Trusted Operating System Design

Tom Kelliher, CS 325

Oct. 30, 2006

1 Administrivia

Announcements

Assignment

Read 5.5

From Last Time

Security models.

Outline

1. Elements of a trusted OS.
2. Security features of ordinary OSs.
3. Additional security features of trusted OSs.
4. Kernelized security component design.
5. Other mechanisms and principles.

Coming Up

Assurance in trusted OSs.

2 Elements of a Trusted OS

1. Least privilege — minimize use of high-privilege accounts.
2. Economy of mechanism — small security kernel.
3. Open design — minimize use of "security by obscurity;" maximize scrutiny by the community.
4. Complete mediation — all access should be checked.
5. Permission based — default access mode should be "denied." (Unlike PHP.)
6. Ease of use — invite use of security features.

3 Security Features of Ordinary OSs

None of this should be too surprising.

1. User Authentication.
2. Memory protection (something DOS lacked).
3. File and I/O access control.
4. Allocation of and access control to general objects (semaphores, pipes, sockets, etc.)
5. Control of sharing.
6. Fair service.
7. Protection of the OS itself.

4 Additional Security Features of Trusted OSs

1. More stringent authentication.

2. Mandatory access control layered over discretionary access control.

3. Object reuse protection.

   This is not foolproof for disk drives.

4. Complete mediation.

5. Trusted path — prevent, for example, user spoofing during login. Windows' "three-fingered" salute.

6. Accountability and audit — log access and use.

7. Audit log reduction. (Ala Splunk.)

8. Intrusion detection — detect differences from normal system behavior. This goes beyond Tripwire.

5 Kernelized Security Component Design

1. "Kernel with a kernel." Performs security functions for entire OS.

2. Small, localized footprint offers numerous advantages.

3. Trusted computing base — everything necessary for enforcing the security policy. Includes hardware, security-related processes, security-related files, memory, and IPC.

   (a) TCB is the foundation for the rest of the OS.

   (b) TCB monitors:

      i. Process activation.

      ii. Execution domain switching (user mode to privileged mode excursions).

      iii. Memory protection.

iv. I/O operation.

6 Other Mechanisms and Principles

1. Virtualization: virtual memory spaces; virtual machines.

2. Layered design: a hierarchical layering from least trusted components to most trusted components.