

Access Control and Trust Negotiation

CS 6463 Lecture 3

Prof. William Winsborough
January 29, 2007

Business

- Second paper:
 - Harrison, Ruzzo, and Ullman
 - Read by Wednesday, 1/31/2007

January 29, 2007

Winsborough CS 6463 Lecture 3

2

Clarification of Terms

- “Security” is used as a rather broad term
 - Includes physical security, security of communication channels, fault tolerance, program correctness
- “Protection” is concerned with access of executing programs to stored data
 - This has become too narrow an interpretation of the term in today’s usage

January 29, 2007

Winsborough CS 6463 Lecture 3

3

Levels of Information Protection

- Unprotected systems
- All-or-nothing systems
 - Fully isolated virtual machines
- Controlled sharing
 - Access to sharable objects through standard operations is controlled
- User-programmed sharing controls
 - Richer authorization policy based on environmental factors and arbitrary operations
 - This is viewed as being very hard in 1975. Encapsulation is much more standard today

January 29, 2007

Winsborough CS 6463 Lecture 3

4

Details of Protection Mechanisms

- These are probably more suited to a course in operating systems
- Isolation of virtual machines based on:
 - Privileged-mode bit
 - Descriptor register
 - Trap instruction that sets privilege bit and jumps to Supervisor
- Protection mechanisms are quite different outside operating system

January 29, 2007

Winsborough CS 6463 Lecture 3

5

Authentication (Today)

- Something you have
 - Key, id badge, credit card, dongle, smart card, one-time-password token
- Something you know
 - Password, pin, cryptographic key
- Something you are
 - biometric

January 29, 2007

Winsborough CS 6463 Lecture 3

6

Trojans and Man in the Middle Attacks

- Motivate 2-way authentication
 - Shared secret is used to encrypt communication after requester identifies himself
- There are other ways to defeat replay today

January 29, 2007

Winsborough CS 6463 Lecture 3

7

List-oriented vs. Ticket-oriented

- Capability systems
 - Having the “key” gets you access to the resource
- Access control lists (ACLs)
 - Introduced in part because administrative permissions can be more flexible
 - More expensive because lists have to be searched

January 29, 2007

Winsborough CS 6463 Lecture 3

8

Authority to Change ACLs

- Requires additional mechanism
 - Limited flexibility
- Hierarchical access controllers
 - Gives too much control
 - Paper suggests using auditing to mitigate misuse

January 29, 2007

Winsborough CS 6463 Lecture 3

9