AVOIDING REDUNDANCIES AND CONFLICTS IN SECURITY PROTOCOLS

Ibrahim S. Abdullah
School of Information Tech
George Mason University
Fairfax, VA, 22030, USA
iabdulla@gmu.edu

E. H. Sibley
School of Information Tech
George Mason University
Fairfax, VA, 22030, USA
esibley@gmu.edu

Sultan Aljahdali
School of Information Tech
George Mason University
Fairfax, VA, 22030, USA
saljahda@gmu.edu

Abstract

Too many security protocols were developed to provide solutions for security aspects that are required to support the revolutionary services appearing on the Internet. However, almost no effort has been made to integrate or coordinate these technologies. This study analyzes the relationship among these different protocols with respect to the promising IPsec protocol. It also identifies the requirements for the integration among them. This study concludes by proposing a mechanism that allows upper layer security protocols to interact with IPsec in order to achieve the necessary integration and improve the overall system performance.

1. INTRODUCTION

The TCP/IP suite was introduced long ago without network security in mind. Recently, with the e-commerce revolution on the Internet, security has become a major issue. Therefore, security protocols were introduced on the Internet to countermeasure the security problems in the TCP/IP applications.

A general assumption in the design of all the Internet security protocols is that they are running over an unsecured connection. This assumption will become invalid if the IPsec protocol is implemented on the Internet. The sole goal of the IPsec protocol is to provide a secure network layer for the TCP/IP stack. However IPsec cannot provide security needs that are at the application layer, so we have to continue to use other upper layer security protocols to address these needs.

What would happen in such a case? When we are in a situation where we have to use multiple security protocols at the same time, the protocols overlap in their functionality and goals. The purpose of this paper is to analyze this situation and propose how to avoid or reduce such risks.

2. TCP/IP SECURITY PROTOCOLS

Standard security protocols are designed either for general security traffic, such as SSL, or for a very specific business transaction, such as payment or e-mail services (e.g., SET, and S/MIME). In both cases the basic assumption is that no other security measures are taken on other layers. Therefore they attempt to take care of all protection within their boundaries. For instance, SSL is a full, completely integrated protocol that runs over the transport layer and does not need any other protocols to provide security for Internet traffic coming from the application layer. Similar to SSL are SET and S/MIME.

In general, security services that are provided by the security protocols are common: authentication, integrity, confidentiality, and non-repudiation. Either the protocol at the top layer or at the lower layer has to provide all or some of these services. Therefore, unless coordination is maintained among the security protocols running together redundancy will occur and conflicts will arise.

In the past, there was no need for coordination during the development process of the security protocols, because they were developed for different purposes, and for different applications; there was no vision involving a need for interaction between these protocols. However with the introduction of the IPsec, redundancies appeared because it provides a wide scope of security measurers and will make other protocols redundant if they want to operate in conjunction with it.

3. IPSEC SECURITY

In addition to the fact that IPsec is mandatory in IPv6, many vendors have announced current and future IPsec products. Sun Microsystems shipped Solaris 8 with IPv6 support. Cisco published its three phase road map for delivering IPv6 services. Microsoft, IBM, NetBSD, Nokia, Novell, NRL, NTHU, OpenBSD, SCO, Silicon Graphics, Fujitsu's GeoStream routers, Sony, and many others have implementations of IPv6 in their products. For a more detailed list of available implementations see [1].

Another strong deployment of IPsec is in the third-generation cellular phone industry. The Mobile Wireless Internet Forum has mandated IPv6 support in its architecture. Also, the Third Generation Partnership

Program (3GPP) has chosen to use IPv6 exclusively, and the Third Generation Partnership Program 2 (3GPP2) is considering IPv6 in its all-IP architecture. Wireless devices, such as cellular phones and PDAs are considered the IPv6 killer applications. Their number of users is expected to reach a billion by 2005 [2, 3].

According to the TCP/IP protocol, each layer has to pass data packets to the next layer, and no more information is passed with respect to the content of these packets or the overall message. On the other hand, the sole purpose of IPsec is to provide protection for the network layer, so no application layer security controls are possible at this layer, because it is not aware of the operations that are carried out at the upper layers. IPsec receives ready-to-go data packets and it cannot access what is inside these packets, nor figure out the message that these packets are carrying. Figure -1- shows the TCP/IP stack and the location of each security protocol.

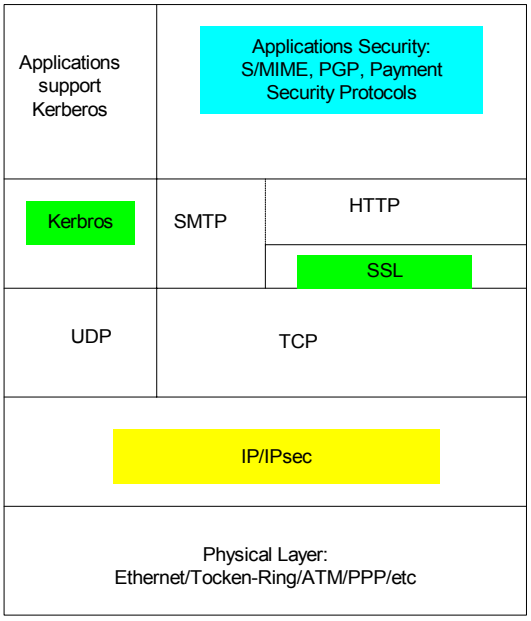

Figure-1- Security Protocols and the TCP/IP stack

The main advantage of implementing security at the network layer is that it can provide security services to both applications and users, and applications need not be changed to benefit from these security services. Also, an increasing number of applications, especially in real time and multicast communications, are based on the connectionless User Datagram Protocol (UDP), which is generally difficult to secure at the transport layer [4].

E-commerce security requirements are beyond the abilities of IPsec, no matter how wide it is deployed, because many requirements are at the application level, such as: message level integrity, user level authentication, and message level confidentiality. The role of IPsec will be limited to protecting the traffic while it is being transmitted over the network and protect the source IP address against alteration.

Therefore, IPsec needs to work with other upper level security protocols to meet the requirements that it cannot address. As we will show in the following sections, none of the available security standards is suitable for working with IPsec without redundancy or conflicts.

4. USAGE ALTERNATIVE

IPsec users have three approaches: use only whatever available in the IPsec, disable the IPsec functionality and use only upper layer security protocols, or use upper layer security protocols over IPsec. For the first approach, it is obvious that it is not possible to provide secure end-to-end e-commerce communications using lower layer security services.

The second approach actually represents what is happening nowadays when using SSL or other application layer standards. SSL only provides protection for the transmission of the traffic; i.e., it does not provide an actual application level end-to-end solution. Therefore, SSL is very similar, in serving the application layer, to IPsec but at the transport layer. Other application layer security protocols, such as payment security protocols, e.g., SET, play a completely different role, by providing a higher level of protection. The end-to-end services provided by these protocols cannot be achieved by lower layer protocols; however these protocols have the disadvantage that the applications need to be configured in order to benefit from their services.

The third approach is the focus of this paper: what happen when upper layer security protocols run over IPsec network? Those upper layer security protocols were designed to work over unsecured networks. Therefore, this situation will create redundancies and conflicts.

5. SSL OVER IPSEC

SSL was designed to provide protection to data traffic over the internet. There was no vision about IPsec at that time. For many reasons SSL gained popularity as a mean of protecting the dialogue between two applications against eavesdropping: it was the first complete protocol, an open free standard, built-in as a part of the wide spread Netscape browser, and there is no need for any registration or sign-up procedure on behalf of clients [5].

As IPsec spreads there will be no need for the SSL to run over IPsec. If it does, there will be many duplicated

processes for encrypting the traffic and protecting its integrity. In general, IPsec supercedes SSL in its functionality and flexibility. On the other hand, SSL has a major advantage over IPsec: SSL is much more robust and faster than IPsec due to the limited services that SSL provides.

From the e-commerce applications point of view, both SSL and IPsec provide redundant security services. Let us take the example of confidentiality. Both provide almost the same set of encryption algorithms to protect the traffic confidentiality. The difference between them is that SSL does it on the fragments of the message before they are processed by the TCP layer, and IPsec does it on the IP packets. The authentication methods of SSL and IPsec are similar except that the later has an advantage of protecting the source machine of the packets, but this does not provide much benefit for applications unless the application requires binding the user to its machine.

Ecommerce applications need to authenticate other applications or users. From the business point of view, authenticating the application or the user makes the IP origin authentication, often, irrelevant for businesses. This requirement is addressed by neither SSL nor IPsec because the information needed to authenticate applications or users are not available at the transport layer or at the IP layer.

.Table –1- Security services in IPsec and PGP

Services	IPsec	PGP
Authentication	IP address authentication	User signature on message
Encryption	Applied on IP packet's payload	Applied on the whole message
Encryption with authentication	Encrypts the payload before authenticating the header	Preferable, signature on the message before encryption
Compression	Rules based on the size of the output	Done by default before encryption

In conclusion, in the future SSL and IPsec will be in competition in terms of serving ecommerce applications. SSL will continue to play a role in protecting short messages, such as passwords, because of its efficiency compared to IPsec. However SSL, if it is running over IPsec networks, has to be able to disable the IPsec functionality on its way, otherwise the performance will degrade because of the repetition of the services. On the other hand IPsec has to develop fine grained security policies and mechanisms to negotiate their needs with upper layer security protocols and allow them to select the right service.

6. SECURE E-MAIL OVER IPSEC

Secure e-mail protocols, such as PGP and S/MIME, provide end-to-end secure e-mail solutions. Again, they are similar to payment protocols in that their protection is wider than that of IPsec, because the protection is applied (at the application level) on the whole mail message. The authentication services that are provided cannot be replaced by those of the IPsec. However the encryption and anti-replay services are similar, in general terms. So, there has to be some sort of coordination mechanism between the secure email protocols and IPsec in order to choose IPsec policy that enhances the performance of the system.

Table -1- shows in brief how the security services are overlapped among IPsec and PGP. The first redundancy occurs on authentication. If user authentication is achieved at the e-mail application level, there will be no need for IP packet authentication unless it has been used deliberately as a double check, which will create a significant overhead load on the system. Another redundancy is in encryption. Once encryption is applied at the message level, it becomes unnecessary to apply it again on the IP packet. Similarly, if authentication is combined with encryption, as is the case of IPsec and PGP, they become totally redundant services.

In the compression process, IPsec has no way to determine that the compression has been applied on the upper layer, so it checks the compressed data and, if the resultant packet size is as large as the original or more, then the packet failed to be compressed. If this happened for few consecutive packets, the system will not attempt to apply compression for a predefined number of packets [5]. This is also unnecessary overhead; the efficient approach would be to pass that information to IPsec to avoid repeating the compression process.

7. SECURITY PROTOCOLS INTEGRATION

The security protocol development process is going through the same types of cycles that other software development processes do. They start as stand alone projects with no interaction or integration. However, because of the fast communication and the Internet, developers soon discovered the importance of integration. So, there is a great deal of pressure now toward making applications integrate and interoperate with each other.

To design more efficient system we need to provide mechanism to coordinate between the upper layer security protocols and IPsec. Upper layer security protocols have

to communicate what kinds of security services that have been applied on the traffic so that IPsec avoids reapplying them. IPsec needs some information from upper layers about what services should be applied and what should be avoided.

To achieve that, we need to have a standard signaling scheme that identify the type of security service that has been applied on the traffic, and a mechanism to allow these codes to be passed through from upper layers down to the IPsec. In addition to that, we need to add proper IPsec policies that allow IPsec to react to these signals when it sees them on the data traffic.

This parameter-passing scheme has to be standardized for two reasons: first, to make it easy for IPsec to reuse the same policy whenever it is appropriate. Second, is to hide the type of application that has assigned this code for the traffic. For example, when SSL, SET, and S/MIME use the same code to tell IPsec that the coming traffic is already encrypted it will be easier for IPsec to have one policy to apply as well as hide the identity of the security protocol that performed the encryption.

The mechanism that we propose to realize this signaling scheme is to assign certain port numbers to indicate the security features of the traffic. For example, assume that the unregistered port number 48500 is used for encrypted traffic generated by any upper layer protocol, 48501 for signed traffic, etc. Then IPsec policies have to be designed to avoid encrypting the traffic coming from port 48500, and avoid signing the traffic coming form port number 48501. Therefore, when an upper layer security protocol feeds data trough these ports, IPsec can apply the policy that results in better system resources utilization.

This mechanism works well for IPsec AH protocol either in transport mode or in tunnel mode but it does not work with the IPsec ESP protocol. The ESP protocol hides the TCP header information which contains the port number by the encryption. So, the recipient system will not be able to determine the IPsec policy that should be applied on the packet (Drop, permit, Apply IPsec) [5,7]. In this case we suggest the use of IPSC/CISPO mandatory access and data classification labels used by the DoD; RFC1108 describes that labeling approach. They insert a data sensitivity label in the options field of the IP header [8]. The ESP encryption does not cover this field, so the recipient can read it and figure out the associate IPsec policy.

The security options for the Internet protocol (RFC1108) define a classification for data sensitivity not for the type of security services therefore it is not suitable for our purpose. We need to adjust its usage by following its framework but with a different coding system. The modified coding scheme classifies the type of security services that have been applied on the traffic at the upper layers instead of the sensitivity of the data or for both.

The IPSC approach is more complicated than the port assignment approach. Therefore, to achieve better system performance we suggest that both approaches made available for developers so each be used in its appropriate context.

8. CONCLUSION

This paper has identified some of the issues related to the interaction of the latest wave of security standards on the internet. It has described the problems of using upper layer security protocols in conjunction with IPsec. The bottom line is that IPsec is a solution that can not replace others, rather it complements them. Therefore, in order to achieve better system performance, these protocols have to integrate and coordinate their operation to avoid the unnecessary repetition of similar operation. We also proposed a mechanism by which those upper layer security protocols can communicate the information about the security services they have performed on the traffic to IPsec so that IPsec does not repeat those operations.

9. REFERENCES

[1] Sun Microsystems Inc., Internet Engineering group of Solaris Software, http://playground.sun.com/ipng

[2] H. J. Wen and J. M. Tarn, “The Impact of the Next Generation Internet Protocol on E-commerce Security,” Information Strategy Journal, Vol. 17, No. 2, winter 2001, pp. 22-28.

[3] G. Lawton, “Is IPv6 Finally Gaining Ground,” IEEE Computer (Aug 2001) 11-18.

[4] R. Oppliger, “Security at the Internet Layer,” IEEE computer, Vol. 31, Issue 9, Sept.1998, pp. 43-47.

[5] J. Tiller, A Technical Guide to IPsec Virtual Private Networks, 2001, CRC Press LLC.

[6] S. Shieh, F. HO, Y. Huang and J. Luo, “Network Address Translators: Effects on Security Protocols and Applications in the TCP/IP Stack,” IEEE Internet computing, Nov-Dec 2000, pp. 11-18.

[7] S. Kent, and R. Atkinson, “Security Architecture for the Internet Protocol,” RFC 2401, BBN and @Home Network, November 1998.

[8] S. Kent, “Security Options for the Internet Protocol,” RFC 1108, BBN communications, November 1991.