Serious Games based approach to cyber security concept learning: Indian context

Raghu Raman [1], Athira Lal [2], Krishnashree Achuthan [2]

[1] Center for Research in Advanced Technologies for Education
Amrita University, India
{ raghu@amrita.edu }
[2] Amrita Center for Cyber Security
Amrita Vishwa Vidyapeetham, Amritapuri, Kollam – 690525
{ athirahari890@gmail.com , krishna@amrita.edu }

***Abstract*—: In the world of computer based gaming most of them are purely for entertainment but recently serious games are also emerging. Our research study focused primarily on a type of serious game with multiple scenarios designed specifically to support cyber security concept learning. We studied the impact of game based learning on cyber security graduate engineering students (N=20). Existing game scenarios were enhanced with summative assessments. A control group (EG1=10) was given the summative test without playing the game and a different group (EG2=10) was given the same test after playing the game. Results indicate that EG2 had better learning outcomes though there was learning curve with the game itself.**

Keywords—Serious games, network security, CyberCIEGE, awareness.

I. INTRODUCTION

Cyber security is an emerging scientific discipline requiring cross-domain solutions to manage the global cyber threat landscape (1,2,3,4,5). The sophistication and frequency of cyber-attacks and the magnitude of impact they cause require employment of dedicated personnel with scientific and practical knowledge to protect and thwart cybercrime. Most computer science curricula in schools and institutes of higher education do not provide specializations in cyber security. Although large initiatives to spread awareness and propaganda to eradicate vulnerabilities have been attempted, relatively large number of people continues to be victimized by malicious offenders (3,6). A mere handful of dedicated programs by the academia and reputed organizations provide certification and essential skills in cyber security, resulting in a hiatus to compliment the societal need today.

The traditional classroom teaching techniques have often been considered lacking in achieving intended learning objectives and problem solving skills. In this digital age where people, especially the youth live mostly in an online environment than offline, better mechanisms to stimulate interest to courses such as cyber security is required. Carl Wieman points out how the scientific community emphasizes on the quality of research, while there is little importance given to the quality of teaching. He further indicates the superiority of teaching students to apply concepts to real-life situations to lectures and homework assignments for learning. Activity based learning has shown to significantly improve the receptivity and retention of concepts in particular contexts.

This paper investigates application of gaming techniques to teach cyber security. A particular game, namely CyberCIEGE (6,7,8) was used to investigate the grasp and application of cyber security concepts amongst graduate students. These results could be further justified by analytical experiment where students are divided into two groups and some experiments are applied to them. Section 2 provides the review of all the papers that are used for this project. Section 3 provides an overview of the game and its components. The results analysis is detailed in section 4 and 5. Section 6 concludes this analysis and gives the direction for future research.

II. LITERATURE REVIEW

Academic institutions and corporations are developing innovative cutting edge games (1,2,3,5,9,10,11,12) for creating cyber security awareness by integrating game theory and human behavioral assessment. Cloud computing environments have (13) can be adapted to provide the required resources. With an objective of delivering an engaging and interactive experience, games based cyber security solutions are developed to help ensure the safe use of internet.

Information security awareness is becoming an important issue to anyone using the internet and the web (2). To overcome this issue, we include this awareness program in higher education. There are lots of methods to improve this program. Sometimes we use some gaming methods in online and offline, some educational videos etc. (1,2,3,14). A serious game is a game designed for a primary purpose mainly includes some educational games other than pure entertainment. These educational games give network security

awareness training. There are different types of serious games. (15).

CyberCIEGE (6,7,8) is a security awareness tool developed by the Center for Information Systems Security Studies and Research at the Naval Postgraduate School at California, USA. It is similar to some current games such as the Tycoon series of video games (6). It is also a serious game that teaches cyber security (15). The CyberCIEGE game consists of a 3 dimensional office environment consist of some characters who access the assets to achieve goals (6,7). This game gives a virtual money concept based on this. The building blocks of CyberCIEGE consist of several elements: a unique simulation engine, a domain-specific scenario definition language, a scenario development tool, and a video enhanced encyclopedia (6,7,8).

CyberProtect is another online game that teaches network security awareness (10,16).CyberSense is an innovative partnership between Serious Games International from Coventry University, Ascot Barclay Group a London Based Cyber Security Specialist and Aston Business Assessments a team of Organizational Psychologists from Aston University (17,18). The partnership was created to tackle the issues of delivering a consistent and compelling cyber security message to students. Rumble Blocks is a 3D game that was developed at the Entertainment Technology Center (ETC) to teach engineering principles of tower stability to children ages 4-7 (19). This tool permits the testing with the student's learning experiences and the entertainment mentality (9,16,19,20). Most of the security games offer Next Generation Security (20). SimBLEND (15), a research program funded by the Air Force Research Laboratory facilitates blending the delivery of computer based training content with simulations and serious games to create a web-based environment where learning is fun and skills can be practiced instantly (15).

In spite of the presence of some of the above described educational games for more than five years, evidence about the effectiveness of games in supporting learning is only beginning to emerge. The body of evidence is much smaller and weaker than the body of evidence related to the effectiveness of simulations. Some of the papers give a comparative study of both students' network security awareness before and after playing the game. In most of the cases research study indicates that the students who play the game had better learning outcomes (6,8,21).

III. CyberCIEGE: Simulation Games on Cyber Security

CyberCIEGE, developed by U.S. Navy and River-mind, is a unique game that teaches cyber security concepts. This game has its own language and creates the scenarios using this language. There are nearly 20 scenarios; each one describes the concepts of network security. The graphic libraries make significant use of the DirectX interface to provide the three dimensional experience. The building blocks of the game consist of several elements: a unique simulation engine, a domain-specific scenario definition language, a scenario development tool, and a video enhanced encyclopedia.

The simulation engine is designed for both games and simulations. It consists of a multiplatform 3D graphics library that supports standard based objects and animation as well as Windows like user interfaces within a fully 3D environment. That creates a 3 Dimensional office environment with users and systems. The engine contains an artificial intelligence, a video-playback library, sound library, memory-management system, resource-management system, and real-time economic engine designed to support resource management simulations. We can test the created scenarios with the simulation engine during the development.

Scenario Definition Language is used to create the scenarios. The simulation engine takes each scenario created by using scenario definition language and presents to students with the resulting simulation (with graphics and other interactive elements). The language includes elements like: Assets, Goal, User, Condition, Trigger, Zone, Phase & Objects.

- **Asset:** Assets are the highly secured Information that has some value to the enterprise.
- **Goal:** An asset goal is described based on the asset. That is, there is a particular goal to achieve each asset.
- **Users:** Each scenario includes a set of virtual users. Each character in the game is the user.
- **Zones**: Each scenario includes one or more physical zones. Physical access to components is limited to specific users only.
- **Conditions and Triggers:** The scenario designer defines conditions to be evaluated by the engine during play, and it specifies an action
- **Objectives and Phases:** Scenarios are divided into several phases and each consisting of one or more objectives.

Scenario Development Tool (SDT) is a tool that helps us to create the scenarios using scenario development language. It displays a graphical representation of the scenario and additionally permits scenario designers to construct scenarios from a library of re-usable scenario elements. Players can invoke the encyclopedia at any time. Encyclopedia entries mainly explain how to play the game. To understand the security concepts in deep includes a set of movies that cover security policy, malicious software, firewalls, assurance, and how to use the game.

IV. Methodology

The objective of our study is to implement game based scenarios and analyze the effectiveness of this approach in learning cyber security concepts. For this, an analytical study was conducted with a group of engineering students from an institution of higher education offering a formal cyber security

curriculum. Five scenarios (Table 1) were selected based on parameters like complexity, level of cyber-security conceptual knowledge needed and time to learn the scenario. Then for each scenario 15 questions were designed and reviewed by the faculty for technical depth and difficulty levels. The students were divided into two groups (EG1, EG2) of ten each. While the EG1 directly attempted the questions, EG2 were allowed to play with the scenarios and then answer the questions. At the beginning of the study, both EG1, EG2 had same levels of exposure to cyber security curriculum through their regular coursework. EG1 was expected to answer questions based on their knowledge from their regular classroom coursework. Additionally EG2 was given an introductory session about CyberCIEGE, scenarios and how to play the game. Both groups were given 45 minutes to complete the questions.

TABLE I. SELECTED FIVE SCENARIOS AND THEIR DESCRIPTION

Scenario Name	**Description**
Patches	Highlights the need to have a patch management plan.
DMZ	Help the office by protecting their secrets using a DMZ.
Link Encrypt	Introduces link Encryptor, basic key management issues and assurance.
SSL/TLS	Use SSL & TLS to help a small business grow and ward off attackers.
Mandatory Access Controls	Use a multilevel server to achieve controlled sharing of sensitive data.

The sample questions based on the above scenarios are given in (Table 2). Total of 15 summative type questions for each scenario were designed with multiple choice type answers.

TABLE II. SAMPLE QUESTIONS FOR SCENARIOS

Scenario	**Questions**	**Questions**
Patches	_____ are designed to fix security vulnerabilities. A. Hotfixes B. Patches C. Updates D. BIOS updates	How do you know whether a system is vulnerable? A. Based on vulnerability report obtained from scan B. Alarm produced C. Admin recognize the vulnerable systems just by viewing D. All of the above E. None of these
DMZ	Which statement best describes the objective of a DMZ? A. To create a security zone that allows public traffic but is isolated from the private network. B. To separate a security zone for an IPS. C. To separate a security zone for a VPN. D. To create a security zone that allows private traffic but is isolated from the public network. E. No idea	DMZ provides security from external attacks. What are the attacks possible? A. DMZ never protect the system from insider attacks, i.e. Attacks from internal attack B. It only gives short time security C. No other attacks , provide double security D. None of these E. No idea
Link Encryption	Devi and Deepak work in two department of same college. Devi wants to send some secret data to Deepak. But the problem is the line is vulnerable. Devi's system and Deepak's system are connected with a leased LAN. How they can communicate securely? A. Encrypt the leased line and pass the information through this line B. Email the details C. Just mail the data through post D. No idea	Dev is increasing the security of his communication to Anju by encrypting the line using Line Encryptor. Which type of encryption is used? A. Asymmetric B. Symmetric C. Public Key D. Secret
SSL/TLS	Rosa is a consumer of Company ABC. Rosa wants to buy some products from that company. For that she uses the web site of ABC, www.abccompany.com. How can she trust that company's site? A. Rosa confidence she is interacting with a known web site. SSL gives confidence that she is interacting with ABC. B. Required Rosa to install a ABC root C. Prevents hackers from masquerading as Rosa D. All of the above E. No idea	Your boss wants to establish growth through the use of secure Web commerce. You create a great Web site with all kinds of pictures and special links to equipment that your company sells. Which of the following should you use for security A. Secure Shell (SSH) B. Secure Sockets Layer (SSL) C. Layer Two Tunnelling Protocol (L2TP) D. IP Security (IPSec)

Mandatory Access Control	Which of the following access controls enforces permissions based on data labeling at specific levels? A. Mandatory access control B. Separation of duties access control C. Discretionary access control D. Role based access control	With regard to the classification of information, the levels of sensitivity used by the U.S. military include all of the following except which one? A. Unclassified B. Controlled C. Confidential D. Secret

V. RESULT ANALYSIS

The one tailed independent t test revealed that there was statistically significant difference between EG1 and EG2 groups of students t(9.519) = 9.8091, $p < 0.05$ (Table 3). The results indicated that the mean score of EG2 (Mean = 68.5, SD = 2.07) is significantly greater than mean score of EG1 (Mean = 30.2, SD =12.17) implying that students who took the assessment after playing with various scenarios had better learning outcomes.

TABLE III. STATISTICAL ANALYSIS OF EG1, EG2 SCORES

	Mean	SD	N	t- value	df	p-value
EG2	68.5	2.07	10	9.8091	9.519	1.381e-06
EG1	30.2	12.17	10			

Equally interesting to observe was the fact that there were certain questions which a very low % of EG1 students answered them correctly while the EG2 students overwhelmingly got correct answers for those very same questions. (Figure 1, 2, 3) This also lends support to the fact that taking the assessment after playing the game had positive impact on the learning outcomes.

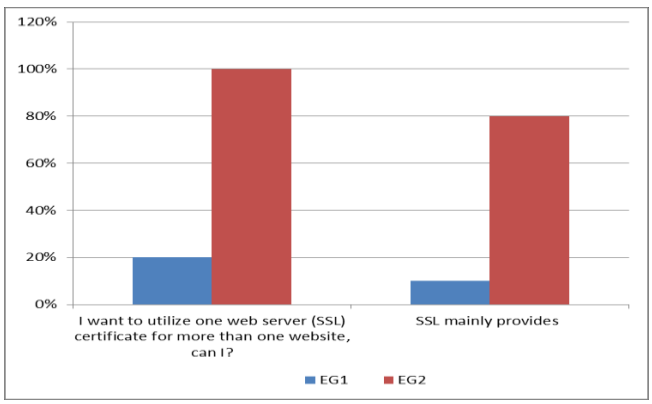

Fig. 1. Question related to SSL

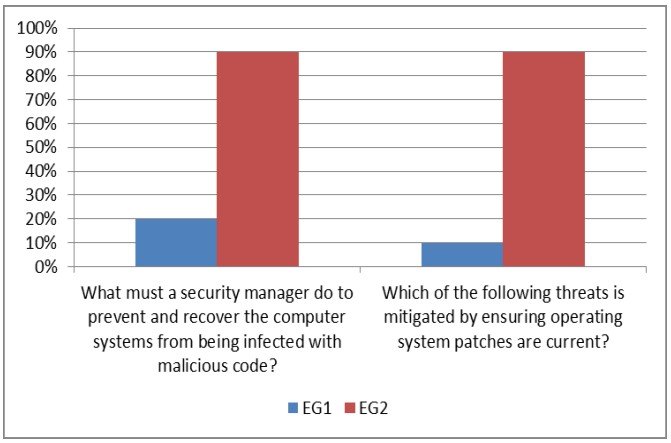

Fig. 2. Question related to Patches

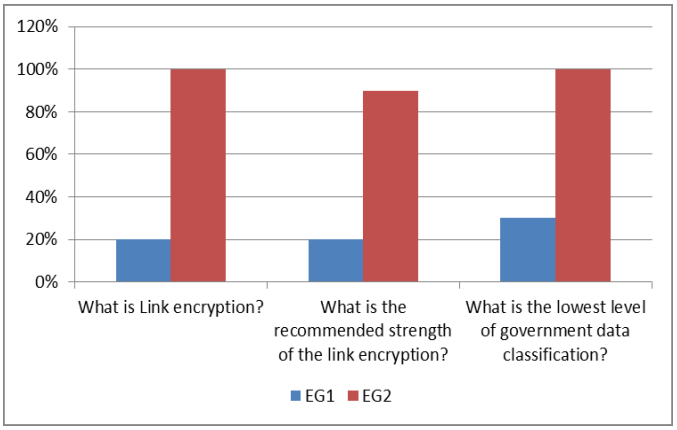

Fig. 3. Question related to Link Encryption and MAC

VI. CONCLUSION AND FUTUREWORK

Based on the objective of the paper, ten scenarios were implemented as Indian context. To study the effectiveness of those CyberCIEGE game, an analytical study was conducted. Five scenarios were selected randomly from ten scenarios for analysis purpose. First step was to prepare 75 questions (15 questions per 5 scenarios). The results highlight three primary observations. First the practical aspects of cyber-security were not delivered to students as part of their formal curriculum. Although investigation of the curriculum revealed several core subjects like cryptography, network security etc. being taught, they were not translated to application of these concepts to real life scenarios. Secondly, when introduced to the game and then the assessment, students had many more questions to ask about the various options that they were not aware of before playing the game. Thirdly the results reveal subjecting students to practical use-cases has an enormous impact on the extent of awareness by increasing their knowledge of the particular theme (network security as in this case), and on their view of cyber security in general.

This paper pointed the results from this analytical study on the evaluation on the use of the game, CyberCIEGE, as compared to traditional curriculum of training. The results

have provided a number of observations for further study and development. The research results show that the students from the group EG2 had better learning outcomes than group EG1. It is proved that the serious games are better than traditional curriculum.

ACKNOWLEDGMENT

Our work derives direction and ideas from the Chancellor of Amrita University, Sri Mata Amritanandamayi Devi. The authors of this paper wish to thank the Naval Postgraduate School, USA for their permission to use CyberCIEGE game in this study, and also the students who took part in this research. The authors would like to acknowledge the contributions of faculty and staff at Amrita University whose feedback and guidance was invaluable.

REFERENCES

[1] Y. Rezgui and A. Marks, "Information security awareness in higher education: An exploratory study," Computers & Security, vol. 27, pp. 241-253, 2008.

[2] R.S. Shaw, C.C. Chen, A.L. Harris and H. Huang, "The impact of information richness on information security awareness training effectiveness," Computers & Education, vol. 52, pp. 92-100, 1. 2009.

[3] Saunders, J. H. 2002: "Simulation approaches in information security education", Colloquium for Information Systems Security Education (CISSE) conference, 2002.

[4] C.E. Irvine, and M.F. Thompson, : "Expressing an information security policy within a security simulation game", Proceedings of the Sixth Workshop on Education in Computer Security (WECS6), Naval Postgraduate School, Monterey, California, July 12-16 2004, pp. 43-49.

[5] Irvine, C.E., Thompson, M.F., "Teaching Objectives of a Simulation Game for Computer Security", Proceedings of the Informing Science and Information Technology Joint Conference, Pori, Finland, June 24-27 2003.

[6] B.D. Cone, C.E. Irvine, M.F. Thompson, and T.D. Nguyen : "A video game for cyber security training and awareness", Computers & Security 26 (2007) pp. 63-72

[7] C.E. Irvine, M.F. Thompson, and K. Allen: "CyberCIEGE: gaming for information assurance", Security & Privacy Magazine, IEEE, May-June 2005, Volume: 3, Issue: 3, page(s): 61- 64, ISSN: 1540-7993.

[8] J. Jones., X. Yuan; E. Carr, H. Yu: "A comparative study of CyberCIEGE game and Department of Defense Information Assurance Awareness video,": "IEEE Southeast Con 2010 (Southeast Con) March 2010, Proceedings, page(s):176 – 180.

[9] Overmars, M.: "Teaching Computer Science through Game Design", Computer (Volume: 37, Issue: 4), April 2004, page(s): 81-83.

[10] Kirriemuir, J. (2002). "Video Gaming, Education and Digital Learning Technologies", D-Lib Magazine, November 27, 2002, Volume 8 Number 2, ISSN 1082-9873

[11] Squire K. : "Changing the game: what happens when video games enter the classroom?", Journal of Online Education , Volume 1, Issue 6, August/September 2005, An official publication of the Fischler School.

[12] Avinash Joshi, Varrun Ramani, Hrishikesh Murali, Radhesh Krishnan, Zubin Mithra, and Vipin Pavithran, Student Centric Design for Cyber Security Knowledge Empowerment , IEEE International Conference on Technology Enhanced Education, 2012, page(s): 1-4.

[13] Shiju Satyadevan, Kloud - A Virtual Elastic Knowledge Cloud, IEEE International Conference on Technology Enhanced Education, 2012

[14] DoD, Australian government, "*CyberSense* video: ASD Australian Signals Directorate", information security, 2009.

[15] L. Buchanan, F. Wolanczyk, F. Zinghini: "Blending Bloom's Taxonomy and Serious Game Design", 2011 International Conference on Security and Management (Las Vegas, Nevada USA) , July 18-21, 2011. CSREA Press, Volume: II, page(s): 518-521.

[16] Labuschagne, W.A. ; UNISA, Pretoria, South Africa ; Veerasamy, N. ; Burke, I. ; Eloff, M.M. : "Design of cyber security awareness game utilizing a social media framework", Information Security South Africa (ISSA), 2011 , page(s): 1-9.

[17] Official website of Ascot Barclay Group: "http://www.ascotbarclay.com/".

[18] Official website of Serious Games International from Coventry University: "http://www.coventry.ac.uk/research/research-directory/computer-science/serious-games-institute/".

[19] Christel, M.G. Pittsburgh, Stevens, S.M. ; Maher, B.S. ; Brice, S. ; Champer, M. ; Jayapalan, L. ; Qiaosi Chen ; Jing Jin ; Hausmann, D. ; Bastida, N. ; Xun Zhang ; Aleven, V. ; Koedinger, K. ; Chase, C. ; Harpstead, E. ; Lomas, D.: "Rumble Blocks: Teaching science concepts to young children through a Unity game ", Computer Games (CGAMES), 2012 17th International Conference, aug 2012, page(s) : 162 – 166.

[20] Suranjith Ariyapperuma1, Amina Minhas2: "Internet security games as a pedagogic tool for teaching network security", Frontiers in Education, 2005. FIE '05. Proceedings 35th Annual Conference, October 2005, pages: S2D – 1.

[21] Chun Che Fung1, Varin Khera, Arnold Depickere, Panjai Tantatsanawong and Poonpong Boonbrahm: "Raising Information Security Awareness in Digital Ecosystem with Games – a Pilot Study in Thailand": Digital Ecosystems and Technologies, 2008. DEST 2008. 2nd IEEE International Conference page(s): 375-380.

[22] Margie Martyn,: "Clickers in the Classroom: An Active Learning Approach", EDUCAUSE Quarterly,Monday, January 1, 2007.

[23] Frode Petter Gilberg: "Using Games to Improve Network Security Decisions": January 2007.