METAPOLICIES AND CONTEXT-BASED ACCESS CONTROL

Ronda R. Henning
Harris Corporation, 1025 W. NASA Blvd, Melbourne, FL, 32904, US

Keywords: Access Control, Context-Based Access Control, Security Policy

Abstract: An access control policy mediates access between authorized users of a computer system and system resources. Access control policies are defined at a given level of abstraction, such as the file, directory, system, or network, and can be instantiated in layers of increasing (or decreasing) abstraction. In this paper, the concept of a metapolicy, or policy that governs execution of subordinate security policies, is introduced. The metapolicy provides a method to communicate updated higher level policy information to all components of a system; it minimizes the overhead associated with access control decisions by making access decisions at the highest level possible in the policy hierarchy. This paper discusses how metapolicies are defined and how they relate to other access control mechanisms. The rationale for revisiting metapolicies as an access control option for federated enterprise architectures is presented, and a framework for further research in metapolicy use as a context based access control representation is described.

1 INTRODUCTION

The phrase security policy has been used to address the protection mechanisms employed to protect an organization's assets from potential misuse. In reality, a security policy is composed of several sub-policies: accountability, authentication, contingency, and access control. The access control policy defines how system users interact with the data stored within the system. In most access control models, access control is defined as a triple consisting of the <subject, object, privileges> associated with a given data container, for example, a file or a row in a database. In the early days of computing, much discussion surrounded how access control models should be represented in computer systems. (Schell, 1979) developed the notion of multilevel mode of operations, stating:

In multilevel mode, the computer must internally distinguish multiple levels of information sensitivity and user authorization. Internal Controls of hardware and programs must assure that each user has access to only authorized information.[1]

The concept of Role-based access control (RBAC) was introduced by (Ferraiolo, 1995; Schell, 1979) and (Sandhu,et al 1996) to more accurately model the workings of a commercial enterprise. In RBAC, access control is based on a four-element set (user, group, object, privileges). A user may belong to many groups, each with a different privilege set. In the worst case model, every user has their own group, and there are as many groups to administer as there are users. In (Ferraiolo, 1995) a role is defined and centrally administered within an organization. However, with the flexibility of RBAC, there are some limitations. In a distributed network centric enterprise, it may take several hours to confirm the update of an application's access control roles. Because several applications may use their own security services instead of the centralized security services of the operating system, it may be difficult to determine whether an access control policy has been completely administered. In fact, it may well be that RBAC in a distributed enterprise can violate the three primary engineering principals of security reference monitors:[2]

1. Completeness – that the policy is invoked on every access to data
2. Isolation – the security mechanism is protected from unauthorized modification
3. Verifiability – the policy must be small and simple for complete test and verification.

There are times when an event may occur that requires comprehensive pre-emption or revocation of an RBAC policy. (Hosmer, 1991) presented the notion of a *metapolicy* to address instances of arbitration among diverse domains implementing

R. Henning R. (2005).
METAPOLICIES AND CONTEXT-BASED ACCESS CONTROL.
In *Proceedings of the Seventh International Conference on Enterprise Information Systems*, pages 355-359
DOI: 10.5220/0002579203550359

disparate security policies. In this paper, the use of a metapolicy to address immediate access control policy changes for an enterprise is presented. .

2 RELEVANCE AND SIGNIFICANCE OF TOPIC

This section discusses the various research and standards about access control policies, with an emphasis on relevancy to the concept of metapolicy formulation and implementation.

2.1 Related Work

In (Hosmer, 1991) the concept of a metapolicy was introduced. A metapolicy is a policy about other policies, the rules and assumptions about the policies, and explicitly states the coordination of interaction among policies rather than implicitly leaving such coordination to the administrators[3]. Hosmer's interpretation was that a metapolicy would address how diverse policies would interact across domain boundaries, how data could be updated across domains, and how precedence could be determined and ambiguity removed. As a way to address multiple security goals or the needs of different organizations with their own policy intentions, the provision was made for multiple policies. The constraints on support for multiple metapolicies were that each metapolicy had its own:

- Source or owner,
- Enforcement authorities, which could be different from the source, and
- Evolutionary timeframe[4].

Metapolicies were envisioned as being flexible, potentially layered, tamperproof, and providing a controlling representation of the organization, system, or security policy it represented. In (Hosmer, 1993), the concept of a *multipolicy paradigm* was presented[5]. A key use of multipolicies was for changing circumstances, for example when a country moves from peace to war. The emphasis was on explicit statements of interaction, such that multiple policies could be formally specifiable and subject to verification of tamper-resistance, the very characteristics Schell presented as desirable for a security kernel's architecture.

In (Bell, 1994), the author discussed modeling an instance of a "Multipolicy Machine" and described 4 levels of abstraction associated with a given security policy:[7]

1. an organization abstraction, written as a narrative, for people to read;
2. a conceptual abstraction, discussing an organizational policy at the concept level;
3. an abstract level, describing the design and tracing the conceptual requirements; and
4. an implementation level, describing the design as developed.

(Baskerville, 2002) addressed the concept of an information security meta-policy for an organization, and the characteristics of such a meta-policy. Security is considered a facilitating capability, not a hindrance, and there is recognition that access control policies change over time. Metapolicies, in this discussion, must possess the attribute of political simplicity, and be criterion-oriented: that is, they must be comprehensible and produce a measurable result[8]. In essence, these metapolicies require an explicit statement of the subjects' capabilities for accessing data objects, and the rules for granting access that will be enforced with the metapolicy.

3 BARRIERS AND ISSUES

3.1 Definition of Context

The dictionary definition of the word "context" is the circumstances or events that form the environment within which something exists or takes place (Press, 2004). Describing the general context of an application would be an infinite problem, as there are always new observations or attributes to incorporate into the context. In (Covington, 2002) the environmental roles are defined as the security relevant aspects of the environment. Covington further emphasizes that environmental roles are used to maintain uniformity across a diverse environment. Further, the sensors, those devices that monitor the environmental conditions, must be authenticated and the integrity of the sensor data guaranteed, or the environmental policy components could be compromised[9].

(Strembeck, 2004) states that "every goal and obstacle can be used to define a context condition and can map to a concrete access control service." It becomes necessary, then, to have an environmental

model in mind prior to exploring a context-based security policy[10].

3.2 Conflicting Policies

(Wang, 2004) discusses the issue of policy reconciliation in heterogeneous environments[11]. The notion of a reconciliation algorithm is introduced to find a security policy that consistently adheres to the security policies of all participating domains. Wang's model applies acyclic graph theory to model the security mechanisms employed by various environments to provide a framework for policy an analysis. Further, the use of acyclic graph theory exposes commonalities in policy and countermeasures to provide an efficient reconciliation method (linear in size v. N-P-complete).

3.3 The existence of supporting modeling tools and concepts

(Jaeger, 2001) and (Jaeger, 2003) discuss the concept of safety in access control models. A *safe access control model* is one in which a given access control will not inadvertently leak access rights to unauthorized persons[12]. Safe models require restrictive security policies, namely policies that apply constant values as constraints, because variable constraint-based policies are difficult to administer. Jaeger also applies graph theory to design comprehensible security policies.

(Bertino, 2001) presents a framework for logical reasoning about access control models. In this framework, access control models are modeled in the C-datalog language to develop a common basis for comparison.

3.4 The existence of more robust security models

The last 10 years have brought the concepts of Usage-controlled models (UCON)[13], Type Enforcement, and other security models that provide a more granular model of access control interactions. In the past, access decisions were binary, validated on an as-needed basis, with the access maintained for the life of the session. The UCON model allows access rights to change during the life of a session, treating access as a consumable, specifiable event that can exist for a single object access or all attempted object access instances within a session.

4 SYNTHESIS & METHODOLOGY

The basic research and technology experimentation required for defining and applying the security context of an application and its information was not available. As (Brézillon, 2004) states, context was very rarely used explicitly for a security specification. Since the security metapolicy concept was first presented, both security modelling and the analysis tools to support replicable mathematical results have matured considerably. The fundamental computing models in place when metapolicies were first proposed evolved into the distributed and federated "systems of systems" architectures of today. In distributed and federated computing models, the use of an overarching policy for queue management or asset allocation is a more accepted concept.

4.1 Characterization of User Data

In FIPS Publication 800-73 (Draft) (U.S. Government, 2005), the requirements for user access information associated with user security credentials are defined. These credentials govern all Federal physical and logical access systems, and were mandated by Presidential Homeland Security Directive 12.[14] Beyond the specifications of the access information; there is a requirement in FIPS 800-73 to apply X.509v3[15] digital certificates for user attribute information. This digital certificate information establishes an individual's unique digital identity, and is normally maintained in an X.500[16] directory for rapid application access. The user attributes as defined in X.509v3[17] certificates and in FIPS Pub 800-73 define the user data available to support this research.

4.2 Characterization of System Data

The Government Information Security Reform Act (GISRA) (Government, 2001) mandates the existence of an enterprise architecture document for any critical infrastructure system in the U.S. Government. The enterprise architecture document enumerates the security attributes associated with an infrastructure system. For a representative critical infrastructure, these attributes will be used to provide the system security data available for use to a metapolicy mechanism.

4.3 Definition of the System Context

Using the system data derived from the enterprise architecture, and the user data derived from the

X.509v3 certificate and access card specifications, define the information that is used to define the security context. This data becomes the formal definition of the security context for the purposes of this research and for use by the metapolicy in access decisions.

4.4 Definition of a Metapolicy structure

With the system security context defined, an information structure for the metapolicy must be created. In (Abadi, 1993), a calculus for access control in distributed systems is defined. To be effective a metapolicy must be created, administered, and enforced. This phase of the research defines a narrative notation for the metapolicy, addressing the definition of:

- subjects, or users of the system;
- objects, or items upon which the policy will act; and
- operations, or privileges associated with the policy.

The result of this phase is a structured set of defined actions that describe the behavior of the metapolicy, written for a human audience. The goal is to express the model in comprehensible terms to obtain understanding of the mechanisms of the metapolicy.

4.5 Modeling of the Metapolicy

Using the modelling techniques developed in (Abadi, 1993) and (Bell, 1994), a logical mathematical model of the narrative metapolicy will be defined. This will allow analysis of the metapolicy for safety, and logical soundness. Set theory and mathematics will be employed to provide a logical basis for metapolicy interaction.

During this phase of the study, a taxonomy of environmental factors that may impact a metapolicy will be defined. This taxonomy will be extended and modified to create a modified taxonomy appropriate for the metapolicy. Once this taxonomy is in place, Bayesian belief networks will be used to model the impact to the metapolicy that could be anticipated in the event a given node would be defined as being in a vulnerable state. Finally, decision tree analysis will be applied to determine combinations of metapolicy states that could result in unsafe conditions.

4.6 Determine a Delivery Protocol

The metapolicy needs to be propagated to the nodes within a network. An analogous model would be the use of Certificate Revocation Lists (CRLS) in X.509 Public Key Infrastructures (PKI). This task will examine the feasibility of developing a similar model for metapolicy propagation. The CRL processing model is used because it does not require immediate propagation to all nodes in a network, but is propagated as nodes/users join the system. That is, the nodes receive the updated metapolicy when they join the network and validate that the policy in force is valid.

5 SUMMARY AND FUTURE WORK

This paper has presented the concept of metapolicies, and their potential contribution to access control in distributed and federated system architectures. The relationship of this technique to existing access control models has been explored, as have the barriers to implementation that existed when the concept of metapolicies were first introduced. As security models have matured, so have computer architectures and artificial intelligence-based analysis techniques. The next steps in the research are to explore the logical basis of metapolicies and determine an appropriate protocol design for establishment, administration, and propagation of these policies in a network-centric environment.

FOOTNOTES

[1](Schell, 1979) p.20.
[2]Ibid, p. 29.
[3] (Hosmer, 1991) p. 2.
[4] Ibid. pp. 4-5.
[5] (Hosmer, 1993) p. 1
[6](Bell, 1994) p. 2.
[7] (Baskerville, 2002) p.341
[8] (Strembeck, 2004) p.p. 395-396.
[9] (Covington, 2002) pp.12.
[10](Strembeck, 2004) p. 400.
[11] (Wang, 2004) p. 1
[12] (Jaeger, 2001) p. 158.
[13] (Sandhu, 2004)p . 1.

[14] Homeland Security Presidential Directive 12 (HSPD-12), 27 August 2004.

[15] ITU-T X.509 (formerly CCITT X.509) or ISO/IEC/ITU 9594-8,X.509v3, 1996.

[16] ISO/IEC 9594-1:1993, X. 500, 1991.

REFERENCES

Abadi, M. B., et al (1993). A calculus for access control in distributed systems. *ACM Transactions on Programming Languages and Systems, Vol. 15*(No. 4), 706-734.

Baskerville, R., and Siponen, Milo. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, Vol. 15*(No. 5/6), 337-346.

Bell, D. E. (1994, February 1994). *Modeling the "multipolicy machine".* Paper presented at the New Security Paradigms Workshop, Little Compton, RI, US.

Bertino, E. C., et al (2001, 3-4 May, 2001). *A logical framework for reasoning about access control models.* Paper presented at the SACMAT'01, Chantilly, VA, USA.

Brézillon, P., and Mostéfaoui, Ghita Kouadri. (2004). *Context-based security policies: A new modeling approach.* Paper presented at the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW'04).

Ferraiolo, D. and. Kuhn., D.M. (1995, October 1999). *Role-based access controls.* Paper presented at the Fifteenth Annual National Computer Security Conference (NCSC), Baltimore, MD.

Gligor, V. (1995). *Characteristics of role-based access control.* Paper presented at the Proceedings of the first ACM Workshop on Role-based access control, Gaithersburg, MD, USA.

Government, U.S. (2001) Defense Authorization Act, Government Information Security Reform Act (GISRA), U.S. Congress, 106 Sess.(2001).

Government, U. S. (2003). The 9/11 commission report, final report of the National commission on terrorist attacks upon the United States. New York, NY: W.W. Norton & Company Inc.

Hafmann, U.; and Kuhnhauser, Winfried. (1999). Embedding security policies into a distributed computing environment. *SIGOPS Operating System Review, Vol. 33*(No. 2), pp. 51-64.

Han, Y. F., Liu; Hong, Zhang. (2000). An object-oriented model of access control based on role. *ACM SIGSOFT Software Engineering Notes, Vol. 25*(No.2), 64-68.

Hosmer, H. H. (1991, 3 December 1991). *Metapolicies I.* Paper presented at the ACM SIGSAC Special Workshop on Data Management Security and Privacy Standards, San Antonio, TX.

Hosmer, H. H. (1993). *The multipolicy paradigm for trusted systems.* Paper presented at the New Security Paradigms Workshop, Little Compton, RI, US.

Jaeger Trent, et al (2003). Policy management using access control spaces. *ACM Transactions on Information and System Security (TISSEC), Vol. 6*(No. 3), 327-364.

Jaeger, Trent. Treadwell., Jonathon. (2001). Practical safety in flexible access control models. *ACM Transactions on Information and System Security, Vol. 4*(No. 2), pp. 158-190.

International Committee for IT Standards/ANSI. (2004). *Information technology -- role based access control*: ANSI/INCITS.

Park, J. S.; et al (2004, 2-4 June). *A composite RBAC approach for large, complex organizations.* Paper presented at the SACMAT'04, Yorktown Heights, NY, U.S.

Press, Microsoft. (2004). Microsoft Encarta dictionary for Office 2003, Windows XP edition.

Sandhu, R. (2004). *A logical specification for usage control.* Paper presented at the Proceedings of the ninth ACM symposium on Access control models and technologies, Yorktown Heights, New York, USA.

Sandhu, R. et al (1996). Role-based access control models. *IEEE Computer, Vol. 29*(No. 2), pp. 38-47.

Sandhu, R.;et al (2000, 26-27 July 2000). *The NISTt model for role-based access control: Towards a united standard.* Paper presented at the Fifth ACM Workshop on Role-based Access Control, Berlin, Germany.

Schell, R. R. (1979). Computer security -- the Achilles' heel of the electronic air force. *Air University Review, Vol. XXX*(No. 2), pp. 16-33.

Strembeck, M. &. N., Gustaf. (2004). An integrated approach to engineer and enforce context constraints in RBAC environments. *ACM Transactions on Information and System Security, Vol. 7*(No. 3), 392-427.

U.S. Government, National Institute of Standards and Technology. (2005). *NIST special publication 800-73, interfaces for personal identity verification* (Draft Standard), 31 January 2005 Washington, DC: Department of Commerce.

Wang, H. J.,et al (2004). *Security policy reconciliation in distributed computing environments.* Paper presented at the Fifth IEEE International Workshop on Policies for Distributed Systems and Networks (Policy'04).