http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 7 (8): 1188-1193, 2008
ISSN 1812-5638

The Web Services with Security Mechanisms Base on IPv4 and IPv6

L.T. Lee and C.W. Chen
Department of Computer Science and Engineering, Tatung University, Taipei City 10452, Taiwan

Abstract: Essential model of web services is for enterprise. Before Web Services was used, the business models are processed by the traditional tools. It takes long time to receive goods and loss the competition. Web Services for us is very convenient. For example, as we want to go a trip, we can use Web Services to order tickets, cars, hotels and so on. Web Services for enterprises can be saved more time. If a factory which manufactures shoes has no materials, they can order all materials by Web Services. Present research will take attentions for Web Services with security mechanism in IPv4 and IPv6. Present study compare the different between Web Services with security in IPv4 and IPv6 and web services with no security in IPv4 and IPv6.

Key words: IP protocol, security, performance, web services

INTRODUCTION

The Internet has become an integral part of our daily lives. The enterprises have been taken notice of trend in Web Services. Web Services can help customers and enterprises to do more processes. For example, Web Services can find their applications in Supply Chain Management. It can manage all its part suppliers, contractors and other related resources efficiently. In the view of customers, we can save money and time using Web Services for many e-commerce. When we will go a trip, we can use Web Services to order tickets, cars, hotels and so on. Another part is IPv6 protocol. In 1995, the IETF has brought up the idea about IPv6. All countries in Asia and Europe research and develop IPv6 because of the IPv6 address is a change for them. Internet grows up very fast and IPv4 will be used out after 2010.

When Web Services transmit data, Web Services have one of problem. Web Services media is XML. XML in Internet can be stolen by hacker and someone who wants to destroy you server. Present research will setup a Web Services platform in IPv6 and IPv4. Besides, we use SSL and IPSec as Web Services security. We will evaluate the Web Services performance and compare the different between HTTP, SSL and IPSec.

THE OVERVIEW OF IPv6

Ipv4 address is with 32bits so the number of IPv4 address is 2 with power 32. There are about 429,496,296 addresses we can use it. IPv6 address uses 128 bits. The address is 2 with power 128. There are about 3,402,823,669,209,384,634 IP addresses we can use. After using the IPv6 address, we can use a lot of IP Address. More specialist expert IPv6 can apply in household appliances. We can expect the applications for IPv6. This image shows this idea is very important. Compare with Ipv4, Ipv6 have been added more functions: (Alain, 2001; Lee and Lough, 1998).

- **Invigorating address ability:** IPv6 is different with IPv4, IPv6 add anycast and auto addressing ability. Computers and laptops have to use the Internet, the users don't configure IP address and IP address. IPv6 will auto-config for your computer and laptops. It's more convenient when you are in hurry to use Internet
- Enhance the performance of routing
- Making the quality of services more elasticity
- Rising up the security ability. For example, IPSec is better for IPv6 protocol

In order to raise the performance of IPv6, IPv6 header has been changed from IPv4. Deleting the header in IPv4 Header Length, Service Type, Identification, flags, Fragment offset, Header Checksum. Some of the fields are changed, for example, TTL changed to Hop Limit, Service Type to Next Header and Length to Payload Length. On other hands, IPv6 header has added two fields: Priority and Flow Label. Those fields will support the media of Internet. We can see good movies with IPv6 protocol (Chao *et al*., 2004).

The length of IPv6 header is increasing, but the number of fields is reducing. In IPv4, option is replaced by extend header and put it between IPv6 header and transformation layer as (Fig. 1). Under below items have already defended:

Corresponding Author: Liang-The Lee, Department of Computer Science and Engineering, Tatung University, Taipei City 10452, Taiwan

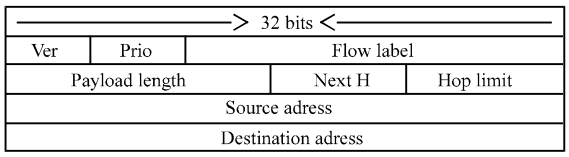

Fig. 1: IPv6 header

- Hop by hop extend header: The definition needs special option of hop by hop processing
- Routing header: Routing header provide the choice of extend routing and play the role which the same function of IPv4 source router
- Fragment Header: It includes the fragment of end to end and the information of recombination. This option is the same with IPv4 control argument
- Authentication Header: This option offer the packet Integrated and authentication
- Encapsulating Security Payload: It provide the function of security and encryption
- Destination Option Header: This option includes the information of the packet to destination address processing

Countries in the world will follow IPv6, but IPv4 is major protocol in the world now. So, we need some mechanisms which two protocols can transfer each other because of reason there are three major transformations. Those are mechanisms, translators, tunneling and dual stack (Chen *et al*., 2004).

WEB SERVICES

A web service is defined by W3C(World Wide Web Consortium). W3C says A Web Services is a software application identified by an Uniform Resource Identifier (URI), whose interfaces and binding are capable of being defined, described and discovered by XML artifacts and supports direct interactions with other software applications using XML based messages via internet-based protocols. According to W3C, Web Services are the services that can use services via Internet. The services not only provide the information but also integrate the information.

Web Services based on Internet can be applied to one or more applications. Through careful coordination, they can accomplish one or a number of tasks. To make the common architecture of these services possible, Web Services standards and protocols were worked out and widely followed. Many companies offer the environment and tools based on the common platform that can facilitate timely. Web Services based on XML include the standards and protocols as shown in Fig. 2 (Vinoski, 2004).

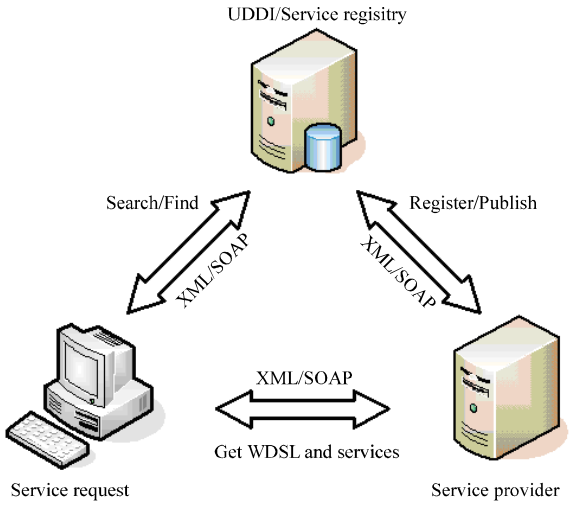

Fig. 2: Web Services

- **UDDI (Universal Description Discovery and Integration):** It defines the registration and search mechanism of web services
- **WSDL (Web Services Description Language):** It defines the description of web services
- **SOAP (Simple Object Access Protocol):** It defines the services protocol for end-to-end users

In order for Web Services to work, data between the server and client need appropriate translation. The important interface is XML. But, when XML data is transferred over the Internet, it is subject to attacks attempting to compromise the security. To solve the problem, there are several alternatives to protect the XML data.

SECURITY

Internet is an open space. It is easy to get the packets with software. We will elaborate on these methods in the following subsections:

IPSec: The security architecture of the network layer has been proposed in IP security protocol Working Group in Internet Engineering Task Force. Since August 1995, Internet Engineering Task Force has published over five papers request for comments (RFCs) and thesis regarding the IP security. These RFCs contribute in the seven areas listed below and the relationship of IPSec as shown in (Fig. 3).

(1) **IP security architecture:** This document describes the security specifications and related mechanism needed in the network layer.

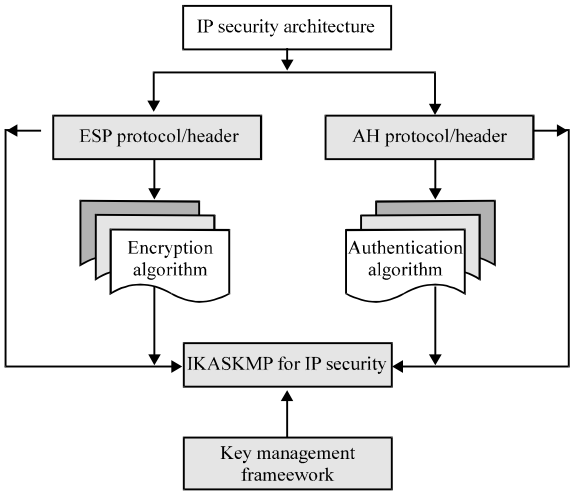

Fig. 3: The seven part of IPSec

(2) **Encapsulated Security Payload protocol/header:** This document describes the encryption algorithm, e.g., DES, 3DES, etc. Encrypted security payload can combine the encryption algorithm and hash function to protect internal data.
(3) **AH header:** This document discusses the problem of authentication mechanism. The authentication header offers confirmed on packet's source and checking validation on packet integrity.
(4) **Encryption algorithm:** The document describes the algorithm of authentication mechanism in ESP protocol/header.
(5) **Authentication algorithm:** This document describes the algorithm of authentication in AH header.
(6) **IKASKMP:** Internet Security Association and Key Management Protocol describe the security ploy and association. The security association mean it establish the information which needs exchange in the security mechanism between receiver and sender.
(7) **Key management framework:** This document describes the architecture of key management. For example, Simple Key-management for IP and Internet Security Association management/Oakley.

IPSec offer the Network Security Services of IP layer. It can be choose by system to decide the algorithm in services and offer the key in time (Raissi, 2004; Kropiwiec *et al*., 2004).

SSL: SSL technology is from Netscape. SSL use TCP to provide the safe service of end to end. SSL isn't only one layer protocol. It is two layers protocol.

In SSL, Connection and Session are important concept. The defined as below:

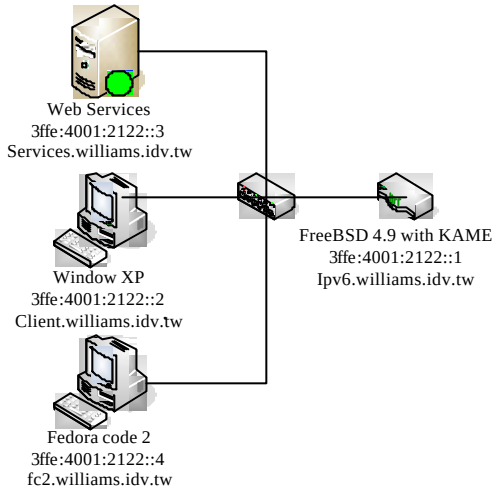

Fig. 4: Experimentation configuration

- **Connection:** One connection is one transmission processing. It offer a good transmission way. For SSL, it's relationship is end to end and is temperate. Every connection is mapping the processing of communication
- **Session:** A SSL is between Client and Server. The connection is made by handshake protocol. It defined a password. The password can be use by many connections

EXPERIMENTATION

In order to use IPv6 protocol, we apply IPv6 address from the computer center of Academia Sinica. We use FreeBSD as our router with tunneling to the computer center of Academia Sinica. The IPv6 address is 3ffe:4001:2122/48. In our internal environment, there are one server and two client personal computer. In Server, the operating system uses Microsoft Windows 2003 Standard, database uses Microsoft SQL Server 2000 and web server is Internet Information Services 6.0. Web Services platform use Microsoft .Net framework. The network structure is shown in the (Fig. 4). At the same time, we develop SOAP and WSDL. In the part of UDDI, we use Ipv4 protocol to link Microsoft UDDI Business Registry Node by .Net PASSPORT. Beside, the part of security, we setup SSL and IPSec as our security mechanism (study area) (Wu *et al*., 2004; Cocquet, 2004; Kanda *et al*., 2004; Hang and Chen, 2004).

We estimate the performance of web services in IPv6 between HTTP, SSL and IPSec base on system response time, the average of files transmission. The formula as

Fig. 5: Web services

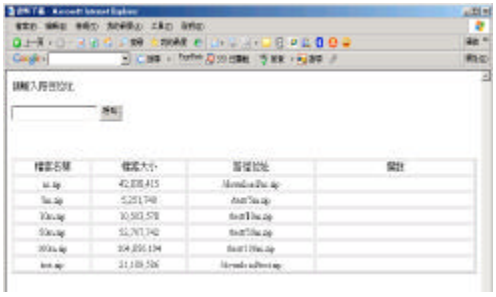

Fig. 6: User research result

below the Fig. 5 is web service main homepage and Fig. 6 is result of searching in the Web Service.

$$\text{Response time} = TH+PS+HT \quad (1)$$

TH = The time client to server
PS = The time of CPU processing
HT = The time server to client

$$Ts = \frac{\sum_{1}^{A} Ni}{A} \quad (2)$$

Ts = Average of files transmission
Ni = The frequency of transmission
A = The total of transmission

Ethereal and the page performance in Windows work manager are the experimentation in order to get the data we need (Fig. 4).

RESULTS

Present web service platform is mainly the data of download. We use localhost to demo present Web Services as below: Users use Internet Explorer (IE) or FireFox and input the URL (http://[::1] for IPv6, http://127.0.0.1 for IPv4) to link to present Web Services (Fig. 5).

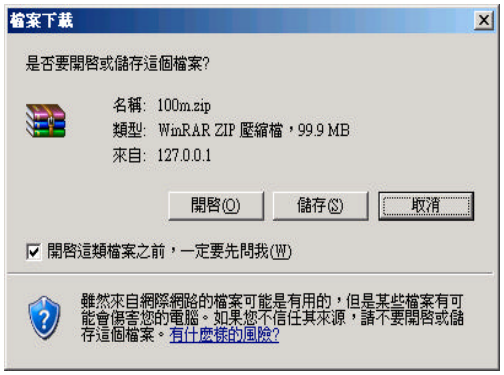

Fig. 7: Download in IPv4 protocol

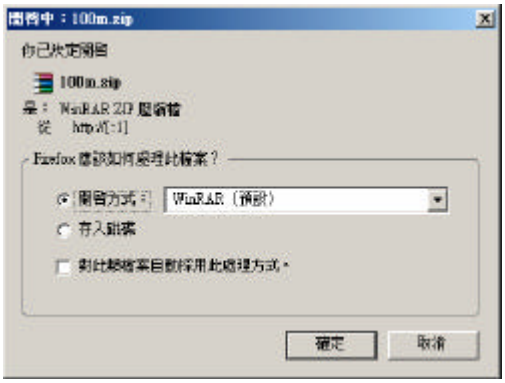

Fig. 8: Download in IPv6 protocol

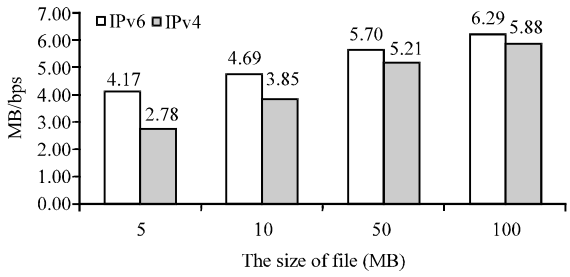

Fig. 9: The average of HTTP transmission

After linking to the Web Services, you can input the file name which you want to search. Present example is searching zip. When you submit the request, you can get the information you want (Fig. 6).

Users only type the file in the field of path and submit. Users can call the services by SOAP to download the file users need. IPv4 protocol is as Fig. 7. IPv6 protocol is as shown in Fig. 8.

Accounting Eq. 1 and 2 we can understand the performances are better than Ipv4 (Fig. 9-14). Because of three reasons, i) In Ipv6 protocol, Package frame are

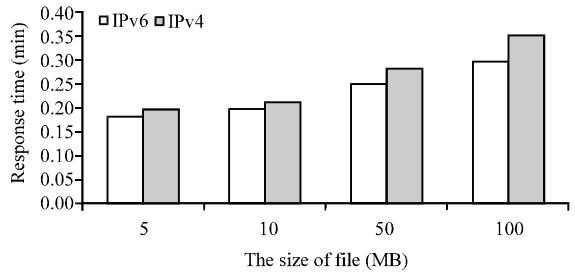

Fig. 10: The response time of system in HTTP

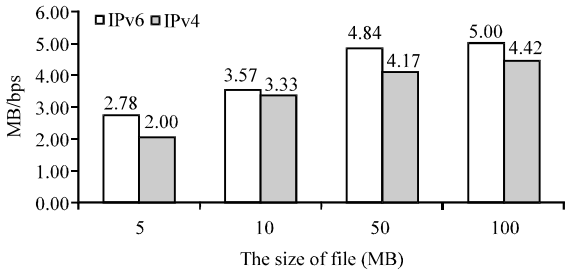

Fig. 11: The average of SSL transmission

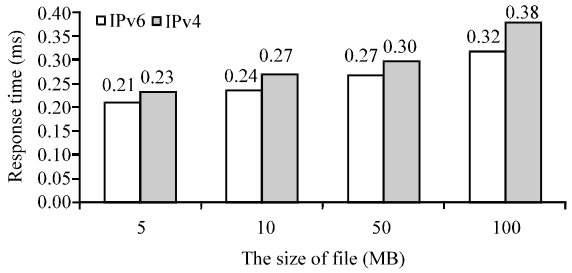

Fig. 12: The response time of system in SSL

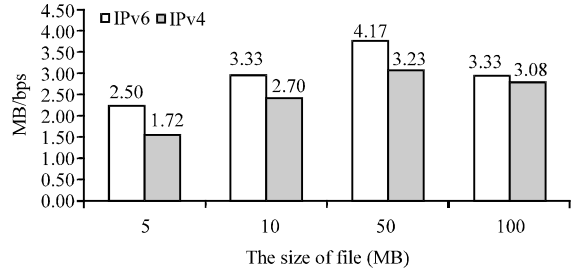

Fig. 13: The average of IPSec transmission

cutting by client, so it can alleviate the loading of router. ii) In the part of packet header, Ipv6 header gets the advantage of IPv4 so the transmission in ipv6 is better than IPv4. iii). IPv6 uses hierarchal, router can search one field.

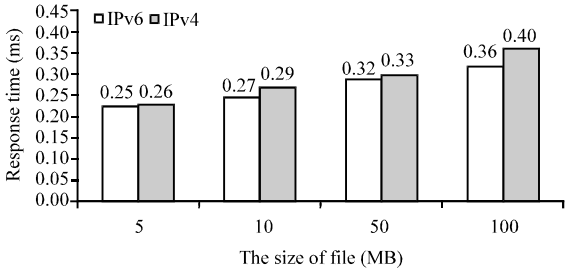

Fig. 14: The response time of system in IPSec

CONCLUSION

The IPv4 address which we can use is less and less. From 1995, IETF have been published IPv6. Every county have noticed IPv6 field and research about this field. Internet mainly uses IPv4 now. IPv6 isn't popular. We can use the two protocols between IPv4 and IPv6 so the translation mechanism is very important. There are three translations each other. Dual Stack, Tunneling, translation are three mainly mechanism. Those translation mechanisms can help IPv6 and IPv4 protocol change packets each other over Internet. Professionals expect IPv4 address will be located in 2010. On that time, IPv6 will be mainly protocol to replace IPv4.

Web Services for electrical commerce have an important place. Present research study in IPv6 protocol. But UDDI are in IPv4 now. Because of those enterprises, ex. Microsoft, IBM and so on, uses IPv4 to link UDDI service. Although we can setup UDDI services in windows 2003, the UDDI services can't exchange the information with external UDDI server. Because of this reason, Services requester can't search services though IPv6.

Although Web Services is convenience, it brings the problem of security at the same time. Web Services' media is XML language. XML's problem is the data is open, everyone can get the XML. It isn't good for enterprise and personal. Many experts have been published the security to prove the problem of web services security, for example, IPSec, SSL, elliptic curve cryptosystem, CA and so on, in order to prove the weakness of web services.

In present study, data in Internet are encrypted by SSL and IPSec. Compare SSL and IPSec, the configure of SSL is easier then IPSec. But IPSec in security is higher than SSL. Because of when we use SSL without any authorization, SSL needs user's authorization to get the information.

REFERENCES

Alain, D., 2001. Deploying IPv6, Internet Computing. IEEE Educational Activities Department Piscataway, 2001, NJ, USA., pp: 79-81.

Ca, L., S. Yu, J.L. Zhou, 2004. Research and implementation of remote desktop protocol service over SSL VPN. Proceedings of the IEEE International Conference on Services Computing, 2004, IEEE USA., pp: 502-505.

Chao, H.C., H.J. Stuttgen and D.G. Waddington, 2004. IPv6: The basis for the next generation. IEEE Internet Commun. Mag., 42: 86-87.

Chen, J.L., Y.C. Chang and C.H. Lin, 2004. Performance investigation of IPv4/IPv6 transition mechanisms. J. Internet Technol., 5: 545-550.

Chou, W., 2002. Inside SSL: Accelerating secure transactions. Professional IT. IEEE USA., 4: 37-41.

Cocquet, P., 2004. IPv6 on DSL: The best way to develop always-on services. Proc. IEEE. USA., 92: 1400-1407.

Kropiwiec, C.D., E. Jamhour and C. Maziero, 2004. A framework for protecting web services with IPsec. Proceedings of the 30th Euromicro Conference, 2004, IEEE USA., pp: 290-297.

Lee, D.C. and D.L. Lough, 1998. The internet protocol version 6. IEEE Potentials, 17: 11-12.

Raissi, J., 2004. NET Security: IPSec vs SSL. Proceedings of the IEEE SoutheastCon, 2004, IEEE, USA., pp: 437-456.

Vinoski, S., 2004. Web services notifications. IEEE Internet Comput., 8: 86-90.

Wu, T.Y., C.C. Hsu and H.C. Chao, 2004. IPv6 home network domain name auto-configuration for intelligent appliances consumer electronics. IEEE Trans. Consumer Elect., 50: 491-497.