Hyper Text Transfer Protocol for Securing Packet Inspection in Intrusion Prevention System Device

A Friyanto
Universitas Komputer Indonesia, Jalan Dipatiukur Nomor 112-116, Bandung, Jawa Barat, Indonesia
Email: gafriyanto@email.unikom.ac.id

Abstract. Analysis of inspection method packet HTTPS or Hypertext Transfer Protocol Secure in Intrusion Prevention System (IPS) device is to explore the methods that IPS do in analyzing HTTPS Paket. Hypertext Transfer Protocol Secure or HTTPS is data communication between client and web server in essentially is end to end secure connection. In network security, IPS device function is inspection every packet that enters and exits to internal network including packet secure connection. HTTPS packet and others secure connection packet are running packet in the network with did not plain text, but all packet was encrypted from source. Packet encryption make IPS difficult to inspection the packet and knows what the content inside the packet. One of the methods IPS to inspection the HTTPS packet is to decrypt and re-encrypt. This method makes two sections end to end secure connection. The first is secure connection between IPS and client using self-sign digital certificate. And the second is secure connection between IPS and web server using digital certificate from trust certificate authority (CA). So the method make HTTPS not end to end secure connection directly between client and web server in essentially HTTPS. However, the method succeeded in making IPS able to carry out inspections and find out the contents of the packet.

1. Introduction
The need of network access for an institution is now a necessity to connect towards the internet and to internal information systems [1]. The more network points connected, the wider the coverage and the higher the security risk. So that network development must be followed by the development of network security. Network security is an important thing to be developed to be able to secure internal networks and users to be more secure in accessing the internet. One method used to secure web servers is to use HTTPS (Hypertext Transfer Protocol Secure) or secure mode, which essentially guarantees communication between the client and server is end to end secure connection. By using HTTPS, the data transmission between the client and the web server is encrypted and can only be opened by the client or server that has the appropriate private key to open it. Thus each network device between the client and the web server cannot know the contents of the web packet that is running.

The IPS (Intrusion Prevention System) device securing networks makes trusted networks from networks not necessarily safe by filtering based on specific security policy [2]. The function of an IPS device is to check every incoming packet and determine whether to accept each packet or discard it. With IPS devices make sure each packet on the internal network is safe because each packet is checked first. But in some packets, IPS devices cannot check the contents of the packet because encryption has been done before. As in HTTPS, client and web server communication has been encrypted so that IPS...
devices cannot check each HTTPS packet. In some devices this is not possible for inspection and some other devices have their own way to do https inspection packet [3,4].

In connection with the two explanations above, there is a lack of synchronization between the IPS function for each packet inspection and the HTTPS function that encrypts end to end between client and web server, making it difficult for IPS devices to ensure that every packet which enters and exits the internal network is safe because it does not inspection of the packet. To overcome this problem, some IPS devices have their own ways to inspect HTTPS packets. One method used is to add an indirect end to end secure connection with a web server, but making an IPS device as another secure communication stage before finally an IPS device makes an end to end secure connection with a web server. Thus, the nature of HTTPS that makes end-to-end communication a secure connection between client and web has changed because with this method, secure connection communication becomes two parts, first communication between client and IPS device and second communication between IPS device and destination website server. This paper discusses the analysis of how the method is carried out and what the impact is related to the concept and purpose of the https protocol basically.

2. Research Methodology
The methodology research is based on TLS inspection [2] (See Figure 1).

![Figure 1. Research methodology](image)

Based on Figure 1, this research started from identifying the concept of HTTPS packet and encryption/decryption process with both self-sign certificate and certificate authority. If HTTPS packet is not encryption, HTTPS packet could inspect and analysis whether the package is dangerous or not.

3. Results and Discussion
In this section, the discussion will begin with HTTPS inspection in general, the concept of SSL certificates and the results of inspection analysis on IPS devices.

3.1. Inspection of HTTPS
IPS devices cannot directly inspect and analyze HTTPS packet that pass through them. This is because each HTTPS packet has been encrypted by the source of the sender. In the HTTPS concept, encryption is carried out end to end between the client and the web server by using a digital certificate from trusted Certificate Authority (CA). One method that can be done for inspection and analysis of https packets on IPS devices is the decryption & re-encryption method. With this method each device communicates that is encrypted between the client and IPS and re-encrypts the communication of the web server and IPS device. However, this method does not allow using the same digital certificate so that different encryption and digital certificates must be done. For the encryption process on communication between the Client and IPS, you can use a self-sign certificate that is generated from IPS or other servers that you have. Whereas encryption on IPS communications and web servers uses SSL certificates that are "signed" by a CA (See Figure 2).
In Figure 2, it can be seen that HTTPS communication between the client and the web server is divided into two parts. The first part is communication from the client and the IPS using a self-sign certificate and the second part is communication from the IPS and the web server using a certificate from a CA. In this picture we can see that the IPS device is decrypted and re-encrypted so that each https packet can be inspected and analyzed.

3.2. Generate the Secure Socket Layer (SSL) Certificate

OpenSSL is an open source in implementing the SSL and TLS protocols. In creating an SSL certificate, one of the services that can be used is OpenSSL. When generating the digital certificates, they ideally make a CA that will "sign" the certificate. However, for certificates in their own environment that do not require validation, they can create a self-sign certificate without requiring a CA. The type of digital certificate that can be created and used by ourselves is the Self-sign certificate. The self-sign certificate is a digital certificate that is used in SSL by creating and "signing" itself by the manufacturer so that the browser will generally be considered unsafe.

3.2.1 Private Key and Certificate Signing Request (CSRs)

When using an SSL certificate from a CA, we need to create a certificate signing request (CSR). This CSR is a public key and some additional information as a component that will be used or added to the certificate when "handled".

```bash
openssl req
   -newkey rsa:2048 -nodes -keyout domain.key 
   -out domain.csr
```

3.2.2 Generate a Self-Signed Certificate

A Self-sign Certificate is the use of an SSL certificate that does not require a CA, but by means of self-sign or "signing" the certificate itself with its own private key.

```bash
openssl req
   -newkey rsa:2048 -nodes -keyout domain.key 
   -x509 -days 365 -out domain.crt
```
3.3 Decryption and Re-Encryption on IPS Devices

The process of encryption and decryption on IPS devices is the same as the process carried out on client and server devices in general. In this case a certificate and a list of CA are needed. A digital certificate stored on IPS for the encryption and decryption process and a list of CA are needed for the validation process of the certificate. Because IPS does a Self-Sign certificate, the IPS device must have the ability to generate or import a CA. Thus, IPS devices generally have two categories, internal and external.

- Internal CAs. A list of self-made CA, both of which are generated directly on the IPS device and imported.
- Trusted CAs. A list of CA that is trusted that is used for communication of IPS devices with web servers.
- External CAs. A list of digital certificates from external.
- Internal CAs. List of digital certificates from internal IPS devices.

HTTPS communication that is built with the existence of an IPS device between the client and the web server is in principle the same which is to make end to end secure connection. But with the IPS device between the client and the web server, the end to end secure connection encryption process is divided into two. The first part is encryption end to end between the client and IPS devices and the second is the encryption of end to end between IPS devices and web servers as in Figure 2. Thus, IPS devices that are between the client and web server perform two processes:

3.3.1 Decryption Process

Decryption is the process of returning data from what has been "randomized" to return to the actual data. IPS devices decrypt each HTTPS packet received from the client and web server. The decryption process is done using a trusted CA or CA that is trusted in communication of IPS devices with web servers. By using the certificate of self-sign on communication conducted by IPS with the client (See Figure 3).

**Figure 3. An example of a Trusted Certificate Authority**
3.3.2 Re-encryption Process
Re-encryption is the process of “randomizing” data back from the actual data with the aim of being unable to be read by people who are not interested. IPS devices encrypt each HTTPS packet sent to the client and web server. The encryption process is done by using a self-sign certificate to send packets to internal clients. And the encryption process is done by using a digital certificate obtained from a trusted CA or CA that is trusted for sending packets to the web server. The encryption process on IPS to a web server is an https communication process in general such as that carried out on end to end client communication and web servers by using a certificate from a trusted CA such as the certificate in Figure 3.

3.4 Analysis of HTTPS Packet Inspection on IPS Devices
The decryption and re-encryption process described in the point (4) is intended so that each data packet can be inspected for content and its security analysis. As explained earlier, communication without encryption can be directly inspected. However, the https package requires an additional process to decrypt and re-encrypt each packet that exits and enters an IPS device.

On network security, the existence of an IPS device functions as a filter of networks that were not necessarily safe to be a safe network to be used. Any unsafe package will be blocked and discarded while a safe package will be allowed to enter the internal network. IPS devices have artificial intelligence in analyzing each packet to be categorized as safe, warning, or dangerous. By utilizing encryption on the https package which is difficult to inspect security devices, many irresponsible people use it by inserting maleware. This is certainly a gap that must be improved by making IPS devices able to inspect HTTPS or other SSL packages. With the method of decryption and re-encryption each packet that exits and enters the internal network can be inspected and analyzed first, but this method is not without flaws. By decryption and re-encryption by IPS devices in the middle between the client and the web server, communication has not become end to end communication anymore. This makes some people disagree because the re-encryption process can allow third parties to enter additional data that is not supposed to be in the re-encryption process carried out by IPS devices.

A self-sign certificate is a digital certificate that is not considered trusted by the browser application. So if the client does not manually enter a digital certificate into the browser then every time you access the https website, the client will be given a warning by the browser application.

4. Conclusion
In some conditions, security is not directly proportional to comfort. When the level of security is good, sometimes it doesn't make it too comfortable. HTTPS and IPS are both aimed at providing security. But the security provided by HTTPS by encrypting is used by some people to trick in carrying out attacks. Conversely, the IPS function for conducting inspections cannot be done directly on HTTPS because each packet has been encrypted. The IPS device technique for inspecting HTTPS packages by generating private certificates themselves has made some debate. Some parties argue that it has changed the purpose of HTTPS to make end to end secure connection. But beyond the debate, the technique is quite effective in making secure communication even though it is made additions in the midst of communication between the client and the web server. An important note in this case is that IPS devices must be able to guarantee that the decryption process and re-encryption performed on IPS devices can remain safe without the possibility of malware entering the encryption process.
References

[1] Jiang D, Xinghui L and Hua H 2011 A Study of Man-in-the-Middle Attack Based on SSL Certificate Interaction (Beijing, China)
[2] Youngxin Y 2011 The Comparative Study on Network Firewalls Performance 2011 IEE 3rd International Conference on Communication Software & Network.
[3] O’Neill M, Routi S, Seamons K and Zappala D 2017 TLS Inspection: How Often and Who Cares? IEEE Internet Computing Vol.21
[4] Preeti S, Amit A and Sapna T 2016 A comprehensive study on security attacks on SSL/TLS protocol (Dehradun, India)
[5] Jake A B and Thaier H 2017 Security issues with certificate authorities (New York, USA)
[6] Cheng K, Gao M and R Guo 2010 Analysis and Research on HTTPS Hijacking Attacks (Hubei, China)
[7] Callegati F, Cerroni W and Ramilli M 2009 Man-in-the-Middle Attack to the HTTPS Protocol (IEEE Computer Society)
[8] Muehlstein J, Zion Y, Bahumi M, Kirshenboim I.; Dubin R, Dvir A and Pele O 2017 Analyzing HTTPS encrypted traffic to identify user’s operating system, browser and application (Las-Vegas: IEEE Annual CNCC)
[9] Stricot-Tarboton S, Chaisiri S and Ko R K L 2016 Taxonomy of Man-in-the-Middle Attacks on HTTPS (Tianjin, China: Trustcom/BigDataSE/ISPA)
[10] Hazief H M, Sabustian T A, Presekal A and Guarddian G 2014 Development of University of Indonesia Next Generation Firewall Prototype and Access Control with Deep Packet Inspection 2014 International Conference on Advanced Computer Science and Information System.
[11] Lu Z, Zhou Y 2014 The Evaluation Model for Network Security fourth International Conference on communication Systems and Network Technologies.
[12] IBM Knowledge Center 2017 “Generating a self-signed certificate using OpenSSL” [online]. Available:https://www.ibm.com/support/knowledgecenter/en/SSWHYP_4.0.0/com.ibm.apimt.cmc.doc/task_apionprem_gernerate_self_signed_openSSL.html. [Accessed: Januari 3, 2019]
[13] GlobalSign 2017 “SSL Inspection – Issuing CAs and Root Considerations” [online]. Available: https://www.globalsign.com/en/blog/what-is-ssl-inspection/. [Accessed: Desember 13, 2018]