Outline for April 20, 2004

Reading: Chapter 29.1–29.4

Discussion Problem

> 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.[1]

How might you apply this philosophy to computer security?

Outline for the Day

1. Security in Programming
   a. Example program: goal
2. Requirements and Policy
   a. Access to role account conditioned on user, location, time
   b. How to handle settings of accounts: override, merge
   c. Who can alter access control information
   d. Allow unrestricted and restricted access
   e. Access to objects owned by role account restricted to those authorized to use role account
3. Threat Analysis
   a. Unauthorized users accessing role accounts
      i. Obtaining access to a role account as though an authorized user
      ii. Authorized user using non-secure channel to obtain access, exposing information to unauthorized user
      iii. Unauthorized user altering access control information
      iv. Authorized user executing Trojan horse to give access to unauthorized user
   b. Authorized users access in role accounts
      i. Performing unauthorized commands (intentionally)
      ii. Executing command that performs unauthorized actions (unintentionally)
      iii. Changing restrictions on ability to obtain access to account
4. Design
   a. User interface
   b. High-level design
   c. Access to roles and commands
5. Refinement
   a. First level
   b. Second level
   c. Functions: location, access control record, error handling

[1] Saul Alinsky, *Rules for Radicals*, Random House, Inc., New York, NY (1972) pp. 72–73.