Outline for January 24, 2003

Reading: Robust Programming handout; text, §2, 3.1–3.2

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. Robust Programming
   a. Principles
   b. Creating, reading tickets
   c. Creating, deleting queues
   d. Adding, removing items
2. Access Control Matrix
   a. Subjects, objects, and rights
   b. Primitive commands: create subject/object, enter right, delete right, destroy subject/object
   c. Copy flag
   d. Attenuation of privileges
3. HRU Result
   a. Notion of leakage in terms of ACM
   b. Determining security of a generic system with generic rights is undecidable
   c. Meaning: can't derive a generic algorithm; must look at (sets of) individual cases