

Access Control and Trust Negotiation

CS 6463 Lecture 5

Prof. William Winsborough
February 5, 2007

Business

- Projects can be done in teams

February 5, 2007

Winsborough CS 6463 Lecture 5

2

Harrison, Ruzzo and Ullman, 1976

- We continue studying this classical paper in access control

February 5, 2007

Winsborough CS 6463 Lecture 5

3

Example 4: Unix

- Privileges are granted to owner and to everyone else
 - Apparently group privileges were added later
- User u owns file f if “own in (u, f) ”
- Files are encoded as subjects
 - User u can read file f if “own in (u, f) and ‘owner can read’ in (f, f) ” or “anyone can read’ in (f, f) ”

February 5, 2007

Winsborough CS 6463 Lecture 5

4

Safety

- Def: A command *leaks* generic right r from configuration Q if
 - The conditions are satisfied and
 - One of the operations puts r in a cell that didn't previously contain it
- Def: Initial configuration Q_0 is *unsafe* for r if there is a configuration Q reachable from Q_0 and a command that leaks r from Q

February 5, 2007

Winsborough CS 6463 Lecture 5

5

Safety in Practice

- If you're trying to decide whether you should grant a right, you may want to remove yourself (the owner) from the initial configuration before asking whether the configuration is safe

February 5, 2007

Winsborough CS 6463 Lecture 5

6

Safety is Decidable in a Restricted Case

- Definition: a protection system is mono-operational if each command's body is a single primitive operation
- Theorem 1: There is an algorithm that decides whether any mono-operational system is unsafe for any given generic right r

February 5, 2007

Winsborough CS 6463 Lecture 5

7

Proof Strategy

- They prove that if there is a sequence of commands leading to a configuration in which some command leaks, then
 - There is such a sequence of length $m \leq g(|S_0|+1)(|O_0|+1)+1$, in which $g = |R|$

February 5, 2007

Winsborough CS 6463 Lecture 5

8

Corresponding Decision Procedure

- Try all sequences of (enter) commands up to length m
 - Exponential in matrix size
 - Using Dynamic Programming, can obtain an algorithm that is polynomial in the size of the initial matrix

February 5, 2007

Winsborough CS 6463 Lecture 5

9

Decision Procedure for all Mono-operational Systems

- When the commands are parameters to the decision procedure, the problem of deciding whether a protection system is safe is co-NP-complete
- Reduce k -clique to safety
- Question: why doesn't this result contradict the result that for a given protection system, a polynomial algorithm can be found?

February 5, 2007

Winsborough CS 6463 Lecture 5

10

Undecidability in the General Case

- Reduction of any Turing machine to a protection system that enters r into a cell if and only if the Turing machine halts

February 5, 2007

Winsborough CS 6463 Lecture 5

11