Cyber Security Training Perspectives

Joni A. Amorim, Dr.
University of Skövde - HiS, Sweden
Kanikegränd 3, Box 408
SE-541 28, Skövde
+46-500-44 80 00
joni.amorim@gmail.com

Maurice Hendrix, Dr.
Coventry University, UK
Coventry University Technology Park
Cheetah Road, Coventry CV1 2TL
+44(0)247615 8201
maurice@mauricehendrix.co.uk

Sten F. Andler, Dr.
University of Skövde - HiS, Sweden
Kanikegränd 3, Box 408
SE-541 28, Skövde
+46-500-44 80 00
sten.f.andler@his.se

James Llinas, Dr.
State Univ. of NY at Buffalo, USA
315 Bell Hall
Buffalo NY 14260
+1(716)645-3624
llinas@buffalo.edu

Per M. Gustavsson, Dr.
Swedish Nat. Def. College, Sweden
Drottning Kristinas väg 37
115 93 Stockholm
+46 8 553 425 00
per.m.gustavsson@fhs.se

Martin Brodin, B.Sc.
Actea Consulting, Sweden
Stora Badhusgatan 18-20
411 21 Göteborg
+46 31-15 26 40
martin.brodin@actea.se

ABSTRACT
Building comprehensive cyber security strategies to protect people, infrastructure and assets demands research on methods and practices to reduce risks. Once the methods and practices are identified, there is a need to develop training for the many stakeholders involved, from security experts to the end user. In this paper, we discuss new approaches for training, which includes the development of serious games for training on cyber security. The identification of the theoretical framework to be used for situation and threat assessment receives special consideration.

Keywords
Cyber Security, Information Fusion, Serious Games, Training.

1. INTRODUCTION
It may be stated that there are two types of cyber vulnerabilities [6]: technical, including holes, flaws or weaknesses, and nontechnical, including inappropriate policies, procedures, standards or guidelines. For the technical part, different solutions exist to protect the given systems. In this way, if only well tested applications from known developers are installed, and if these applications are kept updated and patched, the best results would be achieved in terms of protection. As a way to increase the control of any cyber environment, it is almost always possible to evaluate suppliers and to test applications before deployment. It is also possible to hand over some of the threat identification to the developers. For the nontechnical part, methodologies vary and may include, for example, starting the day looking at social media and different forums to find patterns and clues to new threats from outsiders [9]; this is a kind of context-based threat assessment. But, in this example, the system won't necessarily be protected from insiders like employees from the own organization. The insiders may decide to exploit flaws or, even unconsciously, let intruders in. Research shows that a good way to control threats from insiders is to introduce an awareness program for information security. If properly planed and performed, a program of this kind may be an effective way to reduce the threats from insiders [4]. This context suggests the need to develop training for the different stakeholders involved. Many studies show the importance of information security training [4][11][12][16]. A recent global information security survey [5] shows that careless or unaware employees are the single biggest source of threats. Even though it is important to train all employees, the training must be well planned on how, when and what to achieve for the expected desired result. It is also important to think about how people learn. According to research leading to the development of Edgar Dale's "cone of experience" [13], people generally learn and remember best what they study when they "do the real things" by themselves or, at least, when they are simulating that they are doing. Serious games could provide an environment where the learner may simulate actions in a more engaging way. In fact, it has been shown that serious games can be effective learning materials [2]. With that in mind, the training should be designed in a way that the students function as active participants as occurs in simulations and serious games. Related to this approach, our paper presents the four mains objectives of this research in the next section. While considering the first main objective, the third section of the paper discusses the theoretical background useful for situation and threat assessment. The last section of the paper presents a perspective on future work, which will focus on the gamification of training for cyber security. In this case, gamification [7] refers to the application of game thinking and mechanics to engage users, to solve problems, etc.

2. OBJECTIVES OF THE CURRENT WORK
This research has five main objectives: (1) identification of the theoretical framework to be used for situation and threat assessment; (2) identification of methods and comparison of automated tools for situation and threat assessment; (3) proposals for new ways of training on security using simulations and serious games; (4) development of the new training; and (5) evaluation of the results of the training prototype strategy.

3. ACCOMPLISHMENTS TO DATE
The use of methods and automated tools for situation and threat assessment are considered essential for security in the cyber world [15]. The main accomplishment of this research to date was to identify the information fusion theory as a theoretical framework to be used as an underlying framework for cyber security training.

Information is sometimes used as another word for data. Alternatively, information may be viewed as the meaning given to data by the way in which it is interpreted. The rapid evolution of technology has driven a continuous reshaping of definitions of both data fusion and information fusion [3][14]. Some usual definitions will be presented.

In this text, data fusion may be understood as a "process to organize, combine and interpret data and information from various sensors and sources (e.g., databases, reports) that may contain a number of objects and events, conflicting reports, cluttered backgrounds, degrees of error, deception, and ambiguities about events and behaviors" [8]. On the other hand, information fusion is understood as the "the synergistic integration of information from different sources about the behavior of a particular system, to support decisions and actions relating to the system" [1]. In this perspective, information fusion involves gathering information, fusing this information and interpreting the result. It is necessary to merge information for the subsequent manipulation and treatment.

The realization of a high-quality cyber-security training will clearly require that students be able to process multiple sources and streams of data/information, to include contextual information as previously remarked. Information fusion is a well-established theoretical and application discipline that we expect to underpin a new and effective approach to cyber-security training. A more detailed discussion on the many challenges in information fusion technology capabilities for security problems may be found in [10].

4. FUTURE PLANS

Future work will focus on the gamification [7] of training for cyber security, considering the protection of communication and information systems. Within this perspective, the use of methods and automated tools for situation and threat assessment will be considered while having information fusion theory as a theoretical framework. We will analyze training needs for cyber security and discuss its gamification. The use of game play mechanics will be considered with a special emphasis on strategies to encourage users to engage in desired secure behaviors. The use of games and game play mechanics has been shown [2] to be able to make the training more engaging and it helps increase motivation amongst learners. A requirements analysis of training needs will be made. And a possible design of a gamified training system for cyber security that complies with these requirements will be introduced. In this way, future work will deal with objectives 2, 3, 4 and 5 described previously.

5. ACKNOWLEDGMENTS

The authors would like to thank the following organizations for their support during the development of this work: University of Skövde (www.his.se), SAAB AB (www.saabgroup.com), CISB (cisb.org.br/), CNPq (www.cnpq.br), Swedish National Defence College (www.fhs.se), State University of NY at Buffalo (www.buffalo.edu), Actea Consulting (http://www.actea.se/) and Coventry University (www.coventry.ac.uk).

6. REFERENCES

[1] ANDLER, S. & BROHEDE, M. (2008). Information Fusion Research Program - Proposal. University of Skövde. November 24, 2008. Retrieved June 30, 2013 from http://www.his.se/

[2] BACKLUND, P. & HENDRIX, M. (2013). (Educational Games - Are They Worth The Effort?, Fifth International Conference on Games and Virtual Worlds for Serious Applications (VS-Games) 2013. UK.

[3] BLASCH, E. & STEINBERG, A. (2013). Situation/Threat Assessment and Higher Level Fusion. Tutorial 15. 16th International Conference on Information Fusion. July 9-12, 2013. Istanbul, Turkey. International Society of Information Fusion (ISIF).

[4] EMINAĞAOĞLU, M., UÇAR, E., & EREN, S. (2009). The positive outcomes of information security awareness training in companies - A case study. Information Security Technical Report. 14, 223-229.

[5] ERNST & YOUNG. (2012). Fighting to close the gap – Ernst & Young's 2012 Global Information Security Survey.

[6] HHS (2007). Basics of Security Risk Analysis and Risk Management. U.S. Department of Health & Human Services (HSS). HIPPA Security Series, Volume 2, Paper 6, 2007. Retrieved July 12, 2013 from http://www.hhs.gov/

[7] KAPP, K. M. (2012). The Gamification of Learning and Instruction: Game-based Methods and Strategies for Training and Education. Pfeiffer. ISBN 1118096347.

[8] KESSLER, O. & WHITE, F. (2008). Data Fusion Perspectives and Its Role in Information Processing. In: Handbook of Multisensor Data Fusion: Theory and Practice, Second Edition. Electrical Engineering & Applied Signal Processing Series. M. Liggins II (Editor), D. Hall (Editor), J. Llinas (Editor). CRC Press. September 26, 2008. ISBN 1420053086.

[9] LARSSON, D. (2013). Varför behöver polisen enas globalt och inom Europa om bevishantering och vilken roll har standardiseringen? (Why do the police need to globally agree on evidence collection and what roll does the standardization have?). Rätt säkerhet. May 21, 2013. Stockholm, Sweden.

[10] LLINAS, J. (2013). Challenges in Information Fusion Technology Capabilities for Modern Intelligence and Security Problems. European Intelligence and Security Informatics Conference (EISIC). August 12-14, 2013. Uppsala, Sweden.

[11] MISHRA, S., DHILLON, G. (2006) Information systems security governance research: a behavioral perspective, 1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference, 27-35.

[12] SIPONEN M., PAHNILA S., & MAHMOOD M.A. (2010). Compliance with information security policies: An empirical investigation. Computer. 43, 64-71.

[13] SPRAWLS, P. (2008). Evolving models for medical physics education and training: a global perspective. Biomed Imaging Interv J. 2008 Jan-Mar; 4(1): e16. Published online 2008 January 1. doi: 10.2349/biij.4.1.e16.

[14] STEINBERG, A. (2013). Fundamentals of Data Fusion. Tutorial 4. 16th International Conference on Information Fusion. July 9-12, 2013. Istanbul, Turkey. International Society of Information Fusion (ISIF).

[15] SYMANTEC. (2013). Internet Security Threat Report 2013, Volume 18. Retrieved August 22, 2013 from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

[16] WALTERS, R. (2013). Bringing IT out of the shadows. Network Security. 2013, 5-11.