Lecture 5 Outline

April 12, 2016

Reading: *text*, §14; [SS75, Bis11] **Assignments due:** Homework 2, on Apr. 19

1. Greetings and felicitations!
2. Puzzle of the Day
3. Principles of secure design
   a. Principle of least privilege
   b. Principle of fail-safe defaults
   c. Principle of economy of mechanism
   d. Principle of complete mediation
   e. Principle of open design
   f. Principle of separation of privilege
   g. Principle of least common mechanism
   h. Principle of least astonishment
4. Robust programming principles
   a. Paranoia
   b. Stupidity
   c. Dangerous implements
   d. Can't happen
5. Fragile library

Discussion Problem. Senators Dianne Feinstein (D-CA) and Richard Burr (R-NC) are drafting a law called "Compliance with Court Orders Act of 2016". This bill, according to *The Hill*,[1] says that "all persons receiving an authorized judicial order for information or data must provide, in a timely manner, responsive, intelligible information or data, or appropriate technical assistance to obtain such information or data" (p. 2, ll. 16–21), and further that a "provider of remote computing service or electronic communication service to the public that distributes licenses for products, services, applications, or software of or by a covered entity shall ensure that any such products, services, applications, or software distributed by such person be capable of" (p. 4, ll. 10–16) complying with the above requirement. The covered entities include device and software manufacturers, and "any person who provides a product or method to facilitate a communication or the processing or storage of data." (p. 6, ll. 23–25).

What would the effect of such a law be upon the iPhone or Android encryption mechanisms? Upon using encryption to protect emails? Upon app marketplaces like Apple's App store or Google's Marketplace?

[1] `http://thehill.com/policy/cybersecurity/275567-senate-intel-encryption-bill-mandates-technical-assistance`