Trends in Access Control

Thomas Groß
IBM Zurich Research Laboratory
tgr@zurich.ibm.com

Anthony Moran
IBM Software Group
morana@us.ibm.com

Abstract

Access control mechanisms have until now protected relatively static resources in static environments. However with the increased development in large-scale applications, new forms of access control are starting to emerge. At this turning point, we face the problem that prior research does not address the current evolution in the industry and that there is an increasing gap between well-investigated areas in research and common practices in access control products. This paper identifies three major goals of ongoing trends, and surveys existing industrial access control technology to reveal the status quo.

1 Introduction

Extranet access control products protect resources within a company's intranet against unauthorized access from the external Internet. In the past, these products have evolved to cater for access control for relatively static resources in static environments. Initiated by business scenarios from e-commerce and e-banking as well as the increased development in large-scale applications, new forms of access control are starting to emerge.

Based on the feedback of IBM Tivoli's access control product department, we identify three of the major goals that are associated with this trend: dynamical authorization, identity federation, and inclusion of emerging message formats.

- Dynamical authorization refers to the capability of involving real-time data in the policy evaluation.
- Identity federation means the capability to manage federations of business partners and to map such federations in the exchange and assertion of identity information.
- Emerging message formats e.g. the Security Assertion Markup Language (SAML) or Web Services (SOAP).

We determine for each of these goals the progress extranet products have made to date, and discuss the ongoing trend.

The remainder of this paper is structured as follows: In Section 2, we introduce our approach to describe the status quo. We describe the particular goals and corresponding progress to date in Section 3. Section 4 contains a short conclusion of our discussion.

2 Describing the Progress to Date

Being in an industrial environment, it is difficult to find publishable, objective evidence for the current situation in the market. On the one hand, producers of access control systems only provide marketing-driven subjective information about their own products and their competitors. On the other hand, competitive or market analyses of third parties come with extensive non-disclosure agreements that prevent their excerpt in research publications.

Given this situation, we obtain the basis of our survey in an unorthodox manner. We use one of the latest published quadrant analyses [11] to identify the current market leaders in the extranet access management market. We choose Netegrity SiteMinder [9], IBM Tivoli Access Manager for e-business [7], Oblix NetPoint [10], and RSA ClearTrust [13] as representatives for the market. We describe the progress to date on the basis of their properties.

3 Goals and Status Quo

In this section, we present the three goals we identified and the corresponding progress to date in the extranet access control market.

3.1 Dynamical Authorization

The goal of dynamical authorization is: *Allow dynamical policy evaluation over arbitrary real-time data.* Such a dynamic access control decision is dependent on the

power of the policy language and the kinds of Access Decision Information (ADI) involved. We provide an overview of the three common methods used in access control products:

Static access control matrix: All access control products considered by our analysis provide a format to define an Access Control Matrix (ACM) [14] containing users, resources and actions. While some products use Access Control Lists (ACLs) to express the matrix, the specification mechanisms of other products are not powerful enough to specify all aspects of an ACM. In general, such an ACM is evaluated over static ADI.

Context-dependent conditions: Some access control products such as the Tivoli Access Manager allow an administrator to attach simple conditions to protected resources. These conditions evaluate dynamic ADI, but are restricted in their complexity and to ADI that is strongly related to the context of the access control decision (e.g. the current time).

Rules: Netegrity SiteMinder, RSA ClearTrust, and Tivoli Access Manager let the administrator specify predicates over dynamic ADI. Their implementations differ in the complexity of the rules and the variety of the ADI types involved. According to [13], RSA ClearTrust's Smart Rules are based on dynamic user profile data, which have to be imported in the user database. Netegrity SiteMinder's eTelligent Rules [9] enable any contextual data to be dynamically included in the authorization decision. Tivoli Access Manager [7] also supports rules that use dynamic context- or user-dependent data.

Discussion: Static access control is a good complement to the dynamic approaches, as it is well-investigated and is typically significantly faster than evaluating rules. It is advantageous that one can easily predict and audit static access control decisions. Still, static access control is not powerful enough to solve all kinds of customer scenarios.

Rules have the benefit of being dynamic in nature and can react to more real-world authorization scenarios. They allow administrators to combine various kinds of ADI and to formulate complex policies in a few statements. While none of the presented access products supports role-based access control (RBAC) out-of-the-box, one can implement RBAC by leveraging rules. Nevertheless, utilizing rules and real-time data makes it hard to obtain a snapshot of the state of the access control product. It is especially difficult to reproduce incorrect decisions of the access control system.

To maximize the impact of the rules evaluation, a dynamical retrieval of real-time ADI is necessary. Therefore, the trend towards dynamical authorization will support the development of protocols for attribute exchange and provisioning such as [3, 6, 12].

3.2 Identity Federation

The goal of identity federation is: *Simplify identity management in a cross-enterprise environment*.

We consider the following classes of federation:

Intra-site single sign-on: We merge two types of single sign-on (SSO) into this class. We include products that allow SSO within their site or provide inter-site SSO where each participating site needs to be managed by the same access control product. The Tivoli Access Manager [7] belongs to this group, as this product mainly uses the non-standardized e-Community Single Sign-on (eC-SSO) and Cross-Domain Single Sign-on (CDSSO).

Inter-site single sign-on: While Netegrity, Oblix, and RSA claim that their products support the Security Assertion Markup Language (SAML) [3] directly as message standard for authentication, the Tivoli Access Manager enables integration with several SAML toolkits. In general, the SAML support implies vendor interoperability and thus the capability of inter-site SSO.

Federated Identity Management (FIM): This class exceeds pure SSO by attribute exchange, privacy and management capabilities. Currently, no access control product we considered claims to provide such functionality out-of-the-box. Nevertheless, Liberty [6] and Shibboleth [2] are two projects which attempt to define standards which characterize these types of infrastructures. Recently, several companies jointly published WS-Federation [8], a federation framework based on Web Service technology that is not restricted to SAML assertions or other specific token types.

Discussion: Standardized protocols like SAML are supported by leading players in the extranet access control market. Still, the few federations that are built on these technologies only focus on Web-SSO.

Considering the efforts to establish standards and industry projects in this area, we believe that federated identity management is imminent. It is likely that industry players will firstly focus on intra-business federations, as there is less complexity involved. Business-to-business scenarios where existing contracts for "legal" trust can be leveraged may also be of initial interest.

To implement full Federated Identity Management, problems in the areas of policy exchange, privacy and trust still need to be solved. Policies may need to be compared or converted into other formats retaining their semantics. Privacy needs to be maintained across company sites and multiple software components. Trust relationships need to be defined and formalized. All the challenges above belong to a common super class: Federated Policy Management. Currently there are no solutions emerging from the industry to solve these issues.

3.3 Include Emerging Message Formats

The section addresses the goal to: *Enable extranet access control products to act as point of contact for emerging message formats and to provide authentication and authorization for them*.

Traditionally, extranet access control products analyze communication based on HTTP [4]. As HTTP is a popular binding for other message formats, access control products inherently come in contact with these types of communication. An evolution in these access control products is inevitable as these higher-level protocols become more abundant. Here we introduce three interesting message formats in this area:

SOAP: The Simple Object Access Protocol (SOAP) [1] is an extensible message format that is usually bound to HTTP. The SAML as well as the WS Security family have strong dependencies to SOAP.

SAML: The SAML message standard [3] also focuses on extensibility and is concerned about authentication, authorization, and attribute exchange. All considered access control products claim to use SAML assertions to exchange dynamical ADI and therefore consume SAML tokens.

Web Services: Web Service messages are used for remote method invocation. The emerging Web Service Security [5] framework extends SOAP to protect messages with cryptography and to attach security tokens to them.

Discussion: We observe that Web-Services and SAML are becoming prevalent in emerging technologies. These standards, along with related yet-to-be-announced standards are likely to play an important role in Federated Identity Management. Therefore, access control products will benefit from understanding and interpreting these message formats, tokens and associated protocols.

Such profiles can be considered as a new protocol class with the following characteristics: The protocols are modular and highly extensible. Their security aspects are not specified in cryptographic protocol schemes, but in constraint-based standard documents. In addition, many of these protocols are zero-footprint, i.e. they involve a web browser as participating party, which is not aware of the protocol logic. These aspects hamper in-depth security analyses and render prior research analysis methodology somewhat inapplicable.

4 Conclusion

To reach the goals of dynamical authorization, identity federation and inclusion of emerging message formats, access control systems still have a long way to go. In each case, there are open issues that require the assistance of research.

References

[1] Don Box, David Ehnebuske, Gopal Kakivaya, Andrew Layman, Noah Mendelsohn, Henrik Frystyk Nielsen, Satish Thatte, and Dave Winer. Simple object access protocol (SOAP) 1.1, May 2000.

[2] Scott Cantor and Marlena Erdos. Shibboleth-architecture draft v05, May 2002.

[3] Phillip Hallam-Baker et al. Assertions and protocol for the OASIS security assertion markup language (SAML), 2002.

[4] Roy T. Fielding, Jim Gettys, Jeffrey C. Mogul, Henrik Frystyk, Larry Masinter, Paul Leach, and Tim Berners-Lee. RFC 2616: Hypertext transfer protocol – HTTP/1.1, June 1999. Status: Standards Track.

[5] Phillip Hallam-Baker, Chris Kaler, Ronald Monzillo, and Anthony Nadalin. Web services security: SOAP message security, 2003.

[6] Jeff Hodges and Tom Wason. Liberty architecture overview, 2003.

[7] IBM Corporation. IBM Tivoli Access Manager for e-business, 2002.

[8] Anthony Nadalin. Web services federation language (WS-Federation), 2003.

[9] Netegrity Inc. Netegrity SiteMinder features/benefits, 2003.

[10] Oblix Inc. Oblix NetPoint data sheet, 2002.

[11] J. Pescatore and R. Wagner. Extranet access management 2h02 magic quadrant. Technical Report M-18-9644, Gartner, Inc., 2003.

[12] Birgit Pfitzmann and Michael Waidner. Privacy in browser-based attribute exchange. In *Proceeding of the ACM Workshop on Privacy in the Electronic Society*, pages 52–62, Washington, DC, 2002. ACM Press.

[13] RSA Security Inc. RSA ClearTrust data sheet, 2002.

[14] Ravi S. Sandhu and Pierrangela Samarati. Access control: Principles and practice. *IEEE Communications Magazine*, 32(9):40–48, 1994.