Outline for January 22, 2003

Reading: Robust Programming handout

Discussion Problem

Microsoft spent February of last year teaching its programmers how to check their code for security vulnerabilities and how to introduce common security flaws. Yet many Microsoft programs still have security vulnerabilities. Wha problems do you think Microsoft encountered, and will encounter, in trying to find and clean up the vulnerabilities in its systems?

Outline for the Day

1. Common Implementation Vulnerabilities
   a. Unknown interaction with other system components (DNS entry with bad names, assuming *finger* port is finger and not chargen)
   b. Overflow (year 2000, *lpr* overwriting flaw, *sendmail* large integer flaw, *su* buffer overflow)
   c. Race conditions (*xterm* flaw, *ps* flaw)
   d. Environment variables (*vi* one-upsmanship, *loadmodule*)
   e. Not resetting privileges (Purdue Games incident)
2. Robust Programming
   a. Principles
   b. Creating, reading tickets
   c. Creating, deleting queues
   d. Adding, removing items