A distributed laboratory architecture for game based learning in cybersecurity and critical infrastructures

Jesús Cano, Roberto Hernández, Salvador Ros, Llanos Tobarra
Department of Communication and Control Systems
National Distance Education University (UNED)
Madrid, Spain
{jcano,roberto,sros,llanos}@scc.uned.es

***Abstract*—This paper shows a design based on distributed architectures for a remote laboratory to learn cybersecurity and infrastructure protection systems. Distributed architectures, especially those supported by virtualization and cloud computing, along with other emerging technologies such as Game-based Learning (GBL), currently are a hot trend in educational and professional fields. Around this idea, a key is the concept of educational piece as meaning an element of instructional design where is including a suitable game. Therefore, each piece is characterized. These points among others allow us to plan the game-based lab design and to determine most appropriate time for each learning activity. Eventually, a game-piece-based architecture is able to deploy a kind of laboratories on cybersecurity and critical infrastructures, but that can be generalized for educational activities in other fields. This method provides a coherent reasoning to learning objectives and enough flexibility within a teaching program. In order to get a consistent and effective overcome, a laboratory implementation requires nowadays communication systems, hosts, some virtualization or cloud services, particularly for remote learning, but even for improving the traditional computer classrooms.**

***Index Terms*— distributed architecture, GBL, virtualization, cybersecurity, critical infrastructures.**

I. Introduction

Games as educational resources have been studied in the academic sphere. The trend continues to rise, but even more strongly in the area Government and industry. Even IEEE has estimated that games will be integrated by more than 85% of daily tasks in 2020 [1]. Companies and college will have to find game elements in order to implement a number of training activities. Moreover, there is a general interest of cyber security in various scientific disciplines and the different professional profiles. That makes serious games and game oriented learning can provide relevant resources.

The architectural model for this lab is supported by an analysis from the scientific and educational level. Gagne's event model and Keller's ARCS motivational scheme were considered to assess characteristics and abilities for the learning process. Furthermore, we understand that games should be incorporated into training, providing teaching values. Not enough to be illustrative, entertaining or enjoy themselves to students. They must have some pedagogical value and should be clarified from what educational role performs.

Concern about cyber security training has also been examined. The common body of cybersecurity and critical infrastructures protection includes basic disciplines such as engineering and computer science, law, ethics and psychology, business management and educational, sociological and criminological aspects [2]. As a result, a multidisciplinary approach is set by analyzing cybersecurity globally. As may be seen in Figure 1, we highlight the law, medical-psychological aspects, and business, sociological, educational, economic and ethical as a daisy with multiple petals.

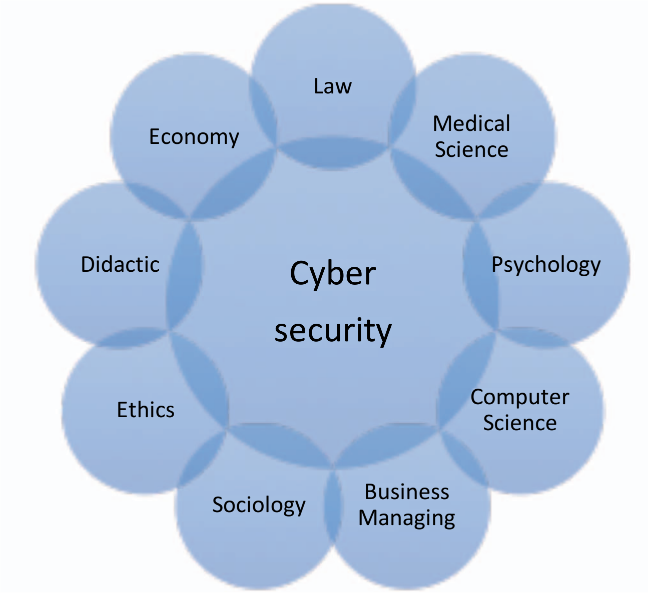

Figure 1. Multidisciplinary view as a multi-petaled daisy.

Thus, the interaction between engineers and non-technical professionals is at a turning point in education today on this this matter [3]. Some authors claim that education in secure software should apply to both programmers and non-programmers [4]. In any case, it seems widely believed that for everyone, particularly in college, it is necessary to upgrade and use the experience and knowledge of private sector and Government institutions [5] [6]. Engineering professional associations working in this direction have ever provided a reference curriculum about information security for the curriculum in computer science [7].

Our research presents the analysis and design of a cybersecurity lab for hands-on learning following the teaching introduced in [8]. In this sense, the literature has been working to explorer how to learn cybersecurity matters in diverse scenarios.

In the following sections, we are including the laboratory resources from which are designed the GBL architecture presented (Section I). Then Section II shows some details about development, like the piece concept for a instructional application to introduce games, laboratory spaces, network concerts and a inventory for taking over this architecture.

II. Games as Laboratory Resources

The first decision to make is what games to incorporate in our laboratory. A first alternative approach is to use a known product [9] in order to try a comfortable context for introducing a game unit oriented to simulate systems and networks. But we also need to explore the state of research [10] which authors worked some applications for online labs.

We certainly understand that the attitude of teachers to incorporate the game should be active and not passive. As a result, we must build the course using games like puzzle pieces that fit together to achieve the desired objectives. Also, a single game can take the teaching staff to adopt a passive attitude so that the game does not determine the course and the course determined by the game. Therefore, we understand that games should play the same role as the well-known learning objects in the eLearning environment.

Moreover, software reuse practice are now a rule in the field of computer science for instance code reuse, programming libraries, open source release, etc. And again this concept has been widely accepted and used in many different ways between users via Internet.

Therefore, we understand the fact of interest to build games based reusable learning course. We understand that the characteristics of the resource-games should be simple enough, flexible, modular and reusable to act as puzzle pieces in the design of a laboratory as well.

TABLE 1. Designing features

#	Elementos de diseño			
	Instructional*	Motivational*	Plataform	Tecno
1	Gaining attention	Attention		Client
2	Informing objetives		Standalone	
3	Stimulating recall	Relevance		Virtualisa tion
4	Presenting content		Online	
5	Providing guidances	Confidence		Internet Intranet
6	Eliciting practice		Multi-user	
7	Providing feedback	Satisfaction		Cloud
8	Assessing		Ubiquitous	
9	Enhancing retention			

* Based on the Gagné and Keller models

In addition, it is important to have multiple source and find the resources available in the network that are available to the general public. First, the resources should be trusted sites. Many institutions, universities, government agencies and reputable companies have incorporated a number of resources on their websites that can be very useful in this context.

Thus, using these resources, students actively understand where can and should find reliable information which will be particularly useful for training along the life. Furthermore, this method has the advantage that teachers have to search, analyze and decide whether a resource (piece) is the right but not only in content. Consequently, they will focus on whether it is appropriate for the particular profile of its students and those motivations of them.

With all this, the work is based on building a laboratory-based course where there is a set of reusable games that service both the educational needs and the real concerns of students in their daily life.

III. Development of the Lab Architecture

A. *Instructional and technological design of a piece*

A piece of our laboratory consists of a combination of a game and instructional supplements. Initially, we proceed to make an exploration of possible games based on the content on cybersecurity. For the design of the piece, we have to consider the own characteristics of the technology with which the game has been implemented from an architectural perspective.

As has been observed, engineering of games have taken advantage of information and communication architectures as well [11]. This is why, to mount a game-based laboratory, we need to analyze the technological requirements of each game.

We can think of a number of different games that can be useful to get a first idea. Although not limited, we can mention some are: platforms player, multiplayer, web games, online, multiplayer online (MMO, short for Massively Multiplayer Online game), role playing (MMORPG, which is the acronym for Massively Multiplayer Online Role-Playing Game), mobile platforms or social networks, among others.

This means that we have to implement different architectural solutions for our laboratory. One approach is based on starting the lab is in local communications network. While standalone games need to be accommodated in each work of the laboratory, it is optimal that the game were virtualized on a machine to be re-used in the network.

Obviously, it is important to know the technical requirements of each game. Games with client-server protocol has a network deployment and another point to consider is that it can be supported on a cloud server or be provided with a service about it. On the cloud, a web-based site can enable links to centralize the game locations and keep track of students' experiences.

Secondly every game is evaluated based on instructional events that may complete. For this learning model is used Gagne [12] about nine events for effective learning.

Third, it is evaluated in terms of motivational aspects under ARCS Keller's model [13]. The design process is iterative. Table 1 depicts events, motivations, platforms and network technologies that outline the laboratory design.

B. *Laboratory spaces*

The laboratory is physically in an area with a number of workstations. A couple of students sit at each position. In a central area is the main machines, servers and virtual machines. Logically, this virtualization can be located internally or through cloud services.

Figure 2 shows the design in an enclosure. Despite the fact that it can be adapted to other sizes, this arrangement can be set on an 8-by-7-meter place.

Definitively, the laboratory can be seen as a collection of pieces based on games. Each piece follows the scheme presented in the previous section, with instructional and technological aspects.

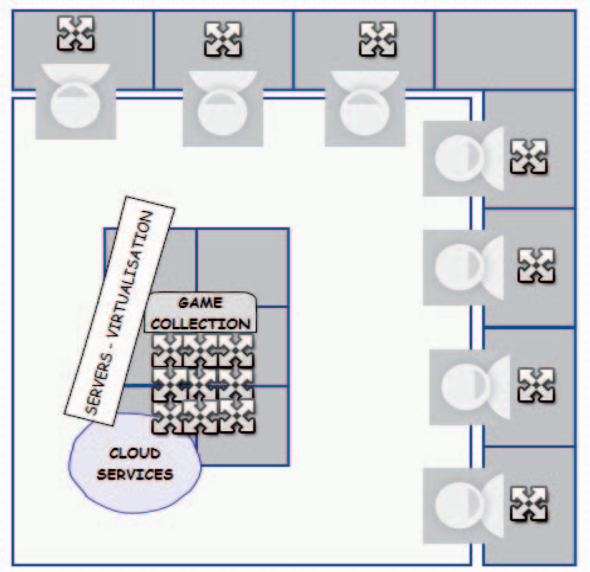

Figure 2. Implementing the lab spaces.

C. The lab as a network

The laboratory is essentially a LAN with certain security considerations. It should take a gateway to the Internet, but it be able to get the access in order to enable the network to be isolated.

In addition, it extends the cybersecurity laboratory for other possible applications in the field of education, not necessarily based on games.

D. Inventory

For the implementation of the cybersecurity lab in our educational context, according to Figure 2, it is stated:

- Seven personal computers, which are mainly for working students.
- Two servers with multiple disks in RAID (Redundant Array) and enough RAM to define virtualised environments.
- Two USB hard for every workstation in the laboratory records. Fourteen in all.
- A workstation for cloning hard drives by hardware device. Also the possibility of cloning by software on each student workstation.
- Additional Software
  - Forensic Tools
  - Vulnerability Analysis
  - Audit and penetration testing
  - Intrusion Detection
- Network and communications devices
- Gateway to access the Internet
- Subscription to a cloud provider

Furthermore, the provision of computer equipment can take advantage of existing IT resources. It requires a preliminary feasibility analysis to enable its implementation and installation.

With regard to human resources, it suggests a lab-oriented preparation of support activities and configuration of computing environments and communications.

IV. Conclusion

A laboratory which has been introduced must be well justified by a strong didactic. It's not just a question of games. But a technological, educational and motivational question.

Using games can enable technical and non-technical students to learn cybersecurity and mechanisms for critical infrastructure protection. As a result, we can overcome the barriers of a more formalized training. That is a spontaneous and undirected approach to learn information security into a lab.

Acknowledgment

Grateful to the Faculty of Law of USP CEU (Madrid) and the Higher Institute of Professional Studies (ISEP) to facilitate this lab.

References

[1] IEEE News, "Everyone's a Gamer - IEEE Experts Predict Gaming Will Be Integrated Into More than 85 Percent of Daily Tasks by 2020," New York, 2014.

[2] M. Theoharidou and D. Gritzalis, "Common Body of Knowledge for Information Security," *Security & Privacy, IEEE,* vol. vol.5, no. no.2, pp. pp.64-67, 2007.

[3] A. McGettrick, L. Cassel, M. Dark, E. Hawthorne and J. Impagliazzo, " Toward curricular guidelines for cybersecurity," in *Proceedings of the 45th ACM technical symposium on Computer science education (SIGCSE '14)*, New York, 2014.

[4] D. Burley and M. Bishop, "Summit on Education in Secure Software Final Report," 2011.

[5] F. B. Schneider, "Cybersecurity Education in Universities," *Security & Privacy, IEEE,* pp. Volume: 11,Issue: 4. Page(s): 3-4, 2013.

[6] C. J. Atman, R. S. Adams, M. E. Cardella, J. Turns, S. Mosborg and J. J. Saleem, "Engineering Design Processes: A Comparison of Students and Expert Practitioners," *Journal of Engineering Education,* pp. 96(4), 359-379, 2007.

[7] A. CS, " The Joint Task Force on Computing Curricula, Computer Science Curricula, Ironman Draft (version 1.0)," 2013.

[8] J. Cano, R. Hernández and S. Ros, "Bringing an engineering lab into social sciences: didactic approach and an experiential evaluation," *Communications Magazine, IEEE,* vol. 52, no. 12, pp. 101-107, 2014.

[9] C. Irvine, M. Thompson and K. Allen, "CyberCIEGE: gaming for information assurance," *Security & Privacy, IEEE,* vol. Volume: 3, no. Issue: 3, pp. 61 - 64, 2005.

[10] K. Henke, S. Ostendorff, H. Wuttke and S. Simon, "Fields of applications for hybrid online labs," in *Remote Engineering and Virtual Instrumentation (REV), 2013 10th International Conference on*, 2013.

[11] S. Cass, "Mind games - computer game AI," *Spectrum, IEEE,* vol. vol.39, no. no.12, pp. pp.40-44, 2002.

[12] R. M. Gagné, W. W. Wager, K. C. Golas, J. M. Keller and J. D. Russell, Principles of instructional design (5th ed.), Belmont, CA: Wadsworth, 2005.

[13] J. M. Keller, Motivational design for learning and performance: The ARCS model approach, New York: Springer, 2010.