Secure XML Aware Network Design and Performance Analysis

Eui-Nam Huh[1], Jong-Youl Jeong[2], Young-Shin Kim[1], and Ki-Young Mun[3]

[1] Seoul Women's University, Division of Information and Communication, Seoul, Korea
[2] National Computerization Agency, BcN Team IT Infrastructure Division, Seoul, Korea
[3] Electronics and Telecommunication Research Institute,
Information Security Research Division, Daejun, Korea
{huh, amary46}@swu.ac.kr

Abstract. Currently, XML as a traffic type on the Internet is widely appeared one-commerce applications rather than HTML. XML based Denial of Service (XDOS) attacks are growing up tremendously. This paper presents a novel appr-oach to manage XML attacks at the network layer efficiently and improves ser-vice performance on server side, while XML data is visible at the application layer. Thus it is clear that the server overhead becomes significant if a number of encrypted, signed, and malformed XML data are requested to the server. The proposed approach handles these issues efficiently and securely. The experimen ts show that the proposed XML Aware Network (XAN) platform is a necessary component for efficient Web Services.

1 Introduction

The use of e-commerce using Internet is increased unexpectedly and so the transaction is now digitalized. The e-commerce security must be kept from illegal transactions, issued privacy, unknown user's resource access and denial of service. Thus encryption for privacy, signed message disposition notification (MDN) for non-repudiation, and digital signature for authentication and integrity are the most important procedures in XML based e-commerce.

Recently, new standardization technology for the extended e-commerce has been developed such as ebXML, RosettaNet, and Web Services. The ebXML enhances basic XML security and authentication technology for e-commerce, and uses a basis of the standardized XML encryption and digital signature. In Web Services (WS), WS-Security is standardized to encrypt and sign the SOAP (Simple Object Access Protocol) message. In addition, WS-Security Policy, WS-Security Conversation, WS-Trust, and WS-Federation are standardized to support secure and scalable Web Services oriented e-business. The XML digital signature, XML encryption, SAML(Security Assertion Markup Language), XKMS(XML Key Management Specification) and XACML(XML Access Control Markup Language) are foundation class of those specifications. The distributed computing technology now like Grid enhances Web services technology to deploy of various field applications.

Hence, information technology will make a convergence of standardized services listed above for secure e-business and uses high performance network infrastructure

O. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3480, pp. 311 – 319, 2005.

for a convenient access to e-business services, which uses conventional XML based technologies.

However, XML oriented data should be handled on nodes efficiently in terms of performance, security, and standardized manner. Thus, this paper presents a novel approach to manage XML data including attacks and wrong format at the network layer efficiently and improves service performance on server side, while XML data is visible at the application layer. So this paper focuses mainly on the performance and security of the service provider domain in addition to consideration of the standardized manners.

2 Analysis of XML Based e-Business

2.1 XML Characteristics

Currently, many acceleration technologies for Web traffic such as HTTP load balancer, content cache equipments, SSL accelerators are developed but there are no capability of handling XML traffic. The XSLT(eXtensible Stylesheet Language Transformation) is designed to convert XML to HTML format, but the processing speed is too slow to serve efficiently. As shown in Fig. 1, transactions per second (denoted to TPS) and processing time (denoted to Latency) with data intensive XML document as shown in Fig. 1 becomes very small when XSLT is applied to server side.

Benchmark Run	TPS	Latency (mSec)
Direct XML to browser	45	1102
Server Convert, XSLTC	2	23300

Fig. 1. XML Processing Benchmark

As shown in Fig. 1, it is clear that secure XML traffic enhanced with encryption and digital signature technology will consume more CPU power. With above results, the secure e-business faces to performance problem. In addition to the above problem, there are more important issues as follows:

- SOAP (Simple Object Access Protocol) message spoofing occurs when the 'actor' element in SOAP message used to get authentication from URI value with ID and password is spoofed by malicious users.
- XML Denial of Service (XDOS) attacks may exist when malformed DTD or XSD, for instance, infinite loop, is delivered to the server side frequently.
- Application threat may exist in the case of wrong URI in XML or SOAP message indicating resource reference.
- Many resources are consumed to process secured Web Services messages as shown in Fig. 2. Given 1 unit to the "parsing" step, overally 25 units for one way XML processing are needed. (see [2])

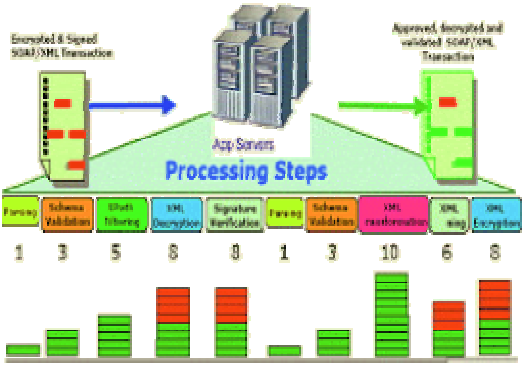


Fig. 2. The XML Processing Overhead

2.2 Related Work

Some XML products enabling digital signature and encryption are developed by IBM (Alpha Works) and Baltimore (X/Secure) for the secure e-business. The Alpha Works is a license free software, providing XML digital signature and its examples followed by the standardized specification [5]. Recently, Apache Group developed the digital signature module for web server called Apache-XML-Security. The .NET framework by Microsoft corporation integrates the XML digital signature for the secure Web Services platform [6]. The X/Secure of Baltimore company (see [6][7]) developed in part according to the standardized specification published by W3C and IETF [8]. The XML encryption as a recommendation standard is published by W3C [9]. Thus basic functions of XML based e-business for privacy, integrity, authentication, and non-repudiation are implemented using

3 XAN S/W Platform Design

In this chapter, firstly, ten design requirements of XML based e-business are discussed as the security in XML Web Services becomes more critical issues. Following lists are carefully considered for secure e-business s/w platform at the design time.

① Transport layer should be secure. Mostly SSL/TLS and VPN technology is used for the requirement and additionally users' certificates are also handled in the manner of hardware processing.

② XML data should be filtered. The content of XML document may contain DOS attack, so deep data inspection is required.

③ Internal resource should be masked. Like NAT(Network Address Translation) and Proxy server in IP service , a technology for XML Proxy is also required to secure internal domain resources.

④ Gateway against XDOS attacks is required. The number of attacks in XML is expected smaller than the number of the "sync flooding" attack

in TCP connection, but the impact of XDOS attack is much bigger than of it.

⑤ Validation of XML message should be tested. The element and the structure of any XML documents must match to its schema or DTD.

⑥ Transformation to other typed documents is required as user interface (browser) capacity might be different, so XSLT is needed as a component in the server side.

⑦ Digital signature must be done before send to inscribe the user identification.

⑧ All messages should be time-stamped to handle precisely the enterprise transactions.

⑨ Element level encryption should be done before send XML data as XML contains structure or meaning of value, for example, "<SSN>123-343-5678 </SSN>" exposure the social security number.

⑩ Finally, auditing system is a required component to audit a user and messages by analysing system logs, which may different from conventional logging approaches as XML signature includes the time-stamp.

Thus, considering the listed requirements, we design a following XAN platform consisting two main components, XAN-Sec (Security) and XAN-Acc (Accelerator) as shown in Fig. 3. XAN-Sec plays an important role in decryption and digital signature, and XAN-Acc does parsing, schema validation, transformation, and grammar validation.

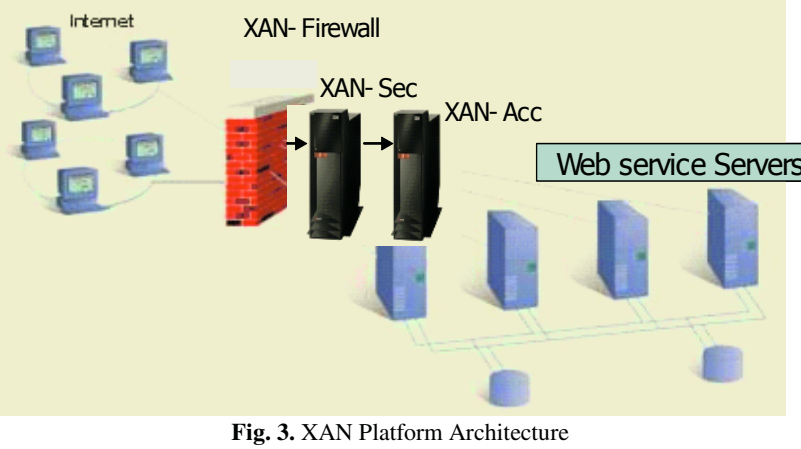


Fig. 3. XAN Platform Architecture

To design XAN-Sec and XAN-Acc platform, we used PCAP (Packet Capture) driver and modified TCP/IP stack modules. As shown in Fig. 4, XML document is now processed between the data link layer and the network layer.

Our detail process steps to handle the XML document are illustrated in Fig. 5. The XAN-Sec decrypts the encrypted XML delivered from clients and passes to the signature validation step. In each step, if errors are detected, then stores the client

information, error information, the step name, and the document information to DB, which is used to compare, filter and reject the wrong documents that appeared repeatedly.

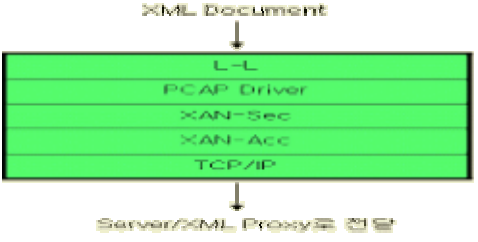


Fig. 4. XAN Flow Structure

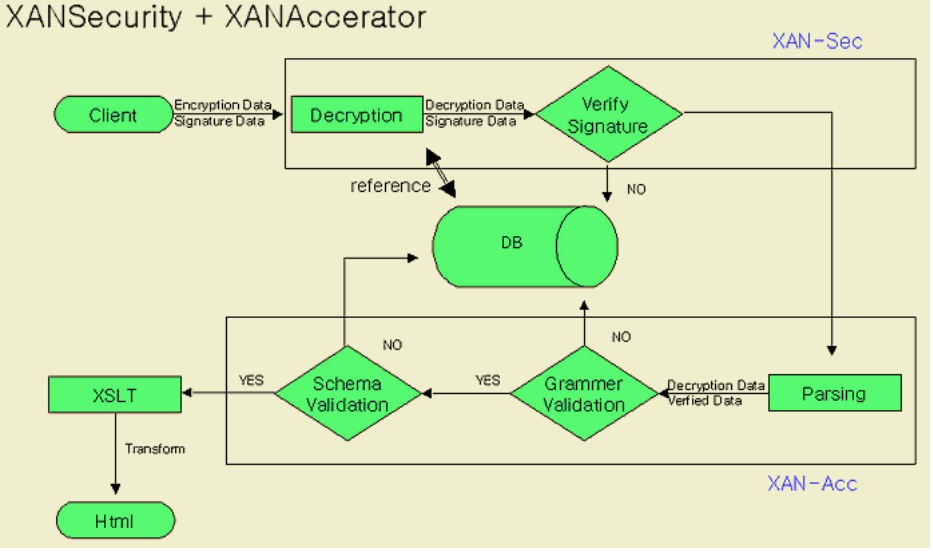


Fig. 5. XAN Processing Steps

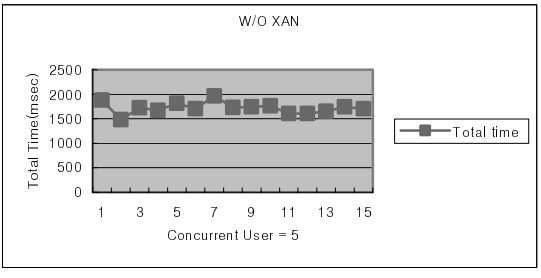
In the XAN-Acc component, parse XML data part, test grammar validation using XPath and validate it with schema. The XSLT converts XML to HTML. When all steps are completed without errors, the decrypted, validated document is routed to the Web Service Provider. If any error occurs in the step, the client information and the document are stored to DB.

4 Performance Analysis

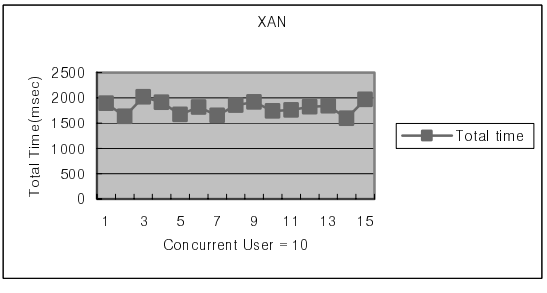
We used two Pentium 4 personal computers to experiment XAN-Sec and XAN-Acc. The four types of XML documents with few elements by 4 to 10 are used. We test 15 times for each experiment to get the average performance.

The first experiment tested with single XML document to know whole processing time of XML. It takes 240msec in encryption and sign validation, and 120msec in parsing, grammar validation and schema validation. We observed performance in case of 5 user request at the same time. It takes 1800msec totally.

In the second experiment, we used separated XAN-Sec and XAN-Acc as a pipelined distributed processor. In case of 10 user request at the same time, 1750msec is measured. The Fig. 6 (a) and (b) shows the two experiments' results mentioned above.



(a) Performance without XAN (5 user request)

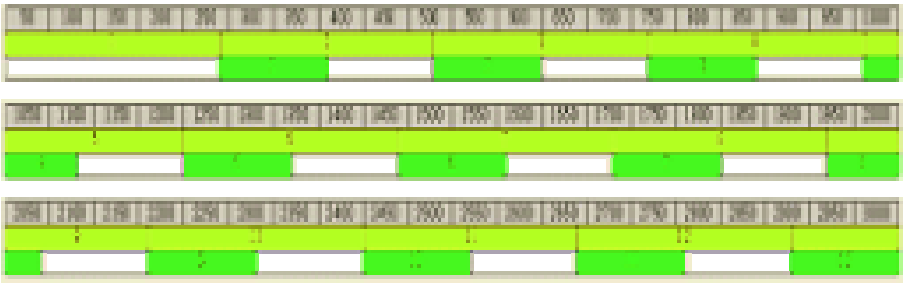


(b) Performance with XAN (10 user request)

Fig. 6. Effective Performance Comparison of XAN

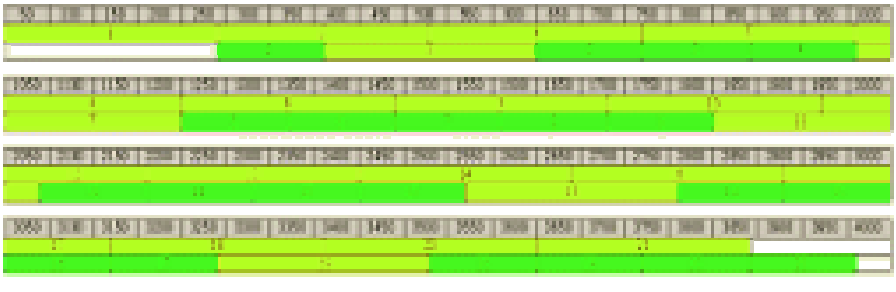
Between the XAN-Sec and the XAN-Acc from the previous two experiments, performance in each component is different, which means load is not balanced. Thus we model performance of XAN to the time chart as shown in Fig. 7. We analyze in detail performance of XAN-Sec and XAN-Acc and found better model in order to fully utilize computing power to handle more documents. The first row with numbered in a rectangle indicates time(msec), and the second row illustrates the processing time of XAN-Sec. The third row indicates the processing time of XAN-Acc. There is many idle time (depicted to white space) in XAN-Acc as shown in Fig. 7.(a). Therefore the Fig. 7 (b) and (c) are proposed to utilize XAN-Acc fully.

The next experiment shows that the performance of the proposed models in Fig. 7. This experiments allows 10 concurrent users to request XML document. When not any optimized or load balance module applied, 1750 msec is required to handle the 10 XML documents. As shown in Fig. 8 (a), the Best-Fit model performs better than any other models. It takes 1600 msec for 10 XML documents, while 1900msec in the round-robbin model is required. From this result, the more user requests in the round-robbin model, the more waiting time occurs as the XML document need to process in sequence.



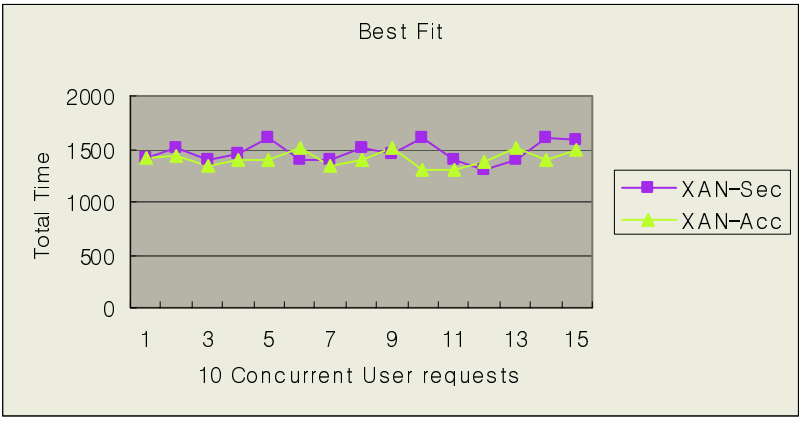
(a) Performance of XAN-Sec and XAN-Acc

(b) Performance of Round-Robbin applied to XAN

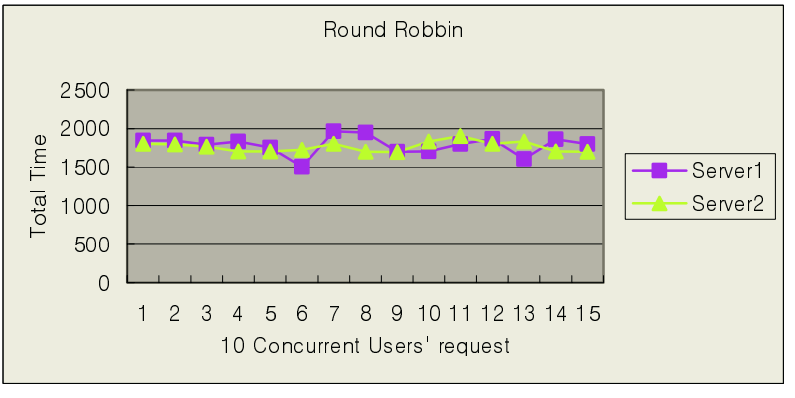


(c) Performance of Best-Fit applied to XAN

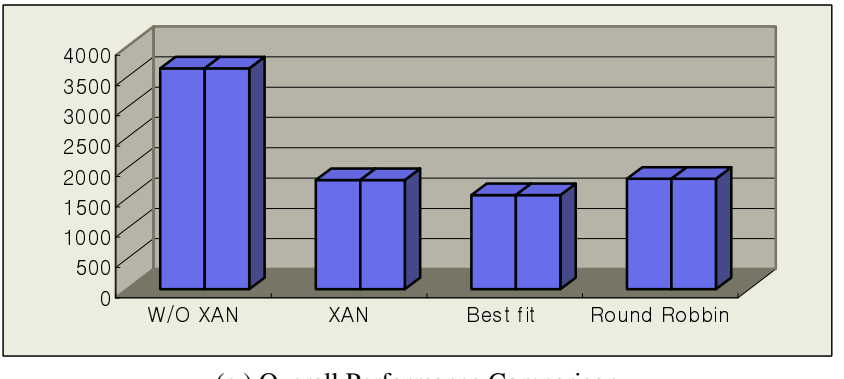
Fig. 7. Performance Time Chart of XAN-Sec and XAN-Acc



(a) Performance of Best-Fit XAN Model



(b) Performance of Round-Robbin XAN Model



(c) Overall Performance Comparison

Fig. 8. Performance Improvement of XAN

5 Conclusion

This paper discusses many important issues in XML to enable the Web Services securely and efficiently. Especially, this paper focus on performance issues in XML based e-business by developing XML Aware Networking (XAN) platform S/W, which can diagnose and improves server side performance. Soon, in generation of ubiquitous, XML is widely used as a standard content format on many embedded platforms, However, still performance is a big question to handle XDOS attack and malformed XML request like SOAP message requiring deep content inspection. Therefore, this developed S/W will give experimental testing platform for Web Services. Also, in near future, XML aware processor might be on the market. The study to enhance speed of network equipment and processor will be continued.

References

[1] The World Wide Web Consortium(W3C)'s XML web page; http://www.w3.org/XML/
[2] Rick McGuir,. XML Acceleration Appliances. Emerging Internet Technologies, IBM Software Group. November 5, 2003
[3] DataPower web page; http://www.datapower.com
[4] XML Security Gateway web page:http://www.datapower.com/products/xs40.html
[5] IBM AlphaWorks Homepage, http://www.alphaworks.ibm.com/tech/xmlsecuritysuite
[6] Baltimore, "X/Secure White Paper," http://www.baltimoreinc.com/library/whitepapers/xsecure.html
[7] Baltimore, "X/Secure Developer's Guide," 1999.
[8] IETF/W3C, XML-SignatureRequirements (WorkingDraft),” Oct.1999, http://www.w3.org/ TR/1999/WD-xmldsig-requirements-19991014.html
[9] W3C XML Encryption WG, "XML Encryption Charter," http://www.w3.org, 2001.
[10] IETF/W3C, XML-Signature Syntax and Processing(Working Draft), Oct. 2000, http://www.w3.org/TR/2000/WD-xmldsig-core-20001012/
[11] xml-encryption@w3.org Mail Archives, http://lists.w3.org/Archives/Public/ xmlencryption/1