On Securing Web-based Educational Online Gaming: Preliminary Study

Kadek Restu Yani*, Ary Setijadi Prihatmanto** and Kyung-Hyune Rhee*

*Department of IT Convergence and Application Engineering,
Pukyong National University, Republic of Korea
**School of Electrical Engineering and Informatics,
Bandung Institute of Technology, Indonesia
kadekyani@pukyong.ac.kr, asetijadi@lskk.ee.itb.ac.id, khrhee@pknu.ac.kr

Abstract

With the deployment of web-based educational game over the internet, the user's registration becomes a critical element. The user is authenticated by the system using username, password, and unique code. However, it cannot be handled properly because the data is transmitted through insecure channel on the network. Hence, security requirement is needed to avoid identity leakage from malicious user. In this paper, we propose a secure communication approach using SSL protocol for an online game. We also describe the security requirements for our approach. In future work, we intend to configure and implement the SSL protocol by enabling HTTPS in web-based online game.

1. Introduction

New technologies and high-speed internet connections have helped online gaming become the most popular application used by people on the internet [1]. Online gaming includes internet gaming, web gaming (gaming in a web-browser), and mobile gaming [2]. Online games are diverse to include adventure games, sports games, strategy games and educational games. Usually, developers use different models to deploy their online gaming services which depend on who are the target users of the game [2]. It is important to consider the requirement needed and to find out whether the security issues are relevant to a specific game [2].

Educational games is mostly developed in web gaming because of the flow of system and the content adjusted to the learning objectives [3]. There are many online educational games that can be accessed for free or at a charge. Commonly, online gaming needs user's personal information during account registration to ensure that only an authorized player can play the game [2]. In this case, security is needed in order to prevent a malicious user who wants to get any information for ulterior purpose.

The study proposes a web-based educational online gaming architecture which allows the users using a unique code, beside a password and a username for registration. The purpose of the proposed design is to control access to an authorized student who plays the game according to their school, teacher and the class level. The study focuses on securing data sharing of user registration which take place in network communication between client and server using SSL protocol, in order to prevent data theft, otherwise many illegal users can play the game.

2. Motivation

Security in online game is very important to protect all elements and critical data are involved on game such as, privacy data user, score, money, etc. [2]. Any malicious behavior become major issues in online gaming such as, phishing attack and eavesdropping. Phishing attack is the attempt to acquire sensitive information such as username, password, and credit card details by masquerading as a trustworthy entity in an electronic communication [4]. In online gaming, an attacker may perform their malicious activity to leakage the identity such as, user ID and password during the data

communication occur for many purposes such as, to play free game or manipulate the data gaming. The attacker may perform phishing attack which contains a fake link in a message or pop-up windows that are highly infected with malware, with the intention to bring users to the website and extract confidential details from them during electronic communication.

Another threat is eavesdropping attacks. Eavesdrop also widely used by attacker in online games [2]. The attacker will launch Man-in-the-Middle attack (MITM) to listens and intercept the communication between a client and a server, and tries to discover the client's password [2]. By considering this kind of the security threats, the process of data sharing between a client and a server in Vidyanusa game must be through in secure channel in order to prevent an unauthorized user played the game. The detail about Vidyanusa is found in section 5.

3. Related Work

In this section, we briefly explain about the previous paper which study on securing online registration using SSL protocol. In [5], design and apply an SSL protocol in order to protect the biometric information when send it to the Hospital Information System (HIS) from a mobile devices. The author in [6, 7], used the HTTPS to protect HTTP attacks by encrypting HTTP message in the web pages. The URLs of the web pages using HTTPS begin with https://, and the data transmitted through port 443 by default. In [8], the author modify the Email Based Identification and Authentication (EBIA) to propose a protocol for user registration. Specifically, the Mail Servers that are accessed securely with SSL/TLS protocol by the email account owners to fetch the email messages in their inbox.

We intend to adopt the version SSL protocol [6] is shown in Fig. 1 that will be implemented in our system. In this case, we need to protect a sensitive data so that, it cannot be intercepted by an attacker during transmission over the internet. Therefore, the server can prove that the user who request for access is the legitimate user belong to the system.

4. SSL Protocol Preliminaries

The Secure Socket Layer (SSL) protects the communications by encrypting messages with a secret key which negotiated in the SSL handshake protocol [9]. The protocol is used by most e-commerce and banking web sites. It guarantees privacy and authenticity of information exchanged sent via HTTPS between a web server and a web browser [6]. To enable SSL on a website, we need to get a SSL Certificate for authorized identity and install it on the server. The certificate is digitally signed by a certificate authority, in which the client is responsible of verifying [10]. The Certificate Signing Request (CSR) and RSA key are two components involved in the generation of an SSL certificate [11], [12].

In SSL protocol, well-known a handshake process which is the initial process to establish an SSL/TLS connection before the client and server perform data exchange. The aim is both parties have to agree on a chipper suit which includes key exchange and encryption algorithm that will be used to the data exchange each other [6].

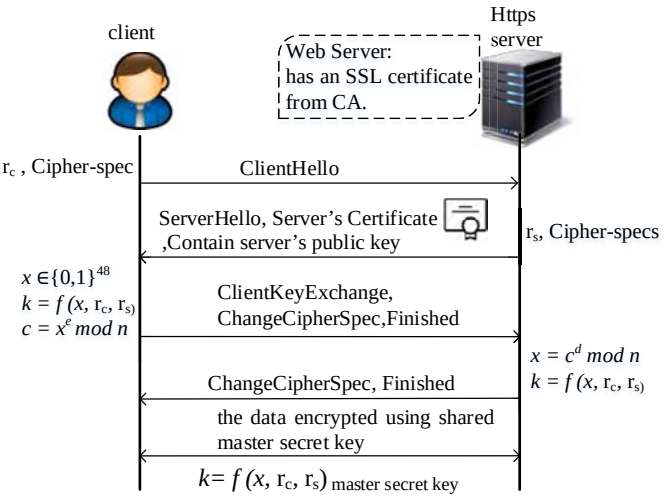

Fig. 1. SSL handshake protocol

Fig. 1 depicts the basic SSL protocol handshake process using RSA key exchange with no client certificates [6]. The following is explanation for each phase which are:

1. The client sends a *ClientHello* message to the server. This indicates that the client want to initialize a SSL session. The message includes an initial random nonce r_c and the cipher suites of a client's support.
2. The server responds with the *ServerHello* message which includes server's digital certificate, server's public key and a random nonce r_s. In addition, a server sends a cipher suites which is specified by the server choice from among client candidates.
3. In this section, a client chooses a secret random 48-byte *pre-master secret* x and

computes the shared master secret k by inputting values of x, r_c, r_s into hash function f. Then, the client encrypts x with the server's public key and attaches the cipher text in a *ClientKeyExchange* message that is sent to a server. This message indicates that a client sends the negotiation of the session key to a server that should be negotiated each other for the data exchange encryption. Also, a client sends the *ChangeCipherSpec* message that aims to confirm the server for the subsequent of entire message within a current session will be encrypted using derived from a session key.

4. The server decrypts the *pre-master secret* using server's private key, and uses x value to compute the shared *master secret* as $f(x, r_c, r_s)$. Then, the server sends a *ChangeCipherSpec* message to the client includes a key hash that indicates confirm the *master key* and the handshake process is finish.
5. Finally, the shared *master secret* k will be used for encrypting application data exchange during communication over the network.

5. System model of Vidyanusa

Our system called Vidyanusa which consist of dashboard site and game area as main application which is developed on web-based platform. Fig. 2 shows both student and teacher are required to register for access user in Vidyanusa. Student can play the game and access their portfolio, while the teacher can manage the student by accessing student account, notification, game score and the student's report/progress. Officially, this game has timing to use it when a conventional learning takes place together in classroom by the student and the teacher.

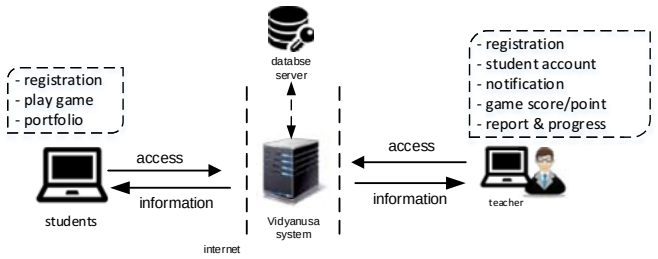

Fig. 2 System model of Vidyanusa

The teacher will give the students a unique code indirectly for registration and at the same time, a teacher will check and verify a notification to allow the students to join in the teacher's class and access the system to play the game. The purpose of proposed design is to manage access of an authorized student who plays the game according to their school, teacher and class level.

The user identity should be protected during transmitted to the server over the network, otherwise, it will be dangerous because many illegal user may be able to use it to establish accounts on user's behalf and can play the game. Moreover, the teacher has many illegal students by attacker who want play the game for free in their class while the teacher does not realize with that because the attacker use the victim account. Fig. 3 shows the possibility malicious attack to identity theft in Vidyanusa.

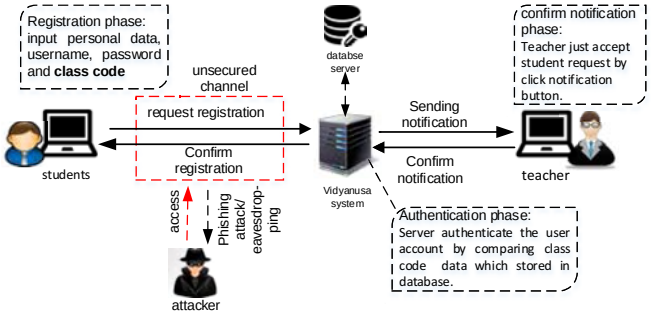

Fig. 3 Possibility malicious attack in Vidyanusa

By enabling SSL protocol in our system to secure communication over the network, the server can guarantee that the users who are accessing the system is an authorized owner of unique code and also we assume that the server is trusted authority.

6. Security requirement

In this study, we consider the following security requirements to design the proposed approach:

a. User authentication: The student should be authenticated by the server to ensure the identity which is derived from an authorized users. The authentication is performed by comparing the unique code which is stored on server with the one sent by user during registration. In this case, the real user identity will stored on server to be used as an authentication when user login to access the system again.
b. Data confidentiality: During data sharing between a client and a server, the system perform an encryption and decryption technique to keep the sensitive information from all client but only those authorized user can have it.

7. Conclusion

In this paper, our approach guarantees the authenticity of the user identity that used to create a user registration in Vidyanusa system. The user identity will be sent through a secure channel which is established by SSL. The message will be authenticated by the server to verify that the user request is the legitimate user who has access to this system according to unique code belonging to the user. In fact, once the connection between users and Vidyanusa is established, the server has certainty that the user is the real owner of the provided unique code. As a consequence, the web server can assume that there exist an adequate channel to send the verification of new account to access Vidyanusa. In future work, we intend to analyze the security requirement of our approach and implement the proposed approach.

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. NRF-2014R1A2A1A11052981).

References

[1] Michael J., Daniel S., Sven S., Tobias H., “Gaming in the clouds: QoE and the users’ perspective”, in: Mathematical and Computer Modelling, 2013, 57, pp. 2883- 2894.

[2] R. van Summeren, Security in online gaming, Available Bachelor Thesis Information Science, January 2011.

[3] Ling He, Min Fu, and Xiaoqiang Hu, “To Improve the Social Interaction of Web-based Collaborative Learning via Online Educational Games for Multi player”, 2010, in: 2nd International Conference on Education Technology and Computer (ICETC), 2, pp. 187-189.

[4] C. Wilson and D. Argles, “The Fight Against Phishing: Technology, the End User and Legislation”, In: Information Society (i-Society), 2011 International Conference, and pp. 501-504.

[5] J.-P. Lee, Y. H. Kim and J. K. Lee, "SSL Application for Managed Security between the Mobile and HIS Biometric Information Collection Client," in Advanced Information Networking and Applications Workshops (WAINA), 2014 28th International Conference on, 2014.

[6] Y. Zi and P. Xu, "The research of improving SSL handshake performance," in Information Science and Technology (ICIST), International Conference on. IEEE, 2013.

[7] T.W. van der Horst, K.E. Seamons, “Simple Authentication for the Web”, in: SecureComm, 2007, pp. 473- 482.

[8] J. Diaz, D. Arroyo, Francisco B. Rodriguez, “On securing online registration protocols: Formal verification of a new proposal”, in: Knowledge-Based Systems, 2014, 59, pp. 149-158.

[9] Yun Zi and Ping Xu, “The Research of Improving SSL Handshake Performance”, in: Third International Conference on Information Science and Technology, 2013, pp. 757-760.

[10] A. O. Freier, P. Karlton, and P. C. Kocher, “The Secure Sockets Layer (SSL) Protocol Version 3.0,” RFC 6101 (Historic), Internet Engineering Task Force, Aug. 2011.

[11] L.D. Manik, S. Navkar, “On security of SSL or TLS-enabled applications”, in: Applied Computing and Informatics, 2014, 10, pp. 68-81.

[12] Lin-Shung H., Alex R., Erling E., Collin J., "Analyzing Forged SSL Certificates in the Wild", in: IEEE Symposium on Security and Privacy, 2014, pp. 83-97.