JFMSE, 28(3), pp. 790~798, 2016.
수산해양교육연구, 제28권 제3호, 통권81호, 2016.
www.ksfme.or.kr
http://dx.doi.org/10.13000/JFMSE.2016.28.3.790

On Securing Web-based Educational Online Game Using SSL Protocol

Kadek Restu Yani* · Yoga Priyana** · Pranoto H. Rusmin* · Kyung-Hyune RHEE*†
(*†Pukyong National University, Republic of Korea · **Bandung Institute of Technology, Indonesia)

SSL 프로토콜을 이용한 안전한 웹기반 교육용 온라인 게임

카댁 르스투 야니* · 요가 프리야나** · 프라노토 루스민* · 이경현†
(*†부경대학교 · **반둥 과학기술 대학교)

Abstract

Currently, web-based online games is becoming popular in supporting learning process due to their effective and efficient tool. However, online games have lack of security aspect, in particular due to increase in the number of personal information leakage. Since the data are transmitted over insecure channel, it will be vulnerable of being intercepted by attackers who want to exploit user's identity. This paper aims to propose an online web-based educational game, Vidyanusa which allows the students to register their personal information using a unique code, a user name and a password. It manages the users according to their schools, subject teachers and class levels. In addition, by adopting a unique code, the confidentiality of the user identity can be kept away from attackers. Moreover, in order to provide a secure data communication between client and server, Secure Socket Layer (SSL) protocol is adopted. The performance of the system after implementing SSL protocol is examined by loading a number of requests for various users. From the experiment result, it can be concluded that the SSL protocol can be applied to web-based educational system in order to offer security services and reliable connection.

Key words : Digital learning, Game-based learning, Vidyanusa, SSL protocol, HTTPS connection

Ⅰ. Introduction

Educational online gaming becomes a hot issue as an alternative tool that can be used to support the classroom learning process (He, Fu, & Hu, 2010; Yani & Rhee, 2015). As the most widely used in the world, online games suffer from security problems such as stealing the user identity which is conducted by malicious users (Van Summeren, 2011). Therefore, security is needed to protect the user's identity. Additionally, elements such as score and money are included in the games, and need to be protected from malicious users (Yani, Setijadi, & Rhee, 2015). Nowadays, there are many well-known threat in online gaming such as piracy, phishing attack and eavesdropping (Van Summeren, 2011). In online gaming, phishing attacks are used for theft of user identity, which includes username and password, necessary to play game or manipulate gaming data (Wilson & Argles, 2011). In web-based online games, a phisher can produce an imitation of a website that looks similar

† Corresponding author : 051-629-6247, khrhee@pknu.ac.kr
※ This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government MSIP (No. NRF-2014R1A2A1A11052981)

to the legitimate one (Shi & Saleem, 2012). Next, eavesdropping attack is widely used by attackers in online gaming; when the attacker try to listen to all communication between the client and the server, and tries to discover the client's password and username to commit fraud (Ki, Cheon, Kang, & Kim, 2004; Yani, Rusmin, & Rhee, 2015).

Considering the threats in online gaming, the process of data sharing between the client and the server must be through a secure channel in order to protect the personal identity of users, otherwise many illegal user can play the game. Our research is primarily focused on developing a secure online web-based educational game, Vidyanusa, along with securing user's identity during registration process. Vidyanusa allows the users to use a unique code, besides the username, password and other information for account registration. A more detailed explanation of Vidyanusa can be found in Section 3 (System model of Vidyanusa). The security is guaranteed by using Secure Socket Layer (SSL) protocol through encryption of information exchanged via Hyper Text Transfer Protocol Secure (HTTPS) connection.

Ⅱ. Related Work

This section briefly explains the literature work associated with our research. Most of the existing researches use SSL protocol to provide a secure communication and data transmission over the Internet. Zi and Xu have implemented the BS1PRSA in SSL web server to improve the SSL handshake performance (Zi & Xu, 2013). A further speedup is obtained by proper use of batch technique, and shifting some decryption work to SSL clients. The theoretical value shows a substantial speedup to SSL handshake. The author in (Rescorla, 2000), enables HTTPS to protect HTTP attacks by encrypting HTTP message in the web page. The URLs of the web pages using HTTPS begin with https://, and by default the data is transmitted through port 443. In (Diaz, Arroyo, & Rodriguez, 2014), the authors proposed a modified Email Based Identification and Authentication (EBIA) protocol for user registration. By securely accessing the Mail Servers with SSL protocol, the email account owners can specifically fetch the messages in their inbox. In (Lee, Kim, & Lee, 2014), the researchers designed and applied an SSL protocol to protect the biometric information sent to the Hospital Information System (HIS) from mobile devices.

We intend to adopt the SSL protocol version from (Shacham & Boneh, 2001; Zi & Xu, 2013) to implement in our system. To verify the user authentication, we use a unique code as one of the data that is sent to the web server during registration. The unique code is authenticated by the server to verify a legitimate user, so the data transmission will be encrypted using SSL protocol to protect the data confidentiality (Shacham & Boneh, 2001).

Ⅲ. System model of Vidyanusa

1. System Environment

Vidyanusa is an online education game being developed by the Crayonpedia Education Ecosystem in Indonesia. Vidya means education and Nusa an island. Vidyanusa is an online mathematical educational game as a digital learning tool which combines e-learning and gamification. This game is expected to be accessed online by average one

million students. The learning goal of Vidyanusa is to engage junior high school students in learning mathematics with fun and attractive learning method. In other side, by simulating the mathematic material into game concept, it will reduce the negative stereotype from students that mathematic is the most difficult subject matter to study. Moreover, this game engages the students to explore the game by solving the problem by their solution. The content of Vidyanusa focusing on 7th, 8th, and 9th grade students in junior high school who are accustomed to playing computer. The mathematical subject accordance with the curriculum of 2013 states of Indonesia. Based on the syllabus, Vidyanusa collect all the material and turn into 23 missions of the game.

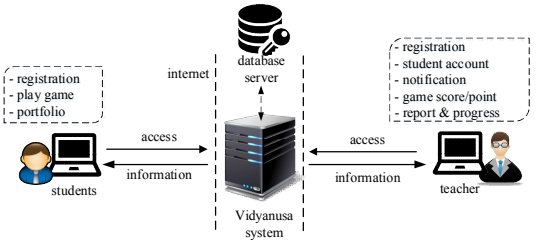
In developing Vidyanusa, the concept of the game is important because the game indicators that are used can be related to the subject matter. Therefore, game indicators ensure that all game quests are representative of the subject matter that is simulated with real-life problems. Vidyanusa generates an interactive game which gives freedom to the ability to explore the game so as to solve a problem. Vidyanusa has a storyline that describes a story game, how the student plays and follows the instruction on a game. Thus, students have to read the storyline first before they play the game. We explain about the game concept of Vidyanusa that consists of two parts which are;

- Area : The game contains six areas, which are garden, factory, distribution, market, aruna's house and dam. A player has to start the game from the first area which is the garden and then be followed by the factory, distribution, market, Aruna's house and dam respectively.
- Quest : There are twenty three quests games in the six areas and each area has a different number of quests. There are seven quests in the garden, two quests in the factory, three quests in the distribution, five quests in the market, two quests in Aruna's house and the last area which is the dam has four quests. A player can choose randomly a quest to play first.

All indicators game used on quests game has to customize with subject material. Table 1 describes and classifies the kinds of mathematical subjects which are related to each of the quest game.

2. System Architecture

In this section, we describe the communication process between the entity (student or teacher) and web server of our system model as shown in Figure 1. The detailed description of system entities are as follows:



[Fig. 1] System model of Vidyanusa system

a. Web server : Vidyanusa system is an online web-based educational online game that requires a unique code as one of entity which is authenticated by the server. These unique codes are automatically generated by the system, when the teacher creates the class group in the dashboard site. The unique code represents the teacher identity, the class level and the class code. Vidyanusa consists of two main parts, the area for game play and dashboard page to manage all data involved in the system. We designed and developed an online web-based

mathematical game for educating students, which focuses on 7th, 8th and 9th grade students in Junior High School. Our system has a storage capability and can be accessed online. We assumed that the web server is a trusted authority which has a certificate from certificate authority (CA).

b. The Teacher: A person who can manage the student account through the dashboard page. A teacher can:
   - access the student's profile,
   - see the notification of students request,
   - check student's portfolio,
   - generate student's report,
   - analyze student's progress,
   - update student's score,
   - create a class.

Moreover, the teacher can share a unique code directly to the students. The unique code is generated automatically by the system when the teacher creates a class.

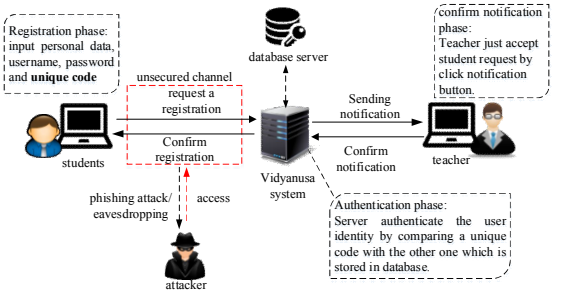
<Table 1> Classify Mathematical Subject

Area	Quest game	Classify Mathematical Subject
1	1. Create garden field according to the plant	Calculate area and perimeter
	2. Put the plant seeds in appropriate packaging	Sets
	3. Plant the orange	Statistics
	4. Catch the pests around on plant	Row of number
	5. Harvest chili	Addition and subtraction of integers
	6. Picking carrots	System coordinate, coordinate Cartesians
	7. Build a bridge to cross from garden to factory	Mean, median and mode
2	8. Construct a pipeline for harvest	Lines and angles
	9. Packing fruit and vegetables into cans and boxes	Bruto, Tara, Netto, and Sets
3	10. Draw up a crate of plantation products to fit when transported wheel	Pythagoras, triangle, and square
	11. Replace the broken wagon wheel	Circle and tangent line of circle
	12. Build a bridge to cross from the factory to the market	Rank, root and pythagoras
4	13. Press the button to open the gate of market.	Least common multiple.
	14. Sell fruit and vegetables.	Sale price, percentage of profit and loss.
	15. Helping Aruna to weigh a strawberry for made cakes.	Comparison of fractions and addition the rational numbers
	16. Calculate the price of strawberries were purchased	Multiplication of fractions and discount concept
	17. Search for materials recipe strawberry cake	Geometric series
5	18. Share strawberry cake to people in the village	Fractions (Addition, subtraction, and division)
	19. Make fruit juices	linear equations one and two variables
6	20. Looking for crystal stones in Vidyanusa's forest to build dams	Transformation
	21. Brings together four types of same stones to build the dam.	Similarity and congruent
	22. Build irrigation dam	Function and relation
	23. Set length crystal to turn on a turbine engine of power plant	Number power not real

c. The students: The user who has access of Vidyanusa to play the game, view profile and portfolios. The student requires a unique code along with the username and the password during the registration process. The student needs to wait for the acceptance confirmation from the teacher before playing the game. Only an authorized student can play the game, which means that only student with a unique code can register and create an account in Vidyanusa system.

Both students and teachers are required to create an account to access the Vidyanusa. They can login directly as student/teacher if they are already a member. However, all the users have to access the dashboard first before accessing their own page. Officially, this system is accessed by the students or the teachers in the classroom. Firstly, the teacher give a unique code directly to the students in the classroom. Figure 2 shows the details phase of the user registration which is performed by the students, the confirm notification phase of teachers, the authentication phase of the web server and depict the possibility of attack by malicious user for ulterior purpose.

- Registration phase; after getting the unique code from the teacher, the students request the registration using the unique code and enter others information. In that case, if the students does not have a unique code, the student is not allowed to create an account.
- Authentication phase; the server will authenticate the user account by comparing a unique code from student with the one which is stored in database. After checking the data, then server send the notification to the teacher.
- Confirm notification phase; the teacher needs to confirm the student's request by accepting the notification request. After verifying the notification, the students can access the system. The students have to login first by using their username and password that already created in registration.
- The possibility of attack; attackers may launch the MITM to eavesdrop or execute the phishing attack to discover the confidential information when the legitimate students sent the data during registration to the web server. The user identity will be easy to be intercepted because the message is transmitted as a plaintext. In this case, the attacker may use the victim's account to login in Vidyanusa and can play the game while the legitimate students get an error when request for login. It will be dangerous for Vidyanusa system because the attacker can easily play the game even modify the data in the system. Moreover, the teacher will has many illegal students in their class by attacker. Even though the teacher does not realize about such condition because the attacker use a victim account.

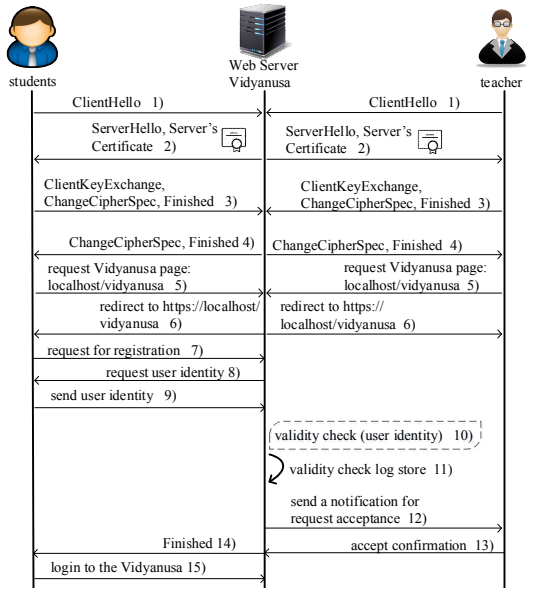


[Fig. 2] The possibility of attack by malicious users

Ⅳ. Design model of Secure Socket Layer (SSL)

In this section, we are going to describe the

handshake design model and the user registration process as shown in Figure 3.



[Fig. 3] Communication process between the entities

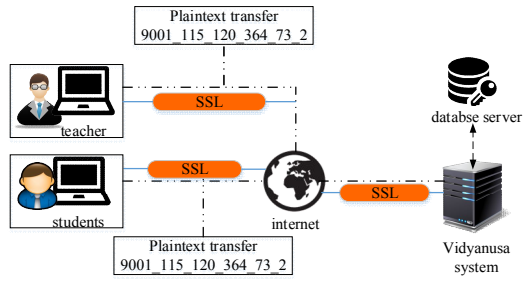
In this figure, we describe only for the students' registration process. However, either the students or the teachers are required to register before access the system. Figure 3 depicts the student performs handshake protocol that indicates the initial process to establish an SSL connection (Zi & Xu, 2013). The handshake protocol is started by sending ClientHello message to the server. Also, server will replay the handshake process by sending the server's certificate together with ServerHello message. After both of entities have negotiated the master secret key, the server sends a ChangeCipherSpec message that indicates the handshake process is finish (Zi & Xu, 2013).

So, the data exchange will be encrypted with a secret key during transmission (Freier, Karlton, & Kocher, 2011). The student requests registration using their personal identity includes the unique code. Then, server checks the validity of data with the one which is stored in the database in order to prove an authorized student who wants access the system. After the teacher accepts request notification, the students can login to the system and play the game. The detail of the process is as follows.

Ⅴ. Result and Analysis

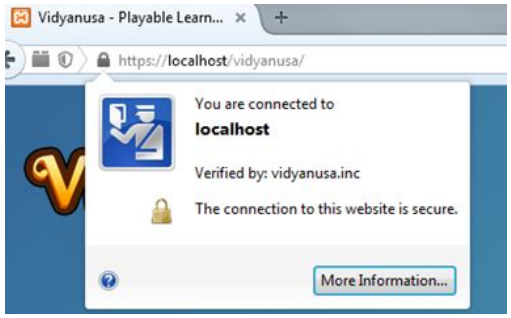
We have implemented the SSL protocol in the Vidyanusa system by configuring and generating a server's certificate. For testing and internal usage, we apply an SSL connection on our local web server using Apache. In order to enable an SSL on a web server, three steps are needed to be configured. First we need to create an SSL certificate as an identity information of our web server. Second, we need to import the certificate into the web browser that will be used to access the web server/Vidyanusa system, otherwise the web browser get a notification for untrusted certificate authority. Third, we need to edit Apache config for encryption that only access to the protected folder with SSL encryption. Also, the XAMPP control panel was run otherwise, the URLs cannot be accessed.

As shown in Figure 4, originally the system performs data transfers as plaintext forms such as user identity of students or teachers, unique code and other private information. Therefore, for securing the data communication, the SSL connection is applied in traffic of data exchange between a client and a server using the symmetric encryption for securing the data communication. After applying SSL connection, the website provides a padlock icon and the URLs change into HTTPS in address bar.



[Fig. 4] Design of Vidyanusa system to apply SSL

The interface on Figure 5 indicates that the certificate is already imported in the web browser. When the padlock icon is clicked by a user, the information shows the certificate issuer and the certificate is verified by vidyanusa.inc.



[Fig. 5] The website after applying SSL connection

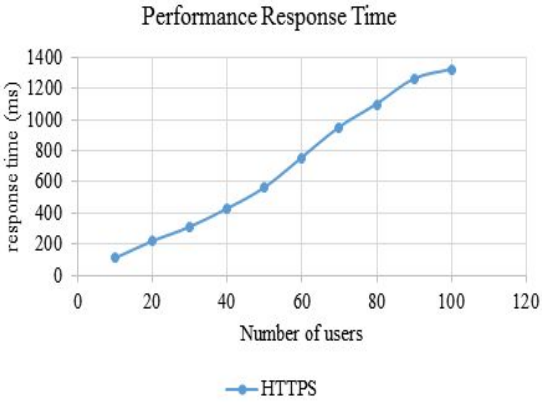
Figure 6 shows the list of personal information which is required when the registration process. A student enter an identity, a username, a password and a unique code. A registration success when the system verify the authenticity of a unique code is valid.

Moreover, we analyze the performance of the server after applying SSL connection by sending a number of threads. A load tester tool, namely J-Meter is used in this experiment. J-Meter allows us to modelling the expected usage by simulating multiple user access on the server concurrently. We vary the students in different number such as 10, 20, 30, 40, 50, 60, 70, 80, 90 and 100. It is assumed that a student has 100 requests and has Ramp-Up period 1 second. The Rump-Up period denotes how long the next students should take to start a new session. For instance, if a server handles 100 users and 100 second of Ramp-Up, then a new session requires 1 second of waiting time before starting the new ones. Figure 7 depicts the performance of the server after applying SSL protocol.

[Fig. 6] The list of student's personal information in registration page

The result shows that the performance of HTTPS as the number of users increase, the response time increases considerably. Nevertheless, the response

time of HTTPS increases, it is still applicable on this web-based online game since it gains security services. In addition, HTTPS can still handle more than 50 students with 5000 requests simultaneously. The server can be accessed conveniently though 100 students perform 10000 requests at the same time. It takes only 1.318 second for the server to handle such requests.



[Fig. 7] Performance HTTPS connection in web server

Ⅵ. Conclusion

In this paper we proposed the application of HTTPS connection in the web-based online game, Vidyanusa, to encrypt the entire message that sent over the internet (insecure channel). By enabling an SSL connection, it provides a secure communication that protect the student's personal information so it cannot be intercepted or modified by attackers. In contrary, the student will not be able to access the system and play the game while an attacker use the victim account to access the system at the same time.

We adopt standard SSL handshake protocol to establish SSL session for securing data transmission between the client and the web server. On the server side, we successfully configured SSL connection by creating self-signed certificate for web server internal usage. In addition, on the client side, we import the server's certificate in order to verify the identity of server for trusted authority. Padlock icon will appear in the address bar of the web browser which indicate the communication is private or the communication is encrypted by SSL session. Finally, we analyze the performance of the HTTPS connection by configuring different number of user and request. HTTPS server is still reliable to handle a number of accesses simultaneously.

References

Diaz, J. · Arroyo, D. & Rodriguez, F. B.(2014). On securing online registration protocols: Formal verification of a new proposal. Knowledge-Based Systems, 59, 149~158.

Freier, A. · Karlton, P. & Kocher, P.(2011). The secure sockets layer (SSL) protocol version 3.0.

He, L. · Fu, M. & Hu, X.(2010). To improve the social interaction of Web-based Collaborative Learning via online Educational Games for multi-player. 2nd International Conference on Education Technology and Computer, 2, pp. 187~189.

Ki, J. · Cheon, H. J. · Kang, J. U. & Kim, D. (2004). Taxonomy of online game security. The Electronic Library, 22(1), 65~73.

Lee, J.-P. · Kim, Y. H. & Lee, J. K.(2014). SSL Application for Managed Security between the Mobile and HIS Biometric Information Collection Client. Advanced Information Networking and Applications Workshops (WAINA), 2014 28th International Conference on, (pp. 55~60).

Rescorla, E.(2000). HTTP over TLS - RFC 2818. Internet Engineering Task Force.

Shacham, H. & Boneh, D.(2001). Improving SSL handshake performance via batching. Berlin Heidelberg: Springer.

Shi, J. & Saleem, S.(2012). Computer Security

Research Reports: Phishing. University of Arizona.

Van Summeren, R.(2011). Security in Online Gaming. RadboundUniversity Nijmegen: Bachelor Thesis Information Science.

Wilson, C. & Argles, D.(2011). The fight against phishing: Technology, the end user and legislation. In Information Society (i-Society) International Conference, (pp. 501~504).

Yani, K. R. & Rhee, K. H.(2015). Design of a Digital Game-Based Learning Application for Junior High School. in Proceeding of the Spring Conference of the Korea Multimedia Society.

Yani, K. R. • Rusmin, P. H. & Rhee, K. H.(2015). Applying SSL Protocol on a Web-based Educational Online Game. Proceeding of the Fall Conference of the Korea Information Processing Society.

Yani, K. R. • Setijadi, A. P. & Rhee, K. H.(2015). On Securing Web-based Educational Online Gaming: Preliminary Study. Proceeding of the Fall Conference of the Korea Information Processing Society.

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

• Received : 11 April, 2016
• Revised : 27 April, 2016
• Accepted : 11 May, 2016