ISSN 1870-4069

Cybersecurity Teaching through Gamification: Aligning Training Resources to our Syllabus

Hugo Gonzalez, Rafael Llamas, Francisco Ordaz

Universidad Politecnica de San Luis Potosí,
Academia de Tecnologias de la Información y Telemática,
San Luis Potosí, Mexico

{hugo.gonzalez, rafael.llamas, francisco.ordaz}@upslp.edu.mx

Abstract. A shortage in Cybersecurity professionals is happening. Universities that offer IT related courses had implemented at least one class related with information security or cybersecurity, we believe that the training and experience gained by students during the term could be improved by using gamification. Gamification was defined as the use of game design elements in non-game contexts, in this context we use game design elements to help the learning process. Gamification has gained attention recently because it had shown that it can achieve positive results most of the time. In this work we offer a classification taxonomy for cybersecurity training resources based on gamification, then we collect and classify a list of training resources that can be used in cybersecurity lecturing. Finally we align some of these resources to the content of our syllabus in Polytechnic Universities system, so instructors and lecturers could improve the learning process for students. We also expect to raise interest on cybersecurity field from students, so we can help to minimize the professional shortage.

Keywords: Cybersecurity, gamification, teaching.

1 Introduction

The frequency and high impact of cyber attacks and cybercrime had been increasing in recent years. Numerous attacks on web applications and IT systems in every day, all time connected actual world, IT security has become a major concern for public and private sectors. More technical experts are demanded into the workforce, also people in management roles should have security knowledge at certain level. Training those experts face unique challenges, like the fast pace IT security moves. Dabrowski et al. [8] consider that security education should not merely rely on technical aspects, but the focus should include the mindset and typical methods of attackers to keep up with their pace. A key element to teach this skill set to students are real-world exercises within a controlled environment. Chotia and Novakovic [5] state that live security exercises, such as Capture The Flag (CTF) competitions, are a popular and fun means of engaging with cybersecurity topics.

pp. 35–43; rec. 2017-08-16; acc. 2017-10-04

While students with majors in cybersecurity will have their syllabus full of training and maybe certifications, it is our perspective that students in IT related fields should have at least one course of information security with a balanced proportions on technical and management skills.

Deterding et al. [10] define “gamification” as the use of game design elements in non-game contexts. Among other tasks gamification is used to engage users and help with the learning process [13]. Recently Li and Kulkarni [15] concluded that gamification is a very effective way of learning.

At the end, if Gamification is integrated properly, it can achieve positive results most of the times. Previous work had shown that gamification is a good option for training and prepare IT students on cybersecurity skills. Recently more people are designing courses and materials for cybersecurity with game elements in mind, so as a result there are several security training courses available, but as Gondree [12] states: there is a lack of alignment to curricular outcomes. Most of those training materials cover specific deep knowledge, meanwhile other material had been developed with a complete syllabus in mind, therefore it is not easy to adapt it to your own syllabus.

To address this gap, our contributions of this study are two fold: First, we collected a list of available resources for cybersecurity training that include game elements. Second, we aligned some of these resources with the syllabus of the Information security course taught in more than 40 Polytechnic Universities in the country.

The remainder of the paper discusses briefly the related work in Section 2, presents the details of our proposal in Section 3. Finally, Section 4 concludes the paper.

2 Related Work

Gamification has seen recenlty different applications [25], from marketing, fitness and health, employee motivation, and social media and website engagement. This technique aims to apply experience from psychology, human computer interaction, and game development to improve engagement and motivation to promote desirable behaviour.

Gamification has also been previously applied in security education and training. From different perspectives and different outcomes since last decade. Shiffman’s book [24] about hacker challenges is a combination of story telling and solve the puzzle. Each chapter presents a case and enough evidence for the reader to solve it. Control-Alt-Hack [9] is a table top card game to introduce people to information security concepts and white hacking world. Serious games, which involves professional game development engines and formal development process have been discussed also. Thornton and Francis [28] presented and discussed all the process to develop a serious game for IT and security training. The authors described the elements for the game design process,compare game engines available and evaluate their results with the students. Using a different approach, computer security competitions are very popular these days, with some of them emphasizing the competitive and entertainment aspects of breaking the systems, other actually have their main purpose for training. Gondree et al. [12] discuss about the cybersecurity competitions and games and how it is necessary to adopt a common vocabulary to express the games goals and characteristics. They also discuss talk about competitions like iCTF, DC3 Forensic Challenge, CyberPatriot, CCDC, PlaidCTF, CSAW CTF where training and education are their main role.

At least three frameworks to deploy Capture the Flag contests are freely available as open source software [27,19,3]. Also Backman [1] presented in details how to deploy and organize a CTF competition for undergraduate students.

Chothia et al. had been working in innovation and development of improved course materials. In 2015 the authors presented an offline CTF system which includes 5 learning activities [5]. The estudents can download the system and play in a controlled environment. In 2016 the authors developed a new course on pentesting using IoT devices, this course was thought at Birmingham University with great engagement and response from students [6]. In 2017 the authors included a story telling, intelligent component on a virtual machine to teach a course on information security in 11 weeks [4]; students chose their own adventure in the game.

Overall, scholars are creating new games, frameworks and systems to adapt their courses. In some cases they are developing courses and games at the same time. Our proposal is to collect available training resources, and align them to our syllabus, offering options for the lectures or instructor to chose, in the context of the Polytechnic Universities System.

3 Our Proposal

In the context of the Polytechnic Universities subsystem, different study programs related with Information Technologies and Telematics include at least one course about Information Security or cybersecurity. This course should follow the same syllabus in all the subsystem, with more than 60 universities around the country. In this work we are proposing to engage the students with more interest in the subject and developing deep knowledge about cybersecurity through gamification. To accomplish this purpose, we first present a classification taxonomy for cybersecurity training resources with relation to gamification, then we identify free available resources or material as such as CTF, vulnerable apps, games etc. Finally, we align these resources with different topics in our syllabus.

Cybersecurity training resources taxonomy We modify the classification taxonomy presented by Beuran et al. [2], adding resources employed, play type and target audience. We summarize this taxonomy in Figure 1.

Content oriented Training resources can have focus on attacks (**A**), defence (**D**), analysis/forensics (**AF**), or could be a hybrid combination (**H**). Attacks will train attendants from the attacker perspective or pen testers. Hybrid orientation will include different tasks for the train

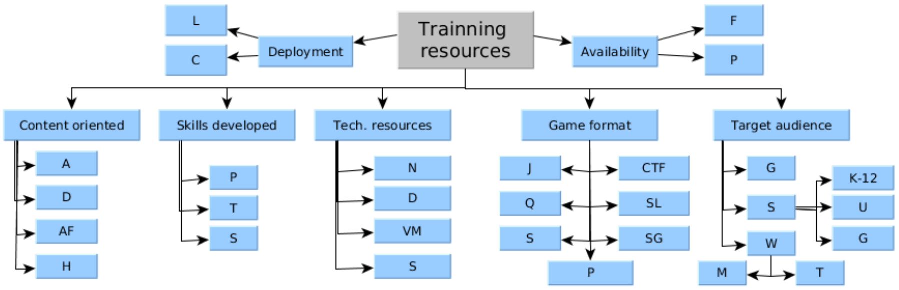

Fig. 1. Cybersecurity training resources taxonomy

Skills developed Training resources will focus in development of different levels of skills, like personal skills (**P**), were the attendant will work by herself. Or team skills (**T**), were the attendants need to collaborate during the training. Even it is possible to develop special skills (**S**).

Technical resources For IT personnel, running security training in the main facilities usually is uncomfortable because some of the risks these training represents. For some training resources it is not necessary to have any special technical resources (**N**), for others only a desktop computer (**D**) will be enough. However, Virtual machines (**VM**) or specialized laboratories (**S**) could be required for some training resources.

Deployment Resources can be deployed as local (**L**), like installing VM's on the students' laptop, or installing a CISCO network laboratory, or they can be available remotely, we consider them as if they were in the cloud (**C**).

Game format In gamification, the type of playing is important. The most common types are: jeopardy style (**J**), question based (**Q**), simulators (**S**), puzzle or challenge based (**P**), capture the flag style (**CTF**), story line games (**SL**) or serious games (**SG**).

Target audience Training resources are developed for a target audience, as such as general public (**G**), students (**S**) or workers (**W**). There exists cases where training resources could be developed for one target audience, but used by other like students taking advance classes, in this case the original target audience prevails for the classification

Availability Training resources could be available trough payment (**P**), or could be freely available (**F**).

Cybersecurity training resources In this part we compile a partial list of cybersecurity training resources. Our main focus is to present resources that involve any level of gamification to help the learning process. From a book that present scenarios and challenges in 2001 to modern serious games and on-line challenges that help with professional training. This list is presented in Table 1.

Table 1. Training resources.

Name	**Content Oriented**	**Skills**	**Tech. resources**	**Deployment**	**Game format**	**Target audience**	**Availability**
Hacker's Challenge: Test Your Incident Response Skills Using 20 Scenarios. [24]	A	P	N	L	ST, Q	G	P
Game of Threats	H	T	D	C	S, C, P	W	P
CyberCIEGE [20]	H	T	D	L	S, SG	PS	F, P
NetRiders Competition [7]	D	P	D	C	Q	S	P
Control-Alt-Hack [9]	H	P	N	L	C	G	P
d0x3d! [26]	H	T	N	L	C	G	F
Cybersecurity Lab [21]	H	P	D	C	ST, P	G,S	F
The Fugle Company [29]	D	P	D	C	S, ST	WM	F
Hacknet_ labyrinths [17]	A	P	D	C	S, P	G	P
True Key [18]	D	P	D	C	S	G	F
Hacker Experience [16]	A	P	D	C	S,ST,SG	G	F,P
iCTF [27]	A,D	P,T	VM	L	CTF	S	F
Root-the-box [19]	A,D	P,T	VM	L	CTF	S	F
EduRANGE [3]	A,D	P,T	VM	L	CTF	S	F
Wombat platform [30]	H	T	D	C	S, C	S,W	P
WebGoat [22]	A	P	VM	L	CTF	G	F
Damn Insecure and Vulnerable App [14]	A	P	D	L	CTF	G	F
Damn Vulnerable iOS app [11]	A	P	D	L	CTF	G	F
Metasplotaible [23]	A	P	VM	L	CTF	G	F

We are aware of the quick evolution of the field, and the vast amount of resources that pop everyday on the Internet. So we also offer a list of websites where you keep tabs on challenges and resources for cybersecurity training. This list of resources about training resources is presented in Table 2.

Overview of our cybersecurity syllabus Our official syllabus includes 5 main learning units to develop over 75 hours course.

Introduction to information security In this unit the student will be aware about the importance of cybersecurity in daily live basis. Also, how cybersecurity impacts the rest of topics in computer science and TI.

Standards, policies and good practices of cybersecurity In this unit the student will grasp the knowledge about established security standards in the industry. He will also explore the security policies and good practices that every company should have implemented, and the importance of having them in place.

Physical security (data, computers) This is a technical unit where students will learn how to protect their personal information resting in a computer. Fundamentals of cryptography and data protection are covered here.

Network and Internet security This is another technical unit where students will learn about security of data in transit, security of network devices and the dangers of software facing directly to the Internet.

Hot-topics in cybersecurity This unit is open to keep the fast pace of evolution in cybersecurity topics. It should be adapted each term for the current class. The mechanics of the unit is designed to offer students different options

Table 2. Cybersecurity training resources.

Url	Description
https://ructf.org/	RuCTF is a challenge in information security among russian universities.
http://www.wechall.net/about_wechall	A challenge site is mainly a site focussed on offering computer-related problems. Users can register at such a site and start solving challenges. There exist lots of different challenge types. The most common ones are the following: Cryptographic, Crackit, Steganography, Programming, Logic and Math/Science. The difficulty of these challenges vary as well.
https://ctftime.org/	a place, where you can get some another CTF-related info - current overall Capture The Flag
http://www.yashira.org/	Web site of IT challenges in Spanish.
https://www.hacking-lab.com/index.html	Hacking-Lab is an online ethical hacking, computer network and security challenge platform, dedicated to finding and educating cyber security talents.
http://smashthestack.org/wargames.html	The Smash the Stack Wargaming Network hosts several Wargames. A Wargame in our context can be described as an ethical hacking environment that supports the simulation of real world software vulnerability theories or concepts and allows for the legal execution of exploitation techniques. Software can be an Operating System, network protocol, or any userland application.
https://w3challs.com/	W3Challs is a penetration testing training platform, which offers various computer challenges, in categories related to security: Hacking, Cracking, Wargame, Forensic, Cryptography, Steganography and Programming. The purpose of this site is to offer realistic challenges, without simulation, and without guessing!
https://hack.me/	Hack.me is a FREE, community based project powered by eLearnSecurity. The community can build, host and share vulnerable web application code for educational and research purposes. It aims to be the largest collection of ”runnable” vulnerable web applications, code samples and CMS’s online.
https://www.root-me.org/?lang=en	The fast, easy, and affordable way to train your hacking skills.
https://www.hackthis.co.uk/	Want to learn about hacking and network security? Discover how hacks, dumps and defacements are performed and secure your website against hackers with HackThis!!
https://www.vulnhub.com/about/	To provide materials that allows anyone to gain practical ’hands-on’ experience in digital security, computer software & network administration.

to conduct research in a relevant topic of their interest.

It is not possible to include gamified resources in all units, but we aim to engage our students with extra work in those appropriated topics. It should be noted that offered degrees are not as cybersecurity specialists, but we are aiming to attract more students to this field.

Proposed Resources to Use With Our Syllabus Among all the resources available, we chose a handful of them that can be aligned and used with our curriculum. For the introduction topic, games developed for AV companies (True Key, the Fugle company) should be employed to present basic topics to the students in a very attractive way. If the game card Control-Alt-Hack is available, students should expend some time playing it.

For physical security, CTF offline games, like the ones offered by vulnhub can be used to help students to better understand the structure and insecurities of an operating system. These resources could also be employed in Operating Systems class to include cybersecurity topics. For Network security, training materials from NetRiders competition should be used. Networking labs related with NetRiders are available to Polytechnic Universities' students.

Finally for hot-topics in cybersecurity, if the topic chosen by the instructor is attacks for example, resources for attacks must be used as such as vulnerable systems or apps. The VM offered by Chothia [4] should be a good exercise for the students in this section.

4 Conclusion

Gamification is a new tendency to engage with students and help them to learn in a different way. Cybersecurity is a very hot topic nowadays, which is or it should be taught in every undergraduate program, however we are making special emphasis in IT degrees in the context of the Polytechnic Universities System. We aligned available resources to teach cybersecurity through gamification and presented them in this study. We are implementing our approach in the current semester and our expectations are into improve highly the students marks and help them to decide if they want to fill the cybersecurity professionals shortage. Our approach can be implemented and used by other Universities with similar syllabus or curriculum. As the field quickly evolves, instructors and teachers must keep active and updated in this field.

References

1. Backman, N.: Facilitating a battle between hackers: Computer security outside of the classroom. In: Proceedings of the 47th ACM Technical Symposium on Computing Science Education. pp. 603–608. SIGCSE '16, ACM, New York, NY, USA (2016)
2. Beuran, R., Chinen, K.i., Tan, Y., Shinoda, Y.: Towards effective cybersecurity education and training. Research report 2016, 1–16 (2016)
3. Boesen, S., Weiss, R., Sullivan, J., Locasto, M.E., Mache, J., Nilsen, E.: Edurange: Meeting the pedagogical challenges of student participation in cybertraining environments. In: Proceedings of the 7th USENIX Conference on Cyber Security Experimentation and Test. pp. 9–9. CSET'14, USENIX Association, Berkeley, CA, USA (2014)
4. Chothia, T., Holdcroft, S., Radu, A.I., Thomas, R.J.: Jail, hero or drug lord? turning a cyber security course into an 11 week choose your own adventure story. In: 2017 USENIX Workshop on Advances in Security Education (ASE17). USENIX Association (2017)
5. Chothia, T., Novakovic, C.: An offline capture the flag-style virtual machine and an assessment of its value for cybersecurity education. 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15) (2015)
6. Chothia, T., de Ruiter, J.: Learning from others' mistakes: Penetration testing iot devices in the classroom. In: 2016 USENIX Workshop on Advances in Security Education (ASE 16). USENIX Association (2016)
7. CISCO Networking Academy: Netriders competition, `http://www.academynetriders.com/index.php`, accessed in September 2017

8. Dabrowski, A., Kammerstetter, M., Thamm, E., Weippl, E., Kastner, W.: Leveraging competitive gamification for sustainable fun and profit in security education. 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15) (2015)
9. Denning, T., Lerner, A., Shostack, A., 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. CCS '13, ACM, New York, NY, USA (2013)
10. Deterding, S., Dixon, D., Khaled, R., Nacke, L.: From game design elements to gamefulness: Defining "gamification". In: Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments. pp. 9–15. MindTrek '11, ACM, New York, NY, USA (2011)
11. Gianchandani, P.: Damn vulnerable ios application, `http://damnvulnerableiosapp.com/`, accessed in September 2017
12. Gondree, M., Peterson, Z.N., Pusey, P.: Talking about talking about cybersecurity games. ;login: USENIX magazine 41(1), 36 – 40 (2016)
13. Hamari, J., Shernoff, D.J., Rowe, E., Coller, B., Asbell-Clarke, J., Edwards, T.: Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning. Computers in Human Behavior 54, 170 – 179 (2016)
14. Jakhar, A.: Damn insecure and vulnerable app, `http://payatu.com/damn-insecure-and-vulnerable-app`, accessed in September 2017
15. Li, C., Kulkarni, R.: Cybersecurity education through gamification. American Society for Engineering Education 123th Annual conference and exposition (2016)
16. Massaro, R.: Hacker experience, `https://hackerexperience.com/`, accessed in September 2017
17. McAfee: True key, `https://game.truekey.com/EN/`, accessed in September 2017
18. Moloch, J.: root-the-box framework, `https://github.com/moloch--/RootTheBox/`, accessed in September 2017
19. Naval postgraduate school: Cyberciege: Can you keep the network alive?, `http://my.nps.edu/web/cisr/cyberciege`, accessed in September 2017
20. Nova Labs: Cybersecurity lab, `http://www.pbs.org/wgbh/nova/labs/about-cyber-lab/`, accessed in September 2017
21. OWASP: Webgoat insecure web application, `https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project`, accessed in September 2017
22. Rapid7: Metasplotaible, `https://information.rapid7.com/metasploitable-download.html`, accessed in September 2017
23. Schiffman, M.: Hacker's Challenge: Test Your Incident Response Skills Using 20 Scenarios. McGraw-Hill, Inc., New York, NY, USA (2001)
24. Schreuders, Z.C., Butterfield, E.: Gamification for teaching and learning computer security in higher education. In: 2016 USENIX Workshop on Advances in Security Education (ASE 16). USENIX Association (2016)
25. TableTop Security: [d0x3d!] a network security game, `https://github.com/TableTopSecurity/d0x3d-the-game/`, accessed in September 2017
26. The Computer Security Group at UC Santa Barbara: ictf framework, `https://github.com/ucsb-seclab/ictf-framework`, accessed in September 2017
27. Thornton, D., Francia, G.: Gamification of information systems and security training: Issues and case studies. Inf. Secur. Edu. J 1(1), 19–29 (2014)
28. Trend Micro: The fugle company, `http://targetedattacks.trendmicro.com/cyoa/esp/`, accessed in September 2017

29. Trobbiani, M.: Hacknet_ labyrinths, `http://hacknet-os.com/`, accessed in September 2017
30. Wombat security technologies: Wombat security education platform, `https://www.wombatsecurity.com/security-education`, accessed in September 2017