Outline: Lecture 7

Date: April 19, 2011
Topic: Vulnerabilities and Finding Them

1. What is a "vulnerability"?
2. Role of assumptions
   a. Lack of paranoia: *the user is not out to get you*
   b. Belief in intelligence: *the user will read and understand all documentation, and will think carefully before doing anything*
   c. Give the user access to everything: *the user will know how everything works internally*
   d. Some things will never, or can never, happen: *everything the program depends on will work as expected, and properly*
3. Types of vulnerabilities
   a. Improper choice of initial protections
   b. Improper validation
   c. Improper synchronization
   d. Improper choice of operand or operation
4. Improper choice of initial protections
   a. Making homework files world readable
   b. Leaving your laptop in a public place, and it automatically logs you in when started
   c. Setting your Internet access zone to fully trusted in your web browser
   d. Allowing your Facebook to share everything by default
   e. Allowing people to change prices when buying something over the Internet
5. Improper validation
   a. Buffer overflow
   b. SQL injection
   c. Updating a remote file: check at the client or at the server?
6. Improper synchronization
   a. Race conditions and file accesses
   b. One-time passwords being used twice
   c. Deadlock
7. Improper choice of operand or operation
   a. Privilege-granting program giving privileges if it could not access the authentication data
   b. The same login name referring to different users on different systems