An Integrated Real-Time Simulated Ethical Hacking Toolkit with Interactive Gamification Capabilities and Cyber Security Educational Platform

Vimalnath N. Mathoosoothenen, Jakanath S. Sundaram, Ram A. Palanichamy, Sarfraz N. Brohi
School of Computing and Information Technology
Taylor's University
Subang Jaya, Malaysia
sarfraznawaz.brohi@taylors.edu.my

ABSTRACT

There has been an alarming rise in the number of cyber crimes occurring lately and stealthier methodologies used by attackers, which has directly contributed to the rise of online victims. With the development of advanced persistent threats, current cyber security defense mechanisms also face a high failure rate in detecting and preventing exploitation of cyber security threats from occurring. This research provides a solution to tackle the issues pertaining to the lack of awareness on the importance of cyber security. This paper presents an improved approach that incorporates three distinct features: an ethical hacking toolkit, a cyber security awareness game, and an educational platform. These components are integrated together as a complete project to spread awareness on the importance of cyber security elements in our everyday lives.

CCS Concepts

•Security and privacy → Software security engineering

Keywords

Security Awareness; Ethical Hacking Toolkit; Gamification; Educational Platform

1. INTRODUCTION

In this new era of globalization, the Internet plays a very important role in being a medium that connects everyone around the world. It also plays a role for people to share and retrieve information and resources of various forms. For example, graphic media (images and videos), educational documents, online books, information files, software and games. Although the Information Technology industry has developed and provides people with many benefits with the existence of the Internet and the availability of resources online, there is a major issue that is currently affecting the life of many. The issue pertains to the lack of awareness among Internet users in regards to the presence of cybercrimes happening online at an alarming rate. According to Microsoft's Digital Crimes Unit, there is a total of 12 people online who become victims every second in which totals to more than 1 million victims around the globe daily [1]. The number of methods to launch cyber security attacks has increased over the years. One of the current primary method used is by embedding malicious software into the victim's devices and accessing the device remotely without the victim's knowledge. In the year 2014, over 317 million malicious software was created that resulted nearly 1 million new threats daily. Verizon states that a person commonly takes about 82 seconds to fall victim to a cyber-attack [2]. In Malaysia, an average of 30 Malaysians fall victim to cybercrime daily. Example of reported incidents includes fraud, intrusion, spam, denial of services and cyber-harassments. In the year 2015, Cyber security Malaysia has received over 3752 cases of online fraud and intrusion, and an addition of 191096 reports on botnet and malware infections. Cyber security Malaysia Chief Executive Officer, Dr. Amiruddin Abdul Wahab stated that "The weakest link in cyber security is people" [3]. Furthermore, the president of EC Council, Sanjay Bavisi also stated that Malaysia lacks in the cyber-world security which is making it prone to cyber terrorism threats and warfare [4].

In order to contribute in the field of cyber security, we have developed an integrated real-time simulated ethical hacking toolkit with interactive gamification capabilities and cyber security educational platform that is aimed to provide a new approach in solving issues pertaining to the lack of awareness on the importance of cyber security. The aim of the developed toolkit was to provide a much engaging and holistic solution that will be able to capture and retain the attention of users that will attend the workshops, seminars and training sessions organized by cyber security specialists. Not only that, by providing a holistic solution with an intuitive user interface to demonstrate and educate users on the latest cyber security attacks, the project is believed to be more convenient and will provide a better user experience for the trainers and users that attends the workshop and training sessions organized.

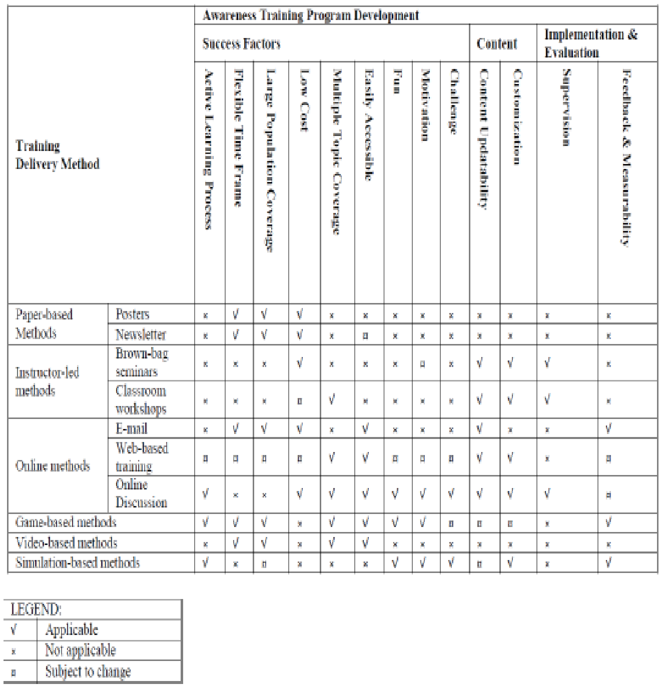
2. RELATED WORK

It is widely accepted within current literature that information security awareness is a key factor in contributing to a successful security strategy [5, 6, 7, 8, 9, 10, 11, 12 and 13]. The primary solution that is used to solve the issue of lack of awareness on the importance of cyber security is cyber security campaigns. The cyber security campaigns are held globally for everyone: students, working adults and organizations. There are four main methods that are used in cyber security campaigns today to deliver the message of cyber security, those include paper-based methods, instructor-led methods, online methods and interactive methods.

CSAI 2017, December 5–7, 2017, Jakarta, Indonesia
© 2017 Association for Computing Machinery.
ACM ISBN 978-1-4503-5392-2/17/12…$15.00
DOI: https://doi.org/10.1145/3168390.3168397

Paper-based methods of delivery are also known as the conventional method of delivering information using mediums like leaflets, posters and newsletters; each usually equipped with information, captivating slogans and catchphrases on a specific topic at a given time. The method of paper-based delivery has evolved and it is currently available in two different formats: electronic and print format. These deliverables are commonly displayed at common areas: student lounge and cafeteria; where many people are found to gather. The instructor-led method uses a top-down approach by using a professional expert with a background on cyber security field to conduct formal presentations: brown-bag seminars and classroom workshops to raise awareness on a subject matter. This approach creates an instructor-student like relationship between the professional expert and the attendees of the awareness session. The main advantage that is obtained from this approach is that instructors are able to look at non-verbal cues portrayed by attendee and is able to change his or her information content that is being delivered accordingly. The approach also allows the instructor and attendees to have a real-time question and answer session during the workshop or seminar. However, this method also brings a certain disadvantage through its approach. In order to conduct an awareness workshop or seminar, there is a need of financial consideration in acquiring an appropriate venue, and for the preparation of information deliverables for the attendees. The success of this method is also solely depended on the capability of the instructor to engage with his or her audience. Incapability of an instructor may lead to the ineffectiveness of the session to spread awareness on the subject matter to the audience. Another common method that is used in today’s technological world is the online method of delivery. This method comprises of email broadcasting, online discussion, blogging, videos and the use of social media sites. The method is generally implemented in accordance to the field of education to educate people in different geographical regions around the globe while providing users the flexibility and availability to access the information and learn it on their own pace. Slideshows and animations are often included to make the approach of this method to be more interesting and increase its capability to attract more users. The downfall of the online methodology is the lack in the ability to measure the full scale of the implementation in terms of the effective in educating the users as there is no way to actually determine how many people has been educated and how much do they understand on what is being portrayed. In the recent years, interactive methods have increased in number in terms of being used as a medium in spreading awareness as it is much engaging and works more efficiently in comparison to the conventional approaches. Interactive methods can be distinctly categorized into 2: gamification and simulation. One of the most popular interactive method used popularly around the world is a gamification approach known as CyberCIEGE, a video game that was created with the intention to provide support in education and training in computer and network security. [6] One major challenge that is faced when gamification approach is implemented especially in regions where language barriers are an issue. Next, simulation has also been obtaining a level of attention lately in being used as a medium to solving the issue in spreading awareness, whereby users will be able to see and understand on the subject matter from a first-hand approach [14].

A cyber security awareness campaign often implements a combination of one or more of the methods mentioned previously at any given time. The selection of the methods to be used is influenced by a number of success factors. Success factors are aspects that needs to be looked into in order to ensure that a given approach will be successful in achieving the primary objective of spreading awareness to a targeted audience with full efficiency. An example of a guideline that is used to determine the appropriate methods to be implemented based on the success factors show in the Figure 1. The solution approach that has been taken in Malaysia to build a security awareness is the launch of a non-profit organization, Cyber security Malaysia in the year 2007. Cyber security Malaysia has conducted a number of awareness programs that is targeted at the youths, parents, home users and organizations; with the aim of making sure that Internet users are aware of current online threats and dangers. Not only that, Cyber security Malaysia also is determined to promote safe and responsible online behavior, and to promote best practices and positive use of the Internet. Example of methods used by Cyber security Malaysia in their initiatives includes publication of newsletters, awareness posters, exhibitions and road shows around Malaysia [15].



Training Delivery Method		Awareness Training Program Development												
		Success Factors									Content		Implementation & Evaluation	
		Active Learning Process	Flexible Time Frame	Large Population Coverage	Low Cost	Multiple Topic Coverage	Easily Accessible	Fun	Motivation	Challenge	Content Updatability	Customization	Supervision	Feedback & Measurability
Paper-based Methods	Posters	x	√	√	√	x	x	x	x	x	x	x	x	x
	Newsletter	x	√	√	√	x	¤	x	x	x	x	x	x	x
Instructor-led methods	Brown-bag seminars	x	x	x	√	x	x	x	¤	x	√	√	√	x
	Classroom workshops	x	x	x	¤	√	x	x	x	x	√	√	√	x
Online methods	E-mail	x	√	√	√	x	√	x	x	x	√	x	x	√
	Web-based training	¤	¤	¤	¤	√	√	¤	¤	¤	√	√	x	¤
	Online Discussion	√	x	x	√	√	√	√	√	√	√	√	√	¤
Game-based methods		√	√	√	x	√	√	√	√	¤	¤	¤	x	√
Video-based methods		x	√	√	x	√	√	x	x	x	x	x	x	x
Simulation-based methods		√	x	¤	x	x	x	√	√	√	¤	√	x	√

LEGEND:	
√	Applicable
x	Not applicable
¤	Subject to change

Figure 1. Selection of Awareness Training Program Guidelines. [16]

3. ETHICAL HACKING TOOLKIT WITH GAMIFICATION AND EDUCATIONAL PLATFORM

The major problem faced in the cyber-world is the lack of awareness in regards to the importance of cyber security. People today have a misconception with the idea that having basic security defense mechanisms like an antivirus software provides enough protection from current cyber-threats. However, there are many vulnerabilities in on-the-shelf software that are available in the market today which are unknown to the users until they have fallen victim to a cyber security attack. This is where the contribution of the undertaken research comes into the main picture. We implemented an integrated real-time simulated ethical hacking toolkit with gamification capabilities and cyber security educational platform through 3 distinct solutions that works as a whole to reach the common objective. The target market that is looked at to promote increase in awareness using this toolkit are students within the age group of 18 to 25 years' old who are still currently pursuing their education in colleges and universities in Malaysia. The three solutions of the research are discussed as follows:

3.1 Ethical Hacking Toolkit

The sole purpose of the ethical hacking toolkit is to provide a real-time simulation of the current cyber security attacks that is being carried out in the cyber-world today. By showcasing a real-time simulation of the attacks, the people will be able to experience first-hand on how an attack is carried out without their knowledge and the effects of the attack. The ethical hacking toolkit currently consist of the 7 main trending cyber security attacks today: Screen capture, Keystroke capture, Web camera access, Microphone access, Command line injection, File transfer and Ransomware.

3.2 Gamification: Cyber Security Awareness Game

The cyber security awareness game is designed and developed to test and evaluate the level of understanding of the individuals on matters related to cyber security. The game consists of simulated questions that represents real life scenarios that an individual may experience while browsing online. An example would be receiving a phishing email that appears to be from a legitimate source. Based on the questions asked throughout the game, the individual playing it would have to analyze each of the questions and identify the key elements or the best practices that an individual needs to follow in order to not fall victim to a cyber-attack.

3.3 Educational Platform

The educational platform is an informative website that acts as a platform for people to learn on the latest cyber security threats, and best practices and preventive measures to prevent themselves from falling victim to such cyber security attack or threats. Using the platform, people can create online forums to conduct discussions with one another or clarify doubts with cyber security professionals on relevant cyber security matters. At the moment, the developed solutions are being implemented through cyber security workshops and certification programs, which are endorsed by Cyber security Malaysia. The proposed solution was used to conduct workshops and certification programs with major well-known industries in Malaysia such as Microsoft Malaysia, Aptech, Trend Micro, ENSILO and Kaapagam Technologies.

4. IMPLEMENTATION

The implementation details of developing the ethical hacking are provided in the following sub-section:

4.1 Ethical Hacking Toolkit

The ethical hacking toolkit was developed using the Java programming language. Besides being an object oriented programming language, Java is also an independent environment that allows the compilation and execution of codes with little or no modification on multiple platforms such as Windows and Linux. There are many applications and websites that are being created today which requires Java to be pre-installed in order to perform efficiently.

The implementation of the ethical hacking toolkit can be broken down into three distinct core programs. The core programs are the hacker-side program, server-side program and also the victim-side program (Malicious program) as shown in Figure 2.The server-side program is a simple web server program that runs on a public Internet Protocol (IP) address, whereas the victim-side program is a malicious program that is created using a reverse User Datagram Protocol (UDP). This is done in order to allow the malicious program to connect to the server as soon as the victim is connected to the Internet. The malicious program on the victim-side updates the server of the victim's Internet Protocol (IP) address every 15 minutes to indicate the status of the victim. Furthermore, the malicious program on the victim device also acts as a medium to obtain instructions from the hacker-side program when executed.

Before being able to send any commands to the malicious program on the victim device to carry out a cyber-attack, the hacker-side program is required to request and obtain the Internet Protocol (IP) address of the victim. The reason why the server-side program is created to receive, store and send the Internet Protocol (IP) address of the victim is because it enables the hacker to be anonymous and prevents the hacker from being identified easily during a forensic investigation. For example, the hacker can be located in any part of the world in order to launch a cyber-attack using anonymous enabled communication channels such as Virtual Private Network (VPN) or Proxy Servers.

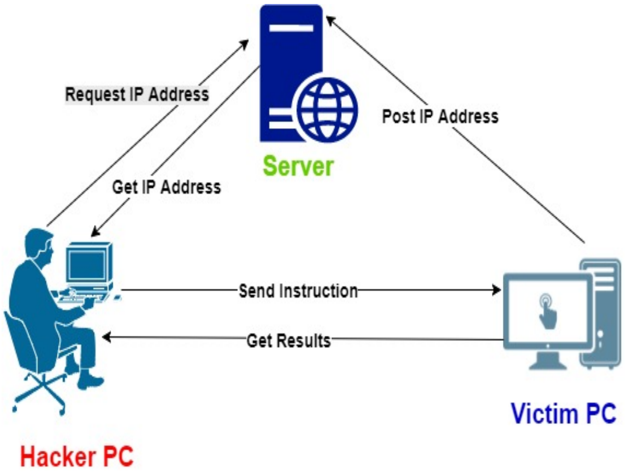


Figure 2. Relationship of the Distinct Core Programs of the Ethical Hacking Toolkit

Moreover, the main transportation layer of the data communication of the ethical hacking toolkit implements the User Datagram Protocol (UDP). This is because current defense mechanism that are installed in most computing devices such as anti-virus, intrusion detection system, intrusion prevention system and firewalls are not able to validate User Datagram Protocol (UDP) packets that are being transmitted to and from a computing device.

In order to prevent the malicious program from being identified by the defense mechanism installed on the victim's computing device, the program executed directly from the memory of the computer. This current defense mechanism only checks and validates data from the hard disk. Thus, this ensures the validation of the malicious program installed on the victim's device is always unsuccessful.

5. EVALUATION STRATEGY

As mentioned previously in this paper, the current evaluation strategy that is being used to evaluate the user's awareness on cyber security is through the cyber security awareness game.

5.1 Cyber Security Awareness Game

Similarly to the ethical hacking toolkit, the cyber security awareness game is also developed using the Java environment but with a gamification approach added to it. The game is designed to educate and to test the understanding of the audience in regards to the cyber security threats that are currently threatening the world. The game is built using a story board that covers a range of topics that are covered in the ethical hacking toolkit that is used during demonstration. The design of the game is shown in Figure 3. The story of the game involves the users to assist the fictional character of the game to identify elements, preventive measurements and concepts that are related to each particular cyber security threat that is being tested. Each topic that is covered consist of several scenarios that requires the user to implement the best practices in order to prevent themselves from falling victim to a cyber security attack. Upon the completion of the game, the user will be rewarded a score based on the user's capability to identify the correct answers for each of the question asked within the game. In order to successfully pass the user awareness test, the user will need to score above 75% of the total score. However, users are also allowed to reattempt the questions to further test themselves into understanding the cyber security threats.

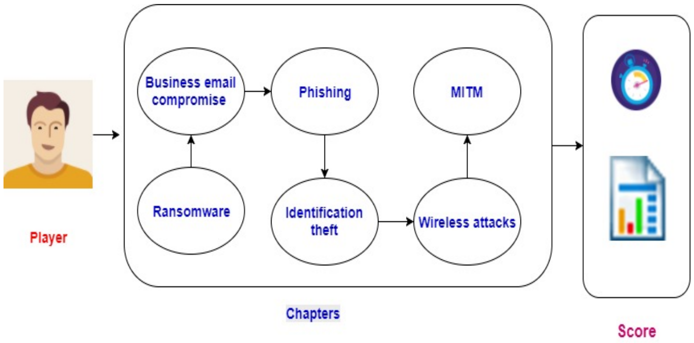


Figure 3. Design of the Cyber Security Awareness Game

6. CONCLUSION AND FUTURE WORK

In this stage, the contribution of this research focuses on providing awareness for the younger generations in schools, colleges and universities. Moreover, the project also aims to spread awareness among working adults in various organizations as mentioned previously in the paper. The ambition for the direction of the project towards the future is to comprehend the three solutions with detailed information and simulation on the latest trends and upcoming cyber security threats and attacks. Once the solution has been successfully developed, the aim is to initiate new certification programs to produce more secure users to the cyber-world and further enlarging our target market into a global scale, especially towards the third- world countries whereby education is significant for their growth.

7. ACKNOWLEDGMENTS

We are grateful to the Taylor's University School of Computing and Information Technology for providing us an opportunity to carry out this research and for funding this project.

8. REFERENCES

[1] Microsoft, 2016. News Center - Digital Crimes Unit. DOI= http://news.microsoft.com/download/presskits/DCU/docs/dcuFS_160115.pdf.

[2] Harrison, V., 2015. Nearly 1 million new malware threats released every day. DOI= http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/.

[3] Cheng, N., 2015. More than 30 Malaysians fall prey to cybercrime daily. DOI= http://www.thestar.com.my/news/nation/2015/10/26/cybercrime-30-msians-daily/.

[4] Jalil, H., 2014. Malaysia needs to improve cyber-security, says expert. DOI= http://www.thesundaily.my/news/1095748.

[5] Cervone, F 2005, 'Understanding The Big Picture So You Can Plan For Network Security', Computers in Libraries, vol. 25, no. 3, pp. 10- 15.

[6] Siponen, M & Vance, A 2010, 'Neutralization: New Insights Into The Problem Of Employee Information Systems Security Policy Violations', MIS Quarterly, vol. 34, no. 3, pp. 487-A12.

[7] Spears, JL & Barki, H 2010, 'User Participation in Information Systems Security Risk Management', MIS Quarterly, vol. 34, no. 3, pp. 503-A5.

[8] McFadzean, E, Ezingeard, J & Birchall, D 2007, 'Perception of risk and the strategic impact of existing IT on information security strategy at board level', Online Information Review, vol. 31, no. 5, pp. 622-660

[9] Knapp, KJ, Marshall, TE, Rainer, RK, & Ford, FN 2006, 'Information security: management's effect on culture and policy', Information Management & Computer Security, vol. 14, no. 1, pp. 24-36.

[10] Mouratidis, H, Jahankhani, H & Nikhoma, MZ 2008, 'Management versus security specialists: an empirical study on security related perceptions', Information Management & Computer Security, vol. 16, no. 2, pp. 187-205.

[11] Hagen, JM, Albrechtsen, E & Hovden, J 2008, 'Implementation and effectiveness of organizational information security measures', Information Management & Computer Security, vol. 16, no. 4, pp. 377-397.

[12] Doherty, NF, Anastasakis, L & Fulford, H 2009, 'The information security policy unpacked: A critical study of the content of university policies', *International Journal of Information Management*, vol. 29, no. 6, pp. 449-457.

[13] Bulgurcu, B, Cavusoglu, H & Benbasat, I 2010, 'Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness', MIS Quarterly, vol. 34, no. 3, pp. 523-A7.

[14] Ambawajy, J., 2014. User Preference of Cyber Security Awareness Delivery Methods. Behaviour & Information Technology, 33(3), pp. 236-247.

[15] Cone, B. D., Thompson, M. F., Irvine, C. E. & Nguyen, T. D., 2006. Cyber Security Training and Awareness Through. IFIP International Federation for Information Processing, vol. 201.

[16] Arash, G & Zarina, S., 2016. Awareness Training Transfer and Information Security Content Development for Healthcare Industry. *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 5, 2016.