Outline for February 12, 2008

Reading: text, §9.1–9.2

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?

Lecture Outline

1. Cryptography
   a. Codes vs. ciphers
   b. Attacks: ciphertext only, known plaintext, chosen plaintext
   c. Types: substitution, transposition
2. Classical Cryptography
   a. Monoalphabetic (simple substitution): $f(a) = a + k \bmod n$
   b. Example: Caesar with $k = 3$, RENAISSANCE → UHQDLVVDQFH
   c. Polyalphabetic: Vigenère, $f_i(a) = a + k_i \bmod n$
3. Long key generation
   a. Autokey cipher: M = THETREASUREISBURIED; K = HELLOTHETREASUREISB; C = ALPEFXHWNIIIKVLVQWE
   b. Running-key cipher: M = THETREASUREISBURIED; K = THESECONDCIPHERISAN; C = MOILVGOFXTMXZFLZAEQ; wedge is that (plaintext, key) letter pairs are not random (T/T, H/H, E/E, T/S, R/E, A/O, S/N, etc.)
   c. Perfect secrecy: when the probability of computing the plaintext message is the same whether or not you have the ciphertext
   d. Only cipher with perfect secrecy: one-time pads; C = AZPR; is that DOIT or DONT?
4. Enigma
5. DES

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