Enhancing Cybersecurity Learning through an Augmented Reality-based Serious Game

Teaching & Learning Experiences in Engineering Education

Mikel Salazar, José Gaviria, Carlos Laorden, Pablo G. Bringas
S^{3}lab, DeustoTech Computing
University of Deusto
Bilbao, Spain
Email:{mikel.salazar, jgaviria, claorden, pablo.garcia.bringas} @deusto.es

Abstract— **As social networks and always-connected mobile devices grow in popularity, the control over personal information weakens. This is especially true for teenagers between 15 and 18 years old, one of the population groups that shares more information online, but also the most unaware of the risks associated with this activity. For this reason, many institutions have developed programs to educate the students in the correct use of the new communication mediums. However, the concepts about information security require a lot of expert knowledge and are very difficult to explain appropriately.**

In this paper, we present a serious game designed to enhance an information security presentation aimed at high school students. This is achieved through the use of augmented reality to give shape and form to the intangible cybersecurity concepts and allow the students to interact with them using the same rule set that was explained during the presentation.

Keywords- information security; serious game; augmented reality, experimental gaming model; game-based learning

I. INTRODUCTION

In recent years, the massive popularization of mobile devices connected to the Internet at all times, in conjunction with the advent of social networks for each and every aspect of our lives, has changed our relationship with technology. In this new reality, where the inability to manage and protect our personal information is a growing concern, the only solution is, paradoxically, to acquire more information about how to make it more secure. However, this is not an easy task.

Cybersecurity (the application of Information Security principles to large computer networks such as the Internet) does not only require a deep understanding of the underlying hardware and software systems over whose the data transference takes place, but also a profound and up-to-date knowledge about how that information can be used for harmful purposes. Consequently, this field of computer science has become extremely difficult to learn –and teach about– due to its inherent complexity and the secrecy in which many institutions (from IT companies to armies) shrouds the issue.

Nevertheless, cybersecurity does no longer affect only computer scientists and telecommunication engineers; in their advancement towards a complete Information Society, many countries are facing new security problems associated with the massive usage of online services: credit card fraud, industrial espionage and, even, attacks to critical infrastructures [1].

Due to the social scale of the problem, the only way to address it is through the education of the entire population in the risks that new technologies pose and reinforce the idea that Information Security is a shared responsibility. However, the complex and abstract engineering concepts in which those technologies are based make teaching (and learning) cybersecurity an arduous and time-consuming endeavour [2].

Against this background, we designed a presentation model aimed to teach cybersecurity measures to teenagers between 15 and 18 years old, since this population group is not only one of the most vulnerable to cyberattacks [3] but also because, in this way, we are able to provide the students a better understanding of technologies that will have a great impact in their futures (whether they pursue a career in engineering or not).

In this presentation, we focus on the main cybersecurity threats that high-school students face in social networks and other online services. This context allows us to provide a direct connection between the cybersecurity measures explained during the presentation and a known environment for the students. However, in order to make a lasting impression, we developed a serious game that employs, with great effect, augmented reality to provide an environment where the "ethereal" concepts explained during the presentation take shape. Since the virtual objects interact with each other following the same rule set, we also make sure that the concepts are correctly understood and will be remembered when the necessity arises.

The remainder of this paper is divided into the following sections: Section two explains why cybersecurity matters for high school students (and educators) and enumerates the different threats and countermeasures. Later, in section three, we detail how the augmented reality-based serious game enhances the presentation. Section four is dedicated to present and analyse the obtained results, with a. Finally, section five presents the conclusions and future work.

978-1-4673-6110-1/13/$31.00 ©2013 IEEE Technische Universität Berlin, Berlin, Germany, March 13-15, 2013
2013 IEEE Global Engineering Education Conference (EDUCON)

II. CIBERSECURITY FOR HIGH SCHOOL STUDENTS

Since schools are enclosed environments where teenagers spend a large portion of their time, they develop all kinds of relationships with their peers. Unfortunately, those also include abusive and derogatory behaviours that, left unchecked, may led to extreme cases of bullying.

Aware of this situation, over the years many educational institutions have created programs to address this issue and implicate all the actors into its resolution. However, these programs have, for the most part, become obsolete by the technological evolution and the new ways of communication that mobile phones offer.

In this new environment, the students take advantage of the technological gap between generations (associated with the effect known as digital divide [4]) to create conversation spaces free from parental and teacher supervision, but not from risks.

The anonymity and age-masking provides a powerful tool for those who want to abuse their victims without being identified, while the ubiquity of the services allows the humiliation to persist outside the school grounds [5] (where the educators have little to no power).

This issue has become even worse since the introduction of smartphones. With more ways to share information (including image and video files), the number and damage of potential attacks grow exponentially. For example, there have been numerous cases of cyber-bullying in whose the aggression is recorded on video and shared with the classmates of the victim to further humiliate him/her [6].

Nevertheless, physical attacks are not the most common tactic for cyber-bullies. Instead, they obtain sensitive information (usually, by extortion or deception) and use it to blackmail the victim or, directly, share it indiscriminately. Since the entire process does not involve actions in the "real" world and their identity is hidden beneath a complex software system, they think themselves away from prosecution. However, this is not only not true (because the communication services available for students usually keep a record of the conversations and the parts involved in them), but it also leads to the commission of very serious criminal offenses such as the distribution of child pornography [7] or suicide induction [8].

Against this background, there are two main options: either to provide tutors with tools to motorize the conversations in the new communication mediums (and, thus, entering a never-ending technological race against the students) or to educate the students in the correct use of those services (and the consequences of their misuse). In our research work, we have chosen the latter approach since we consider that making the students aware of the dangers they are exposed to not only makes them less inclined to take part in any cyber-bullying incident, but it also prepares them better for the highly technological world they will have to face later in their lives.

In order to achieve this goal, we created a presentation aimed for high school students in which we explain the main threats to their virtual existences and the security measures they can take advantage of to defend themselves.

A. *Main Threats*

There are three main ways in which high school students can have their information security compromised:

- Identity Theft: With the personal information shared between several web services and social networks, it is increasingly difficult to maintain an appropriate control over all of it. A situation that can be easily exploited by potential attackers, and that could result in cyber-bullying or blackmailing [9].
- Over-sharing: As more students register into social networks, the possibility that they may inadvertently leak critical information increases. As in the previous case, this information could be used for nefarious purposes, but, this time, it may be much more difficult to identify the culprit.
- Malware: Malicious software has come in many different shapes and sizes over the years. Nowadays, however, malware creators don't go after fame, but after fortune [10]. The main threat are not destructive viruses, but sophisticated *trojan horses* that install themselves into the system —including mobile devices— and relay every bit of personal information they can get, while simultaneously making the computer part of a botnet at the service of the attacker.

B. *Countermeasures*

For each of the aforementioned threats there are several countermeasures that do not even require the installation of any kind of security software (partly because such software is not yet available for mobile platforms):

- Robust Passwords: Although new and more secure authentication mechanisms are implemented every day, password-based systems are still the preferred way to identify users (specially, in online services). That's why storing them in a secure place is not enough. We recommend that they have a reasonable length (at the moment of writing this document, at least twelve characters), to include all sorts of special characters, to be unique for every web site or application and, most important of all, to not be easily deducible from public personal information (which also applies to any "*security question*" mechanism).
- Multilevel Security: Almost all operating systems and social networks offer the option to create multiple layers of protection for the sensitive information. Using them wisely is the key to avoid any kind of data leak. After all, the most secure information is the one that is not shared.
- Healthy Scepticism: The main tool against almost all "social engineering" techniques is a healthy dose of suspicion. Being able to discern between a SPAM message and a legitimate one, or whether a download executable is safe or not is not a competence that should be delegated exclusively on security software (no matter how well designed it may be).

III. ENHANCING THE CIBERSECURITY PRESENTATION

During the creation of the presentation about cybersecurity, we realized that many of the aforementioned concepts were hard for the speaker to adequately explain and even more difficult for the high school students to understand and assimilate. For this reason, we decided to create a complimentary activity to enhance the learning experience by developing an augmented reality-based serious game.

A. Serious Games for Education

In recent years, the development of games for educational purposes has become an important field of research, due to the good reception of students [11] and the popularization of the tools required to obtain satisfactory results without the need of a specialised team.

In this kind of games, the primary objective is not the creation of a fun experience for the players, but to allow the students to intuitively experiment with complex concepts and the relationships between them [12]. A learning process that enables the students to acquire the necessary competences by requiring a constant interaction with the environment (in which the users dynamically discover the elements that can be interacted with, the rules that govern them and the goals they have to achieve) [13]. An environment that promotes the use of the scientific method, by encouraging the students to acquire knowledge for different sources (including their classmates), formulate their own hypotheses and test them without fear of failing.

There are three main learning models associated with the serious games for education depending on when the actual learning process takes place:

- Review: In this model, the game developers do not introduce new concepts, but, instead, present the players with a problem that requires their adequate understanding in order to "win" the game.
- Experimentation: This model presents the concepts and requires the players to use the knowledge to solve increasingly difficult problems with it. In this way, it is possible to adapt the learning process to each individual.
- Reflection: In this last model, created by Garris et Al. [14], the learning is achieved outside the game environment. After the game ends, the players are asked to reflect upon the experience and extract the lessons they have learned from it.

B. Augmented Reality

One of the biggest problems that educational games face is the lack of player immersion [15]. Even if the experience is particularly compelling, the fact that the learning process takes place in the other size of the screen significantly decreases the involvement of the user. Thankfully, Augmented Reality provides a –relatively– easy solution to this issue.

The term Augmented Reality encompasses a wide spectrum of technologies that aim to integrate virtual objects seamlessly into the real world (or, at least, to alter the user's perception to achieve a similar result [16]). These technologies have been applied in many commercial products, greatly enhancing the user experience and providing new ways to interact with the virtual environments [17].

Since the creation of the illusion requires the camera(s) and graphic display(s) to be placed between the real environment and the user, there are basically two different approaches:

- AR lenses: In this interaction model, the user sees an augmented version of the real environment through a mobile platform (usually, a smartphone or a tablet). This allows the free exploration of the environment but the results are limited by the capabilities of the device and the constant change of position requires complex software systems to deal with the occlusion of objects, the changing lighting conditions, physical collisions between users, etc.
- AR mirror: In this paradigm, both the camera and the display are fixed in place and connected to a computer (with higher graphical capabilities than most mobile platforms). The users perceive the augmented reality effect through a display which acts as a mirror surface, but, at the same time, it also integrates the virtual objects in the "reflected" image. This model limits the interaction space but greatly simplifies the complexity of the system while allowing multiple users at any giving time.

Whichever the approach selected, for the virtual objects to be seamlessly integrated in the real environment, additional image analysis techniques are required [18]. For fixed –relative to the camera– objects, background removal algorithms are usually enough to achieve this effect without breaking the immersion (e.g., allowing the users to occlude the virtual objects with their bodies), but the objects that the user can interact with require advanced pattern recognition algorithms that track specific features (from simple shapes to human face characteristics) in a frame-by frame basis.

In a previous work, we have successfully applied the AR mirror paradigm to art exhibitions and three-dimensional data visualization applications by employing custom marker recognition algorithms [19]. As can be appreciated in the figure bellow, this enabled the users to intuitively interact with the virtual objects and explore the entire structure by simply rotating the marker with their hands.

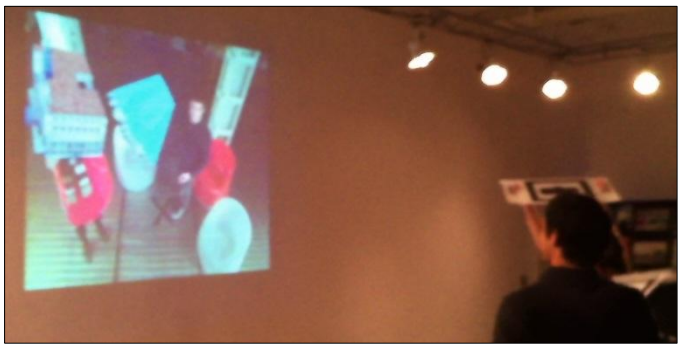

Figure 1. Example of the application of the magic AR mirror paradigm using custommarkers to enhance the user experience.

C. Concept Visualization and Game Mechanics

Since the main objective of the serious game is to help the students to visualize and assimilate the cybersecurity concepts explained during the presentation, we designed several visual representations for the aforementioned security threats and countermeasures. As Figure 4. shows, the security threats are represented as cartoonish three-dimensional models while the countermeasures are drawn as shields (each one with a different icon and colour for easy recognition).

The goal of the game is to defend the victims (classmates) of the security threats that "rain upon" them by using the shields representing the countermeasures to block them. However, there is no shield that can block all threats, so the players are forced to use the knowledge they obtain during the presentation to identify each threat and collaborate to block it with the right shield.

For the game mechanics, the serious game takes inspiration from the classic arcade game Missile Command. Not only the prototypical mechanic of "stopping threats falling from above" fits perfectly with the thematic, but the underlying pessimistic vision contained in it (a result of the fears of the Cold War) also reinforces the message present in the presentation about how there is no such thing as a "happy ending" in cybersecurity, just another, harder "level" every day.

D. Interaction Model

In this experience the users interact with the virtual objects using real wooden shields (one for each of the aforementioned countermeasures). As can be seen in Figure 2, these shields have a custom AR marker in the centre that allows the game engine to track their exact location in the three-dimensional space so it can superimpose an enhanced version of them on screen and identify when the they collide with the three dimensional models of the threats (and, in that case, analyses whether the threat should be destroyed or not, depending on the countermeasure).

Figure 2. The wooden shields used during the experiments.

The main reason behind using shields as the main interaction mechanism –apart from being thematically appropriate– is because the users can hold them using a handle in the back, which allows higher degrees of freedom without the user occluding the marker in the process.

E. Interaction Space

The game we present in this paper has been designed as a multiplayer experience that takes place in the same physical space as the cybersecurity presentation (a normal classroom or a small conference room with an audience of no more than fifty students). As Figure 3 shows, both the presentation and the serious game are displayed on a vertical surface using a common projector. If necessary, the speaker asks the students to sit in front of the projected image (between two to four meters away) in order for the small camera situated below it to take a clear video feed from them.

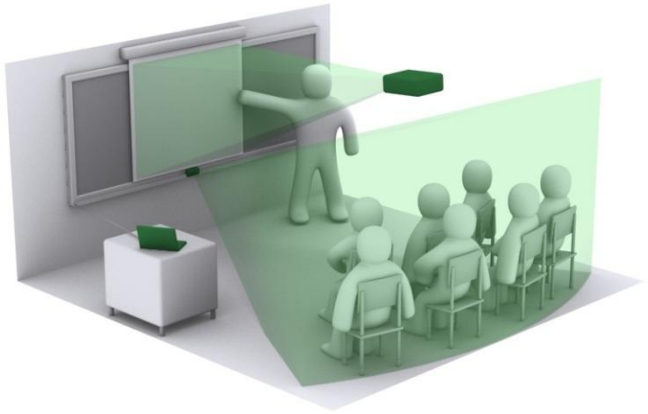

Figure 3. The scenario for the augmented reality-based serious game.

In order to clearly track the shields, during the execution of the serious game, the players are asked to stand in front of their classmates. If the players are too close to the camera, however, the representation of their shield on screen changes colour and becomes inactive. This measure is necessary to avoid accidents due to physical collisions between the shields and/or the players' bodies.

F. Integration within the presentation

The serious game is executed two times during the presentation, intending to serve both as a stunning introduction and as an inspiring ending for the entire presentation in which it takes place:

1) Stunning Introduction

Just after the speaker has presented himself, he asks the students in front of him what they think "security" means and what they consider an "insecure place" to be. After allowing some short answers (that are not meant to be corrected yet in any case), the speaker launches the application for the first time, showing the video image captured by the aforementioned camera, without any augmentation.

After the initial surprise, the speaker tells the students that they are, in fact, in a dangerous situation, but that they cannot perceive it, that they have to "enter the virtual world" in order to see what it is really happening at that moment. Then, the image on screen acquires a greenish tint (a recurring visual technique applied to represent any computer-generated world) while several virtual objects representing different kinds of malware fall slowly over the –reflected– heads of the students.

As the malware reaches the students, the number of "lives" of the students (represented as hearts at the top of the screen) rapidly decreases, and when all of them disappear (in less than twenty seconds, to avoid diminishing the effect), a big "Game Over" message is imprinted on screen. Then, the speaker explains the audience that the previous situation is an exaggerated simulation (although the risks are not less real) and continues with the rest of the presentation.

2) Inspiring Ending

During the presentation, the speaker exposes the cyber-security threats and introduces the countermeasures previously mentioned in the second section of this document. At the end, in order to make sure that the students really understand those concepts and that they will keep them in mind for a long time, he repeats their main characteristics and asks the audience which security measure is being described. For each valid answer, the speaker gives the student a toy shield that represents that measure.

Once the three aforementioned security measures have been named, the speaker asks the students that received the shields to –proudly– stand up and come in front of the class. Then, the speaker reveals the true purpose of the shields ("to defend their classmates against the incoming threats") and starts the game for a second time.

The three students then become the main players of the game and intuitively discover that their shields project a three-dimensional object into the virtual world and that each one is capable of deflecting the types of threats associated with the security measure explained before. Figure 4 shows a recreation of the game in action.

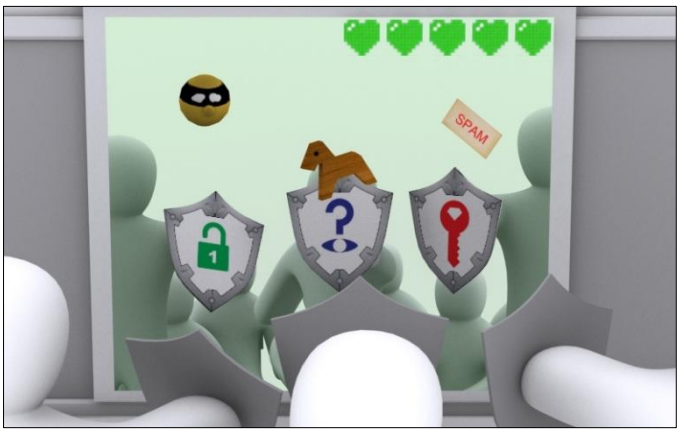

Figure 4. Recreation of the serious game during play.

After a minute of increasingly difficult waves of attacks, the game finishes as a "You Win" message fills the screen. Nevertheless, after the speaker congratulates the three players and asks for a round of applause for the "heroes"', the message on screen automatically changes to a cryptic "Continue?". A cue for the students to realise that the knowledge they acquired in the presentation can –and must– be applied in their daily lives.

IV. Results and Discussion

To adequately evaluate the effect of the augmented reality-based serious game proposed in this paper, we requested the students to complete a simple survey after the presentation. In it, apart from basic anonymous data (gender, age and computer experience), we ask them four questions (which they were required to answer using a 1-5 scale): the knowledge they gained during the presentation, how vulnerable they are to the threats explained, how capable they are to defend themselves and their general confidence in technology.

This survey was answered by a total of 208 (ages between 14 and 19) in three different schools during the first half of 2012. 128 of those students attended the normal presentation (without the serious game) and 79 attended the enhanced version (with the serious game). Figure 5 shows the results for both cases:

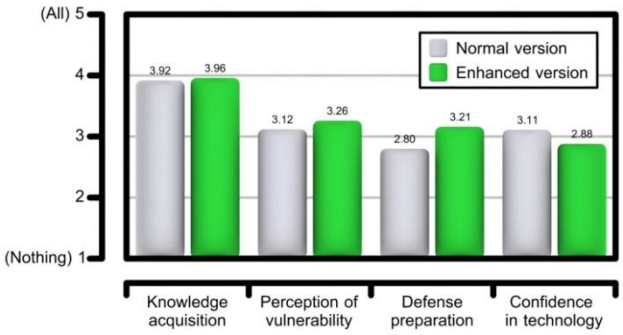

Figure 5. Results of the surveys.

As the graphic suggests, the use of the serious game does not have a significant impact on the knowledge acquisition (since it does not introduce any new concepts), but it greatly affects the students' self-awareness in cyber-security while significantly decreasing their confidence in technology, which is an intended effect.

Additionally, we studied whether the experience suffers from one of the biggest problems associated with multimedia learning materials: the overload of the working memory capacity of the students [20].

In our first tests, the three dimensional icons associated to the security threats were more varied and detailed. However, this made the recognition of the elements too hard for first time users and, when the icons started to accumulate on screen at the end of the experience, the cognitive load sometimes exceeded the capabilities of the users [21] [22].

We solved this issue by simplifying the shape and colour of the icons (which greatly reduced the time required for the correct identification) and by giving the images from the real world the aforementioned green tint. In this way, when the users reach the point when there are more than ten icons on screen, they are already focused just on recognizing the shapes and colours associated with the countermeasure the shield they carry at the time.

V. Conclusions and Future Work

In this paper, we have introduced a serious game that enhances the presentation about information security which bookends. Through a wise use of the magic mirror paradigm and custom marker recognition, we have created an augmented reality experience in which the users feel immersed and where the rules about cybersecurity explained during the presentation are put into practice.

As the results show, the serious game is a valid learning tool that helps to consolidate the concepts about information security by making them "tangible" to the users and by giving them an interactive context for experimentation.

As a next step, we would like to improve our AR engine by developing a more robust tracking system that can deal with the difficult lighting conditions of many classrooms (especially, those with flickering fluorescent lights), partial occlusions and really fast movements.

Additionally, we are exploring up the possibility of introducing an invincible character ("The Hacker") at the end of the game to reinforce the message that there is no such thing as "completely secure system".

Finally, we are researching for new ways to integrate the learning process inside the serious game, incorporating new ways of discover concepts, rules and goals in a more personal, exploratory manner.

References

[1] Grow, Brian, Keith Epstein, and Chi-Chu Tschang. "The new e-spionage threat." *Business Week* 10 (2008).

[2] Pastor, Vicente, Gabriel Díaz, and Manuel Castro. "State-of-the-art simulation systems for information security education, training and awareness." *Education Engineering (EDUCON), 2010 IEEE*. IEEE, 2010.

[3] "Social networking, age and privacy". LSE Research Online. http://eprints.lse.ac.uk/35849

[4] Loges, William E., and Joo-Young Jung. "Exploring the digital divide internet connectedness and age." Communication Research 28.4 (2001): 536-562.

[5] Agatston, Patricia W., Robin Kowalski, and Susan Limber. "Students' perspectives on cyber bullying." Journal of Adolescent Health 41.6 (2007): S59-S60.

[6] Smith, Peter K., et al. "Cyberbullying: Its nature and impact in secondary school pupils." Journal of Child Psychology and Psychiatry 49.4 (2008): 376-385.

[7] Siegle, Del. "Cyberbullying and Sexting: Technology Abuses of the 21st Century." Gifted Child Today 33.2 (2010): 14-16.

[8] Hinduja, Sameer, and Justin W. Patchin. "Bullying, cyberbullying, and suicide." Archives of Suicide Research 14.3 (2010): 206-221.

[9] A. Sengupta and A. Chaudhuri. "Are social networking sites a source of online harassment for teens? evidence from survey data". Children and Youth Services Review, 33(2):284–290, Feb. 2011.

[10] Igor Santos. "Nuevo enfoque para la detección de malware basado en métodos de recuperación de información". PhD thesis, University of Deusto, 2011.

[11] Lee, K. M., Jeong, E. J., Park, N., & Ryu, S. "Effects of interactivity in educational games: A mediating role of social presence on learning outcomes". Intl. Journal of Human–Computer Interaction, 27(7), 620-633. 2011

[12] G.C. Thornton and J.N. Cleveland, Developing managerial talent through simulation, American Psychologist, vol.45, pp.190-199, 1990.

[13] R.T. Johnston and W.de Felix," Learning from video games," Computer in the Schools, vol.9, pp. 199-233, 1993.

[14] R.Garris, R.Ahlers. and J.E.Driskell, "Games, motivation and learning," Simulation & gaming; An Interdisciplinary Journal of Theory, Practice and Research, vol.33, No.4, 2002.

[15] Kritzenberger, Huberta. "Understanding Player Experience in Educational Games." In World Conference on Educational Multimedia, Hypermedia and Telecommunications, vol. 2012, no. 1, pp. 1329-1335. 2012.

[16] Azuma, Ronald T. "A survey of augmented reality." Presence-Teleoperators and Virtual Environments 6.4 (1997): 355-385.

[17] Kang, Changgu, and Woontack Woo. "ARMate: an interactive AR character responding to real objects." Edutainment Technologies. Educational Games and Virtual Reality/Augmented Reality Applications (2011): 12-19

[18] Azuma, Ronald. "Tracking requirements for augmented reality." Communications of the ACM 36.7 (1993): 50-51.

[19] [Reference ommited to comply with the double-blind review guidelines]

[20] K. Kiili, "Learning with technology: cognitive tools in multimedia learning materials," Proceedings of ED-MEDIA 2004,world conference on educational multimedia, hypermedia & telecommunications, Switzerland, 2004.

[21] J. Sweller, J. J. G. van Merrienboer and F.G.W.C. Paas, " Cognitive architecture and instructional design," Educational Psychology Review, vol.10, pp.251–296, 1998.

[22] P.A. Kirschner, " Cognitive load theory: implications of cognitive load theory on the design of learning," Learning and Instruction, vol.12, pp.1–10, 2002.