Geographically Secured SSL-VPN Using GPS

Suresh Limkar
Department of Computer Engineering,
SVN I T Surat INDIA
{Faculty at G. H. Raisoni College of Engineering &
Management, Pune}

Dhiren Patel
Department of Computer Science & Engineering,
IIT Gandhinagar INDIA

ABSTRACT

We are moving towards an era where location information will be necessary for access control. The use of location information can be used for enhancing the security of an application, for critical applications, such as the military. A formal model for location-based access control is needed that increases the security of the application and ensures that the location information cannot be exploited to cause harm. In this paper, we show how the SSL VPN model can be extended to incorporate the notion of location. We show how this location information can be used to determine whether a subject has access to a given object. A novel improved VPN (Virtual Private Network) system based on geo-secured SSL (Secure Socket Layer) protocol is proposed to overwhelm the defects of traditional SSL VPN. It enhances current security applications granting access to sensible information and privileges to execute orders only to entities that are in a trusted location. This system not only authenticates authorized user but also the location of the user

Keywords- SSL, VPN, Geo-encryption, Location based security, GPS based encryption

I. INTRODUCTION

We are moving towards an age of ubiquitous computing where location information will be an integral part of many applications. Denning, MacDoran [1] and other researchers have described how the use of location information can make applications more secure. For instance, a user should be able to control or fire a missile from specific high security locations only. Verifying the location information in addition to the checks that are performed by traditional methods of authentication and access control will improve the security of the underlying application.

Let's discriminate how location information can be used to augment traditional access control in order to cater to more sophisticated applications. Few examples will help to motivate our work. In a military application, if a computer containing top secret information is placed in a public place, then the computer should automatically become inaccessible. A critical application that is involved with the firing of missiles may have the following requirements: A user should be able to control or fire a missile from specific high security locations only. Moreover, the missile can be fired only when it is in a certain location. For such critical applications, we need additional checks, such as verification of the location of the user and the location of the missile, that must be satisfied before the user is granted access. Such checks based on location are not provided by the traditional access control models. The above examples illustrate how the use of location information can increase the security of an application. Geographically

In this paper we propose one such formal model that is suitable for military applications. Rather than developing such a model from scratch, we are extending the existing SSL [2-4] based VPN to geo-secured SSL VPN. We illustrate how the SSL VPN can be extended to incorporate the concept of location based access control. We illustrate how the different components in geo-secured SSL VPN are related with location and how location impacts these different components. Finally, we show how this location information can be used to determine whether a subject has access to a given object.

The remainder of the paper is organized as follows. Section 2 Introduces and review the background technologies, section 3 proposes a new scheme to strengthen the SSL VPN with its architecture and data flow, section 4 presents security analysis of the proposed scheme. Section 6 concludes the paper with pointers to future directions.

II. BACKGROUND

A. Structure of SSL VPN

Since our work is based on SSL VPN, we present the main concept of the SSL VPN model. Fig.1 shows a typical example of SSL VPN structure [5]. When a client needs to connect to an internal application server, at first, the client should request to create a VPN connection with SSL VPN gateway, and then the VPN peers authenticate each other through their digital certificates and negotiate security parameters. After the VPN peers were authenticated, a SSL VPN tunnel will be created, connecting the client and the SSL VPN gateway.

Then the SSL VPN gateway sets up a TCP connect to the internal application server on behalf of the client. Thereafter, the SSL VPN gateway relays data between the client and the internal application server, all data flows of the VPN should be encapsulated or unwrapped at the SSL VPN gateway according to SSL protocol. Inside the LAN, communication data between the SSL VPN gateway and the internal application server can be either in plain text, or protected by additional internal SSL tunnels, it's up to internal security requirement. Compared with IPSec VPN, SSL VPN has some outstanding advantages [6], like easy-to deploy, fine-grained access control, etc.

However, SSL is not a robust secure protocol in the real world [7-10], because it doesn't obey the strict trust model of PKI and valid length of SSL session key is too short to resist exhaustive attack.

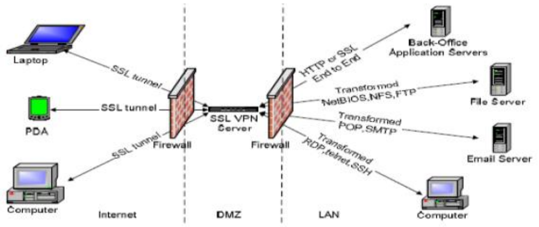

Figure 1. A typical example of SSL VPN [10]

Various methods are proposed for the security of data transmission in SSL [7-10]. However, these methods are location independent as the sender cannot restrict the location of the receiver for data decryption. If sender can restrict the location of receiver to access the data then it is very useful form the security perspective.

III. A SCHEME TO STRENGTHEN THE SECURITY

In location-based access control, it is extremely important to accurately determine the location of users and objects. There are different technologies for doing this, but here we are using GPS technology.

The location of an object or user can be determined through the GPS system. The object whose location we are trying to determine must have a GPS receiver device which communicates with different satellite constellations to determine its location. The GPS covers a very wide area and the location information is accurate to within a few meters [1]. Although the GPS was originally used only by military organizations, it is now being used by commercial organizations as well.

In this scheme remote user system is connected with anti-spoof GPS receiver, So that it captures its current position parameter. At the other side location based access control server contains the database of client's location from where client can access the application server.

The scheme aims to develop an architecture that will provide access control based on location obtained by GPS. The scenario of the proposed approach is presented in fig.2. There are two phases: register and operation phase. First, before a remote client want to establish a connection, he must have a unique ID, that will be given by server upon successful completion of the registration phase.

A. Registration Phase

Server register each client by giving a unique ID associated with each client and stores that client unique ID in its database. Along with this client ID, it also stores the desired location of the client from where he can access the server. Other than this location client won't be able to access the server.

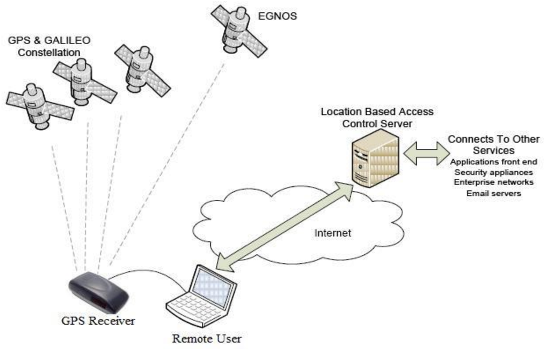

Figure 2. Architecture of the geo-secured SSL VPN

B. Operation Phase

The modified hand-shake protocol is shown in Fig.2. In the 1st step of hand-shake protocol, we add the remote client's location (i.e latitude & longitude) into the ClientHello message, and the server will use it later to look for the corresponding Client unique ID. In the 6th step (after the web browser receives the certificate of the server, and before it computes master key), we pop up a dialog to let the user input it's unique client ID. And then web browser will use the deal password, two random number and other key materials to compute master key, key-block and session keys. Symmetrically, the server will perform the same operations to compute keys.

C. Generating Keys

Below, we show our solution to strengthen the security of keys in SSL. Here, we use the client ID as a credible secret value to transform the two public random values to cause the transformed values secret to an adversary. Then we use the transformed random numbers to compute keys. In our scheme, we use the idea of Hill cipher [11] to transform random numbers: Suppose part of the 32-byte random number of the user is:

10101100 10111010 10101011

01001010 10101001 01111111

…

We look each byte of the random values as a block. Suppose the client ID is an 8-byte character string: 1s3df4rc. And we decode the deal password into ASCII codes:

00110001 01110011 00110011 01100100

01100110 00110100 01110010 01100011

We use this decoded 64 bits data as a permutation to transform each random block. The transformation of the first block is shown in Fig.3, and the result is 11000011. The second block is transformed in the same way, and the result is 01110011.

$$\begin{pmatrix} 0&0&1&1&0&0&0&1 \\ 0&1&1&1&0&0&1&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&1&0&0&1&0&0 \\ 0&1&1&0&0&1&1&0 \\ 0&0&1&1&0&1&0&0 \\ 0&1&1&1&0&0&1&0 \\ 0&1&1&1&0&0&1&1 \end{pmatrix} \begin{pmatrix} 1\\0\\1\\0\\1\\1\\0\\0 \end{pmatrix} = \begin{pmatrix} 1\\1\\0\\0\\0\\0\\1\\1 \end{pmatrix} \quad \text{mod2}$$

Figure 3. Transformation of each random block

For example:

The master key is:

$$\text{MD5}(pre\_master\_secret \,\|\, \text{SHA}(A \,\|\, pre\_master\_secret \,\|\, \text{Transformed random})) \,\|$$

$$\text{MD5}(pre\_master\_secret \,\|\, \text{SHA}(BB \,\|\, pre\_master\_secret \,\|\, \text{Transformed random})) \,\|$$

$$\text{MD5}(pre\_master\_secret \,\|\, \text{SHA}(CCC \,\|\, pre\_master\_secret \,\|\, \text{Transformed random}))$$

The key-block is:

$$\text{MD5}(master\ \ secret \,\|\, \text{SHA}(A \,\|\, master\ \ secret \,\|\, \text{Transformed random})) \,\|$$

$$\text{MD5}(master\ \ secret \,\|\, \text{SHA}(BB \,\|\, master\ \ secret \,\|\, \text{Transformed random})) \,\|$$

$$\text{MD5}(master\ \ secret \,\|\, \text{SHA}(CCC \,\|\, master\ \ secret \,\|\, \text{Transformed random})) \,\|$$

The session key of the user is:

$$\text{MD5}\{key\_block32...36 \,\|\, \text{Transformed random}\}$$

In addition, the transformed random values are:

$$f(randomc0) \,\|...\|\, f(randomc32) \,\|\, f(randoms0) \,\|\, ...\|\, f(randoms32)$$

And f () is a permutation function mentioned above.

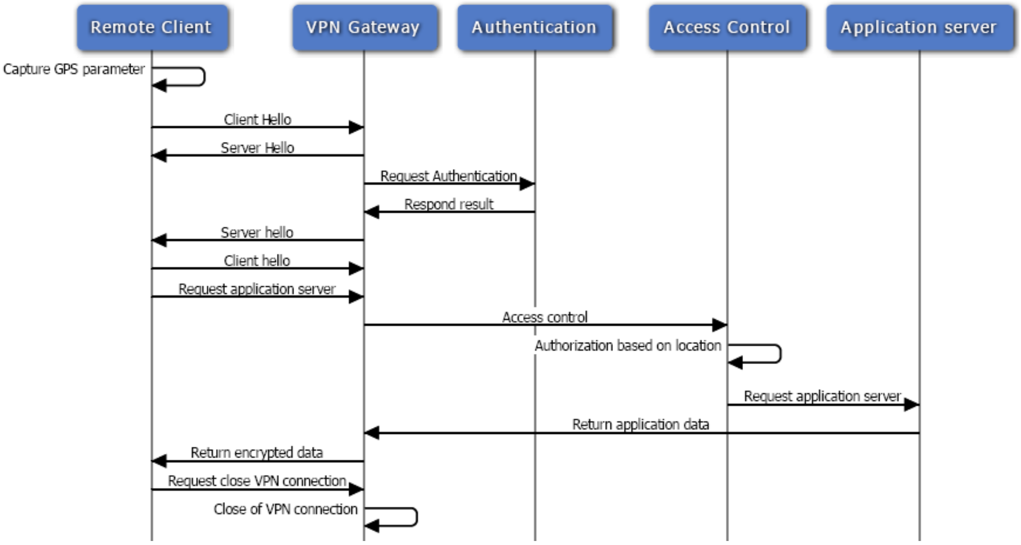

Figure 4. Geo-Secured SSL VPN work flow

Geographically secured SSL VPN flow

The Geo-Secured SSL VPN work flow as fig.4 illustrate, it is composed of 3 steps: Create VPN Connection, access internal application server and close VPN connection.

In the create VPN connection step,

Remote user captures its GPS parameter from the anti-spoof GPS receiver which is connected to it.

Remote user request to create a VPN connection with SSLVPN gateway by sending its location parameter along with client hello message.

SSL VPN gateway sends this (location parameter along with client hello message) towards authentication.

During authentication step, stored location parameter is compared with the received location parameter. If the values are correct then SSL VPN gateway authenticates the remote user.

Meanwhile remote user send its certificate to each other and negotiate the secure parameter of a session including protocol version, cipher keys and encryption/decryption function and version etc through hello message.

Once the remote user was authenticated by the SSL VPN gateway, SSL tunnel connecting the remote user and SSL VPN gateway is created.

In the access internal application server step, the access control management modules validates the remote users access act according to the access controls firstly defined in access module and it locates the remote users request to one application server.

1. Additionally, the application server return the data to the SSL VPN gateway, SSL VPN gateway encrypt the application data and sent the encrypted packet to remote user.

Here we are trying to modify only handshake protocol rest of the protocols are kept as it is.

IV. SECURITY ANALYSIS OF PROPOSED SYSTEM

Analysis can show our scheme can resist the security defects in [12].

A. *Resisting faked evil certificate*

In our scheme, when the adversary installs a faked evil root certificate into the user's web browser, he can get the encrypted per-master key using his private key, but he can not compute the correct keys (including master key, keyblock, two session keys and MAC keys). The reason is: after the user sends encrypted pre-master key, he will use GeoLock value to transform the public random numbers, and use the transformed numbers to compute all kinds of keys. Due to without the GeoLock, an adversary can not compute the correct session keys and MAC keys. So the adversary cannot compute the right Server's Finished message to cheat the user.

B. *Resisting exhaustive attack*

The lengths of session keys are 128-bit MD5 values, and the input of MD5 function is a 40-bit key-block and two 32- byte transformed random numbers that are derived from an 8-byte deal password. For less workload of exhaustive attack, the first thing adversary should do is to guess the 8-byte deal password. Thus, if an adversary wants to make an exhaustive attack to a session key, he has to guess the 40-bit key block and deal passwords, and uses the first four characters of the "finished" message to verify the guess. The workload is much more than that of exhaustive attack to original SSL.

C. *GeoLock Security and DOS attacks*

An effective denial of service attack can be launched by either jamming the Global Positioning System (GPS) or by feeding the GPS receiver fake information [13]. With the determined 'location parameters' used to generate part of the session key, there is still a possibility of risk of an attacker reproducing the location parameters given an understanding of how the key is computed. Here we have assumed that the remote client uses anti spoof GPS receiver to capture its location parameter. But in this case client unique ID know only to the client. So if any one tries to provide the fake GPS information it won't work.

V. CONCLUSION

A novel improved geographically secured SSL VPN system based on GPS is proposed to overwhelm the defect of traditional SSL VPN. This scheme enhances current security applications granting access to sensible information and privileges to execute orders only to entities that are in a trusted location. However, the security of our improved scheme has a pre-condition that is the radio frequency signal (GPS signal) is secure, and an adversary could not capture the radio frequency signal.

The proposed scheme can be extended to the other application domains, e.g., Employees can access sensitive data only inside a specified geographical area, an email can be decrypted only in predetermined locations, critical operations could be performed only inside a predetermined zone, managers can analyze in real time the locations from which employees or customers are accessing the enterprise network on a geographical map (if privacy policy allows it), and attestation (proof) of position and contextual data (e.g. time) which could be included in the digital signature of an email, providing information on where and under what conditions the email was written.

REFERENCES

[1] Dorothy E. Denning and Peter F. MacDoran. Location-Based Authentication:Grounding Cyberspace for Better Security. In Proceedings of the Computer Fraud and Security,Elsevier Science Ltd, February1996 .

[2] Alan Freier and Philip Karlton, “The SSL Protocol Version 3.0 ”, http://wp.netscape.com/eng/ssl3 /draft302.txt, Oct.2004.

[3] T. Dierks and C. Allen, “RFC2246: The TLS Protocol Version 1.0”,http://www.ietf.org/rfc/rfc2246.txt, 1999.

[4] Jingli Zhou, Hongtao Xia, Xiaofeng Wang, and Jifeng Yu, “A New VPN Solution Based on Asymmetrical SSL Tunnels”, Proceedings of the Japan-China Joint Workshop on Frontier of Computer Science and Technology (FCST'06), Nov.2006, pp.71-78

[5] Alshamsi, A. and Saito, T. 2005. “A Technical Comparison of IPSec and SSL”. In Proceedings of the 19th international Conference on Advanced information Networking and Applications - Volume 2 (March 25 - 30, 2005). AINA. IEEE Computer Society, Washington, DC, 395-398. DOI= http://dx.doi.org/10.1109/AINA.2005.70

[6] Zhao Huawei, Liu Ruixia, “A Scheme To Improve Security of SSL” Pacific-Asia Conference on Circuits, Communications and Systems, paccs, pp.401-404, 2009

[7] Byung kwan Lee, Tai-Chi Lee, Seung Hae Yang, "HESSL (Highly Enhanced Security Socket Layer) Protocol," cec, pp.456-460, Seventh IEEE International Conference on E-Commerce Technology (CEC'05), 2005

[8] Lamprecht, C. J. & van Moorsel, A. P. “A.Adaptive SSL: Design, Implementation and Overhead Analysis”,IEEE Computer Society, 2007, 289-294

[9] Ibrahim Hajjeh, Ahmed Serhrouchni, Frédérique Tastet, “ISAKMP Handshake for SSL/TLS” Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE,2003,pp-1481-1485

[10] J. Overbey, W. Traves, and J. Wojdylo, “On the Keyspace of the Hill Cipher,” Cryptologia, January 2005, 29(1), pp. 59–72.

[11] Zhao Huawei, Liu Ruixia, “A Scheme To Improve Security of SSL” Pacific-Asia Conference on Circuits, Communications and Systems, paccs, pp.401-404, 2009.

[12] P. Enge and P. Misra. Scanning the Issues/Technology. Proceedings of the IEEE, Special Issue on GPS, 87(1):11, January 1999.

[13] John A. Volpe National Transportation Systems Center Report. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System, August 2001.