Outline for December 1, 2003

Reading: Chapters 22.5, 23

Discussion Problem

Two MIT graduate students bought a number of used hard drives on E-Bay and analyzed them. They were able to recover lots of files, including files containing very personal information (such as a love letter), and in some cases even restore the operating system of the computer to which the hard drive belonged. Some of these disks had simply been discarded, but others had files deleted, or were reformatted—and still the students could recover the files!

The news article said that the students' results showed how unaware people were of security issues. Is the data being on the discarded disks in fact a vulnerability? Are the "delete," "rm," "format," and other such commands used to erase these disks secure? If not, what is the vulnerability in these programs, and how would you fix it?

Outline for the Day

1. Practise: detecting writing
    a. Integrity check files such as binaudit, tripwire; go through signature block
    b. LOCUS approach: encipher program, decipher as you execute.
    c. Co-processors: checksum each sequence of instructions, compute checksum as run; if different, complain
    d. Sandboxes: confine protection domain of process
2. Penetration Studies
    a. Why? Why not direct analysis?
    b. Effectiveness
    c. Interpretation
3. Flaw Hypothesis Methodology
    a. System analysis
    b. Hypothesis generation
    c. Hypothesis testing
    d. Generalization
4. System Analysis
    a. Learn everything you can about the system
    b. Learn everything you can about operational procedures
    c. Compare to other systems