Conceptualization of Game Based Approaches for Learning and Training on Cyber Security

Menelaos N. Katsantonis
Department of Applied Informatics
156 Egnatia st, GR-54636
Thessaloniki, Greece
mkatsantonis@uom.gr

Panayotis Fouliras
Department of Applied Informatics
156 Egnatia st, GR-54636
Thessaloniki, Greece
pfoul@uom.gr

Ioannis Mavridis
Department of Applied Informatics
156 Egnatia st, GR-54636
Thessaloniki, Greece
mavridis@uom.gr

ABSTRACT

Utilizing game based approaches for learning and training on cyber security is a way to foster innovative methods and effectively train learners in highly-motivating settings. In this work, we investigate related works on such approaches. Our study reveals only a limited set of works focusing on diverse target groups and methodologies and a lack of conceptual analysis and design standards. To this end, we analyse the structure of cyber security learning and training approaches that utilize gamification and game based learning notions; we decompose these approaches into their respective elements; we define their relations; and we construct a concept map of pedagogical and technological elements of game based learning and training approaches on cyber security.

CCS CONCEPTS

• **Applied Computing** → Education • **Applied Computing** → Computer games

KEYWORDS

Cyber, security, game based, learning, training, learning theories

ACM Reference format:

M. N. Katsantonis, P. Fouliras and I. Mavridis. 2017. Conceptualization of Game Based Approaches for Learning and Training on Cyber Security. In *Proceedings of ACM Pan-Hellenic Conference on Informatics, Larisa, Greece, September 2017 (PCI2017).*

1 INTRODUCTION

The emergence of new cyber-threats provokes corresponding reflections on the provided cyber-security learning and training models and their connection to the education of cyber-security professionals. In this light, game based approaches are promising to improve cyber security learning and training effectiveness.

PCI 2017, September 28–30, 2017, Larissa, Greece

ACM ISBN 978-1-4503-5355-7/17/09...$15.00
https://doi.org/10.1145/3139367.3139415

As game based learning and training is a recent approach for cyber security education, there are few studies in this field. Nagarajan et al. [1] explore the field of cyber security training and present considerations on the design of games for cyber security training. Additionally, they present the shortcomings of the non-game based learning approaches; the design elements of their approach; and the improvements that can be made on their approach to upgrade the engagement, the entertainment and the educational impact.

Compte et al. in [2] rely on standard game design frameworks and methodologies (such as [3] and [4]) and they propose a six-step design framework for the development and deployment of games particularly in informal contexts. Additionally, they discuss the limitations of the current approaches including the issues of considering only the serious games deployment in formal settings.

Vykopal and Barták ([5]) present their study on the design and deployment of a prototype cyber security game for penetration testing training in a networked environment. According to their approach, the training activity of the game is decomposed into individual levels that learners have to accomplish to satisfy specific learning objectives. The researchers' efforts focus on scaffolding the learners towards the objectives achievements and on the prediction of user actions. The users' scaffolding is featured through a hints system that measures time, presents optional hints when learners struggle to solve an exercise and penalizes them with negative points. Furthermore, their approach includes a predicting users' actions facility through an advanced logging system that records participants' learning activities.

Allen and Straub in [6] presented an approach for the construction of effective cyber warrior's training program using various digital and physical games. Their approach suggests a gamified integrated and layered solution ranging from always on cell phone games to full scale operational exercises. Additionally, it provides continuous training and proficiency feedback to assess learning and mission readiness on individual and team basis. Trainees advance their skills, as they traverse towards more realistic and immersive environments (e.g. Lumosity-like games) that require reinforcement of soft skills, such as collaboration. Finally, trainees participate in simulation multiplayer exercise games to prove individual and team cyber proficiency.

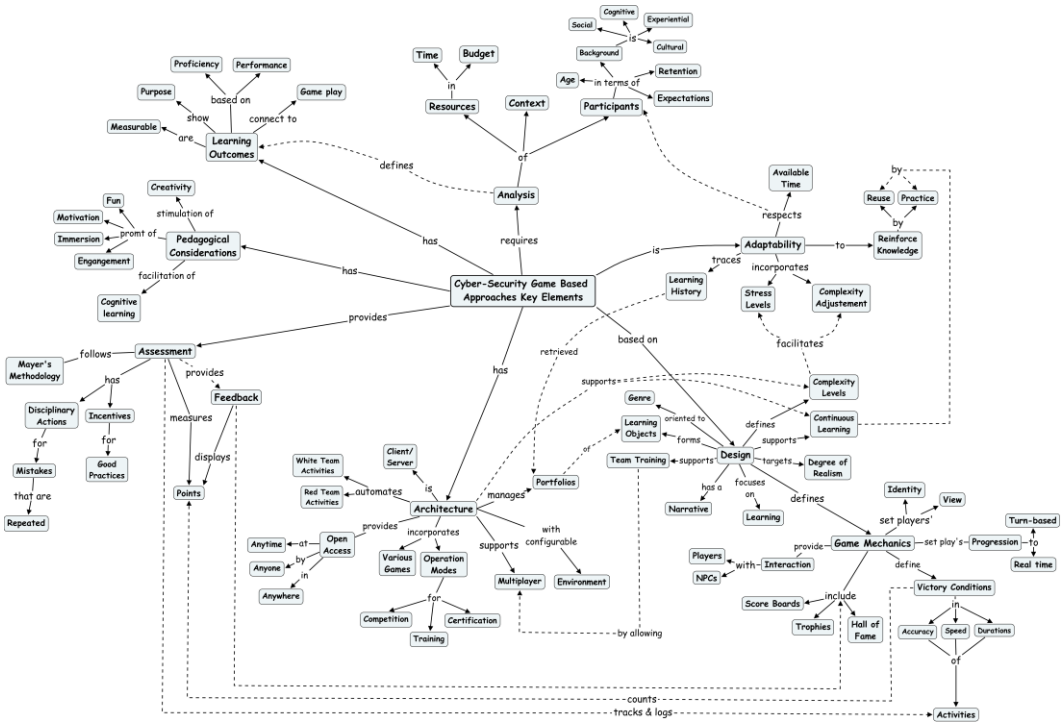

Figure 1: Concept Map of Cyber-Security Game Based Approaches Key Elements

Amorim et al. in [7] discuss a gamified training system for cyber defense. Researchers claim that traditional training schemes fail in cyber security domain because cyber world changes continually and rapidly. They claim that new training approaches are needed to provide new "on demand" material during the confrontation of a new threat. Thus, a component is necessary that will dynamically keep track of trainees' profiles and background. Moreover, authors claim that serious games and simulations are more suitable for cyber security training for which agile philosophy need to be adopted.

2 THE PROPOSED CONCEPTUALIZATION

Fig. 1 depicts the proposed concept map of key elements of game based learning and training on cyber security referred in the presented approaches. The concept map contains numerous elements that reflect the diversity of the topic. In particular, it consists of 78 concepts organized in 8 segments that share 14 cross-links represented in Fig. 1 with dashed lines for readability reasons.

The concepts in the proposed concept map are organized in a network structure, as game based learning and training on cyber security is a complex topic containing several concepts with multiple connections among them. Consequently, the concept map is logically organized in two clusters. The inner cluster contains the central node of characteristics of game based learning and training on cyber security and the general concepts, whereas the latter are depicted as labels of the concept map's segments. The outer cluster includes more specific notions belonging to the domain of each general concept.

3 CONCLUSIONS

As game based learning and training has only been used recently in the cyber-security field, a lot of efforts have to be put forward to produce a de-facto standard for developing such approaches. To this end, we briefly presented indicative related works from the literature, we decomposed them into their elements and we constructed a concept map of such approaches' characteristics.

REFERENCES

[1] A. Nagarajan, J. M. Allbeck, A. Sood, and T. L. Janssen. 2012 May. Exploring game design for cybersecurity training. In Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on (pp. 256-262). IEEE.

[2] A. Le Compte, T. Watson and D. Elizondo. 2015. A renewed approach to serious games for cyber security. Cyber Conflict: Architectures in Cyberspace (CyCon), 2015 7th International Conference on. IEEE.

[3] S. Arnab, T. Lim, M. B. Carvalho, F. Bellotti, S. De Freitas, S. Louchart, N. Suttie, R. Berta and A. De Gloria. 2015. Mapping learning and game mechanics for serious games analysis. British Journal of Educational Technology, 46(2), 391-411.

[4] B. Winn. 2008. The design, play, and experience framework. Handbook of research on effective electronic gaming in education 3: 1010-1024.

[5] J. Vykopal, and M. Barták. 2016, August. On the Design of Security Games: From Frustrating to Engaging Learning. In ASE@ USENIX Security Symposium.

[6] P. D. Allen and K. A. Straub. 2015. Using Games to Enrich Continuous Cyber Training. Johns Hopkins APL Technical Digest, Volume 33, Number 2 (2015), www.jhuapl.edu/techdigest.

[7] J. A. Amorim, M. Hendrix, S. F. Andler and P. M. Gustavsson. 2013. Gamified training for cyber defence: Methods and automated tools for situation and threat assessment. In NATO Modelling and Simulation Group (MSG) Annual Conference 2013 (MSG-111).