MATEC Web of Conferences **28**, 06004 (2015)
DOI: 10.1051/matecconf/20152806004

Development and Evaluation of Secure Socket Layer Visualization Tool with Packet Capturing Function

Masayuki Arai

Graduate School of Science and Engineering, Teikyo University, Utsunomiya, Japan

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, implementation methods, and evaluation of the tool. The evaluation results show that the visualization tool is effective for learning SSL.

1 Introduction

The Secure Socket Layer (SSL) protocol is a fundamental technology that secures browser-processed personal details sent to the server. 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. A packet capturing tool such as wireshark [1], is one solution. However, it is also difficult for students to use such tools because they are directed towards network engineers. Therefore, we developed a tool for visualizing SSL with a packet capturing function [2]. This paper shows evaluation results of the tool.

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.

2 Outline of the 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 [2] 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 [15] to capture packets that the user computer sends and receives and JGraph [16] to draw the sequence diagram.

3 Function and Implementation Methods of the Tool

[a] Corresponding author: arai@ics.teikyo-u.ac.jp

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

3.1 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.

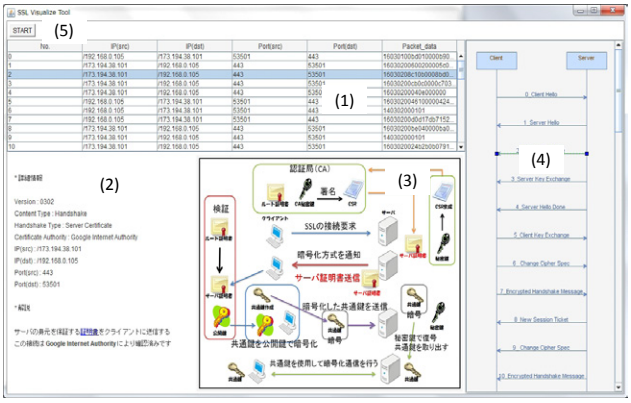
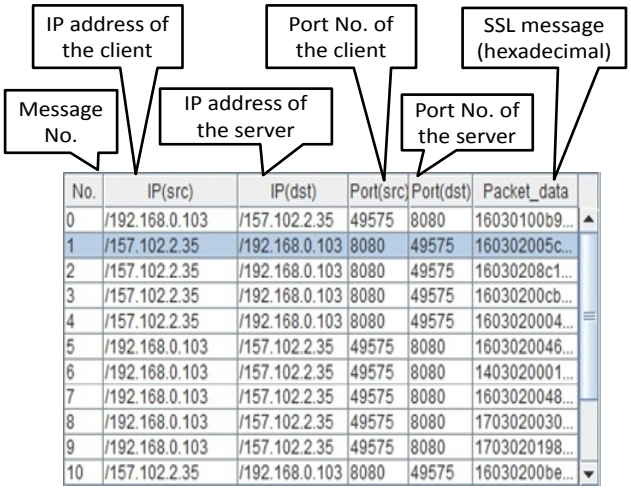


Figure1. The main window of the tool



No.	IP(src)	IP(dst)	Port(src)	Port(dst)	Packet_data
0	/192.168.0.103	/157.102.2.35	49575	8080	16030100b9...
1	/157.102.2.35	/192.168.0.103	8080	49575	160302005c...
2	/157.102.2.35	/192.168.0.103	8080	49575	16030208c1...
3	/157.102.2.35	/192.168.0.103	8080	49575	16030200cb...
4	/157.102.2.35	/192.168.0.103	8080	49575	1603020004...
5	/192.168.0.103	/157.102.2.35	49575	8080	1603020046...
6	/192.168.0.103	/157.102.2.35	49575	8080	1403020001...
7	/192.168.0.103	/157.102.2.35	49575	8080	1603020048...
8	/192.168.0.103	/157.102.2.35	49575	8080	1703020030...
9	/192.168.0.103	/157.102.2.35	49575	8080	1703020198...
10	/157.102.2.35	/192.168.0.103	8080	49575	16030200be...

Figure 2. The brief information table for SSL messages

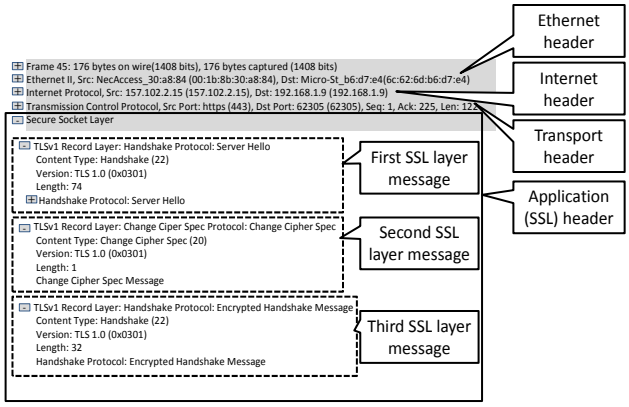


Figure 3. An example of a packet consisting of three SSL messages

3.2 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)). Figure 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. 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 [17]. Therefore, users can obtain more information from the sites.

3.3 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. Figure 5 is an example in which the handshake message “Server Hello” is selected.

3.4 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.

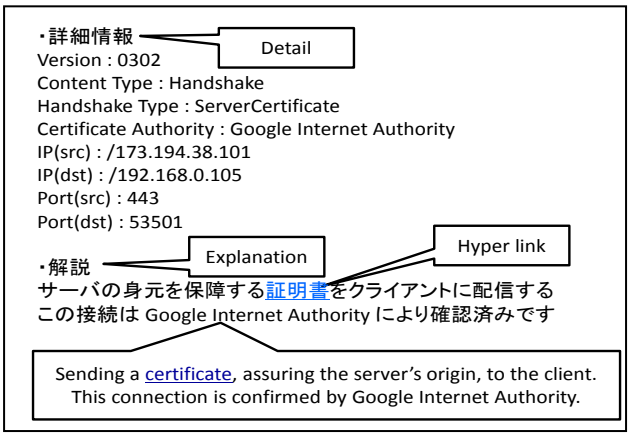


Figure 4. An example of the detail and explanation for the selected packet

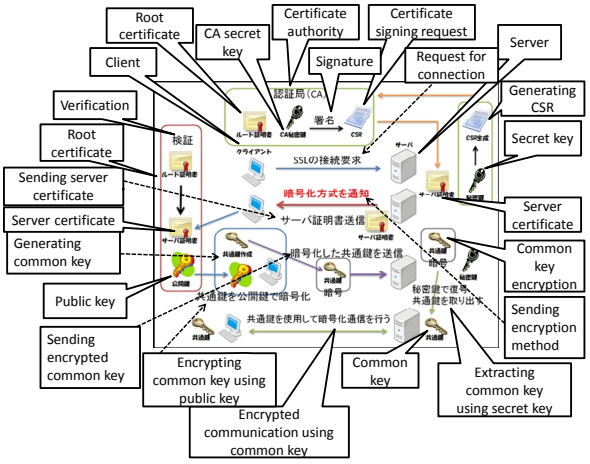


Figure 5. An example of a display of SSL communication flow and roles of each message

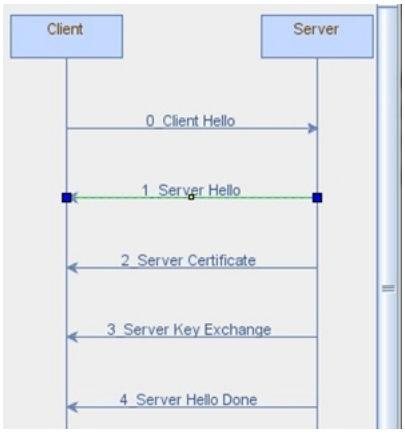


Figure 6. An example of the message sequence diagram between a server and a client

4 Evaluation And Discussion

For evaluations, we prepared three kinds of learning materials: the proposed tool, ten printed pages from a textbook [18], and wireshark [1]. Twelve students at the School of Science and Engineering, Teikyo University, used the materials to learn SSL. These students (two graduate school students, three juniors, and seven seniors) had already completed a TCP/IP course. After learning, a questionnaire was distributed to assess the students' evaluations of the tool.

4.1 Contents of the questionnaire

The following questions and example answers were provided to evaluate the learning effectiveness of the tool.

Question 1: How much do you understand the roles of the following SSL messages using the tool?
- Client hello and Server hello
- Server certificate
- Server key exchange
- Client key exchange
- Flow of key exchange

Question 2: How much do you understand the SSL communication flow using the tool?

Question 3: Which is the best learning material to understand each SSL message?

Question 4: Which is the best learning material to understand the SSL communication flow?

Question 5: Other questions:
- Are you interested in learning SSL using the tool?
- Do you want to study SSL more deeply using the tool?
- Do you hope to use the tool again?

4.2 Contents of the questionnaire

All twelve students answered the questionnaire.

(1) Questions 1 and 2: The results of questions 1 and 2 are shown in Table 1.
For question 1, the message "Client hello and Server hello" was fully understood by eight learners and almost understood by two learners. For other messages in question 1, most learners answered that they fully or almost understood the messages by using the tool.

Similally, for question 2, most learners answered they understood the SSL communication flow by using the tool.

(2) Questions 3 and 4: The results of questions 3 and 4 are shown in TABLE 2. (A), (B) and (C) in TABLE 2 represent the tool, the textbook, and wireshark, respectively.

For question 3, two learners answerd the best way to understand each SSL messege was using the tool. Nine learners answered using both the tool and the textbook was best. In contrast, for question 4, eight learners answered the best way was using the tool. In any case, for both questions, all answers included the tool.

(3) Question 5: Figure 7 shows the result of question 5. Approximately 70% of the users answered they wanted to use the tool again. Over 50% of the users were interested in learning SSL by using the tool.

Table 1. Results of questions 1 and 2

		Fully understand	Almost understand	Moderately understand	Insufficiently understand	Cannot understand
Q1	Client hello and Server hello	8	2	2	0	0
	Server certificate	9	2	1	0	0
	Server key exchange	6	5	1	0	0
	Client key exchange	6	3	2	0	1
	Flow of key exchange	5	4	3	0	0
Q2	SSL communication flow	7	4	1	0	0

Table 2. Results of questions 3 and 4

	(A)	(B)	(C)	(A)&(B)	(A)&(C)	(B)&(C)	(A),(B) &(C)
Q3	2	0	0	9	0	0	1
Q4	8	0	0	3	0	0	1

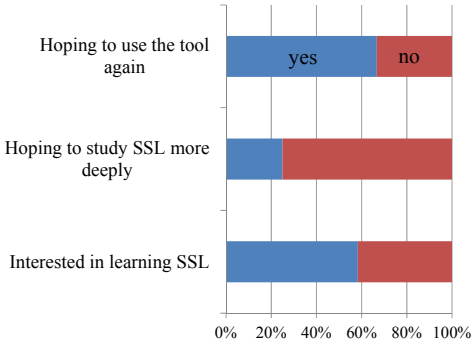


Figure 7. Result of question 5

5 Conclusions

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. The evaluation results show the tool is effective for learning SSL. Further evaluation is planned through actual use in a class.

Acknowledgements

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 http://www.wireshark.org/ (May 24, 2014 access).
2. Shinozaki,J. & Arai,M., Secure Socket Layer Visualization Tool with Packet Capturing Function, *International Journal of Future Computer and Communication*, 3(3), pp,187-190, 2014.
3. Arai,M., TCP/IP Visualization Systems with a Packet Capturing Function, *International Journal of Information and Education Technology*, 2(4), pp.291-293, 2012.
4. Arai,M., Takahashi,S. & Kitamura,G., Visualization Tools for Learning TCP/IP, *Proc. of the 2010 IEEE-RIVF International Conference on Computing and Communication Technologies*, pp. 262-266, 2010,.
5. Arai,M, Tamura,N., Watanabe,H., Ogiso,C. & Takei,S, Design and Implementation of a Learning Tool for TCP/IP Protocols, *Proc. of the 9th International Conference on Computers in Education*, 2, pp. 1010-1015, 2001.
6. Takahashi,S. & Arai,M. Development and Evaluation of Visualization Tools for Understanding the Control Method of TCP Packet Arrival Order and the Difference between TCP and UDP, *The 12th IEEE International Conference on Computer and Information Technology*, pp.140-143, 2012.
7. Yanase,T. &a Arai,M., TCP/IP Application Protocol Visualization System with a Packet Capturing Function, T*he 2011 2nd International Congress on Computer Applications and Computational Science*, 8-7, 2011.
8. Arai,M., Watanabe,H., Ogiso,C. & Takei,S., A Learning Tool for TCP/IP Control Methods, *Proc. of the 11th International Conference on Computers in Education*, 1, pp. 814-815, 2003.
9. Tajima,H. & Mukaidani,H., Development of Visual Teaching Materials for Understanding TCP/IP Protocol in Subject "Information", *Japan Society for Educational Technology Research Reports*, JSET05-6, pp. 7-10, 2005 (in Japanese).
10. Hayakawa,M., Tanno, K., Yamamoto,H., Nakayama,M. & Shimizu,Y., Development of LAN Construction Simulator and an Improvement of the Educational Method, *The 26th Annual Conference on Japanese Society for Information and Systems in Education*, E5-4, pp. 367-368, 2001 (in Japanese).
11. Toguro,M., & Kimura,M., Development of Education-Oriented Network Simulator, *The 65th National Convention of Information Processing Society of Japan*, 2D-2, pp. 4-273 - 4-274, 2003 (in Japanese).
12. Nakagawa,Y., Suda,H. & Miida,Y., Development of a LAN Configuration Support System for Study Using VMware, *Transactions of Japanese Society for Information and Systems in Education*, 24(2), pp. 126-136, 2007 (in Japanese).
13. The Network Simulator-ns2 http://www.isi.edu/nsnam/ns/ (May 24, 2014 access).
14. OPNET http://www.opnet.com/ (May 24, 2014 access).
15. Jpcap http://sourceforge.net/projects/jpcap/ (May 24, 2014 access).
16. JGraph http://www.jgraph.com/ (May 24, 2014 access).
17. e-Words http://e-words.jp/ (May 24, 2014 access).
18. Rescorla,E. *SSL and TLS: Designing and Building Secure Systems*, Addison-Wesley, 2001.