Information Visualization for Rule-based Resource Access Control

Jaime Montemayor, Andrew Freeman, John Gersh, Thomas Llanso, Dennis Patrone
The Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, MD 20723 USA
1 443.778.4497
jaime.montemayor@jhuapl.edu

ABSTRACT
A conventional approach to protecting sensitive information is to use different and unconnected physical networks. However, physical separation complicates data sharing and information fusion. Recently researchers have begun to introduce ways to reunify disparate systems while providing sophisticated access control mechanisms, for example through rules. Rules offer flexibility and protection at varying levels of control granularity, but the resulting complexity can quickly overwhelm the resource access control administrator. In this paper we suggest various information visualization techniques that may help the administrator more quickly to gain situational awareness of interactions among the access control rules.

1. INTRODUCTION
Today, a direct approach to protecting sensitive data from unauthorized access has been to physically separate and isolate data by attributes like security classification. A main reason for this drastic approach is that we simply do not trust today's hardware or software to protect these resources in a multi-level system. As long as we can guarantee that physical access to the system is granted only to authorized users, our worries only involve the trustworthiness o f those users.

This data isolation, however, comes at a great cost. Data sharing and fusion (that is, "connecting the dots") become difficult, if not impossible. Furthermore, physical networks take up space, consume power, and are costly and time-consuming to set up and maintain. This problem is exacerbated when the networks are temporary, designed to operate only during the life of an activity. These and other reasons, have motivated researchers to consider solutions that can collapse the different networks and reunify the data. The data, though, must still be protected from unauthorized accesses. Rule-based access control schemes are one method for allowing administrators to specify resource access conditions at any levels of control granularity (e.g. [5]).

However, the availability of rich access control expression has a downside. As administrators take advantage of rich policy specifications, they may create collections of access control rules that, when combined with rules authored by others (e.g., rules at higher levels in an organizational structure), become difficult to comprehend in their totality. Confusions about these complex rule interactions could be costly. Bellotti, for example discusses concerns over privacy issues in collaborative computing environments [2]. Effective visualization tools are a powerful mechanism to enable policy enforcement administrators to more readily understand access control policies, rules, and their combinatorial effects. We are investigating the enhancement of *access control situational awareness* through visualizing resource requests, *in the context* of the rules that are in effect.

Thus, we want to design tools to provide: 1) simple and direct situational awareness of system-wide access control behavior, and 2) concise representation of questions and analyses by the user, such as, "*What group has access to which files during what time duration*?" "*If I implement this policy, what conflicts will result*?" "*If I change this policy/rule, what conflicts will result, and when*?"

2. RELATED WORK
While there exist many access control models (e.g. [6]), a wealth of literature on visualization (e.g. [3], [6]), and some graph-based visualization of access control rules (e.g. [8]), approaches to access control tend to be theoretical, in which graph depiction is used to show consistency or conflicts in rules within models. Few user-interaction systems have been designed with the combined knowledge from these domains to assist the user in managing access control policy (e.g. [4]).

3. FORMATIVE WORK
Our formative research (including literature review, interviews with system administrators, and conversations with researchers in the security and privacy domains) revealed that, as far as we know, few, if any, efforts focus on mitigating access control situational awareness problems of the administrator. There has been significant work on formal models to represent access control, secured transmission of data, transformation of natural language policies into machine understandable and enforceable commands [4], and privacy of users, but little on supporting the *use* of such techniques in operational situations. System administrators, charged with safeguarding highly personal and sensitive data, still rely heavily on text-based tools (e.g. the unix command *grep*) and often rely on communication technology, such as instant messaging, email, and phone, to enlist the help of other administrators and experts [1].

We have developed a prototype, RubaViz [7], with two design goals: 1) offer multiple visual representations, since no single visualization technique can adequately represent the different, but complementary, perspectives needed by the administrator to understand the interactions and effects of the rules; and 2) instead of discarding trusted current practices, whenever possible, enhance the "ground truth" (even when represented as text) with visualization/diagrammatic cues. We show three user interfaces

from RubaViz below. The graphical explorer (Figure 1) constructs a diagram for the administrator as he or she explores subjects (people or processes), resources, and groups of them. (left side of the window). The administrator's interaction with graphical representations of these items causes the incremental construction (information-on-demand) of a diagram that depicts connections from subjects to resources that are allowed by rules within policies. The access matrix (Figure 2) depicts a typical resource access grid, with the requester and the resource (or groups of them) defining the axes. The matrix view, as do the other views, supports dynamic queries: user selection of individual requesters, resources, or groups immediately changes the contents of the matrix.

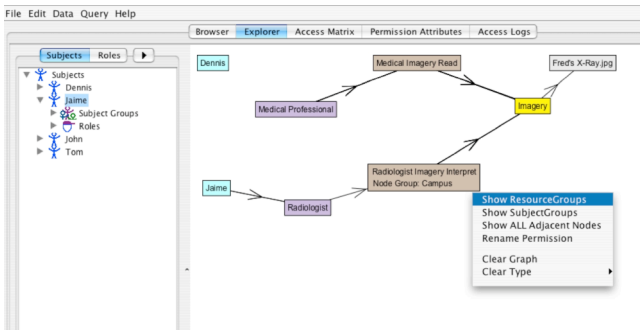

Figure 1: A graphical explorer. Here, we see that Jaime, in the role of the Radiologist, has access to the Fred's X-Ray.jpg resource via the Radiologist Imagery Interpret rule.

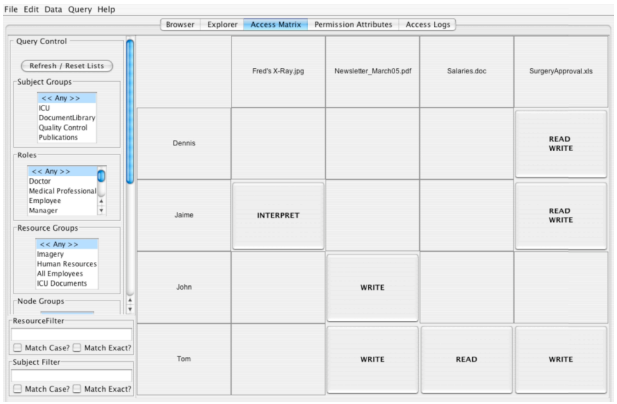

Figure 2: The access matrix shows a typical view of resource access grid, defined by the requester and the resource axes. The content can be controlled by dynamic filter controls, on the left side of the window.

Figure 3 shows a user-selected access event in a log file. Selection of the event generates a graphical representation of the rule-path that exists from the requester (Tom) to the resource (Newsletter_March05.pdf). This representation answers a question about *why* access was granted in a particular case.

So far, our focus has been on access control tasks (*what* and *why* a resource was granted). An administrator might also be interested in management tasks, such as resource allocation. A simple and effective way to depict usage might be to vary the size (or thickness) of graph elements to represent access frequency.

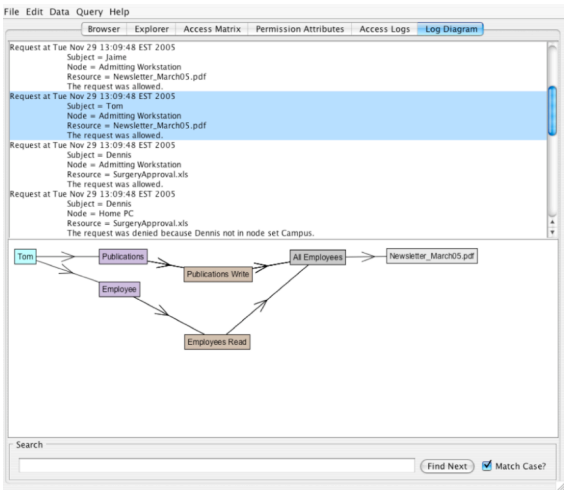

Figure 3: Tom is granted access to Newsletter_March05.pdf because he is an Employee in the Publications group. The Employees Read rule allows access to those groups

4. ACKNOWLEDGMENTS

The work described here was supported by JHU/APL's Independent Research and Development program.

5. REFERENCES

[1] Barrett, R., Kandogan, E., Maglio, P. P., Haber, E., Takayama, L. A., and Prabaker, M. Field Studies of Computer System Administrators: Analysis of System Management Tools and Practices. In Proceedings of Computer Supported Cooperative Work. pp 388-395, 2004.

[2] Bellotti, V., What You Don't Know Can Hurt You: Privacy in Collaborative Computing User Involvement. In Proceedings of the HCI'96 Conference on People and Computers XI. p.241-261, 1996.

[3] Botafogo , R. and Shneiderman B., Identifying aggregates in hypertext structures. In Proceedings of Hypertext '91, pp 63-74, New York, December 1991.

[4] Brodie, C., Karat, C., and Karat, J., Usable Security and Privacy: A Case Study of Developing Privacy Management Tools. In Proceedings of the Symposium On Usable Privacy and Security, 2005.

[5] eXtensible Access Control Markup Language (XACML), http://www.oasis-open.org/committees/xacml/repository/cs-xacml-specification-1.1.pdf. Specification as of August 7, 2003.

[6] Herman, I., Melancon , G., and M. S. Marshall, Graph Visualization and Navigation in Information Visualization: a Survey. In IEEE Transactions on Visualization and Computer Graphics, 6(1), pp. 24-43, 2000.

[7] Montemayor, J., Freeman, A., Gersh, J., Llanso, T., and Patrone, D., An Information Visualization Software System to Manage Resource Access Control. Applied Physics Laboratory intellectual property disclosure sheet, 2005.

[8] Nyanchama, M. and Osborn, S., The role graph model and conflict of interest. In ACM Transactions on Information and System Security, Vol 2, No. 1, pp 3-33, 1999.