



Access Control and Trust Negotiation

CS 6463 Lecture Two

Prof. William Winsborough
January 24, 2007

Business

- Office Hours:
 - 5-6pm Monday and Wednesday and by appointment
- First paper:
 - Saltzer and Schroeder, 1975
 - See course web page: <http://www.cs.utsa.edu/~winsboro/teaching/CS6463-S07>
 - Read by Monday, 1/29/2007
 - Paper focuses on stand-alone systems

January 24, 2007 Winsborough CS 6463 Lecture 2 2

Principles of Access Control (Saltzer and Schroeder 75)

- Economy of mechanism
 - Keep the design as simple and small as possible
- Fail-safe defaults
 - Default is no-access

January 24, 2007 Winsborough CS 6463 Lecture 2 3

Principles of Access Control

- Complete mediation
 - Every access must be checked
- Open design
 - Security does not depend on the secrecy of mechanism

January 24, 2007 Winsborough CS 6463 Lecture 2 4

Principles of Access Control

- Separation of privilege
 - A system that requires two keys is more robust than one that requires one
- Least privilege
 - Every program and every user should operate using the least privilege necessary to complete the job

January 24, 2007 Winsborough CS 6463 Lecture 2 5

Principles of Access Control

- Least common mechanism
 - "Minimize the amount of mechanism common to more than one user and depended on by all users"
- Psychological acceptability
 - "Human interface should be designed for ease of use"
 - The user's mental image of his protection goals should match the mechanism

January 24, 2007 Winsborough CS 6463 Lecture 2 6

Access Matrix Model

- Lampson'1971
 - "Protection"
- Refined by Graham and Denning'1972
 - "Protection---Principles and Practice"
- Harrison, Ruzzo, and Ullman'1976
 - "Protection in Operating Systems"

January 24, 2007

Winsborough CS 6463 Lecture 2

7

Access Matrix

- A set of subjects S
- A set of objects O
- A set of rights R
- An access control matrix
 - One row for each subject
 - One column for each subject/object
 - Elements are rights of subject on another subject or object

January 24, 2007

Winsborough CS 6463 Lecture 2

8

Implementation Issues

- Storing the access matrix
 - by rows: capability lists
 - by column: access control lists
 - through indirection:
 - e.g., key and lock list
 - e.g., groups, roles, multiple level of indirections, multiple locks
- How to do indirection correctly and conveniently is the key to management of access control.

January 24, 2007

Winsborough CS 6463 Lecture 2

9

Evolution of Access Control State

- Commands:
if $a_1 \in M[s_1, o_1]$ & ... & $a_m \in M[s_m, o_m]$ then $op_1 \dots op_n$
 - op_i is one of: enter a into (s,o); delete a from (s,o); create s; create o; destroy s; destroy o
- A system is *safe* if no sequence of commands gives the right, a, to subject s on object o, in which a, s, and o are specified
- Result: Determining whether a system is safe is undecidable
[Harrison, Ruzzo, and Ullman, 1976]

January 24, 2007

Winsborough CS 6463 Lecture 2

10

Deciding Safety is not Always Undecidable

- For the trust management language, *RT*, it is polynomial
 - Beyond Proof-of-compliance: Security Analysis in Trust Management. Ninghui Li, John C. Mitchell, and William H. Winsborough. *Journal of the ACM*, 2005.

January 24, 2007

Winsborough CS 6463 Lecture 2

11