Lecture 9, April 19

Reading: §23.1–4; 2 **Assignments due:** Homework #2, due April 26, 2013 at 11:55pm

Discussion Problem. *Wired* today reported:

> All of those questions, messages, and stern commands that people have been whispering to Siri are stored on Apple servers for up to two years, Wired can now report.
>
> [. . .]
>
> Here's what happens. Whenever you speak into Apple's voice activated personal digital assistant, it ships it off to Apple's data farm for analysis. Apple generates a random numbers to represent the user and it associates the voice files with that number. This number — not your Apple user ID or email address — represents you as far as Siri's back-end voice analysis system is concerned.
>
> Once the voice recording is six months old, Apple "disassociates" your user number from the clip, deleting the number from the voice file. But it keeps these disassociated files for up to 18 more months for testing and product improvement purposes.[1]

Does this raise any privacy concerns? If so, what are they?

Lecture outline.

1. Aslam
   a. Goal: Treat vulnerabilities as faults
   b. Coding faults: introduced during software development
      i. Synchronization errors
      ii. Validation errors
   c. Emergent faults: introduced by incorrect initialization, use, or application
      i. Configuration errors
      ii. Environment faults
   d. Introduced decision procedure to classify vulnerabilities in exactly one category
2. Models of Attacks
   a. Example attack: *rsh* and synflooding ("the wily hacker")
   b. Capabilities and requires/provides models
   c. Attack trees
3. Access Control Matrix
   a. Subjects, objects, and rights
   b. Primitive commands: create subject/object, enter right, delete right, destroy subject/object

[1] Robert McMillan, "Apple Finally Reveals How Long Siri Keeps Your Data," *Wired (A*pr. 19, 2013); available at `http://www.wired.com/wiredenterprise/2013/04/siri-two-years/`