Game Based Cyber Security Training: are Serious Games suitable for cyber security training?

Hendrix, M. , Al-Sherbaz, A. and Bloom, V.

Game Based Cyber Security Training: are Serious Games suitable for cyber security training?

Maurice Hendrix[1], Ali Al-Sherbaz[2], Victoria Bloom[3]
[1,3] *Department of Computing, School of Computing, Electronics and Maths, Coventry University, UK*
{ab0776, ab9488}@coventry.ac.uk
[2] *Department of Computing, School of Science and Technology, The University of Northampton, UK, Ali.Al-Sherbaz@northampton.ac.uk*

Abstract

Security research and training is attracting a lot of investment and interest from governments and the private sector. Most efforts have focused on physical security, while cyber security or digital security has been given less importance. With recent high-profile attacks it has become clear that training in cyber security is needed. Serious Games have the capability to be effective tools for public engagement and behavioural change and role play games, are already used by security professionals. Thus cyber security seems especially well-suited to Serious Games.

This paper investigates whether games can be effective cyber security training tools. The study is conducted by means of a structured literature review supplemented with a general web search.

While there are early positive indications there is not yet enough evidence to draw any definite conclusions. There is a clear gap in target audience with almost all products and studies targeting the general public and very little attention given to IT professionals and managers. The products and studies also mostly work over a short period, while it is known that short-term interventions are not particularly effective at affecting behavioural change.

Keywords: *Games, Serious Games, Cyber Security, Training, Online Safety;*

1. Introduction

The security industry is a complex and high value industry. The security landscape has been fast changing over recent years and security research and training is attracting a lot of investment from governments and the private sector. The majority of training interventions have so far focused on physical security. Less importance has been given to the security of computer infrastructure. While it may not be as clearly visible as physical security, computer infrastructure and networks control many vital functions in society, e.g. banking traffic and air traffic. A number of recent high profile attacks on major organizations have highlighted the issue and it has become clear that training of both the general public as well as security professionals is required. The use of training exercises with elaborate scenarios and roles is well established in both the security industry and among the emergency service. While not often noted as such this in effect amounts to the use of role play and could therefore be seen as so called role play games. This is often achieved in non-digital form but exercises supported by digital technology, such as Hydra [1], are also being used [2]. Therefore cyber security appears to be a topic that is especially well-suited to training via digital games, especially given the digital nature of cyber security.
Serious Games can be defined as games with a purpose other than pure entertainment. As Serious Games have gained increasing interest in fields such as healthcare [3], [4] advertising [5], and behavioural change [6]. Studies have shown that games can not only be effective training tools, but can also be effective tools for encouraging behavioural change.

The term Cyber security means protecting digital systems and assets from crimes. This includes protecting data and preventing undue release and usage for criminal purposes. Protecting data in cyberspace is very challenging. According to the UK Cabinet office [7], the cost of cybercrime is about £27 billion per annum to the UK economy. Of this approximately £2.2 billion directly affects the Government, approximately £3 billion directly affects individual citizens, mainly through identity theft and online scams, and UK businesses lose £21 billion per annum. The need to reduce the risk and the cost of cybercrimes is clear. One of the main ways to achieve this is by educating people and making sure people are aware of the latest prevention measures and have access to the latest tools. Serious Games allow people to practice in a safe and playful way and therefore developing cyber security Serious Games may be a cost effective solution to educate people and reduce cybercrimes.

This paper explores the current state of the field with regards to cyber security training games and investigates the current evidence on the effectiveness of using games as cyber security training tools for both the general public and for security professionals. This is achieved by reviewing both existing products and academic studies in the area. The rest of this paper is organized as follows. The next section explains in detail the research methods used in this study, followed by a discussion the results. Finally, the current state of training games for cyber security is discussed and directions for further development of training games discussed.

2. Methods

The number of computer games has increased dramatically over recent years and the development of Serious Games has become very popular. Serious Games are starting to be used for Cyber Security and this survey gives an accurate overview of the current state of the field. As the field develops rapidly and these developments are taking place both in academic and commercial settings, it is necessary to consider both scientific studies as well as currently available products. This overview therefore consists of two distinct parts: a structured review of research literature and a product search.

The structured review of the literature was carried out in September and October 2014 and includes papers published in journals and conferences. Google scholar was chosen as the academic database for the search, as it is a very popular source in the field of serious games and most relevant literature will end up in here. The database search was carried out using the following key words, and combinations of them:

- Game
- Computer game
- Serious Games
- Cyber Security
- Online Security
- Safety Gamification

The search was initially restricted to empirical studies with some kind of effect measurements, but since there were only very few of these the search was expanded to include any academic paper that describes a cyber security game. The search yielded a total of 49 hits. Each of these was inspected by the authors, for relevance, which resulted in the final selection of 28 papers. It is worth noting that many of the papers that were not selected addressed topics related security and game theory and thus the choice of keywords had unintentionally included a different sub-field of security. The selected studies were grouped by the game they describe. For each of these the different methodologies used in the studies were listed and a note added on whether any significant results were found. As a Google web search brings up a large amount of results, only the first 20 results for each keyword were considered and results with titles that appeared not relevant were not inspected further.

The original product search was carried out in August 2014 and updated in November 2015. The search was carried out using generic web search engines Google and Bing, popular gaming websites funlus.com and gamespot.com, and Serious Games specific database Serious Game Classification [8]. For this product search, the same keywords were used as for the literature search and Google (UK) web search was used. Only games directly related to cyber security were selected. Games were only included if enough information was freely available to assess their relevance. An evaluation of the learning effectiveness of these games is however beyond the scope of this article.

The search yielded 15 games that offer cyber security training. Detailed results are shown in section 3.2.

3. Results

3.1 Results of the literature review

An extensive literature search identified 28 papers discussing cyber security training games. Details of these papers are shown in table 1. Only 8 of these are from before 2010, which shows that this is a young and developing field. The 28 selected papers were classified and summarized by the authors, and described a range of different type of games. The most popular type of cyber security games studied is a 3D virtual world or simulation (5 games), with mobile applications (3 games) also proving popular. Most game studies, address general cyber security awareness (7), with network security (6), phishing (4) and end-user PC protection (3) also popular topics.
While the number of studies into cyber security training games is growing, almost all studies focus on efforts to train or raise awareness within the general public. Training security professionals is only investigated by 3 studies which use games to train professionals in handling insider threats, computer forensics and cryptography and infrastructure availability.
Evaluation is an important part of any rigorous study. However, surprisingly 6 of the studies explored did not evaluate the cyber security training game or the approach in any way. A further 6 indicated that an evaluation had taken place but were superficial on the methods, the results or both. Only 11 studies conducted an evaluation which can be scrutinized, with clearly described research methods and outcomes. These studies concern the following games:
Anti Phishing Phil, 'Security games by Next Generation Security (NGSEC)', CyberCIEGE, PicoCTF, Control-Alt-Hack, and 'A series of interactive visualisations'. All of these studies report a positive outcome, indicating that the game studies contributed to training or raising awareness of cyber security.
However only *Anti Phishing Phil and Security games by Next Generation Security (NGSEC)* are shown to have a measurable effect on learning outcomes and even then the sample sizes were quite small. The other games mentioned showed positive feedback from educators and/or students but did either not study effects on learning outcomes, or the results were not quite conclusive, but the authors were convinced they gave a positive "early indication".
While this does indicate that cyber security training games can be could be effective training tools, it also shows the immaturity of the field, with a need for more and different types of training games, especially for security professionals, and a need for more rigorous evaluations.

Table 1 Papers about Cyber security Training Games found.

Paper	*Game Name*	*Game Type*	*Methodology*	*Results*
[9]	TiER1	Interactive role-play	EEG and Eye tracking	Unclear
[10]–[14]	Anti Phishing Phil	Mobile application training safety of link URLs	Think aloud, pre-test & post-test experimental vs. control, SUS usability questionnaire	Positive impact on learning, awareness and phishing susceptibility
[15]	Security games by Next Generation Security (NGSEC)	Web-based	Comparing on-task performance	Significant improvement in game group
[16]–[22]	CyberCIEGE	3D virtual world (sims style)	Unclear ([17]) Experiment & self-assessment ([18]) Theoretical review of cognitive principles ([19])	Sufficiently flexible to illustrate a wide range of topics and positive early indication ([17]) Positive ([18]) Unclear, but there is a need to create a science of games ([19])

Paper	*Game Name*	*Game Type*	*Methodology*	*Results*
				Conclusions about software development ([20])
[23]	PicoCTF	Web-based	Survey	Positive educational experience according to students & instructors
[24]–[26]	Control-Alt-Hack, [d0x3d!],	Puzzle card & board games	Puzzles used as assessment in class in 2 groups (intervention vs. control) ([24]) Playing together ([25]) Survey of 22 educators teaching 450 students ([26])	Initial feedback positive, but more formal evaluation needed ([25]) Game is effective model for dissemination ([26])
[27]	Baltic Cyber Shield (BCS) international cyber defence exercise	Large training exercise with group of virtual attackers and defenders	Lessons learnt (informal)	A number of recommendations for IT infrastructure management
[28]	No specific games mentioned	Unclear	Review of initiatives	Initiatives need more synergy, no conclusions about games
[29]	"The Internet"	Unclear	Literature review	A review of elements a security network game should have
[30]	Internet Hero	Puzzle mini-games	Experiment with children	The children liked the games
[31], [32]	Security awareness program	Unspecified	Experiment with pre-test & post-test	No significant increase in awareness
[33]	CyberNEXS	Network simulation	None	Overview of game design
[34]	None (review paper)	Various	Literature review	More tools need to be developed
[35]	A series of interactive visualisations	Interactive visualisation	Case study	Account of positive experience of using interactive visualization
[36]	Multimedia and Interactive Courseware Synthesizer	Website with interactive animations	None	None

3.2 Results of the product search

In terms of products specific to cyber security, a number of training games have been identified. Table 2 shows detailed results listing the type of game, topics and target audience. Most of the games found were free to play, and focused on online security. The most popular target audiences were children, teenagers and students. We did however also find corporate training games with more detailed threats studied [37], [38] and even a game used as recruitment tool for cyber security experts [39]. Virtually no information is available about the effectiveness of any of these games with the exception of CyberCIEGE [40].

Table 2 Results of the product search.

Game Name	*Game Type*	*Topic / learning outcome*	*Target audience*
CyberCIEGE [40]	3D virtual world (sims style)	Information security for enterprise	Science curriculum students
CyberSecure Contingency Planning [38]	2D point & click turn-based scenarios	Contingency planning to prevent data loss at health practices	Health practice decision makers
CyberSecure Your Health Practice [38]	2D point & click turn-based scenarios	Contingency planning to prevent data breaches at health practices	Health practice decision makers
OnGuard [41]	2D point & click turn-based scenarios	Online security (viruses and malware as well as social networks)	Teenagers / Children
Budd:e [42]	2D point & click turn-based scenarios	Staying safe online (viruses and malware as well as social networks)	Children
NSteens [43]	Mini-games: 2D point & click turn-based scenarios and puzzle games	Staying safe online (viruses and malware as well as social networks)	Teenagers
Carnegie Cadets [44]	Various 2D mini-games	Staying safe online (viruses and malware as well as social networks)	Children
McGruff [45]	2D point & Click	Staying safe online (viruses and malware as well as social networks)	Children
FBI Cyber Game [46]	Puzzle games	The FBI, it's history and staying safe online	Children
PBS Cybersecurity Lab [47]	2D puzzles with extensive narrative cuts-scenes	Staying safe online, spotting scams and defending against cyber attacks	Children
The Cyber Security Challenge UK [48]	National competition (physical role-play)	Over 20 different competitions on various topics	School and university students
Game of Threats [37]	Partially digital via tablet controller, but controlled by facilitators	Cyber breach (companies being hacked into and losing data / data being compromised)	Companies
High School Cyber Security Game - global cyberlympics [49]	Global competitions, exercises scored by human facilitators	Forensics, computer network defence,	High School students

Game Name	*Game Type*	*Topic / learning outcome*	*Target audience*
CyberProtect [50]	2D simulation	Fundamentals of Cyber Security and Information Assurance	students and security professionals
Cyphinx [39]	Virtual world with puzzles	various	Students and young adults

4. Conclusion

Cyber security as an area consists of a number of different aspects, from digital equipment, software and cryptography to human processes and psychology. Training of cyber security using serious games is a young and developing field. Cyber security can be broadly categorized into security of IT network and infrastructure and security on the user side. The IT infrastructure security includes Network defence, DNS Protection, IP security, the defence of databases and data and zero day vulnerabilities. The Security on the user side includes secure behaviour of the user and recognizing web-based attacks, phishing and spam emails. As this paper has identified, better training of both the general public and businesses in cyber security is needed [7]. This paper investigated the games as effective cyber security training tools.

A number of games have been developed and academic studies have been conducted and some include an evaluation of the effectiveness of the game developed or the approach in general. The results from these studies are generally positive, however the sample sizes are small and selected and no effect sizes have been mentioned or can be calculated. It is clear that more robust evaluations with sizeable samples are needed, in order to be able to conclude on the effectiveness of serious games for cyber security. All interventions found focused on developing games that can be finished over a relatively short period and in one session. This is surprising considering that these games do not just aim to inform, but ultimately aim to change the player's long-term security behaviour. It is also interesting to note that all but one of the interventions evaluated targeted home computer users or the general public.

There are also quite a few products available, developed mostly by governmental organisations or charitable intuitions. There are also corporate training and recruitment initiatives. The effectiveness of these initiatives is however unclear. CyberCIEGE [40], was the only game to show up in both academic studies and the product search. The other games we found in the academic studies are either not easy to find without reading the paper or no longer available at all. This does raise questions about sustainability of games developed for academic studies.

Most of the academic studies found, target the end user and there is a clear lack of games that target IT infrastructure and especially management decisions around IT infrastructure, although we did find a few games available on the web that have not yet been rigorously evaluated. Furthermore, the games found are designed for very short-term interaction and those papers that included an evaluation only considered immediate short-term impacts. Therefore, although there are some positive early indications, the question of whether serious games are affective at training cyber security is at this point difficult to answer conclusively.

In this light, perhaps a different question should be asked rather than the original one posed. While it is very difficult to answer generically whether games are effective cyber security training tools perhaps the focus should be more on the type of scenario-based training that is already common in the security field which often includes gaming elements. Games could then represent specific case studies and facilitate a case-based learning approach.

5. Further Work

We are planning to elicit user requirements from both IT professionals and management decision makers. As this would clearly depend on the context of the organization, we aim to focus on law enforcement services. The intervention will need to be interacted with over a longer period of time, for example by integrating security scenarios, with ongoing working practices over a period of time (e.g. couple of weeks), both managers and IT professionals get presented with issues and their responses measured over a time frame much longer than a traditional game. If we take the example

of phishing emails than managers or employees will receive these from the game scenario and their response will be monitored as well as IT professionals' responses.
The next step would be to revisit the games with positive evaluation found and classify them according the taxonomy by Popescu at al. [51] as well as to develop game scenarios, taking into account the requirements of the different stakeholder groups. This will then inform our game design. Finally, an evaluation will establish whether this approach can in fact elicit behavioural change in terms of cyber security. For this we will use an appropriate methodology and reasonable size sample.

Acknowledgements

We would like to thank Nuffield for providing a student bursary. We would also like to thank Daniel Blisset whose work as a Nuffield student provided the starting point for the web search contained in this study.

References

[1] Flin, R. H. and Arbuthnot K., Incident command: Tales from the hot seat. Ashgate Pub Limited, 2002.
[2] Eriksson H., Kovordányi, R. and Rankin A., "CRISIS–Virtual-Reality-Based Training for Emergency Management," presented at the First National Symposium on Technology and Methodology for Security and Crisis Management (TAMSEC), Linköping, Sweden, 2010.
[3] Arnab S., Dunwell I., Debattista K., and Global I. G. I., Serious games for healthcare: Applications and implication. Medical Information Science Reference, 2013. http://dx.doi.org/10.4018/978-1-4666-1903-6
[4] Cugelman B., "Gamification: What It Is and Why It Matters to Digital Health Behavior Change Developers," JMIR Serious Games, vol. 1, no. 1, p. e3, Dec. 2013. http://dx.doi.org/10.2196/games.3139
[5] Cauberghe V. and De Pelsmacker P., "Advergames," J. Advert., vol. 39, no. 1, pp. 5–18, 2010. http://dx.doi.org/10.2753/JOA0091-3367390101
[6] Dunwell I., Petridis P., Arnab S., de Freitas S., Lameras P., Stewart C., and Hendrix M., "A Game-Based Learning Approach to Road Safety: The Code of Everand," in CHI'14: Proceedings of the 2014 CHI Conference on Human Factors in Computing Systems, 2014. http://dx.doi.org/10.1145/2556288.2557281
[7] UK Cabinet Office, "The Cost of Cyber Crime."
[8] "Serious Game Classification," 2014. [Online]. Available: http://serious.gameclassification.com/.
[9] Andre T. S., Fidopiastis C. M, Ripley T. R., Oskorus A. L, Meyer R. E., and Snyder R. A., "Augmented cognition methods for evaluating serious game based insider cyber threat detection training," in Foundations of Augmented Cognition. Directing the Future of Adaptive Systems, Springer, pp. 395–403, 2011. http://dx.doi.org/10.1007/978-3-642-21852-1_46
[10] Arachchilage G. and Asanka N., "Security awareness of computer users: A game based learning approach," Brunel University, School of Information Systems, Computing and Mathematics, 2012.
[11] Arachchilage N. A. G. and Love S., "A game design framework for avoiding phishing attacks," Comput. Hum. Behav., vol. 29, no. 3, pp. 706–714, 2013. http://dx.doi.org/10.1016/j.chb.2012.12.018
[12] Arachchilage N. A. G. and Love S., "Security awareness of computer users: A phishing threat avoidance perspective," Comput. Hum. Behav., vol. 38, pp. 304–312, 2014. http://dx.doi.org/10.1016/j.chb.2014.05.046
[13] Nyeste P. G. and Mayhorn C. B., "Training Users to Counteract Phishing," in Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 54, pp. 1956–1960, 2010. http://dx.doi.org/10.1177/154193121005402311
[14] Sheng S., Magnien B., Kumaraguru P., Acquisti A., Cranor L. F., Hong J., and Nunge E., "Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish," in Proceedings of the 3rd symposium on Usable privacy and security, pp. 88–99, 2007. http://dx.doi.org/10.1145/1280680.1280692

[15] Ariyapperuma S. and Minhas A., "Internet security games as a pedagogic tool for teaching network security," in Frontiers in Education, 2005. FIE'05. Proceedings 35th Annual Conference, p. S2D–1, 2005. http://dx.doi.org/10.1109/FIE.2005.1612218
[16] Cone B. D., Irvine C. E.,. Thompson M. F, and Nguyen T. D., "A video game for cyber security training and awareness," Comput. Secur., vol. 26, no. 1, pp. 63–72, 2007. http://dx.doi.org/10.1016/j.cose.2006.10.005
[17] Cone B. D., Thompson M. F., C. E. Irvine, and T. D. Nguyen, Cyber Security Training and Awareness Through Game Play. Springer, 2006. http://dx.doi.org/10.1007/0-387-33406-8_37
[18] Fung C. C., Khera V., Depickere A., Tantatsanawong P., and Boonbrahm P., "Raising information security awareness in digital ecosystem with games-a pilot study in Thailand," in Digital Ecosystems and Technologies, 2008. DEST 2008. 2nd IEEE International Conference on, pp. 375–380, 2008. http://dx.doi.org/10.1109/dest.2008.4635145
[19] Greitze F. L., Kuchar O. A., and Huston K., "Cognitive science implications for enhancing training effectiveness in a serious gaming context," J. Educ. Resour. Comput. JERIC, vol. 7, no. 3, p. 2, 2007. http://dx.doi.org/10.1145/1281320.1281322
[20] Irvine C. E., Thompson M. F., and Allen K., "CyberCIEGE: an information assurance teaching tool for training and awareness," DTIC Document, 2005.
[21] Irvine C. E. and Thompson M. F.,, "Simulation of PKI-enabled communication for identity management using CyberCIEGE," in MILITARY COMMUNICATIONS CONFERENCE, 2010-MILCOM 2010, pp. 906–911, 2010. http://dx.doi.org/10.1109/milcom.2010.5679591
[22] Thompson M. F and Irvine C. E., "Active Learning with the CyberCIEGE Video Game.," in CSET, 2011.
[23] Chapman P., Burket J., and Brumley D., "PicoCTF: A Game-Based Computer Security Competition for High School Students," 2014 USENIX Summit Gaming Games Gamification Secur. Educ. 3GSE 14, 2014.
[24] Dasgupta D., Ferebee D. M., and Michalewicz Z., "Applying puzzle-based learning to cyber-security education," in Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference, p. 20, 2013. http://dx.doi.org/10.1145/2528908.2528910
[25] Gondree M., Peterson Z. N., and Denning T., "Security through play," Secur. Priv. IEEE, vol. 11, no. 3, pp. 64–67, 2013. http://dx.doi.org/10.1109/MSP.2013.69
[26] Denning T., Lerner A., Shostack A., and Kohno T., "Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, pp. 915–928, 2013. http://dx.doi.org/10.1145/2508859.2516753
[27] Geers K., "Live fire exercise: preparing for cyber war," J. Homel. Secur. Emerg. Manag., vol. 7, no. 1, 2010. http://dx.doi.org/10.2202/1547-7355.1780
[28] Grobler M., Flowerday S., Von Solms R., and Venter H., "Cyber awareness initiatives in South Africa: a national perspective," 2011.
[29] Irvine C. E. and Thompson M., "Teaching objectives of a simulation game for computer security," DTIC Document, 2003.
[30] Kayali F., Wallner G., Kriglstein S., Bauer G., Martinek D., Hlavacs H., Purgathofer P., and Wölfle R., "A Case Study of a Learning Game about the Internet," in Games for Training, Education, Health and Sports, Springer, pp. 47–58, 2014.
[31] W. A. Labuschagne, N. Veerasamy, I. Burke, and M. M. Eloff, "Design of cyber security awareness game utilizing a social media framework," in Information Security South Africa (ISSA), 2011, pp. 1–9, 2011.
[32] Labuschagne W. A. and. Eloff M, "The Effectiveness of Online Gaming as Part of a Security Awareness Program," in 13th European Conference on Cyber Warfare and Security ECCWS-2014 The University of Piraeus Piraeus, Greece, p. 125, 2014.
[33] Nagarajan A., Allbeck J. M., Sood A., and. Janssen T. L, "Exploring game design for cybersecurity training," in Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on, pp. 256–262, 2012. http://dx.doi.org/10.1109/cyber.2012.6392562
[34] Pastor V., Díaz G., and Castro M., "State-of-the-art simulation systems for information security education, training and awareness," in Education Engineering (EDUCON), 2010 IEEE, pp. 1907–1916, 2010.
[35] Schweitzer D. and Brown W., "Using visualization to teach security," J. Comput. Sci. Coll., vol. 24, no. 5, pp. 143–150, 2009.

[36] Wang A. J. A., "Web-based interactive courseware for information security," in Proceedings of the 6th Conference on information Technology Education, pp. 199–204, 2005. http://dx.doi.org/10.1145/1095714.1095760
[37] "Game of ThreatsTM -- A cyber threat simulation," PwC. [Online]. Available: http://www.pwc.com/us/en/financial-services/cybersecurity-privacy/game-of-threats.html. [Accessed: 26-Nov-2015].
[38] "Cybersecure Contingency Planning." [Online]. Available: http://www.healthit.gov/sites/default/files/CyberSecure_103_FINAL/index.html. [Accessed: 20-Oct-2014].
[39] McGoogan C., "Cyphinx could recruit the cybersecurity experts of the future (Wired UK)," Wired UK. [Online]. Available: http://www.wired.co.uk/news/archive/2015-10/01/cyphinx-cybersecurity-game. [Accessed: 26-Nov-2015].
[40] "Cyber Ciege Educational Video Game." [Online]. Available: http://cisr.nps.edu/cyberciege/. [Accessed: 20-Oct-2014].
[41] "OnGuardOnline." [Online]. Available: http://www.onguardonline.gov/media. [Accessed: 20-Oct-2014].
[42] Australian Department of Broadband Communications and the Digital Economy, "Stay Smart Online Cybersecurity Education Modules - Primary." [Online]. Available: https://budd-e.staysmartonline.gov.au/primary/main.php#. [Accessed: 20-Oct-2014].
[43] "NSteens." [Online]. Available: http://www.nsteens.org/. [Accessed: 20-Oct-2014].
[44] Carenegie Mellon, "Carnegie Cyber Academy." [Online]. Available: http://www.carnegiecyberacademy.com/. [Accessed: 25-Nov-2014].
[45] Vermont Department of Information and innovation, "McGruff." [Online]. Available: http://www.mcgruff.org/#/Games. [Accessed: 25-Nov-2014].
[46] "Kids Games," FBI. [Online]. Available: https://www.fbi.gov/fun-games/kids/kids-games. [Accessed: 25-Nov-2015].
[47] "Cybersecurity Lab | NOVA Labs | PBS." [Online]. Available: http://www.pbs.org/wgbh/nova/labs/lab/cyber/. [Accessed: 26-Nov-2015].
[48] "cybersecurity challenge uk." [Online]. Available: http://cybersecuritychallenge.org.uk/. [Accessed: 26-Nov-2015].
[49] "High School Cyber Security Game," Global CyberLympics. .
[50] Information Assurane Support Environment, "CyberProtect." [Online]. Available: http://iase.disa.mil/eta/Lists/IA%20Simulations/AllItems.aspx. [Accessed: 26-Nov-2015].
[51] Popescu M.-M. and. Bellotti F, "Approaches on metrics and taxonomy in serious games," in Conference proceedings of" eLearning and Software for Education"(eLSE) pp. 351–358, 2012.