TWC: Medium: Collaborative: Foundations of Application-Sensitive Access Control Evaluation†

PIs: Timothy L. Hinrichs, Adam J. Lee, Von Welch, Lenore Zuck

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

UIC UNIVERSITY OF ILLINOIS AT CHICAGO

Motivation

Historically, most formal comparison of access control schemes is rooted in some form of expressive power analysis

- Useful for separating schemes based on raw capabilities
- Provides little insight into practical utility of these schemes

Access control needs are not "one size fits all" and must be considered on a per-application basis‡

Our goal: Develop a formal suitability analysis framework that allows analysts to assess the access control needs of an application and determine the access control scheme that best meets their needs

‡ V.C. Hu, D.F. Ferraiolo, and D.R. Kuhn, *Assessment of Access Control Systems*, National Institute of Standards and Technology Report No. 7316, September 2006.

Problem Formalization

Hypothesis: We must consider two classes of suitability measures

- Binary assessments of expressiveness
- Ordered cost measures

Suitability Analysis: Given an access control workload W, a set of candidate access control schemes $S = \{S_1, \ldots, S_n\}$, a notion of safe implementation $\mathcal{I}$, and a set of ordered cost measures $C = \{C_1, \ldots, C_m\}$, determine:

i. The subset $S' \subseteq S$ of schemes that admit implementations of W that preserve $\mathcal{I}$
ii. The schemes within S' whose cost assessments relative to C are optimal within the lattice $C_1 \times \ldots \times C_m$

Intellectual Merit and Broader Impact

Goals and Expected Outcomes:

- Development of an application-sensitive suitability analysis framework
- Cost analysis tools and methods for assessing analyst-defined costs
- Automation tools based on formal methods techniques
- Comprehensive evaluation based on PKI scenario

Broader Impact

- Better understanding of applications' access control needs
- Enhanced ability to respond to evolving organizational needs
- Generalization to broader security workloads

Initial Two-Phase Analysis Framework

Expressiveness Analysis: Which schemes can implement this workload?
Cost Evaluation: How well do these implementations work?

1. State machine representations

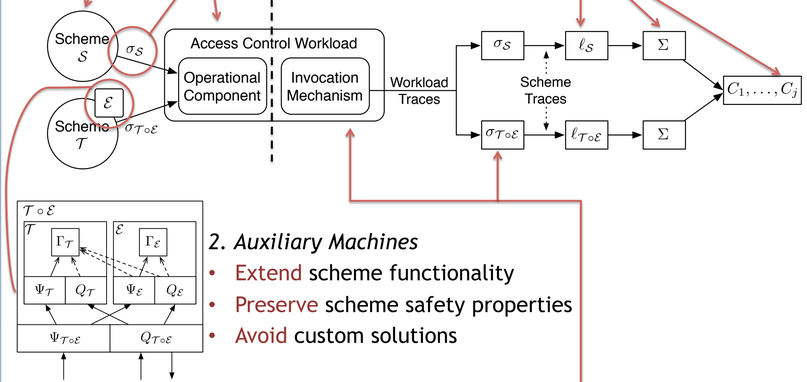
- Protection state (Γ)
- Queries to inspect state (Q)
- Commands to alter state (ψ)

3. Implementations

- Map workload machine to schemes
- Preserve user-defined safety properties ($\mathcal{I}$)
- Correctness proved via reduction

5. (Partially) ordered cost measures

- Encoded as ordered abelian monoids
- Represent many system- and human-centric costs
- Aggregated during trace exploration



2. Auxiliary Machines

- Extend scheme functionality
- Preserve scheme safety properties
- Avoid custom solutions

4. System utilization model

- User/daemon behavior via probabilistic actor machines
- Coordination and cooperation via constrained workflows
- Workload traces mapped to scheme traces via implementations
- Enables cost analysis via Monte Carlo simulation
- Simulation is fixed-parameter tractable, even with constraints

Case Study: Group Messaging System

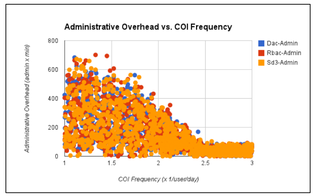
We study a group-centric information sharing system proposed by Krishnan et al. to highlight the importance of application-centric access control solutions.★ Of particular interest within this class of applications is the fact that the temporal properties required to handle various types of subscription and COI models are not handled well by existing approaches.

Cost Analysis Setup

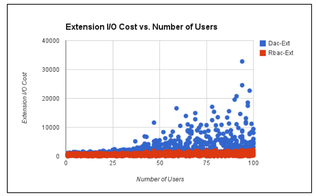
- *Schemes considered:* DAC, GTRBAC, RBAC, SD3-GM
- *Independent variables:* users, admins, user/admin ratio, COI rate, message post rate
- *Initial cost analysis:* Extension I/O overheads, Administrator overheads

Interesting Findings:

- DAC, RBAC, and GTRBAC require extensions to implement this workload
- Despite several types of temporal capabilities, GTRBAC does not enable a more efficient implementation than RBAC



COIs limit more administratively expensive tasks



Extension operations are user-related, not COI related

★ R. Krishnan, R. Sandhu, J. Niu, and W.H. Winsborough, *Foundations for Group-Centric Secure Information Sharing Models*, ACM Symposium on Access Control Models and Technologies (SACMAT), June 2009.

Ongoing and Future Work

σ $\mathcal{I}$

Alternate notions of implementation and safety

Evaluation and refinement using broader case studies

Automation tools and techniques

Generalize framework to support broader security workloads

† CNS-1228697 (University of Pittsburgh), CNS-1228947 (University of Illinois at Chicago), and CNS-1228668 (Indiana University)

Award Period: September 2012 - August 2015