Lecture 6, April 12

Reading: §23.1–2, [Bis07][1] **Assignments due:** Homework #1, due April 12, 2013 at 11:55pm

Discussion question. From Saul Alinsky, *Rules for Radicals*, Random House, Inc., New York, NY (1972) pp. 72–73:

> Actually, Socrates was an organizer. The function of an organizer is to raise questions that agitate, that break through the accepted pattern. Socrates, with his goal of "know thyself," was raising the internal questions within the individual that are so essential for the revolution which is external to the individual. So Socrates was carrying out the first stage of making revolutionaries. If he had been permitted to continue raising questions about the meaning of life, to examine life and refuse the conventional values, the internal revolution would soon have moved out into the political arena. Those who tried him and sentenced him to death knew what they were doing.

How might you apply this philosophy to computer security?

Lecture outline.

1. Greetings and felicitations!
2. Penetration Studies
   a. Why? Why not direct analysis?
   b. Effectiveness
   c. Interpretation
3. Flaw Hypothesis Methodology
   a. System analysis
   b. Hypothesis generation
   c. Hypothesis testing
   d. Generalization
4. System Analysis
   a. Learn everything you can about the system
   b. Learn everything you can about operational procedures
   c. Compare to other systems
5. Hypothesis Generation
   a. Study the system, look for inconsistencies in interfaces
   b. Compare to other systems' flaws
   c. Compare to vulnerabilities models
6. Hypothesis testing
   a. Look at system code, see if it would work (live experiment may be unneeded)
   b. If live experiment needed, observe usual protocols
7. Generalization
   a. See if other programs, interfaces, or subjects/objects suffer from the same problem
   b. See if this suggests a more generic type of flaw
8. Elimination
9. Where to start
   a. Unknown system
   b. Known system, no authorized access
   c. Known system, authorized access
10. Examples
    a. Burroughs system
    b. Corporate site
11. Vulnerability models

[1] These are available in the Resources area of SmartSite; look in the folder "Handouts"

- a. PA model
- b. RISOS
- c. NRL
- d. Aslam

12. Example Flaws
    - a. *fingerd* buffer overflow
    - b. *xterm* race condition