Performance Evaluation of Secure Call Admission Control (SCAC) and Secure Socket Layer (SSL)

A. Al-Haj, J.Mellor, I.Awan

Mobile Computing, Networks and Security Research Group,

Department of Computing, School of Informatics, University of Bradford, UK

BD7 1DP, Bradford, West Yorkshire, United Kingdom

{Aaalhaj, J.e.mellor, I.u.awan}@bradford.ac.uk

Abstract **— with the increasing demand for computer communications the need for security is growing dramatically. The existing research related to security mechanisms focuses on security of the data transmission in the communication networks only. Our developed specific Secure Call admission control (SCAC) is a set of technologies and solutions to enforce security policy and bandwidth compliance on all devices seeking to access network computing resources, in order to limit damage from emerging security threats** and **to allow network access only to compliant and trusted endpoint devices.**

IPSec is a suite of protocols that adds security to communications at the IP level. Protocols within the IPSec suite make extensive use of cryptographic algorithms. Since these algorithms are computationally sophisticated, some hardware accelerators are needed to support high throughput. In this paper we compare between secure call admission control and SSL to improve the properties of the SCAC and the Virtual Private Networks (VPN) built with both protocols.

Index Terms **— SCAC, SSL, VPN, IPsec, Network Security.**

I. INTRODUCTION

The increasing demand for communication over public networks has brought with it a need to securely protect sensitive information sent over this open network. The SSl protocol has become a de facto standard for cryptographic protection of the Internet http traffic. After developing its limitations, SSL3.0 aims to provide Internet client/ server applications with a practical security mechanism [8].

IPSec is a suite of protocols designed to provide high quality cryptographically-based security for IPv4 and IPv6. IPSec provides security services: access control, integrity, authentication, confidentiality (encryption), and replay protection to the IP layer as well as the layers above [4].

IPSec is a suite of protocols that adds security to communications at the IP level. This suite of protocols is becoming more and more important as it is included as mandatory security mechanism in IPv6. IPSec is mainly composed of two protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP). The former allows authentication of each IP datagram's selected header fields or – depending on the operational mode that has been selected – of the entire IP datagram. The latter allows encryption – and optionally authentication – of the entire IP datagram or of the IP payload, depending on the operational mode that has been selected, namely the transport and the tunnel modes. The former was designed for being used in host machines, while the latter is for secure gateways. In tunnel mode the entire original IP datagram is processed; the result becoming the data payload of a new IP datagram with a new IP header. In transport mode only parts of the original IP datagram are processed (e.g., the data payload for the ESP protocol) and the original IP header is kept with some small modifications. Through encryption, authentication, and other security mechanisms included in IPSec (e.g., anti-reply), data confidentiality, data authentication, and peer's identity authentication can be provided [1, 2, 3].

The SCAC will investigate IPSec to secure the communication between one or more paths, between two pairs of hosts, between a pair of security gateways, and a host and a security gateway (SG). This is why we will compare between SSl and the SCAC to show the properties of the SCAC.

II. DESCRIPTION OF THE SCAC

The main goal of the SCAC is to secure call admission control in heterogeneous networks and providing quality of service data transmission: possibly, maximising throughput, minimizing delay and lost packets by implementing the strongest security strategy and investigating various security algorithms.

The main features of the SCAC:

- When SCAC is implemented in a firewall or gateway, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a workgroup or company does not incur the overhead of security–related processing.
- SCAC in a firewall is resistant to bypass if all traffic from the outside must use IP, and the firewall is the only means of entrance from the Internet into the organization.
- SCAC as it investigates the IPsec is below the transport layer (TCP, UDP) and so is transparent to application. There is no need to change software on a user or server system when it is implemented in the firewall or gateway.
- SCAC can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.
- SCAC can provide security for individual users if needed. This is useful for off site workers and for setting up a secure virtual sub network within an organization for sensitive application.
- SCAC can provide a quality of service data transmission by possibly increasing throughput, decreasing delay and lost packets.

The main idea underlying our SCAC is to receive the packets generated by the host computers to be processed on the gateway (i.e., either one of the accelerators or the CPU) which can provide the shortest processing time. Our SCAC processes each packet as follows:

- SCAC will be implemented in a firewall or gateway, will have a Malicious Packet Filter (MPF), which will analyze all the incoming packets and will decide to deny or pass the packets through the gateway.
- For the passed packets a set of accelerators will be able to perform the cryptographic algorithm(s) required by the considered packet is selected and a modified version of the flow-based Weighted Fair Queuing (WFQ) priority management mechanism.
- As the main goal of this research is to provide the more secure path to data transmission through the network, so SCAC will investigate the IPsec as the future standard security protocol with Advanced Encryption Security (AES), which was already improved and chosen by National Institute of standards and Technology in USA as the more secure encryption algorithm [1].

III. COMPARISON BETWEEN SCAC AND SSL

A. *Authentication*

SSL support only one authentication algorithm Digital Signature, but SCAC support Digital Signature and Secret Key algorithm, so we can implement SCAC with the absence of Digital Signature but SSL can not be implemented.

Regarding the authentication method SSL is better, because it supports various types of authentication: Server Authentication, Client Authentication and Anonymous, But SCAC supports only one type which is Mutual authentication.

B. *Encryption*

SSL firstly creates the Message Authentication Header (MAC) for the plaintext and then encrypts the data, but SCAC is doing the opposite, encrypts the data first then creates the MAC for encrypted data. If a modified data were inserted into the transaction, SCAC would verify the MAC before performing any decryption process, but SSL is enforced to decrypt it first then verifies the MAC which could result in wasting the CPU time.

C. *Multi-User Service*

Using SSL, each user should have independent connection and individual session with different encryption keys for multi-users, but SCAC allows multi-users to use one tunnel between two endpoints in the same time.

D. *Message Authentication Header (MAC)*

After establishing the connection, Mac is used for authenticating the exchanged messages; both SSL and SCAC require the implementation of MAC algorithms HMAC-AHA-1 and HMAC-MD5. The length of the output is reflecting the strength of the Hash algorithm has been used.

E. *Transport layer*

SCAC Handshake is not exchanged over TCP, but SSL Handshake is exchanged over TCP and the port can be changed according to the application.

As a client, SCAC is bound to specific port, but SSL is not, where as sever both bound to specific ports as (for example port 500 only for exchanging negotiations SCAC over the UPD).

F. *Interoperability*

SSL works only over the TCP where UDP can cause data to be arbitrarily lost or reordered; SCAC overcomes this problem by adding new TCP header to the original packet's field which allow both based applications (UDP or TCP) to work with SCAC.

G. *The Overhead Size*

SSL does not need overhead like SCAC; in tunnel mode SCAC requires adding another 20 bytes IP header.

H. *Compression Algorithm*

*Open*SSL is used compression in small range with SSL [6], but compression is widely used by SCAC through a compression protocol called IPComp [5]. Compression increases the throughput for SCAC and SSL, as it is in low bandwidth and it will increase the throughput for both SSL and SCAC, as it uses the AES algorithm.

I. *Handshake Process Time*

The handshake process time is the time needed to establish a session for SCAC or SSL. Of course this will be depended on the authentication method and authentication algorithm.

IV. A SCAC OR SSL VIRTUAL PRIVATE NETWORK (VPN)?

VPNs allow companies, workgroups and corporate enterprises to extend access to their internal networks to their remote hosts, employees and partners over standard Internet public networks. The primary reason VPNs came to be was the immensely expensive lease line solutions [7].

A. *What is a VPN really?*

VPNs are the enabling technology which allows clients, Host-users, employees and partners to use standard public Internet ISPs and high-speed lines to access closed private networks. As a SCAC with IPsec provide VPN solutions. In fact, there are many encryption and security protocols which offer the functionality of a VPN. SSL is one such protocol.

After comparing between SCAC and SSL separately, I will try to show which is the better for building VPN, to secure the Host-user and the data transit?

We have to discuss separately about data security and host security. Both SSL and SCAC VPNs are highly effective remote access solutions that use field-tested protocols and methodologies. They offer roughly the same performance bandwidth and the same level of encryption, but as the SCAC exploits the characteristics of both IPsec and AES, so:

1) SCAC VPNs are considered ideal for site-to-site security, static, long-term connections between offices, whereas SSL VPNs are the better for providing access for large numbers of mobile employees and for business partner extranet environments.
2) SCAC VPN gives better security for the host, because SCAC works lower in the protocol stack and there is a lack of built-in authentication methods in the traditional SSL protocol.
3) The prices will depend on what is included. SCAC is heavy-duty and offers better central management, i.e. it scales better to huge numbers of users. A SCAC VPN can be deployed across any existing IP network, avoiding the capital and operational costs of building a new network. But you probably have to buy the client and the management system (Nowadays in most cases the clients are free). In the other hand SSL VPN clients come for free.
4) Cellular users don't like SSL if they have to negotiate a separate security association for each service, which means for them an extra communication cost... With SCAC they can use the services of a host (or a subnet) over a single SA.

V. CONCLUSION

In this paper we presented a technical comparison between SSL and SCAC, each of them has unique properties. Choosing SCAC or SSL depends on the security needs. More important than the question of which is better transport encryption protocol is the question: “Which security technology best fills the need for a remote access solution?” Since SAC can be used to secure any IP traffic and SSL is focused on application-layer traffic, SCAC is well suited for long-lived connections where broad and persistent, network-layer connections are required. SSL, on the other hand, is well suited for applications where the system needs to connect individuals to applications and resources.

VI. REFERENCES

[1] S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol – RFC2401,” IETF RFC, 1998. [Online]. Available: http://www.ietf.org/rfc.html

[2] ——, “IP Authentication Header – RFC2402,” IETF

RFC, 1998. [Online]. Available: http://www.ietf.org/rfc.html

[3] ——, “IP Encapsulating Security Payload (ESP) – RFC2406,” IETF RFC, 1998. [Online]. Available: http://www.ietf.org/rfc.html.

[4] William Stallings, Cryptography and Network security, chp16, pp 481-491, 3rd edition Prentice Hall 2003.

[5] A. Shacham, B. Monsour, R.Pereira, M. Thomas, IP Pay load Compression Protocol IPCOMP RFC Dec., 1998.

[6] www.openssl.org, [Online]. Available: http://www.openssl.org .

[7] Juniper Networks, Inc. Juniper Networks VPN, Decision Guide, [Online]. Available: http://www.juniper.net/products/integrated.

[8] Eric Rescorla, SSL and TLS Designing and Building Secure Systems, Addison Wesley rd Printing, Aug., 2001.