementing DRM
  - e. preventing or limiting piracy
5. Electronic voting
  - a. Goals as compared to the use of paper
  - b. Different types of e-voting systems
  - c. Safeguards and certification
6. Insider problem
  - a. Security perimeter
  - b. Definition of insider
  - c. Countermeasures
7. Computer forensics
8. Cyberwarfare
9. Cyberphysical systems
  - a. Power grid: traditional vs. smart grid, meters
  - b. Stuxnet
10. Privacy and anonymity
  - a. What to anonymize
  - b.  $k$ -anonymity,  $\ell$ -diversity
  - c. Data sanitization
  - d. Repudiation, non-repudiation