Outline for January 8, 2003

Reading: Chapters 1, 13

Discussion Problem

This comes from a Microsoft web page entitled “Linux Myths.” What do you think about Microsoft’s criticisms of Linux? Specifically, does this argument demonstrate that Windows is more secure than Linux?

Myth: Linux is more secure than Windows NT.

Reality: The Linux security model is weak

All systems are vulnerable to security issues; however it’s important to note that Linux uses the same security model as the original UNIX implementations—a model that was not designed from the ground up to be secure.

- Linux only provides access controls for files and directories. In contrast, every object in Windows NT, from files to operating system data structures, has an access control list and its use can be regulated as appropriate. Linux security is all-or-nothing. Administrators cannot delegate administrative privileges: a user who needs any administrative capability must be made a full administrator, which compromises best security practices. In contrast, Windows NT allows an administrator to delegate privileges at an exceptionally fine-grained level.
- Linux has not supported key security accreditation standards. Every member of the Windows NT family since Windows NT 3.5 has been evaluated at either a C2 level under the U.S. Government’s evaluation process or at a C2-equivalent level under the British Government's ITSEC process. In contrast, no Linux products are listed on the U.S. Government’s evaluated product list.
- Linux system administrators must spend huge amounts of time understanding the latest Linux bugs and determining what to do about them. This is made complex due to the fact that there isn’t a central location for security issues to be reported and fixed. In contrast, Microsoft provides a single security repository for notification and fixes of security related issues.
- Configuring Linux security requires an administrator to be an expert in the intricacies of the operating system and how components interact. Misconfigure any part of the operating system and the system could be vulnerable to attack. Windows NT security is easy to set up and administer with tools such as the Security Configuration Editor.

Outline for the Day

1. Policy vs. mechanism
    a. Policy
    b. Mechanism
2. Trust and Assumptions
3. Types of mechanisms: secure, precise, broad
4. Assurance
    a. Specification
    b. Design
    c. Implementation
    d. Maintenance and operation
5. Operational Issues
    a. Cost-benefit analysis
    b. Risk analysis
    c. Laws and customs
6. Human issues
    a. Organizational problems
    b. People problems

7. Principles of Secure Design
    a. Principle of Least Privilege
    b. Principle of Fail-Safe Defaults
    c. Principle of Economy of Mechanism
    d. Principle of Complete Mediation
    e. Principle of Open Design
    f. Principle of Separation of Privilege
    g. Principle of Least Common Mechanism
    h. Principle of Psychological Acceptability