TDM: Enforcement of Security Management System for XML-Centric Electronic Commerce

Minji Kim and Younghee Lee

Information and Communications University (ICU)
58-4 Hwa-am Dong, Yuseong Gu, Daejeon, 305-732, Korea
{mjkim,yhlee}@icu.ac.kr

Abstract. There are many types of security that have been applied to secure Electronic Commerce nowadays. Mainstream security depends on equipment-based security mechanisms, which are a concern in terms of security issues as a whole. The necessity of strong security for Electronic Commerce has increased as a result of the whole process and the devices used. This thesis proposes an appropriate security management system TDM which is enforced security management system for E-Commerce. The idea of QoSS and a Threat-Adaptive Security Policy is examined in detail in order to apply a conceptual approach to the XML document which is a standard data format for data exchange including that of the Internet. An analysis of the existing system is used in order to suggest appropriate next-generation security management for XML document security. This work contributes to expanding existing security management in the XML document area in order to establish a flexible security policy.

1 Introduction

'E-Commerce[1]' has required an independent platform for easy data exchange among enterprises, private Netizens, and governments. As part of E-Commerce, the 'Web Service[2]' platform has been proposed as a means of overcoming system dependency. Therefore, the Web Service platform requires system-independent language in order to provide efficient data exchange.

It is a XML[3] that has a documented format, providing data exchange for any type of platform. Within the Web service, any participant can be a server or a client. The question of devices used is of no significance in terms of service contents and the relationship between service participants. The most important sector of the Web Service World is security such as secure end-to-end service, communication paths, authentication, and so on[4]. However, the existing security has a tendency to concentrate on a particular aspect of defense or depends on uniform mechanisms. It is time to develop security service into a more individualized structure. From an E-commerce point of view, web based security management policy is urgently needed to control and understand diverse mechanisms, because E-Commerce should not be

C.-W. Chung et al. (Eds.): HSI 2003, LNCS 2713, pp. 751-756, 2003.

restricted to its service platform. It is possible for any type of document to be hacked into on the system.

In conclusion, the Web Service platform needs positive security management for flexible service management. In this thesis, the research area is limited to an XML-centric Web Service. Even though a large number of different documents can be used for Web Service, because it conducts transactions, providing system independency by means of XML. This study presents flexible security mechanisms, containing various kinds of security technology, management, and policies. Based on this analysis, 'Trusted Data Management(TDM)' is proposed. This thesis aims to achieve an enhanced security mechanism focusing on XML-centric document E-Commerce.

2 Related Works

2.1 QoSS: Quality of Security Service

QoSS uses security as a key provision of Quality of Service in distributed systems. It treats user specified security variables and methods at a range of service levels. QoS enhances the reliability, predictability, and efficiency by including security as a real part of QoS. There is correlation between security and service [5]. The QoSS needs a variable security system which includes a range is a set of elements, which define the possible choices for a security variable[6]. It has 3 ranges for security service modes: normal, impacted, and emergency. This security service taxonomy can be useful in understanding how security is involved in a Quality of Service request[7].
the QoSS system should be also equipped with a Translation Matrix[8] translating quantitative mechanisms into qualitative terms to provide an easy indication of standards to users such as situational mode. A table of preliminary taxonomy includes security services, example mechanisms and associated service areas.

2.2 Threat-Adaptive Security Policy

Current security systems provide a unified security policy to all users. It does not provide an individualized level of trust treatment for each user at run-time. A Threat-Adaptive security policy proposes a dynamic security policy, which considers the trade-off between security and performance. This idea combines a level of trust to every user during runtime and serves an individualized security policy. This system monitors user's activity individually with a presumed level of threat, varying degrees of security, and the needed system enforces a corresponding level of security[9]. User behavior is a major standard in terms of threat perception to determine users normality with respect to past or current acceptable behavior.

3 Problem Definition

A security mechanism must obtain mutual complementary of security concerning weak points within the application. An E-Commerce system has to enforce multi-level security using Encryption, IDS, firewall, VPN, Access Control, Virus Detection and so on. A security management system should consider various preceding conditions such as a different security domain, user requirements, user authentication level, and variable conditions of security.

At a certain point in the participant's system, it should assess the level of security, the level of user trust, the method of user authentication, service treatment, local service management, capacity of intrusion detection and protection from harmful packets, viruses, and malicious codes. Moreover E-Commerce security should furnish security requirements such as information confidentiality, integrity, availability, and accountability. In this type of domain, a new type of security management system is required the same condition to provide a secure management policy in the case of XML documents dynamically.

The system dealing with Electronic Commerce has to overcome the difficulty of intrusion detection and application interface threats[10]. Besides, diversity of security should be taken care of from a security management point of view. This is the reason for generalization in terms of security policy required for the XML-centric Web Service. The idea contributes to proposing a flexible management policy for data management security. It also helps to establish enhanced security management in terms of XML-centric Electronic Commerce.

4 TDM: Trusted Data Management Scheme

This thesis adopts advantages of both QoSS and a Threat Adaptive security policy. The former services individual security level service using variable security, the latter depends on the security assessing trust level of users. TDM explains its mechanism with 'the security level of the document', and 'user trust level', which indicates the current secure level compared to required service level. Moreover, it must be established based on security level validation, user trust level, and the methodology of each component treatment.

Figure 1 shows the TDM process. The Manager of Web Services presets the security level of applications according to its security requirement. When a requestor asks a specific service allowance, the system checks requesters' reliability rating and document security level, including specific aspects or the whole document. In the next step, the system examines the validation of service requests to prove the propriety of service allowance. Service providers verify the level of security compared to corresponding service conditions. After the requested service is established, service processing is completed by the appropriate service policy.

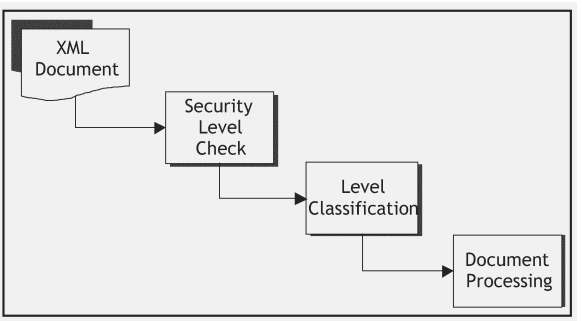

Fig. 1. TDM Processing

4.1 Architecture

There are various modules that consist of the proposed scheme. The composition consists of Security Trust Machine(STM), Trust State Description(TSD), Trust Level Maker(TLM), and Service Execution Machine(SEM). STM contains 'Trust Level Inspection Module', which interacts with TSD. TLM receives data from STM and matches it with an available service range for next step service. The service system requires many considerations to achieve complete service with a security module.

5 Evaluation

5.1 Comparison of Process Time

The factor that must be considered first in evaluating TDM performance is 'processing time of security for documents'. Generally, computing power is wasted during encryption and decryption processing. The condition of the current status such as activating the network area and blowing up web applications based on the Internet, the concern about security has increased along with its cost. Especially, in the case of collaborative on operations such as Web Services, the separated security management module must be applied before data exchange operation and processing. This will induce many bottlenecks during the data exchange process based on the Internet.

According to Figure 3, TDM is a considerable security management model for Electronic Commerce, which has to process a huge amount of information. Document process time has to sacrifice the rate of accuracy at the security level, because the TDM sorts requested services according to be preset policy and process by selected service levels. Therefore, the accuracy of the whole scanning process should be higher than the TDM. The document for TDM is XML document and DTD.

Compared to other security mechanisms, TDM is a solid and compactable mechanism. It is time to enhance the current security management system with the exception of excessive security policies, which can be a burden to service participants. In conclusion, TDM is an advanced model for Web Services. This scheme will be developed based on XML document features appropriate for Web Service in E-Commerce.

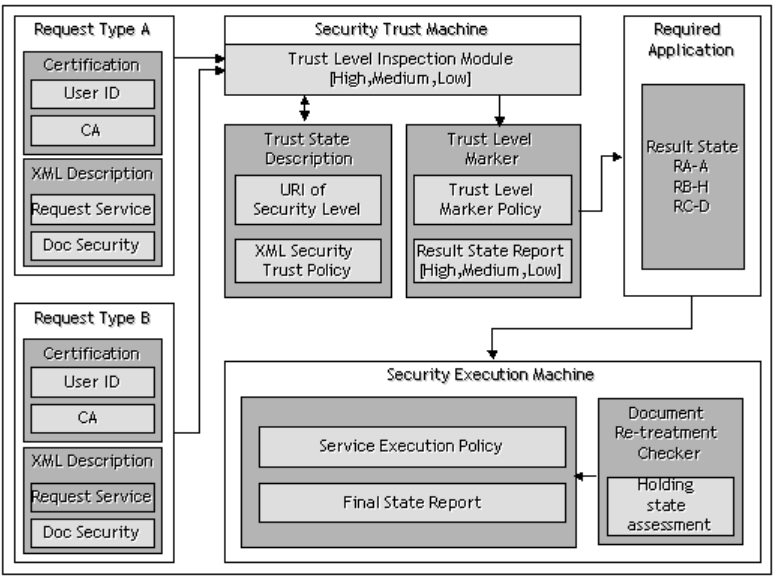

Fig. 2. Trusted Data Management Model

6 Conclusion

TDM is proposed for secure data management on the Internet. It adopts the concept of QoSS and a Threat-Adaptive security policy. Even though, the reference system depends on Network infrastructure, there are many strong aspects that can be applied to document security management.

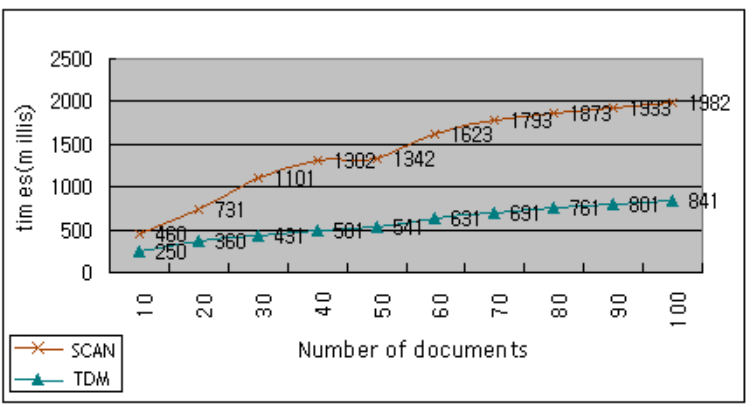

Fig. 3. Comparison of Process time between Scanning and TDM

Web service is a new paradigm that can provide a platform for independent business. To enhance secure Web Service, it should overcome diverse barriers such as unification of the service description format. Platform independent service is an indispensable condition for Web Services. From this point of view, this approach contributes to fulfilling security service requirements.

But it should solve lots of technology constraints and policy barriers such as standardization of abstraction concerning different security domains. This thesis organizes an association of different security management concepts. TDM presents an efficient XML-centric security management system. It can be adopted by any Web Service system with a flexible security policy, which can be controlled by any participants. This thesis will make steady progress in terms of laying a foundation stone in the Web Service security area, which would a steady complement to the most concrete unsolved problem: inspection, classification, assessment, categorization, and segmentation. This means the area of security management is rapidly being organized as an essential aspect of the Web Service component.

References

[1] Allamaraju , Ronald Ashri et., Professional Java E-Commerce, Wrox Press, 2001
[2] Patrick Cauldwell, and Rajesh Chawla, Professional XML Web Service, Wrox Press, 2001
[3] David Hunter, Jon Pinnock , and Jeff Rafter, Beginning XML, Wrox Press, 2001
[4] Ray Djajadinata, Yes, you can secure your Web services documents, Part1, Javaworld, August 2002
[5] Irvine, C. and Levin, T., Toward Quality of Security Service in a Resource Management System Benefit Function, Proc. of the Ninth Heterogeneous Computing Workshop (HCW 2000), Cancun, Mexico, May 2000, pp133-139
[6] Irvine, C. and Levin, T., The Effects of Security Choices and Limits in a Metacomputing Environment, Technical Report NPS-CS-00-004, Naval Postgraduate School, Monetary, CA, January 2000
[7] Irvine, C. and Levin, T., Toward a Taxonomy and Costing Method for Security Services, Proc. of the Computer Security Applications Conference, Phonix,AZ, December 1999, pp183-188
[8] Irvine, C. and Levin, T., A Note on Mapping User-Oriented Security Policies to Complex Mechanisms and Services, Naval Postgraduate School Technical Report, NPS-CS-99-008, Monterey, CA, June 1999
[9] Ramkumar M. Venkatesan, and Sourav Bhattacharya, Threat-Adaptive Security Policy, ASU CSE TR 960108,1997
[10] R.M.Venkatesan, S.Bhattacharya, “Threat Adaptive Security Model”, ASU CSE TR 96-108