Secure Socket Layer Visualization Tool with Packet Capturing Function

Jin Shinozaki and Masayuki Arai

***Abstract*—Secure Socket Layer (SSL) has become a fundamental technology that secures browser-processed personal details sent to the server. As a result, communication and computer engineers are advised to learn the protocol. However, understanding SSL is very difficult because of its intricate communication procedure. To solve this problem, we developed a visualization tool for understanding SSL. This paper describes the design and implementation methods of the tool.**

***Index Terms*—SSL, visualization, learning, packet capturing, TCP/IP.**

I. Introduction

The Secure Socket Layer (SSL) protocol is a basic technology to maintain security between web browsers and web servers. Thus, students who intend to become computer and communication engineers are advised to learn the protocol. However, it is difficult for students to learn the concepts of the protocol by traditional learning methods, such as textbooks and lectures, because such methods apply routine communication patterns that are not as effective as using the protocols in reality. Packet capturing tools such as wireshark [1] and ssldump [2] are one solution. However, it is also difficult for students to use such tools because they are directed towards network engineers. Therefore, this paper proposes a tool for visualizing SSL with a packet capturing function.

It is assumed that the learning systems for computer networks are divided into three categories: showing effective understating of the protocol theories, showing effective understanding in constructing LANs, and providing a learning environment for constructing LANs.

Four systems were developed to teach the theories of TCP/IP for a communication and network course at a local university. Three systems teach the communication procedures and data formats with a packet capturing function [3]-[7]. The other system simulates both control methods that rarely occur in real communication and combinations of control methods [8].

Tajima et al. developed a system for high school students. That system provides teaching information on TCP/IP basic mechanisms with a packet capturing function [9]. Hayakawa et al. proposed a system that sets the IP addresses and network cables in a virtual LAN [10]. Therefore, users can learn about the Internet and data link layers. Toguro *et al.* developed a simulator that constructs a virtual network to teach network configuration [11]. Nakagawa et al. proposed a system that provides a teaching environment for constructing computer networks using VMWare [12]. In addition, Network Simulator ns-2 [13] and OPNET [14] are well-known systems that simulate computer networks.

In this paper, an SSL visualization tool with a packet capturing function for learning protocol theories is proposed.

Manuscript received July 20, 2013; revised November 1, 2013.

The authors are with the Graduate School of Science and Engineering, Teikyo University, 1-1 Toyosatodai, Utsunomiya, Tochigi, Japan (e-mail: arai@ics.teikyo-u.ac.jp).

II. SSL

This section outlines SSL [15] with reference to a website [16]. SSL has become the standard security technology for establishing an encrypted link between a web server and a browser. The link ensures that all data passing between a web server and browsers remain private and integral. SSL is an industry standard that is used on millions of websites to protect online transactions with customers.

To create an SSL connection, a web server needs an SSL Certificate. Typically, an SSL Certificate contains our domain name, organization name, address, city, state, and country. It also contains the expiration date of the Certificate and details of the Certification Authority responsible for issuance of the Certificate. When a browser connects to a secure site, it retrieves the site's SSL Certificate and checks the following: it has not expired, it was issued by a Certification Authority trusted by the browser, and it is being used by the website for which it has been issued. If any of these checks fails, the browser displays a warning to the end user letting them know that the site is not secured by SSL. All SSL Certificates are issued to either organizations or to the legally accountable individuals.

When we choose to activate SSL on our web server, we are prompted to complete a number of questions about the identity of our website. Our web server then creates two cryptographic keys: a private key and a public key.

The public key does not need to be secret and is placed into a Certificate Signing Request (CSR), a data file also containing our identity details. We then submit the CSR. During the SSL Certificate application process, the Certification Authority validates our details and issues an SSL Certificate containing our details and allows us to use SSL. Our web server matches our issued SSL Certificate with our private key. Our web server is then able to establish an encrypted link between the website and our customer's web browser.

The complexities of the SSL protocol remain invisible to our customers. Instead, their browsers provide them with a key indicator to let them know they are currently protected by an SSL encrypted session.

As mentioned above, SSL is a very useful but

DOI: 10.7763/IJFCC.2014.V3.293

complicated protocol. Therefore, it is difficult for learners to understand it.

Fig. 1. The main window of the tool.

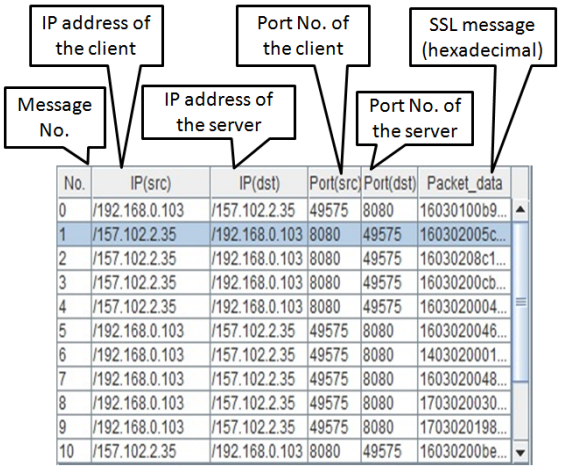

Fig. 2. The brief information table for SSL messages.

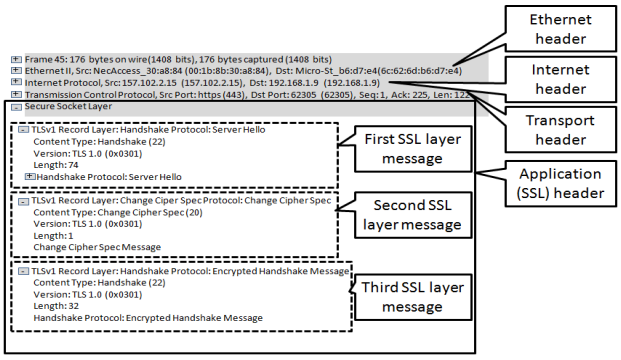

Fig. 3. An example of a packet consisting of three SSL messages.

III. Outline of the Visualization Tool

We defined the following requirements for the visualization tool to support user understanding:

- Recognize how to establish an SSL connection between the server and the client.
- Provide real communication patterns using packets that the client sends or receives.
- Display only important data for understanding SSL and packet capturing without providing extra data.

To satisfy the abovementioned requirements, we developed the tool shown in Fig. 1. The tool consists of the following four sub-windows: a brief information table for messages (Fig. 1(1)); an explanation for each message (Fig. 1(2)); the entire SSL communication flow (Fig. 1(3)); and the sequence diagram between the client and the server (Fig. 1(4)). The tool uses Jpcap [17] to capture packets that the user computer sends and receives and JGraph [18] to draw the sequence diagram.

IV. Functions and Implementation Methods of the Tool

This section depicts the functions of the visualization tool and the methods to implement the functions.

A. Dividing Packet and Displaying Messages

The tool starts to capture packets when the user clicks the start button (Fig. 1(5)). After completing the packet capturing, the tool displays all SSL messages, as shown in Fig. 2. A row in Fig. 2 represents one SSL message, and each column shows the message number, the IP address of the client computer, the IP address of the server computer, the port number of the client computer, the port number of the server computer, and the SSL message.

A packet is comprised of an ethernet, a network, a transport, and an SSL application header, as shown in Fig. 3. Furthermore, the SSL application header consists of messages, as shown in Fig. 3. The SSL application header in Fig. 3 has three messages: Server Hello, Change Cipher Spec, and Encrypted Handshake. Therefore, we implemented a function into the tool to divide a packet into each message.

At this point, if a user clicks a row in the table, the other three sub-windows (Fig. 1(2)(3)(4)) change according to the

selected message.

B. Displaying Details and Explanation for the Selected Message

The tool can display details and explanations for the selected message, as shown in Fig. 4. Users can select the message by clicking a row in the brief information table (Fig. 2) or an arrow in the sequence diagram (Fig. 1(4)). Fig. 4 depicts an example of the detail and the explanation for the selected message. The detail has the following information: SSL version, content type, handshake type, Certificate Authority, IP addresses, and port numbers, as shown in Fig. 4.

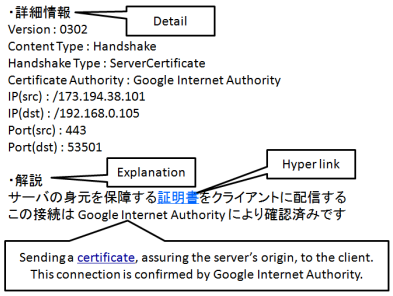

Fig. 4. An example of the detail and explanation for the selected packet.

If the explanation includes difficult technical words (for example, the explanation in Fig. 4 includes the difficult word "Certificate"), the difficult words have hyperlinks to dictionary websites such as e-Words [19]. Therefore, users can obtain more information from the sites.

C. Displaying Communication Flow and Role of Each Message

The tool is able to display the entire SSL communication flow, as shown in Fig. 5. The message selected in the brief information table (Fig. 2) or the sequence diagram (Fig. 1(4)) is shown with red characters. Therefore, users can understand how the message works in the entire SSL procedure. Fig. 5 is an example in which the handshake message "Server Hello" is selected.

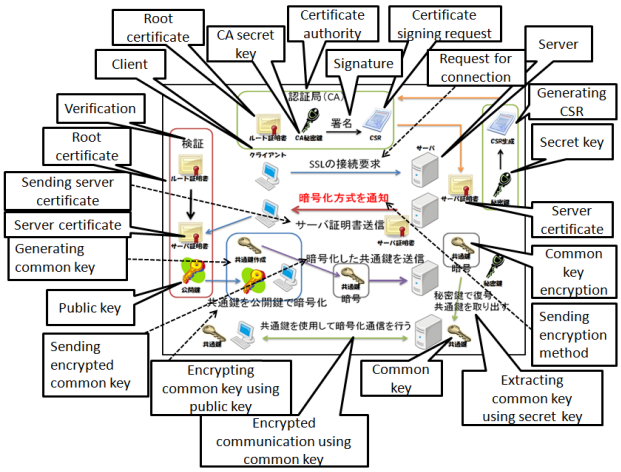

Fig. 5. An example of a display of SSL communication flow and roles of each message.

D. Displaying Message Sequence Diagram between Server and Client

The tool can display the sequence diagram for the messages communicated between the server and the client of the users, as shown in Fig. 6. The numbers and messages in Fig. 6 correspond to those in the brief information table (Fig. 2). If a user clicks an arrow in the diagram, the other three sub-windows (Fig. 1(1) (2) (3)) change according to the selected message.

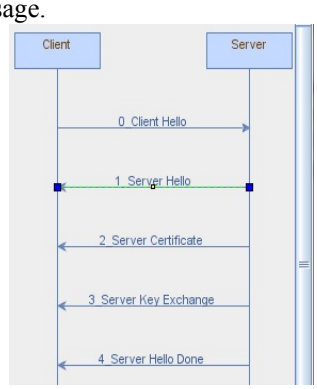

Fig. 6. An example of the message sequence diagram between a server and a client.

V. Conclusion

SSL has grown to be a fundamental technology that secures browser-processed personal details sent to the server. However, it is difficult to understand SSL because of its complicated communication procedure. We developed a visualization tool to help learners understand this procedure. Further evaluation is planned through actual use in a class.

Acknowledgment

The authors would like to thank the members of the Arai Laboratory, Department of Human Information Systems, School of Science and Engineering, Teikyo University and the Graduate School of Science and Engineering, Teikyo University for their useful advice and help in the system evaluation. This study was supported in part by the Japan Society for the Promotion of Science; Grant Number (KAKENHI 24501150).

References

[1] Wireshark. [Online]. Available: http://www.wireshark.org/
[2] Ssldump. [Online]. Available: http://www.rtfm.com/ssldump/
[3] M. Arai, S. Takahashi, and G. Kitamura, "Visualization tools for learning TCP/IP," in *Proc. of the 2010 IEEE-RIVF International Conference on Computing and Communication Technologies*, 2010, pp. 262-266.
[4] M. Arai, "TCP/IP visualization systems with a packet capturing function," *International Journal of Information and Education Technology*, vol. 2, no. 4, pp. 291-293, 2012.
[5] S. Takahashi and M. Arai, "Development and evaluation of visualization tools for understanding the control method of TCP packet arrival order and the difference between TCP and UDP," in *Proc. The 12th IEEE International Conference on Computer and Information Technology (CIT2012)*, 2012, pp. 140-143.
[6] T. Yanase and M. Arai, "TCP/IP application protocol visualization system with a packet capturing function," in *Proc. The 2011 2nd International Congress on Computer Applications and Computational Science*, 2011, pp. 8-7.
[7] M. Arai, N. Tamura, H. Watanabe, C. Ogiso, and S. Takei, "Design and implementation of a learning tool for TCP/IP protocols," in *Proc. the 9th International Conference on Computers in Education*, vol. 2, 2001, pp. 1010-1015.
[8] M. Arai, H. Watanabe, C. Ogiso, and S. Takei, "A learning tool for TCP/IP control methods," in *Proc. the 11th International Conference on Computers in Education*, vol. 1, 2003, pp. 814-815.
[9] H. Tajima and H. Mukaidani, "Development of visual teaching materials for understanding TCP/IP protocol in subject "Information," *Japan Society for Educational Technology Research Reports*, JSET05-6, 2005, pp. 7-10.

[10] M. Hayakawa, K. Tanno, H. Yamamoto, M. Nakayama, and Y. Shimizu, "Development of LAN construction simulator and an improvement of the educational method," in *Proc. the 26th Annual Conference on Japanese Society for Information and Systems in Education*, E5-4, 2001, pp. 367-368.
[11] M. Toguro and M. Kimura, "Development of education-oriented network simulator," *The 65th National Convention of Information Processing Society of Japan*, 2D-2, 2003, pp. 4273-4274.
[12] Y. Nakagawa, H. Suda, and Y. Miida, "Development of a LAN configuration support system for study using VMware," *Transactions of Japanese Society for Information and Systems in Education*, vol. 24, no. 2, 2007, pp. 126-136.
[13] The Network Simulator-ns2. [Online]. Available: http://www.isi.edu/nsnam/ns/
[14] OPNET. [Online]. Available: http://www.opnet.com/.
[15] SSL rfc6101. [Online]. Available: http://tools.ietf.org/html/rfc6101
[16] SSL. Com. Knowledge Base. [Online]. Available: info.ssl.com/article .aspx?id=10241/
[17] Jpcap. [Online]. Available: http://sourceforge.net/projects/jpcap/
[18] JGraph. [Online]. Available: http://www.jgraph.com/
[19] E-Words. [Online]. Available: http://e-words.jp/.

Jin Shinozaki graduated from Department of Science and Engineering, Teikyo University, Japan in 2013. He was mainly engaged in developing the tool. At present, he works in NTT-ME Corporation.

Masayuki Arai is a professor in the Graduate School of Sciences and Engineering at Teikyo University. He received his B.E. degree from Tokyo University of Science in 1981 and Dr. Eng. degree from Utsunomiya University in 1995. His research interests include pattern recognition, natural language processing and information visualization. He is a member of the Information Processing Society of Japan and IEEE.