MIT Sloan School of Management

Working Paper 4259-02
October 2002

Directions for Web and E-Commerce Applications Security

Bhavani Thuraisingham, Chris Clifton, Amar Gupta, Elisa Bertino, Elena Ferrari

Directions for Web and E-Commerce Applications Security

Bhavani Thuraisingham	Chris Clifton	Amar Gupta	Elisa Bertino	Elena Ferrari
The MITRE Corporation		MIT	U. of Milano	
thura@mitre.org	clifton@mitre.org	agupta@mit.edu	bertino@dsi.unimi.it	elena.ferrari@uninsubria.it

Abstract

This paper provides directions for web and e-commerce applications security. In particular, access control policies, workflow security, XML security and federated database security issues pertaining to the web and e-commerce applications are discussed.

1. Introduction

For the effective operation of the web and e-commerce applications, security is a key issue. The security threats include access control violations, integrity violations, sabotage, fraud, privacy violations, as well as denial of service and infrastructure attacks. All of these threats collectively have come to be known as cyberwar or cyberterrorism. Essentially cyberwar is about corrupting the web and all of its components so that the enemy or adversary's system collapses. There is currently lot of money being investigated by the various governments in the US and Western Europe to conduct research on protecting the web and preventing cyberwars and cyberterrorism. In the book by Ghosh [7], an excellent survey of the various security threats as well as solutions have been proposed. As Ghosh points out, the web threats discussed here occur because of insecure clients, servers and networks. To have complete security, one needs end-to-end security; that means secure clients, secure servers, secure operating systems, secure databases, secure middleware and secure networks. There is a lot of emphasis these days on developing security solutions for clients, servers, databases, middleware, operating systems and networks. Programming languages such as Java and systems such as Microsoft's ActiveX are being made secure. Sophisticated encryption mechanisms are being developed for network security. Some of the security aspects are also discussed in [14].

While some of the underlying systems such as operating systems, the middleware, and databases have to be secure, it is also critical that the web applications have to be secure. These essentially include the database systems as well as the applications. The focus of our paper is to provide some directions for web and e-commerce applications security. We also include directions for related areas such as security for workflow management systems and secure federations. Note that this paper does not attempt to solve any web security problems or discuss any experiences and systems developed. However, some of the solutions, experiences, and systems are given in the references (e.g., [2] and [7]). Note also that various standards are evolving for web security. These include standards being developed by organizations such as the W3C and OMG (see for example, www.w3c.org and www.omg.org). Security for languages such as Java is also very relevant to the discussions on web security. A discussion of all of these issues is beyond the scope of this paper. We only discuss some of the key points.

2. Security Directions for the Web and E-Commerce Applications

2.1 Overview

Various aspects of security are relevant to e-commerce. These include database security, in particular federated database security, workflow security, role-based access control, e-commerce security and XML security. Various efforts have been reported in [13], [7], [2] and [5]. For example, in [13] multilevel security issues for federated databases are discussed. Many of these issues are relevant for access control in federated databases also.

By contrast, [21] provides an in-depth coverage of security for e-commerce systems. It described end-to-end security including security for clients and servers as well as transactions. One of the key issues here is how do you protect your assets while collaborating with other organizations. The idea is that each organization must have suitable methods and mechanisms for specifying which information it would like to share while collaborating with other organizations and which information is for internal distribution only. Moreover, we need the ability to specify, for data to be shared outside the organization boundary, which subjects are allowed access to the data and under which privileges. Relevant research efforts made in the field of federated and centralized databases can be exploited. However, there are also some differences between e-commerce and database management system environments that need to be taken into account, these are discussed in the following sections. Additionally, another key aspect in dealing with e-commerce and web security is providing security mechanisms for Workflow Managements Systems (WFMSs) [6]. WFMSs can be used to coordinate and streamline business processes of an organization or of a pool of collaborating organizations. A workflow separates the various activities of a given process into a set of well defined tasks. The various tasks in a workflow are usually carried out by several users according to the organizational rules relevant to the process represented by the workflow. An important issue is thus how to provide mechanisms to regulate the execution of the various tasks in a workflow, for instance tools for specifying authorization constraints on the set of users that can execute the various tasks in a workflow.

Thus we believe that, in addition to the security mechanisms proposed in [7], the main building blocks for secure e-commerce and web system from the point of view of applications are the following:

- Tools and mechanisms supporting the specification of access control policies suitable for the e-commerce environment
- Secure federations of collaborating organizations
- Secure Workflow Management Systems

In the following, we deal with all the above issues in detail.

2.2 Access control policies for e-commerce and the web

Various policies are needed to ensure that users access only the information they are authorized to. Although several efforts have been made [5] in the development of access control models for traditional database environments, the e-commerce environment is quite different from traditional database environments for which such models have been specified. The main difference is that e-commerce requires the ability to specify access control policies more expressive than those provided in traditional DBMSs. In conventional database environments access control is usually performed against a set of authorizations stated by security officers or users according to some security policies. An authorization in general is specified on the basis of three parameters < **u, o, p**>. This triple specifies that user **u** is authorized to exercise privilege **p** on object **o**. Such simple paradigm is not well suited for a dynamic environment like e-commerce that requires revisiting of such paradigm. Furthermore, in an e-commerce environment the resources to be protected are not only traditional data but also knowledge and expertise. Such peculiarities call for more flexibility in specifying access control policies. The access control mechanism must be flexible enough to support a wide spectrum of heterogeneous protection objects.

A second related requirement is the support for content-based access control. Content-based access control allows one to express access control policies that take the protection object content into account. This is an important requirement since very often protection objects with the same type and structure have contents of different sensitivity degrees. In order to support content-based access control, access control policies must allow one to include conditions against protection object content.

A third requirement is related to the heterogeneity of subjects which requires access control policies based on user characteristics and qualifications, rather than based on very specific and individual characteristics (e.g., user IDs). A possible solution, to better take into account user profiles in the formulation of access control policies, is to support the notion of *credential* [17]. A credential is a set of properties concerning a user that are relevant for security purposes (for example, age, position within an organization, projects a user is working on). The use of credentials allows the security officer to directly express relevant security policies in terms that are closer to the organizational structure. For instance, by using credentials, one can simply formulate policies such as “Only permanent staff can access documents related to the internals of the system”.

We believe that the XML language [18] can play a key role in access control for e-commerce applications. The reason is that XML is becoming the common representation language for document interchange over the web, and it is also becoming the language for e-commerce. Thus, on the one hand there is the need of making XML representations secure, by providing access control mechanisms specifically tailored to the protection of XML documents. On the other hand, access control information (that is, access control policies and user credentials) can be expressed using XML itself. The Directory Service Markup Language [19] provides a foundation for this: A standard for communicating with the directory services that will be responsible for providing/authenticating user credentials. This uniform representation of both protection objects and access control information has several benefits. First, access control policies can be applied to policies and credentials themselves. For instance, some credential properties (such as the user name) may be made accessible to everyone, whereas other properties may be visible only to a restricted class of users. Additionally, the use of an XML-based language for specifying credentials and access control policies facilitates secure credential submission and export of access control policies. Issues related to the protection of XML documents and to the use of XML to represent access control information are discussed in [2].

2.3 Secure Federations

Once each organization has a set of access control policies (possibly specified in XML) and a proper access con-trol mechanism in place, the next step is providing mechanisms for the interoperation of access control policies among various organizations. This ability is needed because if information and data must be shared across the organization boundaries, different local security policies have to be represented and integrated at a global level, to guarantee interoperability and to detect possible inconsistencies and security breaches. In this respect, several relevant research efforts have been carried out in the area of secure federated database systems (see for instance [4,8,12,15]). In most of these proposals, users can state which objects they wish to export at the global level. These objects are then used to build a single federated schema. Access control policies can be specified both at the global and local level, with some mechanism in place to check the consistency of access control information at the two levels.

Specifying and enforcing access control policies in a federated system is a difficult task. Information is duplicated, transformed, and otherwise derived from base sources – where possible, the access control policies should be derived as well. One approach (from the Data Warehouse world) is view security [20]. This approach splits *information* and *physical* permissions: Permission to access data on a particular system, and permission to access a particular piece of data, are separated. The question “Can user **u** access object **o** on system **s**?” is computed automatically based on the permissions. This saves the task of defining both local and global access permissions on the same object.

Credential-based access control can also simplify the integration task in that it provides a high-level representation of access control policies and a better qualification of authorization subjects. Moreover, the use of credentials offers a spectrum of options that can be used to integrate access control policies at the federated level. For instance, if a *tightly-coupled* approach is used, each site joining the federation agrees on a common credential scheme. In this case credentials are issued by trusted third parties and are evaluated at the global level against a set of access control policies expressed in terms of the global scheme of credentials. An alternative solution, that we refer to as *loosely-coupled*, does not require a global credential scheme. By contrast, each site has its own credential scheme that may differ from the scheme of the other sites. Such heterogeneity requires an additional step before performing access control, in that it is necessary to establish a mapping of the credentials associated with the user requesting the access onto the credential scheme of the site to which the access is required.

In a federated environment, different organizations may enforce different security policies. The differences between these policies have to be reconciled when corporations have to collaborate with each other on the web. Figure 1 illustrates security policy integration for e-commerce organizations. We have essentially used Thuraisingham's view of integrating security policies for federated databases [13]. Note that in the case of schemas, each organization may export schemas, which may be a subset of the schemas for the local organization. However, in the case of security policies, the export policies may be more restricted. That is additional access control mechanisms may be needed for foreign organizations to access data at another site. Policies are not restricted to security. They also include integrity policies and administrative policies. The differences between organizations have to be handled for all types of policies. The business rules discussed earlier may also be a type of policy. Note that this is similar to Sheth and Larson's approach to integrating federated schemas [11].

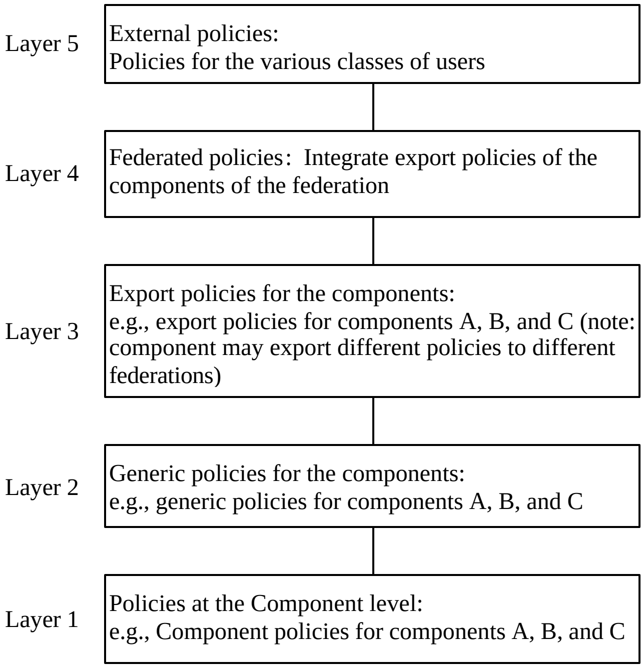
Layer 5
External policies:
Policies for the various classes of users
Layer 4
Federated policies: Integrate export policies of the components of the federation
Layer 3
Export policies for the components:
e.g., export policies for components A, B, and C (note: component may export different policies to different federations)
Layer 2
Generic policies for the components:
e.g., generic policies for components A, B, and C
Layer 1
Policies at the Component level:
e.g., Component policies for components A, B, and C

Figure 1. Policy Integration and Transformation

2.4 Secure Workflow Management Systems

Workflow Management Systems (WFMSs) have gained popularity both in research as well as in commercial sectors. WFMSs are used to coordinate the business processes of organizations and thus they represent one of the key components of e-commerce. With respect to security, one of the key aspects is that of developing suitable access control mechanisms for workflow applications. In what follows we review the most important features an access control mechanism for WFMSs must provide. A first requirement is the support for *credential-based access control* that we discussed in the previous section. A second requirement is the ability of expressing *authorization constraints* on user assignments to tasks. Such constraints must either be expressed on specific users (e.g., only user Bob can perform a specific task) or may involve credentials and credential properties (e.g., only senior managers can perform a given task). A typical authorization constraint, which is very relevant and well known in the security area, is *separation of duties* [10]. It aims at reducing the risk of frauds by not allowing any individual to have sufficient authority within the system to perpetrate a fraud on his own. Separation of duties is a principle often applied in everyday life. E.g., opening a safe requires two keys held by different individuals, approval of a business trip requires approval of the department manager as well as an accountant and a paper submitted to a conference requires review by three different referees apart from the author(s).

If no proper support is provided, constraints like separation of duties must be implemented as application code and embedded into the various tasks. Such an approach makes it difficult, if at all possible, the specification and manage-ment of authorization constraints, given also the large number of tasks that typically occur in a workflow.

A step in the direction of defining an access control model specifically tailored to the WFMS domain is the model presented in [3]. Such a model provides a logical language for defining constraints on user assignment to tasks in a workflow. Such constraint language supports, among other functions, both static and dynamic separation of duties. The model also provides formal notions of constraint consistency, and algorithms to check for the consistency of the constraints and to assign users to tasks that constitute the workflow in such a way that no constraints are violated.

Another relevant research direction is the casting of access control models for WFMSs in the context of the standard for workflow management systems developed by Workflow Management Coalition (WfMC) [16]. WfMC has defined a standard workflow reference model for the specification of business processes. With respect to access control, such reference model supports a role-based access control model. Roles [10], which bear many similarities with credentials, can be seen as a set of actions or responsibilities associated with a particular working activity.

Under role-based access control models, all authorizations needed to perform a certain activity are granted to the role associated with that activity, rather than being granted directly to users. Users are then made members of roles, thereby acquiring the roles' authorizations. Thus, an interesting research issue is the extension of the access control model defined by WfMC with innovative features, such as the authorization constraints previously discussed.

3. Summary and Directions

This paper has described direction for web and e-commerce security. We believe that the main building blocks for secure e-commerce and web applications are the following:

- Tools and mechanisms supporting the specification of access control policies suitable for the e-commerce environment
- Secure federations of collaborating organizations
- Secure Workflow Management Systems

One of the main questions we are asked often is what are the differences between securing say object models and XML documents. In fact we believe that many of the issues and challenges for securing object models apply for se-curing XML documents also. Furthermore we believe one could learn a lot from the work that has been carried out on securing object models (see for example, [1]) and learn from that experience in securing XML documents. In other words, we do not have to come up with entirely new mechanisms for securing the web. WE can use lot of the security mechanisms that have already been developed. Nevertheless there are cases where new solutions are needed and we need to explore these areas.

This paper has provided directions for research and development for each of the areas discussed above. There are several areas for further research. First of all, can we define a suitable security architecture for e-commerce? How can we handle differences with respect security polices for different organizations? What are the security concerns? What information management technologies need to be examined? How do we develop security standards for e-commerce? This paper has provided some initial directions in this area. We believe that there are plenty of opportunities for re-search and development for e-commerce and web security applications.

References

[1] Bertino, E. et al, Authorization Models for Objects, Proceedings of the OOPSLA Conference Workshop on Objects, Washing-ton DC, September 1993.

[2] Bertino E., Castano S., Ferrari E., and Mesiti M. Specifying and Enforcing Access Control Policies for XML Document Sources, World Wide Web Journal, Baltzer Science Publishers, 3(3), in press..

[3] E.Bertino, E.Ferrari e V. Atluri. The Specification and Enforcement of Authorization Constraints in Workflow Management Systems, ACM Transactions on Information and Systems Security, 2(1), 1999.

[4] W. Esmayr, F. Kastner, G. Pernul, S. Preishuber, and A. Min Tjoa. Authorization and Access Control in IRO-DB. In Proc. of the 12th International Conference on Data Engineering, New Orleans, Louisiana, 1996.

[5] Ferrari E., and B. Thuraisinham, "Database Security: Survey," Advanced Database Technology and Design by Artech House, 2000 (Editors: M. Piattini and O. Diaz)

[6] Georgakopoulos D., Hornick, M., and Sheth, A. "Overview of Workflow Management: From process Modeling to Workflow Automation Infrastructure, Distributed and Parallel Databases, 1995.

[7] Ghosh, A., "E-commerce Security, Weak Links, Best Defenses," John Wiley, NY, 1998.

[8] D. Jonscher and K.R. Dittrich. An Approach for Building Secure Database Federations, In Proc. 20th Conference on Very Large Databases (VLDB'94)}, Santiago, Chile, 1994.

[9] Morey, D., M. Maybury, and B. Thuraisingham, (Editors) "Knowledge Management" MIT Press, 2001.

[10] Sandhu, R. Role-based access control models, IEEE Computer, 1996.

[11] Sheth A., and J. Larson, "Federated Database Systems," ACM Computing Surveys, September 1990.

[12] M. Templeton, E. Lund, and P. Ward. Pragmatics of Access Control in Mermaid, Data Engineering Bulletin}, 10(3), 1987.

[13] Thuraisingham, B., "Security for Federated Database Systems, Computers and Security," 1994.

[14] Thuraisingham, B., "Web Information Management and Electronic Commerce," CRC Press, June 2000.

[15] C. Wang and D.L. Spooner. Access Control in a Heterogeneous Distributed Database Management System, In Proc. IEEE Symposium on Security and Privacy, Oakland, CA,1987.

[16] Workflow Management Coalition, The Workflow Model, TC00-1003, 1995. Available at http://www.w3.org.

[17] M. Winslett, N. Ching, V. Jones, and I. Slepchin. Using Digital Credentials on the World Wide Web, Journal of Computer Security, 7, 1997.

[18] Word Wide Web Consortium, Extensible Markup Language (XML) 1.0, 1998. Available at http://www.w3.org/TR/REC-xml.

[19] DSML Working Group, Directory Services Markup Language 1.0, December 1999. http://www.dsml.org.

[20] A. Rosenthal and E. Sciore, "View Security as the Basis for Data Warehouse Security", in Proceedings of the International Workshop on Design and Management of data Warehouses (DMDW'2000), Stockholm, Sweden, June 5-6, 2000.

[21] A.K. Ghosh. E-Commerce Security: Weak Links, Best Defenses, John Wiley & Sons, New York. January 1998