Tracking the Students' Learning Behavior for Cybersecurity Scenarios*

Antonio Uzal[1], Llanos Tobarra[1][0000−0003−2779−4042], Alejandro Utrilla[1], Antonio Robles-Gómez[1][0000−0002−5181−0199], Rafael Pastor-Vargas[1][0000−0002−4089−9538], and Roberto Hernández[1][0000−0002−0967−0874]

Communication and Control Systems Department, ETSI Informática
Universidad Nacional de Educación a Distancia (UNED), Spain
auzal@pas.uned.es;
{llanos,arobles,rpastor,roberto}@scc.uned.es;
autrilla14@alumno.uned.es
http://casper.scc.uned.es

Abstract. The ability to prevent dangerous cyber-threats in critical infrastructures depends on the availability of a security trained workforce and, therefore, an education system that can achieve this capacity. This work presents the key elements of a framework for hosting educative games based on the cybersecurity topics, by tracking the students' performance during learning competitions, further than standard log capabilities. This feature allows faculty to adapt and evolve the learning process to the students' needs. What is more, helping students to learn in an effective and efficient way with technological resources. Data privacy considerations are also given by adapting regulations to our proposal.

Keywords: cybersecurity · gamification · learning analytics.

1 Introduction

Today's society is purely digital; the use of digital technologies is employed in a multitude of sectors with non-stop growth. It is evident that it brings significant benefits, but new problems also appear, as is the case of cyber-security. The need

* Authors would like to acknowledge the support of the eNMoLabs research project for the period 2019-2020 from UNED; our teaching innovation group, CiberGID, started at UNED in 2018 and its associated CiberScratch PID project for the year 2020; another project for the period 2017-2018 from the Computer Science Engineering School (ETSI Informática) in UNED; and the Region of Madrid for the support of E-Madrid-CM Network of Excellence (S2018/TCS-4307). The authors also acknowledge the support of SNOLA, officially recognized Thematic Network of Excellence (RED2018-102725-T) by the Spanish Ministry of Science, Innovation and Universities.

for professionals in this field is a challenge, and it is growing at a faster rate than the training of qualified professionals [23]. The ability to prevent successful cyber-attacks against a nation's critical infrastructure depends on the availability of a skilled cyber-literate workforce and, therefore, on an educational system that can build such capabilities [5]. The next generations of engineers must be qualified to address technological threats on the Internet both theoretically and practically. This approach helps to develop critical thinking skills [11,26,40]. Applying the gamification of the learning process through case studies achieves improvements in outcomes [20,4,3].

It is clear that incorporating this type of initiative into our learning methodology, especially in distance education, can offer significant advantages. However, the deployment of such competencies is often very time consuming for lecturers. The design of security contests is complicated, as they must be at the appropriate level of difficulty concerning the target audience. If a competition is too difficult, the participants get frustrated. If a competition is too easy, participants are not challenged and will lose interest. Ideally, a competition would offer a variety of challenges of different difficulties, so that all participants of various skill levels would be challenged by tasks and gratified by success.

In addition to this, when competitions are included as an evaluation element in the educational curriculum, we may encounter dishonest behavior on the part of participants. Moreover, of course, it is complex to share this type of experience with other lecturers. Once the competition has been carried out, it is likely that the participants will publish their solutions in blogs or forums and therefore, the competition has already lost its freshness and the possibility of reuse.

Our project focuses on the idea of developing an approach that exploits the advantages already presented of such a context and that in turn allows solving the problems already mentioned. Therefore, the project presents its own scenario editor and allows the possibility of generating content whose solutions are different for the participants, which would help to solve part of the problem of honesty. However, it also provides enough tools for tracking and intervenes in the learning process of the participants during the game.

This work is organized as follows: Section 2 introduce the related work of the paper. Section 3 presents the principal objectives of our current work, as well as the architecture and definitions of the proposed game platform. The learning monitor of the game platform is given in Section 4, as well as a set of data privacy considerations adapted from current regulations. Finally, some conclusions and future works are specified in Section 5.

2 Related Work

First, it deserves to distinguish between platforms aimed at hosting competitions to capture the flag and generation environments for the competition itself. This work is mainly focused on the second type of frameworks.

To achieve this purpose, meaningful and enriching activities must be offered. Currently, the Capture the Flag (CTF) competitions are very popular and suc-

cessful [41]. These competitions can have three different game dynamics: quizzes, hidden elements (flags) and challenges. Through this type of competition, participants apply the knowledge they have acquired through theoretical study, which increases their motivation. Also, another advantage is the need for group collaboration to solve problems [24]. Similarly, performing and publishing the solutions to the challenges, known as write-ups, allows for learning beyond the competition itself [6].

Deploying CTF competitions is complex and requires valuable lecturer time. Automated problem generation [2] is applied to Pico-CFT. The work [38] presents a solution for the 2017 iCTF competition. It consists of a set of pre-configured virtual machines (VMs). On the other hand, the work [32] introduces a Security Scenario Generator in order to provide a flexible general technique to define and deploy VMs for education and training in security. In this sense, an alternative is to use personalized Docker containers for speeding the deployment phases of the infrastructure. Additionally, the platform Git-based CTF [39] allows lecturers to deploy a Red/Blue Team challenges with high interactivity among participants.

Closer to our approach, the work [30] presents a formal language oriented to the definition of professional cyber-ranges exercises, although it is only oriented to the validation/verification of scenarios. Finally, the work [14] presents Alpaca, a novel dynamic cyber range generator, based on a multi-step sequence of exploits from a vulnerability database and some generation of thinking paths.

As a result of this type of competition, the honesty of the students could be called into question. It is possible that for some of the participants, their main objective is to achieve the score without making an effort to learn. Within the CTFs there have appeared approaches to solve this problem. Some works [7,16,8] have introduced anti-plagiarisms methods, such as strong encryption randomized flags.

Most of these platforms are focused on the recreation of realistic environments. However, they provide very few tools for monitoring the performance of students. Most of them only provide simple tracking elements, such as the registry of the awarded flags. This work is focused on increasing those elements into a real learning analytic system, which will be deployed in an efficient dynamic infrastructure, based on Docker containers.

3 Motivation and Architecture

3.1 Contextualization

This work is supported by an innovation educational project at UNED, named CiberScrath [9] (*In English*, CyberScratch). The principal objective of this project is to innovate in the design of mechanisms for the inclusion of gamification techniques within remote and virtual laboratories aimed in the context of cybersecurity, as well as their integration into the field of education. The resulting framework should provide the following features [12,37]:

– Easing the development of CTF competitions, reducing the time invested in the design of the technical part.

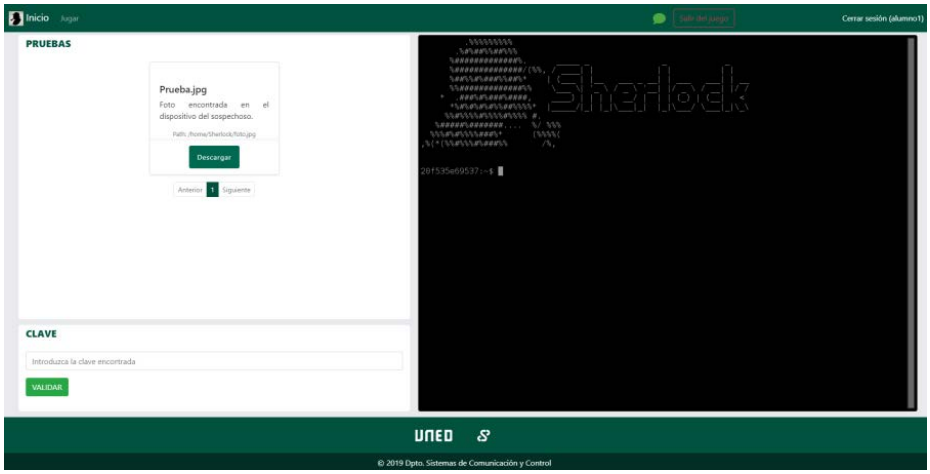

Fig. 1. Sh3rl0ck H0lm3$ application interface

- Including mechanisms to personalize the context to participants, allowing for the replication of the process, but not the sharing of the flags.
- Allowing the creation of motivating games with stories that allow the bifurcation of the development based on the decisions of the player.
- Facilitating the monitoring of the players' performance by the teaching team.

The research group had previously worked on the creation of remote virtual laboratories aimed at cybersecurity by using containers [29,35]. This approach seems interesting to generate a customized container for each player. This way, the students' gaming experience can be adapted to the requirements of the project. In addition to this, a final degree project (called Sh3rl0ck H0lm3$), has been proved to be a suitable option (see Fig. 1). One of its main drawbacks was the lack of monitoring features or intervention elements further than the basic log module, although this development is a good starting point for our CyberScratch project.

This work focuses on the definition of the initial architecture and the development of a prototype. This prototype includes a graphic editor by adding monitor tools to analyze the students' learning. In addition to this, some efforts have initially performed to match the phases of Learning Analytics (LA) [33] with current privacy and data control requirements from Spanish and European guidelines and standards.

3.2 The Proposed Platform

Conceptually, a game consists of one or more cases, as observed in Fig. 2. In fact, in each case, we can find one or more mission and some characters. The development of the missions can be sequential or concurrent. A mission (or a set of missions) can be available after solving some previous events. There are some

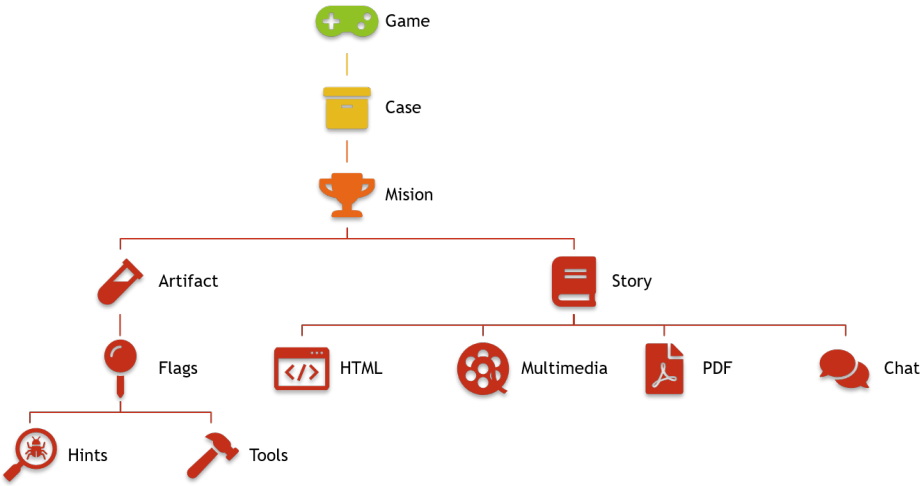

Fig. 2. Conceptual structure of the game definition

key missions that once they are solved, the rest of active missions are closed. The mission order is determined using two attributes inside the mission element: the previous mission and cancel events.

Each mission is guided by some artifacts and on or more stories. A story element is composed of one or several messages. A message can be a video, an audio file, an HTML fragment or a PDF file with the narration of the story, or a set of messages that are used to train a character bot. This last option allows players to chat with a bot character. A message can be associated with a particular character of the case. An example of this chat feature is represented in Fig. 3.

A preliminary architecture of this game platform is depicted in Fig. 4. The XML definition of the game is used to create the game dynamics for each player. Additionally, the game resources and the game docker template is compiled in order to create a specific Docker container [13] for the player. This container is remotely accessed utilizing the Apache Guacamole project [18] for the game platform. The proposed game platform is being developed using the Django web framework [17].

Developing a game platform for learning cybersecurity is challenging because the competition's execution environment is often hostile and, thus, it is difficult to monitor and control the game. It is essential to have mechanisms and policies for the easy diagnosis of possible problems in educational and security terms. Therefore, it is clear the need for a specific strategy that allows lecturers to track the students' performance.

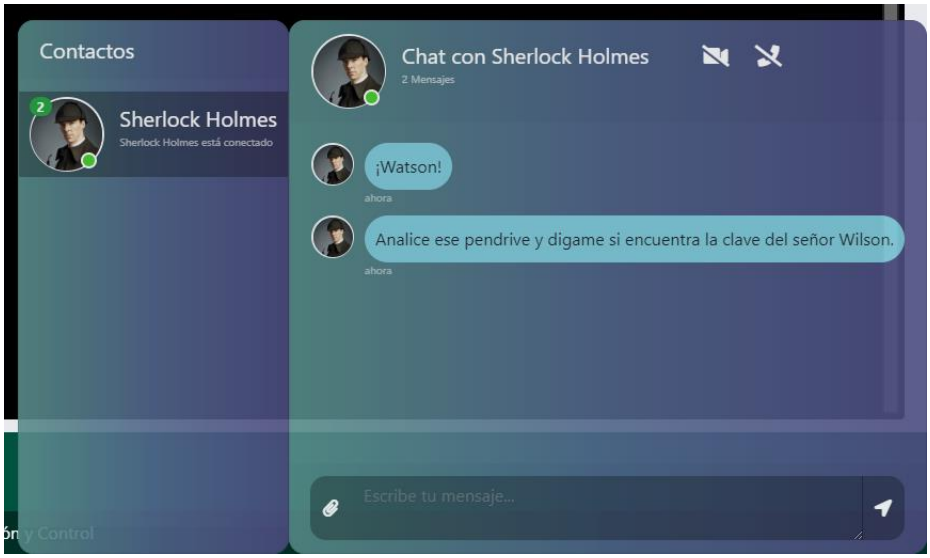

Fig. 3. Example of a game chat with a character bot

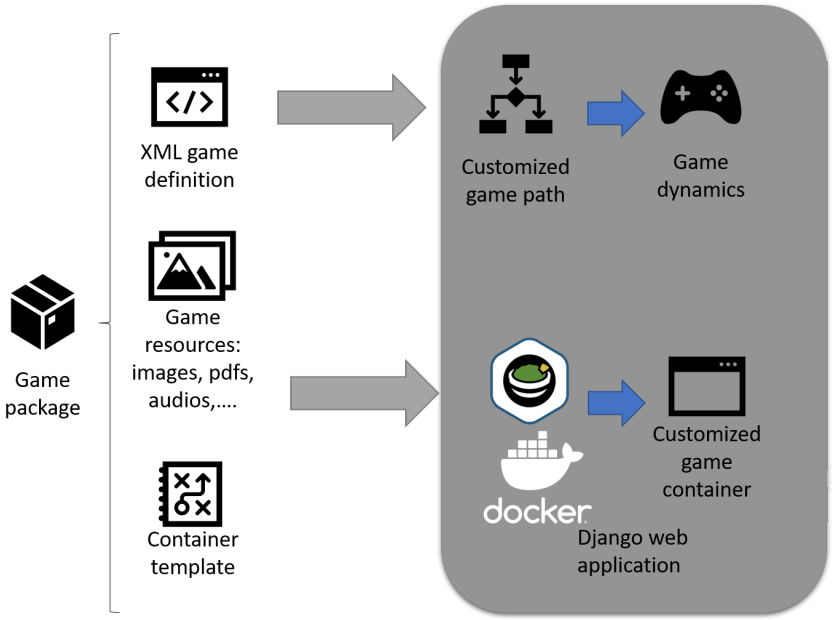

Fig. 4. Proposed architecture for the CyberScratch game framework where analytics engine is deployed

4 Game Monitor and Learning Analytics

ISO/IEC TR 20748-1:2016 [15] is a technical report oriented to describe conceptually the behavior of all the elements involved in the interoperability of Learning Analytics (LA). Specifically, it proposes a reference model in its clause 6 for the various processes that make up the LA cycle.

According to ISO/IEC TR 20748-1:2016, six phases compose a LA circle: learning and teaching activity, data collection, data processing and storing, data analyzing, data visualization, and feedback and recommendation. Learning-teaching activity has been described in the previous section. Thus, the following subsections are focused on the data collection phase and data processing and storing phase. The rest of the phases are thought for further work.

The results of the analysis are intervening in the learning process as an internal mechanism. On the one hand, the game provides with hints. So, when a student is stacked, she/he can request a hint. Also, it is automatically detected that the player does not progress in a prudential time. The hint will be provided using a chat with a character. On the other hand, students are provided with several visualizations of their progress through the game in comparison with other participants. Further analysis of these visualizations will take place in order to select those more suitable. Finally, lecturers provide with visualizations to help them to tackle the game. Additionally, the platform will be programmed with alert messages to report about students at risk or unusual situations.

4.1 Data Collection, Processing and Storing

Many learning tools export their activity registry into a Learning Registry System (LRS) that implements the xAPI specification [10,1,25,33]. In this case, to record our students' activity on the platform, we are formatting those events as xAPI statements. xAPI statements are managed by TinCanPython library [31] inside the created framework. One of the main advantages of this approach is the ability to reuse existing learning analysis techniques and incorporating them into our gaming platform in a simple way. Another advantage of this solution is the capability of exporting the activity towards a cloud LRS.

xAPI statements are composed of three main elements: actor, verb and object. In our framework, we have three main actors: students, lecturers and group of students. Verbs in xAPI are URIs, and they should be paired with a short display string. In our case, most of the verbs included in the data collection phase are already described in the xAPI registry [34], such as accessed (platform, game, mission ...), completed (game, case, mission), found (a flag), and so on. The third element represents the activity: a game, a mission, a case, a flag, a reward, etc. Again, xAPI registry provides a vast number of types of activities that easily fit in our statements.

Since 2019, the context element has been added to the xAPI statement to include some contextual information to a statement. This contextual information includes the group that students belong to or the course related to the game. Finally, a statement can also end in some measured outcome by a result element.

In our case, result statement can be used in conjunction with the resolution of a case, indicating if it is successfully found or it is a failure.

Apart from occasional actions, a challenge in data collection is the gathering of the commands used for solving the challenges. The game provides a customized docker container with the needed tools to solve missions. Alternative students can download the artifact associated with the mission and work locally. To retrieve the session commands, before the player's container is stopped, the registry of commands is retrieved. The representation of this learning event must be represented by the use of the result element recording the commands in the response property.

xAPI statements are stored in a MongoDB NoSQL database [27]. MongoDB allows us to create a JSON document-based database that stores the xAPI statement directly. MongoDB offers security features, such as encryption at rest, transport encryption by TLS, authentication, access control and role-based access control feature, and auditing mechanisms.

4.2 Data Privacy Considerations

Automatic learning analyses are increasingly integrated within educational institutions, training in work environments or platforms oriented to long life learning, such as our project. It is inevitable concerning about privacy and data protection. Confirmation of this fact can be found in [19]. In that work, framed within the LA Community Exchange (LACE) project and funded by the European Union, the question of the impact of privacy on the area of the development of LA was raised. Another project that follows this idea is the Sheila project [28] focused on the development of a privacy data framework in educational institutions. In parallel with the growth of the LA community, there was an enormous development in data protection regulation, both internationally and nationally. According to a survey conducted by the United Nations Conference on Trade and Development [36], by 2018, 107 countries (58%) had developed data protection legislation, and 10% were in the process of doing so. As an example, in Spain, the regulation of data protection is determined by the following laws: Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDGDD) and General Data Protection Regulation (GDPR), the second one is the general data protection law approved by the European Union in April 2016.

Following this spirit of the regulation, in ISO/IEC TR 20748-1:2016 [15], the importance of the user's control of his/her data is highlighted, emphasizing the need to implement mechanisms that give the student (or his/her legal tutors) the possibility to avoid monitoring. It also put the focus on the need to manage data control and user identification through a federation of identities. The detailed correspondence among ISO/IEC TR 20748-1:2016 phases and their corresponding privacy requirements has been correlated at [21]. According to this work, each phase must fulfill the following privacy requirements:

- *Learning and Teaching Activity*: Giving information of processing operation and purpose.

Table 1. Relationship between the various phases of LA, the privacy and data control requirements of the proposed model at ISO/IEC TR 20748-1:2016 and our approach implementation

GDPR Requirements	**LA Phases**	**Implementation**
Right to be informed	All phases	Students will be informed their sign previously up in the platform through an informative form. Further details are provided by a privacy document attached to the informative form.
Right to access	All phases	Students can access the following data: personal information from profile section, activity data through session reports, data used for analysis from their personal profile section (as a JSON document), and stored results of analysis from personal performance visualizations.
Right to rectification	Learning activity, Data Collection, Data Processing and Storing	Students can update their data at the profile area of the framework.
Right to erasure	Learning activity, Data Collection, Data Processing and Storing	Students can request the deletion of their data from the profile section. LA will be an integral part of the course, and the student is given the option to terminate the course and have his/her data deleted.
Right to restrict processing	Data Processing and Storing	Similar to the previous item. Data will be preserved as long as it is needed for evaluation purposes. Later, it is deleted.
Right to data portability	Data Processing and Storing	Their data can be downloaded from the profile section. The file is zipped with the same password as the user profile.
Right to object	All phases	There is a service agreement that informs about the learners' rights to object to any aspect of the LA processes at the profile section.
Right related to automated decision making and profiling	Analyzing, Visualization, Feedback and Recommendation	There is an email account to retrieve students opinions in the agreement form.
Accountability and governance	All phases	Audit, role-based control access and authentication based on MongoDB security features.
Breach notification	Data Processing and Storing	Notification will follow the procedure determined by UNED.
Transfer data	Data Processing and Storing	Data will not be transferred outside UNED.
Data protection by design and default	All phases	Policy of data applying security measures, such as encryption for data at rest and TLS transport for data in communication.

- *Data Collection*: Affirmative action of consent to data collection.
- *Data Processing and Storing*: Access to, and rectification or erasure of personal data. Having the right to be forgotten. Pseudonymization and risk assessment.
- *Analyzing*: Meaningful information about the logic involved. Information of profiling, e.g., predictive modeling.
- *Visualization*: General requirements for transparency and communication.
- *Feedback and Recommendation*: Information about the significance and envisaged consequences of data processing.

Thus, we have adapted these recommendations to our framework, as summarized in Table 1. Additionally, universities must have an active role in the ethical regulation of the use of educational data. UNED has created a research ethical committee [22] to report the results of this framework and the collected data before to any further research.

5 Conclusions and Further Works

The current work presents a platform for gamification and its relevant characteristics, which will allow us both the monitoring of learning and the lecturers' intervention when considered convenient. We have also included into the platform a set of tools to ease the collaborative learning among students (and with the lecturers), peer recognition, and promote healthy and constructive competitiveness. Data privacy is also taken into account in this work, by adopting regulations to the case of UNED and our concrete project. There is still much work to be done, specially to improve the offered visualizations to students and lecturers as well as, adding new elements to our platform, such as characters with a higher intelligence which allow a more fluid interaction with students.

Although our preliminary results are promising, a first test full-experience of the gaming platform in the context of a security degree subject is running at the moment. Therefore, providing statistical data or analysis for the platform's satisfaction and acceptance, or analyzing its impact on the learning process, is planned as future work.

References

1. Berg, A., Scheffel, M., Drachsler, H., Ternier, S., Specht, M.: The dutch xapi experience. In: Proceedings of the Sixth International Conference on Learning Analytics & Knowledge. p. 544–545. LAK '16, Association for Computing Machinery, New York, NY, USA (2016), https://doi.org/10.1145/2883851.2883968
2. Burket, J., Chapman, P., Becker, T., Ganas, C., Brumley, D.: Automatic problem generation for capture-the-flag competitions. In: 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15). USENIX Association, Washington, D.C. (Aug 2015), https://www.usenix.org/conference/3gse15/summit-program/presentation/burket

3. Cano, J., Hernández, R., Ros, S., Tobarra, L.: A distributed laboratory architecture for game based learning in cybersecurity and critical infrastructures. In: 2016 13th International Conference on Remote Engineering and Virtual Instrumentation (REV). pp. 183–185 (2016)
4. Cano, J., Hernández, R., Ros, S.: Bringing an engineering lab into social sciences: didactic approach and an experiential evaluation. IEEE Communications Magazine **52**, 101–107 (2014)
5. Catota, F.E., Morgan, M.G., Sicker, D.C.: Cybersecurity education in a developing nation: the Ecuadorian environment. Journal of Cybersecurity **5**(1) (03 2019). https://doi.org/10.1093/cybsec/tyz001, https://doi.org/10.1093/cybsec/tyz001, tyz001
6. Childers, N., Boe, B., Cavallaro, L., Cavedon, L., Cova, M., Egele, M., Vigna, G.: Organizing large scale hacking competitions. In: Kreibich, C., Jahnke, M. (eds.) Detection of Intrusions and Malware, and Vulnerability Assessment. pp. 132–152. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)
7. Chothia, T., Novakovic, C.: An offline capture the flag-style virtual machine and an assessment of its value for cybersecurity education. In: 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15). USENIX Association, Washington, D.C. (august 2015), https://www.usenix.org/conference/3gse15/summit-program/presentation/chothia
8. Chothia, T., Novakovic, C., Radu, A.I., Thomas, R.J.: Choose Your Pwn Adventure: Adding Competition and Storytelling to an Introductory Cybersecurity Course, pp. 141–172. Springer Berlin Heidelberg, Berlin, Heidelberg (2019), https://doi.org/10.1007/978-3-662-59351-6_12
9. de Innovación Docente en Ciberseguridad (CiberGid), G.: Ciberscratch. on line at http://casper.scc.uned.es/ciberscratch/index.html (2020), last accesed: 7th april 2020
10. Co-Laboratories, A.D.L.A.: Experience api. versión: 1.0.2. Tech. rep., Advanced Distributed Learning (ADL) Initiative (2016), https://github.com/adlnet/xAPI-Spec/blob/1.0.2/xAPI.md
11. Dasgupta, D., Ferebee, D.M., Michalewicz, Z.: Applying puzzle-based learning to cyber-security education. In: Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference. p. 20–26. InfoSecCD '13, Association for Computing Machinery, New York, NY, USA (2013). https://doi.org/10.1145/2528908.2528910, https://doi.org/10.1145/2528908.2528910
12. 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. p. 9–15. MindTrek '11, Association for Computing Machinery, New York, NY, USA (2011). https://doi.org/10.1145/2181037.2181040, https://doi.org/10.1145/2181037.2181040
13. Docker: Docker. debug your app, not your environment. on line at https://www.docker.com/ (2020), last accesed: 7th april 2020
14. Eckroth, J., Chen, K., Gatewood, H., Belna, B.: Alpaca: Building dynamic cyber ranges with procedurally-generated vulnerability lattices. In: Proceedings of the 2019 ACM Southeast Conference. p. 78–85. ACM SE '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3299815.3314438, https://doi.org/10.1145/3299815.3314438

15. technology SC 36. Information technology for learning education, I.J.I., training.: Information technology for learning, education and training — learning analytics interoperability —part 1:reference model. Tech. rep., ISO and IEC (2016), https://www.iso.org/standard/68976.html
16. chang Feng, W.: A scaffolded, metamorphic CTF for reverse engineering. In: 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15). USENIX Association, Washington, D.C. (Aug 2015), https://www.usenix.org/conference/3gse15/summit-program/presentation/feng
17. Foundation, D.S.: Django. the web framework for perfectionists with deadlines. on line at https://www.djangoproject.com/ (2020), last accesed: 7th april 2020
18. Foundation, T.A.S.: Apache guacamole. on line at https://guacamole.apache.org/ (2020), last accesed: 7th april 2020
19. Griffiths, D., Drachsler, H., Kickmeier-Rust, M., Steiner, C., Hoel, T., W.Greller: Is Privacy a Show-stopper for Learning Analytics? A Review of Current Issues and Solutions. LACE project (2016), retrieved from http://www.laceproject.eu/learning-analytics-review/is-privacy-a-show-stopper/
20. Hamari, J., Koivisto, J., Sarsa, H.: Does gamification work? – a literature review of empirical studies on gamification. In: 2014 47th Hawaii International Conference on System Sciences. pp. 3025–3034 (Jan 2014). https://doi.org/10.1109/HICSS.2014.377, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6758978&tag=1
21. Hoel, T., Griffiths, D., Chen, W.: The influence of data protection and privacy frameworks on the design of learning analytics systems. In: Proceedings of the Seventh International Learning Analytics & Knowledge Conference. p. 243–252. LAK '17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3027385.3027414, https://doi.org/10.1145/3027385.3027414
22. Vicerrectorado de Investigación, T.d.C.y.D.C.U.: Comite de Ética de la investigación. Available at http://portal.uned.es/portal/page?_pageid=93,639534,93_20530755&_dad=portal&_schema=PORTAL (2020)
23. (ISC)^2: Strategies for building and growing strong cybersecurity teams. cybersecurity workforce study, 2019. on line at https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482 (2019), last accesed: 7th april 2020
24. Jariwala, S., Champion, M., Rajivan, P., Cooke, N.: Influence of team communication and coordination on the performance of teams at the ictf competition. Proceedings of the Human Factors and Ergonomics Society Annual Meeting **56**, 458–462 (10 2012). https://doi.org/10.1177/1071181312561044
25. Manso-Vázquez, M., Caeiro-Rodríguez, M., M.Llamas-Nistal: An xapi application profile to monitor self-regulated learning strategies. IEEE Access **6**, 42467–42481 (2018)
26. Martini, B., Choo, K.K.R.: Building the next generation of cyber security professionals. ECIS 2014 Proceedings - 22nd European Conference on Information Systems (01 2014)
27. MongoDB, I.: Mongdb. the database for modern applications. Available at https://www.mongodb.com/ (2020)
28. Project, S.: Sheila. using data wisely for education futures. on line at https://sheilaproject.eu/ (2020), last accesed: 7th april 2020

29. Robles-Gómez, A., Tobarra, L., Pastor, R., Hernández, R., Duque, A., Cano, J.: Analyzing the students' learning within a container-based virtual laboratory for cybersecurity. In: Proceedings of the Seventh International Conference on Technological Ecosystems for Enhancing Multiculturality. p. 275–283. TEEM'19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3362789.3362840, https://doi.org/10.1145/3362789.3362840
30. Russo, E., Costa, G., Armando, A.: Scenario design and validation for next generation cyber ranges. In: 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA). pp. 1–4 (2018)
31. RusticiSoftware: Tincanpython library. Available at https://github.com/RusticiSoftware/TinCanPython (2020)
32. Schreuders, Z.C., Shaw, T., Shan-A-Khuda, M., Ravichandran, G., Keighley, J., Ordean, M.: Security scenario generator (secgen): A framework for generating randomly vulnerable rich-scenario vms for learning computer security and hosting CTF events. In: 2017 USENIX Workshop on Advances in Security Education (ASE 17). USENIX Association, Vancouver, BC (Aug 2017), https://www.usenix.org/conference/ase17/workshop-program/presentation/schreuders
33. Ángel Serrano-Laguna, Martínez-Ortiz, I., Haag, J., Regan, D., Johnson, A., Fernández-Manjón, B.: Applying standards to systematize learning analytics in serious games. Computer Standards & Interfaces **50**, 116 – 123 (2017). https://doi.org/https://doi.org/10.1016/j.csi.2016.09.014, http://www.sciencedirect.com/science/article/pii/S0920548916301040
34. Software, R.: Experience api registry. Available at https://registry.tincanapi.com/#home/verbs (2020)
35. Tobarra, L., Robles-Gómez, A., Pastor, R., Hernández, R., Duque, A., Cano, J.: Students' acceptance and tracking of a new container-based virtual laboratory. Applied Sciences **10**(3), 1091 (Feb 2020). https://doi.org/10.3390/app10031091, http://dx.doi.org/10.3390/app10031091
36. conference on Trade, U.N., Development: Data protection and privacy legislation worldwide. Available at https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (2018)
37. Trapero, A., Tobarra, L., Pastor, R., Robles-Gómez, A., Hernández, R., Duque, A., Cano, J.: Game-based learning approach to cybersecurity. In: 2020 IEEE Global Engineering Education Conference (EDUCON). pp. 1125–1132 (2020)
38. Trickel, E., Disperati, F., Gustafson, E., Kalantari, F., Mabey, M., Tiwari, N., Safaei, Y., Doupé, A., Vigna, G.: Shell we play a game? ctf-as-a-service for security education. In: 2017 USENIX Workshop on Advances in Security Education (ASE 17). USENIX Association, Vancouver, BC (Aug 2017), https://www.usenix.org/conference/ase17/workshop-program/presentation/trickel
39. Wi, S., Choi, J., Cha, S.K.: Git-based CTF: A simple and effective approach to organizing in-course attack-and-defense security competition. In: 2018 USENIX Workshop on Advances in Security Education (ASE 18). USENIX Association, Baltimore, MD (Aug 2018), https://www.usenix.org/conference/ase18/presentation/wi
40. Willingham, D.: Critical thinking why is it so hard to teach? Arts Education Policy Review **109** (08 2010). https://doi.org/10.3200/AEPR.109.4.21-32
41. Zhang, X., Liu, B., Gong, X., Song, Z.: State-of-the-art: Security competition in talent education. In: Chen, X., Lin, D., Yung, M. (eds.) Information Security and Cryptology. pp. 461–481. Springer International Publishing, Cham (2018)