International Journal of Security and Its Applications
Vol.7, No.6 (2013), pp.137-146
http://dx.doi.org/10.14257/ijsia.2013.7.6.14

Development of Information Security Contents for Learning Hacking Principles

Ji Yeon Hong[1], Ik Jun Kang, Seong Baeg Kim[1,1] and Chan Jung Park[1]

[1] *Dept. of Computer Education, Jeju National University, Jeju-do, Republic of Korea*
{hongjy713, crazyboyz111}@naver.com, {sbkim, cjpark}@jejunu.ac.kr

Abstract

Most of people, who have no solid background of information security, are prone to be attacked by hackers. Furthermore, although they often receive the news of hacking cases, they do not know what the hacking-principles are and how they can protect themselves against the hacking attacks. Also, the learning contents for information security suitable for them have not been yet developed sufficiently because most of the existing information security learning contents have mainly been developed for computer experts or students major in computer security. Therefore, we created a principle-based learning scenario about typical four cases of hacking attacks and simulation game in this paper. Then, we proposed the customized information security contents for hacking-principle learning on the web.

Keywords: *Hacking Principles, Information Security, Learning Contents, Simulation Game*

1. Introduction

The computer is essential in our lives and we can enjoy the convenience of information technology as the network is extended throughout the world. However, there are the side effects such as invasion of privacy, exposure to harmful sites, data hacking, system failure, etc. 'Love bug', which astonished the whole world, notified the fact that the problem of information security could be a social threat regardless of region and country.

According to the result of the data analysis from the National Statistics Office in Korea, we can see the fact that the increasing hacking cases have become more sophisticated recently by adding the new skills like spam relay, phishing route, and falsification of home pages to the existing hacking skills [1]. However, even though many people have already recognized the fact, they do not know how to solve the hacking problems practically. Also, the problems of information security are not limited to the technology scope monopolized by IT experts. They are recognized as social concerns and issues that have an impact on the daily lives of information society.

The recent invasion of information security has exploited a mechanical error or technical weakness as well as users' psychology. Therefore, in order to solve these security problems, our approach aims to provide the proper learning contents to people by analyzing the cases, types, and ways of security accidents [2, 3].

[1] Seong Baeg Kim (sbkim@jejunu.ac.kr) is the corresponding author of this paper.

ISSN: 1738-9976 IJSIA

2. Background

In this paper, we conducted a survey [4] on 50 undergraduate students to analyze an actual situation of information security and to examine the necessity of the related contents for people. The questionnaire consists of the survey items such as the experience on private information leakage, the necessity of security-related education, and the degree of understanding the security-related contents provided, as shown in Figure 1 through 4 [4].

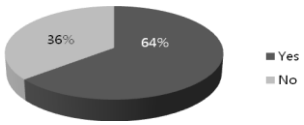

Figure 1. The Percentage of Respondents Who Think that their Information has been Exposed

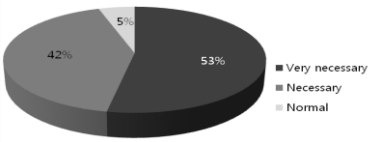

Figure 2. The Percentage of Respondents who Think that the Security-Related Education is Necessary

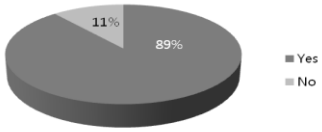

Figure 3. Learning experience for the security-related knowledge

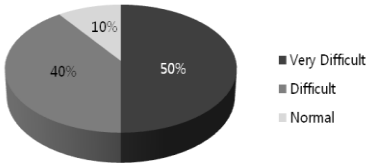

Figure 4. The degree of understanding the security-related knowledge

The survey showed that the 64% of the respondents thought that their information has been exposed and the 95% of the respondents felt the necessity of the security-related education. Learning experience for the security-related knowledge was very lower because the 11% of the respondents showed up, and the 90% of them had trouble in understanding for the security-related knowledge.

One of the research works about a secure access to educational resources [10] focused on proposing an educational web model. Most of the security-related research consisted of the detailed description and theoretical knowledge [11, 12]. Thus, it is difficult for non-experts to understand the research. The proposed contents for hacking-principle learning are developed for non-experts like our respondents. The form of the contents was designed not for providing comprehensive and deep contents to experts proposed in the previous research but for preventing the security intrusion accidents and for improving the awareness of information security by realizing hacking-principle clearly.

3. Design and Implementation

3.1. Writing a Hacking-Principle Scenario

The hacking-principle scenario proposed in this paper consists of four parts. We explain each scenario considering a situation element that can make general people understand about ARP spoofing, DDoS attack, keylogger, and SQL injection attack described in the following.

3.1.1. ARP Spoofing

The network that has the same internet communication path can be attacked. Data in PCs pass through the gateway to be sent to the internet. ARP spoofing can occur when an attacker personates the gateway in the middle and steals the data. Since vaccine software can detect most of the malicious programs, the attacker develops it not to be detected.

When a malicious program is operated, it causes an attacker to intercept data frames by sending fake ARP messages onto a LAN. Now that all data are sent to the attacker through the internet, falsification and deletion are possible by the attacker. The ARP spoofing attack includes PCs as well as appliances like smart phone and laptop in the same network. Actually, the attacker can get and falsify the all data by ARP spoofing in the environment which uses the same network such as apartment network, university wireless network, and company intra-network [5].

3.1.2. DDoS Attack

Because the resources in a server are not sufficient, the number of computer accesses to the server is limited. However, if many PCs access to the server simultaneously and reach beyond the limit, the server cannot work normally. An intentional malfunction attack on the server by an attacker is called 'DDoS attack'. Because most of the malicious programs are detected by vaccine software, the attacker develops a program to control many PCs in order to avoid to be detected. After the hacking program is developed, the attacker plants the developed program to many PCs. The PCs infected by the malicious program become zombie PCs.

However, though the zombie PC conducts ordinary activity as usual, millions of PCs can access to the server controlled whenever they are ordered by attackers. Typical case of DDoS attack is 'the National Election Commission DDoS attack'. On October 26th, 2011, the voting day of the Seoul mayoralty election, the National Election Commission sever was down, and then the vote was interrupted because of DDoS attack [6].

3.1.3. Keylogger

'Keylogger' means that an attacker catches what key is pressed. All values inputted through the keyboard can be sent over the attacker. Because the ‘Keylogger’ program can be detected by vaccine software, the attacker develops it using a hacking skill in order to be undetected. After it is developed, the attacker installs it on the target PC. There are many ways to install it on the target PC: plugging-in USB, executing an attached file on e-mail, making an automatic installation when specific web sites are visited, *etc*. If it has been installed on the target PC, it operates secretly to get data directly from the databases of the target PC [7].

3.1.4. SQL Injection

Currently, users login by accessing their ID/password stored in the database on most of web pages. Among the 'SQL Injection' attacks, there is a way that an attacker can access a computer by taking a detour authentication. If the ID is 'hong' and the password is '1234', the login can be successful because a PC system judges it as true. The PC system is so simple that it abnormally filters SQL query including escape characters created by the attacker, and then the attacker can login. Without knowing the real password '1234', the attacker inserts a value that is always true in the PC such as '?' or 'A'='A' as the password. In this way, the attacker can make a detour of the database and then can login. Therefore, the attacker can login without knowing the password at all and then can access the database of a web server. This attack can be prevented simply by restricting special characters as input. However, because a specific web site does not filter this function yet, the attack is still allowed [8].

3.2. Implementation of Contents for Hacking-Principle Learning on the Web

We basically used Adobe Illustrator to make contents for hacking-principle learning. By using Adobe Illustrator, we designed the elements such as more than 100 main screens and characters, objects, backgrounds, glossary of the contents scenario, and so on, in the form which users can feel friendly. Then, we made the screens and characters designed by Adobe Illustrator running on the web respectively.

The starting screen for hacking-principle learning is shown in Figure 5. The contents were designed for people to learn the hacking-principles. The users can study one of the four hacking cases, as shown in Figure 6. Figure 7 is a main screen of DDoS and the zombie PCs and the attacker are represented as characters in the figure. We implemented that users are able to learn hacking-principle based on the DDoS scenario after passing the main menu, as shown in Figure 8.

Figure 5. Starting Screen

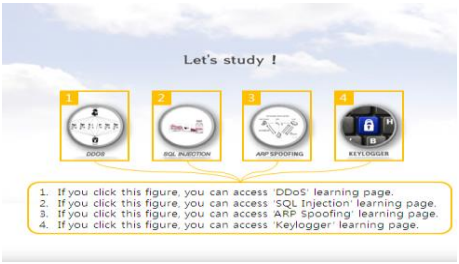

Figure 6. Selection of Hacking Cases

Figure 7. DDoS Selection Screenshot

Figure 8. DDoS Scenario Screenshot

We made use of figures and sample situations that are easy to understand as far as possible. Also, for additional explanation about unfamiliar words, we appended the symbol '★' as shown in Figure 9. We inserted glossary menu in the contents for users to search those words when they click '★' –symbol, as shown in Figure 10.

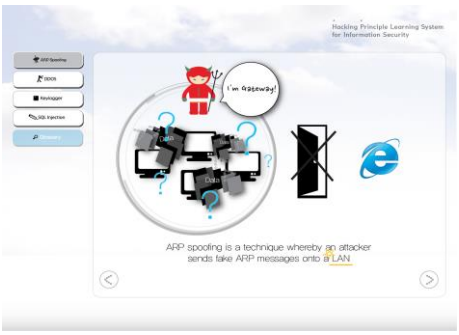

Figure 9. ARP Spoofing Scenario Screenshot

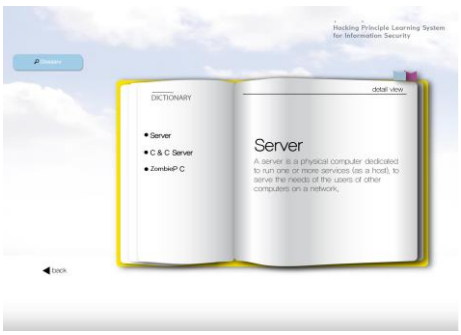

Figure 10. Glossary

4. Hacking-Principle Simulation Game

The hacking-principle simulation game developed in this paper was designed for considering interesting elements. After learners learn the basic principles of hacking techniques on the web contents as the first step, they can start the game. In the game, missions are assigned to gamers and they proceed virtual hacking in the game with the four attack missions based on the hacking-principles. While hacking, they realize the seriousness of cyber crime.

Figure 11 shows the flow diagram of the hacking-principle simulation game. After starting the game, attack missions are granted to gamers. The attack missions are divided into ARP spoofing, DDoS, keylogger, and SQL Injection as shown in Figure 11. The gamers perform a random mission for themselves. Based on hacking-principle theory, gamers proceed hacking looking into mission that is granted to gamers. For example, a mission is 'Find out the email password'.

As it goes on, the success of the hacking-principle simulation game depends on the mission completion in the limited hours. The hacking-principle simulation game proceeds virtual simulation activity by adding challenging elements like time limit and hints given by the mission completion in order to succeed the mission.

Figure 11. Flow Diagram of Simulation Game

Using the challenging elements, gamers repeat various situations and learn each of hacking-principles repeatedly. Thus, we expect that learners can accomplish mastery learning from the similar situation on the cyber.

The prototype is as follows. A gamer can select one of the hacking cases as shown in Figure 13. If hacking skills and words are difficult to understand, the gamer refers to the tip, 'help', as shown in Figure 14. The gamer can click 'help' button on the right top of the page and get the information at every page. Suppose that a gamer selects ARP spoofing hacking skill. The gamer knows the ARP spoofing because he/she has already learned in the hacking principle contents. Then, the mission is assigned to gamers randomly.

Figure 12. Starting Screen

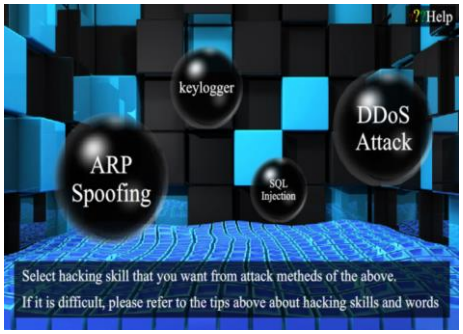

Figure 13. Selection of Hacking Cases

For example, a mission is 'Find out the email password'. A gamer has to find out an email password by using the ARP spoofing hacking skill. If the gamer finds out the password, he/she types it in the blank box as shown in Figure 15. In big data, if it is hard to find out the password, the gamer can use hints up to 3 times. The gamer can get a hint by clicking '★' on the right bottom as shown in Figure 15.

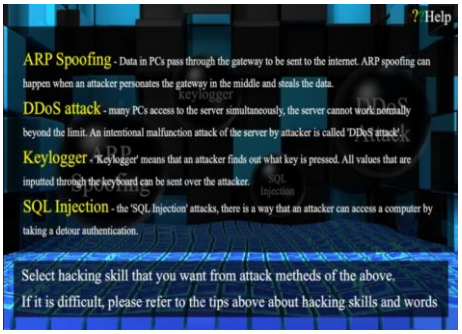

Figure 14. Help

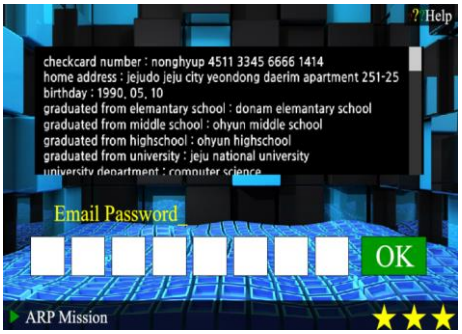

Figure 15. Input the Answer

A gamer can select one of the hint functions in Figure 16. After using a hint, if the gamer finds out the email password, he/she can input the answer in the blank box again. After the successful mission, the gamer can see the screenshot shown in Figure 17. After finishing the game, the gamer can challenge another mission or exit the game.

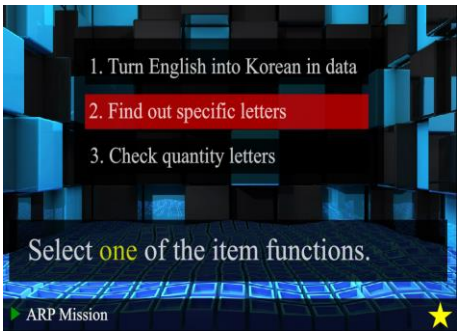

Figure 16. Hint Category

Figure 17. Mission Success

5. Evaluation

We conducted the second-step survey in order to examine the degree of non-experts' understanding of the hacking-principle learning contents proposed in this paper. Figure 18 and Figure 19 show the survey results of the questionnaires: the degree that how much hacking-principle learning contents help to improve security awareness and the degree that how much the contents help the non-experts to understand information security after learning it during the exhibition.

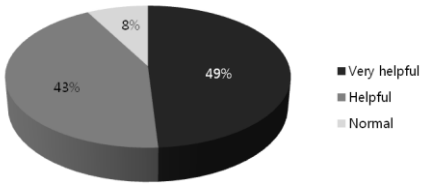

Figure 18. The Degree that Hacking-Principle Learning Contents Help to Improve Security Awareness

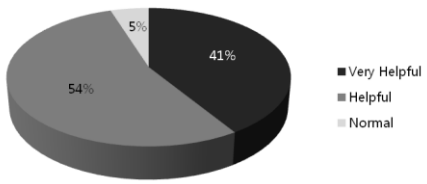

Figure 19. The Degree that the Contents Help the Non-Experts

Our

survey showed that as the response of the question that asked whether hacking-principle learning contents help to understand information security, 92% of the respondents answered that 'it will be helpful generally' and 'it will be very helpful'. Also, the survey showed that as the responses of the question that asked whether the contents can be helpful to the non-experts as information security contents, 95% of the respondents answered 'it will be helpful generally' and 'it will be very helpful'.

6. Conclusion and Suggestion

The components for hacking-principle learning proposed in this paper were based on the contents of 'Online Information Security e-Learning Center' [9] that can improve information security awareness to general people and educate them. We developed our contents for the non-expert users.

We firstly confirmed the necessity of producing contents for information security through the survey on March 2012. On November 23, 2012, we exhibited the contents for hacking-principle learning proposed in this paper at our Department's Computer Education Exhibition. And then, we made people experience the hacking-principle. In fact, general hackings have many kinds of ways in the various fields such as numerous systems, networks, passwords, etc. Also, there are different ways to attack or handle various weaknesses. Therefore, it is difficult for even computer experts to learn and organize the hacking-principles easily. Furthermore, general people, who do not have any solid knowledge of computer science, are highly exposed to the security threats. However, although they just know hacking cases, they do not know what the hacking-principle is and how to protect themselves from hacking.

Thus, we focused on creating an easy explanation of the hacking-principles, which is difficult to understand. Also, we designed the scenario-based learning contents in order to help people to understand. In addition, to make easier learning, we considered the internal elements in the design and tried to enhance the association of each screenshot and each object.

The contents for the hacking-principle learning proposed in this paper focused on the learner's easy understanding. However, based on the contents, we expect that an interesting element of information security, which can make interaction with learners, will be added. Also, we expect that non-experts, who couldn't get the knowledge of security due to the difficulties of understanding, can do the information security learning about the typical hacking cases, based on hacking-principle learning contents and simulation game proposed in this paper.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2013009428).

References

[1] Korea Internet & Security Agency (KISA): Monthly return of internet invasion accidents trend and analysis, **(2010)**.
[2] J. Choi and C. Woo, "Web-based ITS for Training Computer Security", Proceedings of KIISE (Korean Institute of Information Scientists and Engineers) Spring Conference, vol. 29, no. 1, **(2002)**, pp. 703-705.
[3] W. Shin and S. Cho, "Information Security Training Plan of Applying Virtualization Technology", Journal of the Korea Institute of Information Security and Cryptology, vol. 19, no. 1, **(2009)**, pp. 59-66.
[4] I. Kang, S. Kim, J. Hong, S. Kim and C. Park, "Development of an AP Containing ARP Detect-Spoofing and a Web-based Management Tool", Proceedings of The KACE, vol. 16, no. 2, **(2012)**, pp. 131-134.

[5] S. Hong, M. Oh, S. Lee and S. Lee, "Efficient Technique for Preventing ARP Spoofing Attacks using Reliable ARP Table", Journal of KIISE, vol. 17, no. 1, **(2011)**, pp. 26-30.
[6] A. Kim, D. Lee and S. Jang, "The Effectiveness Evaluation Methods of DDoS Attacks Countermeasures Techniques using Simulation", Journal of The Korea Society for Simulation, vol. 21, no. 3, **(2012)**, pp. 17-24.
[7] S. Hwang and K. Park, "A Keyboard Security Method Based on a Subclassing", Journal of Korea Multimedia Society, vol. 14, no. 1, **(2011)**, pp. 15-23.
[8] J. Seung, B. Noh and S. Ahn, "Recent Major Hacking Damages Trend and Countermeasures", Journal of the Korea Institute of Information Security and Cryptology, vol. 16, no. 1, **(2006)**, pp. 80-84.
[9] Online Information Security e-Learning Center, http://www.sis.or.kr.
[10] O. N. Qunoo and H. Hamad, "Secure Model for Educational Resources", International Journal of Security and Its Applications, vol. 7, no. 1, **(2013)**, pp. 31-50.
[11] J. Piao and S. B. Kim, "The Design and Analysis of a Hardware-based Anomaly Detection Scheme", International Journal of Security and Its Applications, vol. 6, no. 2, **(2012)**, pp. 367-372.
[12] S. Song, H. Park and B. Choi, "E-LPG: Energy Efficient Location Privacy Scheme Against Global Attackers in Sensor Networks", Secure Model for Educational Resources", International Journal of Security and Its Applications, vol. 7, no. 2, **(2013)**, pp. 27-46.

Authors

Ji Yeon Hong, he is currently an undergraduate student of the Dept. of Computer Education at Jeju National University. Her research interests include computer science education, English education, and computer security education.

Ik Jun Kang, he is currently an undergraduate student of the Dept. of Computer Education at Jeju National University. His research interests include computer science education and computer security education.

Seong Baeg Kim, Professor Kim received the B.S., M.S., and Ph.D. in Computer Engineering from Seoul National University, Korea, in 1989, 1991, and 1995 respectively. He is currently a professor of the Dept. of Computer Education at Jeju National University, where he has been since 1996. He was a visiting scholar at Dept. of Computer Science, Montana State University from 2001 to 2002 and Dept. of Electrical & Computer Engineering, University of Cincinnati from 2008 to 2009. His research interests include computer science education, computer system architecture, and computer security.

Chan Jung Park, Professor Park received B.S. at Dept. of Computer Science of Sogang University, Korea. She received M.S. and Ph.D. at KAIST and Sogang University, respectively. From 1990 to 1994, and also from 1998 to 1999, she worked for Korea Telecom as a researcher. Since 1999, she has worked for the Dept. of Computer Education at Jeju National University. Currently, she is a professor in Jeju National University. In 2010, she was a visiting scholar at University of California, Berkeley. Her research interests include creative problem solving, web app development, and data mining.