

January 10, 2024 Outline

Reading: *text*, §2.3–2.4, 3.1–3.3; [1,2]

Assignments: Homework #1, due January 19; Project selection, due January 26

Module 4 (Reading: *text*, §2.3–2.4)

1. Primitive operations
 - (a) **enter** r **into** $A[s, o]$
 - (b) **delete** r **from** $A[s, o]$
 - (c) **create subject** s (note that $\forall x[A[s', x] = A[x, s'] = \emptyset]$)
 - (d) **create object** o (note that $\forall x[A[x, o'] = \emptyset]$)
 - (e) **destroy subject** s
 - (f) **destroy object** o
2. Commands and examples
 - (a) Regular command: *create•file*
 - (b) Mono-operational command: *make•owner*
 - (c) Conditional command: *grant•rights*
 - (d) Biconditional command: *grant•read•if•r•and•c*
 - (e) Doing “or” of 2 conditions: *grant•read•if•r•or•c*
 - (f) General form
3. Miscellaneous points
 - (a) Copy flag and right
 - (b) Own as a distinguished right
 - (c) Principle of attenuation of privilege

Module 5 (Reading: [1])

4. Attribute-Based Access Control Matrix
 - (a) Attributes
 - (b) Predicates
 - (c) Modified primitive operations
 - (d) Commands

Module 6 (Reading: *text*, §3.1–3.2; [2])

5. What is the safety question?
 - (a) An unauthorized state is one in which a generic right r could be leaked into an entry in the ACM that did not previously contain r . An initial state is safe for r if it cannot lead to a state in which r could be leaked.
 - (b) Question: in a given arbitrary protection system, is safety decidable?
6. Mono-operational case: there is an algorithm that decides whether a given mono-operational system and initial state is safe for a given generic right.
7. General case: It is undecidable whether a given state of a given protection system is safe for a given generic right.
 - (a) Approach: represent Turing machine tape as access control matrix, transitions as commands
 - (b) Reduce halting problem to it
8. Related results

- (a) The set of unsafe systems is recursively enumerable
- (b) Monotonicity: no *delete* or *destroy* primitive operations
- (c) The safety question for biconditional monotonic protection systems is undecidable.
- (d) The safety question for monoconditional monotonic protection systems is decidable.
- (e) The safety question for monoconditional protection systems without the *destroy* primitive operation is decidable.

References

- [1] X. Zhang, Y. Li, and D. Nalla, "An Attribute-Based Access Control Matrix Model," *Proceedings of the 2005 ACM Symposium on Applied Computing* pp. 359–363 (Mar. 2005); DOI: 10.1145/1066677.1066760.
- [2] M. Tripunitara and N. Li, "The Foundational Work of Harrison-Ruzzo-Ullman Revisited," *IEEE Transactions on Dependable and Secure Computing* **10**(1) pp. 280–309 (Jan. 2013); DOI: 10.1109/TDSC.2012.77.