Lecture 12 Notes; April 12, 1997; Notetaker: Peter Mell

I. Discussion of Penetration Study by Students
a. Within an NFS domain, root on one machine is not equivalent to root on the target machine. However, bin on one machine is equivalent to bin on the target machine. Thus, all files exported by the target machine can be changed except root owned files.
b. Matt suggested learning about nsfbug for the next stage in the study

II. Vulnerabilities Analysis

Vulnerability Models
- RISOS (1975)
- PA (1976-78) automated checking
- Landwehr, classify according to attack purpose as well as type
- NSA, material is classified
- Aslan, only for C code
- Bishop

Detailed Discussion of RISOS:
He tested 6 different systems

7 Classes of vulnerabilities
- Improper parameter validation
  (i.e. division is sometimes implemented in kernel and on one system you could have the remainder overwrite your uid by giving larger numbers than expected)
- Inconsistent parameter validation
- Implicit sharing of priveledged data
- Asynchronous validation/incorrect serialization
  (Time of check to time of use flaw:TOCTTOA)
  (i.e You check someone's right to write a file but then when you actual write to the file for the person, it is another file that they shouldn't write into)
- Inadequate ID/authorization/authentication
- Violable prohibition/limit
  (if you are persistent then you will be allowed to do something)
- Exploitable logic error
  (i.e. some version of su used to give root if su failed. But one could make it fail by first opening the max number of file descriptors)

Detailed Discussion of PA:
Done by Bisbey
Goal: Find problems and automate detection

4 Classes
- Improper protection domain
  a. improper initial protection domain
     (i.e. a computer ships will all files writeable)
  b. improper isolation of implementation details
     (i.e. you can write to raw disk bypassing security mechanisms)
  c. improper change, (TOCTTOU flaws)
  d. improper naming
  e. improper deletion/deallocation
     (i.e. when you free memory it may not actual be deleted and someone else could get it by doing a malloc)
- Improper validation (i.e. of arguments)
- Improper Synchronization
  a. Improper divisibility
  b. Improper sequencing
- Improper choice of operand and operation

Note: PA maps into RISOS and vice versa