CyberAware: A Mobile Game-based app for Cybersecurity Education and Awareness

Filippos Giannakas
Department of Information and Communication Systems Engineering
University of the Aegean
Samos, Greece
Email: fgiannakas@aegean.gr

Georgios Kambourakis
Department of Information and Communication Systems Engineering
University of the Aegean
Samos, Greece
Email: gkamb@aegean.gr

Stefanos Gritzalis
Department of Information and Communication Systems Engineering
University of the Aegean
Samos, Greece
Email: sgritz@aegean.gr

***Abstract*—Nowadays, basic cybersecurity education and awareness is deemed necessary, even for children as young as elementary school-aged. If knowledge on this topic is delivered in the form of a digital game-based activity, then it has greater chances of being more joyful and efficient. The paper at hand discusses the development of a novel mobile app called CyberAware, destined to cybersecurity education and awareness. At present, the game is designed for K-6 aged children and can be used to support either or both formal or informal learning. Also, due to its mobile nature, it can be experienced as an outdoor or classroom activity. Opposite to similar studies found in the literature so far, our attention is not solely drawn to game's technological aspects but equally to the educational factor.**

***Keywords*—Security education and awareness; m-Learning; mDGBL; motivation; ARCS.**

I. Introduction

Digital Game Based Learning (DGBL) is known to make learning more attractive, motivating and personalized from the learner's viewpoint. Due to its undisputed advantage this learning approach has been applied to numerous science education fields and curricula, more lately to cybersecurity education and awareness, which is the topic of this paper. Lately, with the advances in mobile computing, the positive outcomes of DGBL become even more reachable in the form of mobile DGBL (mDGBL).

Being a multidisciplinary challenge, the creation of a truly effective mDGBL platform or app for science education is far from being trivial; technological advances and facilities should be seen and faced in conjunction with the human player in order to maximize their payoffs. Moreover, the right blending of learning theories in a (serious) game's storyline is decisive yet often neglected by designers. In some cases, this overlook may be due to the undisputed difficulties designers face in applying the discrete stages of the learning theory directly to the app in a way it fulfills specific learning outcomes. Last but not least, seeing this issue from a Bring Your Own Device (BYOD) point of view, there is a need for such apps to work on arbitrary mobile devices and platforms. This is certain to not only overcome several mobile platform peculiarities, but to also increase learning independency and augment the anywhere, anytime learning experience.

Our contribution: Motivated by the aforementioned issues, the paper at hand discusses the development of a novel mDGBL app called CyberAware destined to cybersecurity education and awareness. Among others, the topics considered by CyberAware include: firewall technologies, antivirus software, security patches and updates, and email spam filters. Contrary to other works in the literature, our contribution is not solely focused on technical aspects but to the pedagogical factor as well. Thus, the design of the game is based on the Attention, Relevance, Confidence, and Satisfaction (ARCS) motivational model [1]. At present, CyberAware is designed for K-6 educators and can be used to support either or both formal or informal learning exercised as an outdoor or indoor activity. The game prototype is developed using standard software tools, including Android Development Kit (ADK) and the open-source libGDX game engine [2]. A preliminary evaluation of the game app is also performed using both pre and post-questionnaires.

The rest of the paper is structured as follows. The next section briefly addresses related work on the topic. Section III details on CyberWare app. The conceptual framework and the ARCS motivational model are discussed in section IV. The evaluation results are presented in Section V. The last section concludes and gives pointers to future work.

II. Related Work

Nowadays, due to the Internet penetration and the popularity of social networking sites among adolescents, basic cybersecurity education and awareness is deemed necessary. In this context, digital serious games may be proved valuable for teaching security issues to this audience more effectively [3] and in a more personalised way towards cultivating security culture. Thus far, only a handful of works in the literature combine cybersecurity training and awareness with DGBL, and more scarcely with mDGBL. However, as explained further down, none of them is specially designed for K-6 or K-12 students. Also, the overwhelming majority of these works mostly neglect the educational factor and concentrate solely on the technological one, i.e., the implementation of the game.

The authors in [3] developed "PhishGuru" a personalized story-based anti-Phishing educational software aiming to alarm people about phishing attacks pertaining to email use. A similar work, namely "Anti-Phishing Phil" [4] is an online game that teaches end-users how to use cues in URLs to avoid becoming victims of "Phishing" attacks. "CyberProtect" [5]

978-1-4673-8243-4/15/$31.00 ©2015 IEEE
19-20 November 2015, Thessaloniki, Greece
2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL)

and "SecurityCartoons" [6] are both interactive online web-based games dedicated to information security assurance. Note, all the above mentioned works have been implemented for desktop computing platforms. In the context of mDGBL the only work dedicated to cybersecurity is the one given in [7]. Specifically, the authors presented an educational mobile app designed to alert home computer users against "Phishing" attacks.

III. CYBERAWARE

As already pointed out, today, Internet penetration is more evident to young people, mostly due to the popularity of social networking sites and the multiplayer online games among others. This situation makes cybersecurity education for adolescents an important and urgent issue. In this context, CyberAware is destined to support learners with an alternative, joyful and more efficient way for learning data security issues and raising security awareness. At a nutshell, the aim of the game is to familiarize students with fundamental cybersecurity technologies that are required to keep their Internet-connected devices protected against malware, cyber-attacks, and spam.

In the game scenario the student selects a learning topic (e.g., security or privacy) and plays a series of mini-games. For providing extrinsic motivation, upon the successful completion of each mini-game, the virtual "security shield" that is associated with it unlocks. If at the end of the game all the corresponding shields have been removed, the player unlocks the "Arena Security" mini-game for that topic. Lastly, upon the completion of all the game's challenges, the learner is awarded with a "CyberAware certificate".

This design is in contrast to classical approaches that require the student to follow a full reading process and then answer a series of questions, which is well-known to cause boredom to students. Further, its main aim is for the student to discover new knowledge entirely by herself. For the security learning topic, the first two mini-games actively support and guide the student toward the correct answer by offering advising tips and hints, when, say, the player's answer is incorrect. Another key goal of CyberAware is to enhance learner's motivation towards an autonomous and self-directed learning process. As explained in section IV, this is achieved by problem-solving activities that promote critical thinking. In such an environment, the student is motivated to not only understand the various concepts being taught, but also to recognize their application in various real-life situations as well. In the following subsections we detail on the conceptual framework and ARCS motivational model on which Cyberware is built on.

IV. CONCEPTUCAL FRAMEWORK & MOTIVATIONAL MODEL

Motivation is considered as the theoretical construction for explaining learner's behavior. Generally speaking, motivation is the key factor to alter or improve learning outcomes in an intrinsic or extrinsic way [8]. As a result, the effort required from the educator to capitalize on motivation during the design of the learning process is considered as a challenging and demanding procedure. It also implies that the educator needs to carefully prepare the course being taught, and design it so as the instructional material to satisfy the following requirements: a) to be content-rich, b) to be blended with appealing characteristics for "keeping learning on track".

Having the above in mind, we carefully design our learning strategy before starting the development of the app so as to be clear content, relevant, and adapted to modern platforms, including the mobile ones. To do so, we considered that the design of CyberAware for a mobile environment should be guided by a instructional strategy in which a learning theory should guarantee the learning process and outcomes. This can be addressed by an Instruction Design Model (IDM) [9]. The latter details on how the learning experience can be orchestrated for the learner to acquire knowledge and skills in a more efficient, effective, and attractive way. In a more abstract form, such a model consists of guidelines and/or set of strategies for organizing clear-cut pedagogical scenarios toward the achievement of specific instructional goals. Below we detail on the ARCS motivational model and how this is embedded in the conceptual framework we used during the design of CyberAware.

A. Conceptual Framework

The conceptual framework we used in CyberAware is depicted in figure 1. It outlines the logical links among three components; the CyberAware app, learner's motivation, and the instructional design model. As already mentioned, motivation is considered as the key factor during the learning process. This is becoming more evident, when learner's motivation is kept at a high level, which in turn implies higher positive impacts during the learning process in terms of learner's engagement with the app. As a direct result, this situation is anticipated to spur the learner to keep in track and meet the expected learning outcomes.

For CyberAware we used ARCS as the IDM. Specifically, regarding the conceptual framework we used, the learner is placed in the center of knowledge acquisition, while she engages and interacts with CyberAware learning material. As explained further in section IV, ARCS model specifies all these strategies, guidelines and processes enabling us to design a suitable instructional material that sustains motivation and actively engages the learner in the learning process.

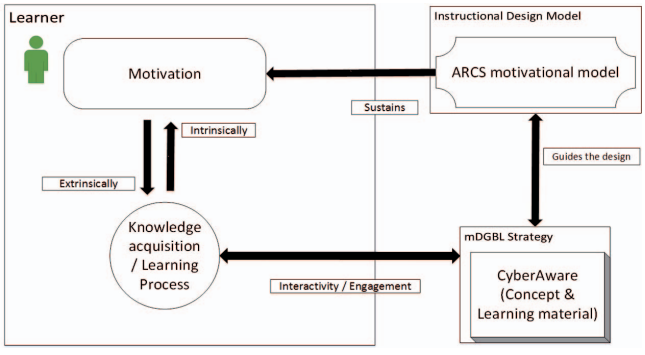

Fig. 1. CyberAware conceptual framework

The aforementioned conceptual framework could be also seen as a continuous adjustment procedure between the app and learner's motivation. Specifically, if necessary, the developer may alter the designing characteristics of the app to

embed new challenges and/or procedures towards increasing its motivation effects on the learners.

B. ARCS motivational model

ARCS [1] is a synthesis of several motivational theories, including: behavioral contingency design and management, skills and knowledge, cognitive accounting of individual abilities, and expectancy-value of theory, which is met in the context of social learning theory. In this theory, the learner participates to problem-solving tasks and expects specific learning outcomes according to her behavior. Putting another way, the model is a systematic design process for promoting and spurring motivation during the learning process. Overall, the main purpose of the model is to instruct the design of a learning app to be more intrinsically interesting to the learners.

The interconnection of ARCS components with the structural elements of CyberAware is depicted in figure 2. As observed from the figure, ARCS consists of 4 major components for promoting and sustaining motivation during the learning process, namely Attention, Relevance, Confidence, and Satisfaction. Each of them, consist of several other sub-components that qualify how the motivated self-directed learning can be succeeded. Within the next sub-sections we detail on how the above mentioned qualities are involved in the design phase of CyberAware.

1) Attention: The ARCS motivational model describes the necessary stages that a learning strategy should encompass in order to keep learner's attention during learning. This quality is proved to be one of the major factors in ARCS, since the challenge is to retain learner's attention during the learning process by keeping her engagement in a high level. As observed in figure 2, this is fulfilled by the "Active Participation", "Inquiry Arousal", and "Maintain Attention" components.

CyberAware is a problem-solving environment in which the student experiences active participation and accomplishes a series of sort challenges. Again, this is achieved by a limited number of mini-games that the student mandatorily plays in a row. For instance, the security learning topic is consisted of 3 mini-games. As illustrated in figure 3, in the first one, the learner is presented with several relevant and irrelevant technologies pertaining to basic cybersecurity technologies and is challenged to select the correct ones and place them to the four "NEED for protection" horizontal compartments.

Upon the successful completion of the previous challenge, a second mini-game starts. This aims at teaching the student to correctly associate each security technology (she has already identified) with its specific value in keeping her device safe. This situation for the second mini-game of the security topic is illustrated in figure 4. After that, as seen in fig. 5, the "Arena Security" mini-game unlocks.

Fig. 3. First mini-game: Identify the correct cybertechologies.

Fig. 4. Second mini-game for the security topic.

The goal of this third mini-game is for the student to figure out those cyber-technologies needed for handling specific online scenarios. These scenarios are based on typical real-life actions on the web. This challenge is crucial for a student in order to associate the knowledge she gains while interacting with the app with real scenarios she encounters while being on the web. More precisely, this mini-game consists of balls that fly from the right to the left side of the device's screen. When a ball appears on the screen it is randomly assigned to a specific scenario, e.g., "You received an email containing a music file. You should open and hear it", "You are using a streaming app to download video files", etc. First off, the mini-game, the student must use the magnifier tool to start scanning a ball in order to investigate the corresponding scenario. In the current version of the game, each scenario appears at the bottom of the screen. Then, based on the already acquired knowledge, the player needs to correctly identify the threat and select accordingly the right data security technology (colorful arrow on the right side of fig. 5) that eliminates it. This is achieved by selecting and throwing against the ball of interest the correct arrow, which is assigned to the appropriate cybersecurity technology (i.e., Antivirus, Firewall, Spam Filter, or Security Updates). If a ball is hit by the proper cyber-technology (arrow), then the player collects 10 points. The learner is given 4 mins to collect as many points as she can. Note that currently the player does not receive any negative points when she selects a wrong arrow.

2) Relevance: Relevance is also a key component of ARCS model. As given in figure 2, it splits into the "Present Worth" and the "Future Worth" sub-components. According to the model, it must be clear to the student why this course is worthy of being accomplished and how it is connected to real-life problems and situations. Both the aforementioned requirements are achieved via the mini-games discussed in the previous section as well as a specially crafted storyline. That is, when CyberAware starts, a specific storyline inquiry is being displayed on the screen. The same procedure is followed before the initiation of an individual mini-game.

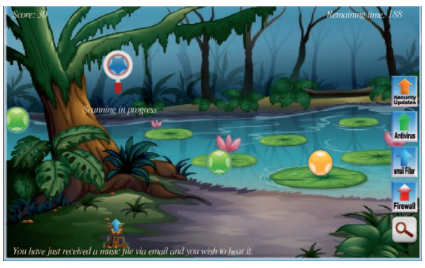

Fig. 5. "Arena Security": Identify the threat and face it.

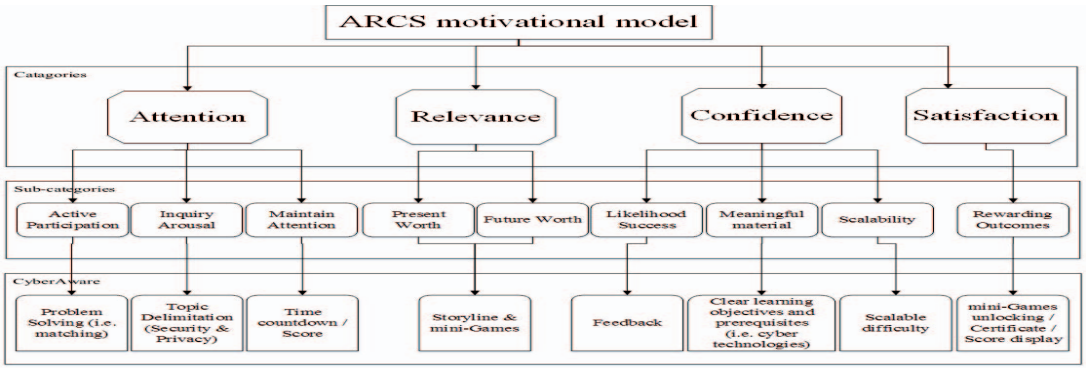

Fig. 2. CyberAware and ARCS interconnection

This is to stimulate learner's interest in exploring why it is valuable for her to attend this particular module. Precisely, as observed in figure 6, the game displays the main inquiry, indicating this way to the student which is the present worth (interests and goals) for her to be engaged with this course/module. Similarly, upon the selection of a learning topic, a consecutive inquiry is displayed pops up.

3) Confidence: As depicted in figure 2, confidence is split out into two subcomponents, namely "Likelihood success" and "Meaningful material". Specifically, it is very important for the player to feel that she is capable of performing a task successfully. Hence, to increase the chances of student's success, CyberAware actively supports and guides the student toward the correct answer. This is done by offering advising tips and hints, when, say, the player's answer is incorrect. For instance, in the first mini-game of the security topic, when the student's answer is erroneous, a personalised message guides her in finding the correct answer.

Further, in order to cultivate confidence between the learner and the app, it is essential the learning material to be designed in such a way that its objectives to be clear to the learner. Additionally, the learning material should place realistic expectations, and if possible to accommodate scalable levels of difficulty. Under this prism, CyberAware has clear learning objectives with the aim to familiarize students with fundamental cybersecurity technologies. Moreover, the mini-games have been designed to have a scalable difficulty that increases a mini-game after the other. Specifically, "Arena Security" is more difficult that the previous two. More precisely, in this third mini-game, the players must first think about the scenario and then choose the correct arrow to hit the ball.

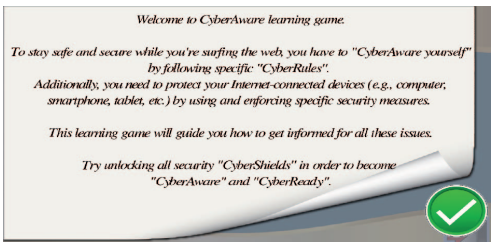

Fig. 6. Starting page: Main inquiry.

4) Satisfaction: This is the last component of the ARCS model. It is considered as a decisive component to preserve motivation, because if the student feels contented about the learning results, then she is very likely to feel the urge to play the game again. As depicted in figure 2, CyberAware fulfills this requirement by including the "Rewarding Outcomes" subcomponent. This is achieved by extrinsically rewarding the learner via unlocking security shields and new challenges such as the "Arena Security" one described in section IV. Further, it displays the player's score on the screen during the "Arena Security" mini-game. Ultimately, it rewards the learner with the "CyberAware certificate", which certifies that she is security aware and proficient.

C. Platform independency and Development technology

Another significant issue that a developer needs to take into consideration while implementing a serious app is that of the platform on which the app is destined to. Today, due to the plethora of devices of all kinds, porting an app to run on different platforms requires a significant effort in coding and testing. Consequently, most of the time such an implementation approach is proved to be ineffective. Additionally, as pointed out in section I, platform independency is closely related to the BYOD concept as well. Is such a case, learners are able to use their own device to play the game. This increases user's satisfaction because the player feels more comfortable using her own device. Further, seeing BYOD from an educational organization viewpoint, it needs a lot of effort from their side to develop and maintain different versions of the learning app. Therefore, it becomes clear that such a deployment creates additional costs not only for the development of the app, but also for upgrading its features and functionalities. To cope with this issue, CyberAware has been built in a way that can be run on the majority of modern platforms, ranging from desktop to mobile ones.

Specifically, for the development of CyberAware we used the Android Development Tool (ADT) plugin and libGDX game engine [2]. As with other game engines, libGDX consists of several subsystems and layered software modules. This architecture focuses on code reusability and scalability as well as to the easy export of the final product so as to be executable on multi-platform environments. This engine consists of 4 modules, namely Desktop, Android, iOS, and HTML5. For more details on libGDX engine the interested reader can refer to [2]. Therefore, by capitalizing on such an open-source cross-platform framework, CyberAware is able to run on a variety

of popular desktop and mobile platforms, including Windows, Linux, Android and iOS.

V. EVALUATION

We performed a preliminary evaluation of CyberAware by means of both pre- and post-questionnaires (i.e., before and after using the CyberAware). Our goal was to assess both the functional characteristics of the app (user satisfaction and usability) and student learning outcomes (effectiveness). Both evaluations were conducted using a sample of 43 elementary-age students, 20 boys and 23 girls, who ranged in age from 9 to 11 years. Before playing CyberAware all the participants have attended a security learning course in the classroom according to their curricula.

A. Usability and satisfaction

A questionnaire consisting of 12 Likert-type questions was designed to collect students' experiences about the usage of the app. Each statement has 5 alternatives to choose from: strongly disagree, disagree, neither agree nor disagree, agree, and strongly agree. The participants had to answer the questions shortly after playing CyberAware. The highlights of the findings are summarized below.

- 66.6% of the learners did not encounter any problem while playing the game.
- 74% of them did not face any problem with moving the relevant and irrelevant cybersecurity technologies in the correct place.
- 61% of the participants agreed that any message the app displays is fully informative.
- 44.4% of the learners do not prefer reading any further learning material during the game play, and 27.8% of them have a neutral opinion on the same question. This outcome also strengthens our view on designing the app to be as minimalistic as possible in terms of the volume of information provided to the student in an effort to avoid boredom.
- About 74% of the learners understand the learning objectives of each mini-game.
- 81.5% of them would play again the game in the classroom, and about 85.2% would play it at home or at any other place.
- 37.3% agreed that the Arena Security mini-game succeeds to relate the subjects being taught with real-life online situations, while another 39% had a neutral opinion on this. After observing learners behavior when interacting with the app, we conclude that they faced some problems in determining the scenario, and selecting the correct cybersecurity technology. These are caused due to the ball moving speed and the time required for the learner to deactivate the magnifier before launching an arrow toward the ball of interest.
- 63% of the learners state that they understand better "what cybersecurity is all about" after playing CyberAware and 85.2% of them stated that CyberAware challenges were very interesting.

Last but not least, CyberAware is considered as a lightweight app in terms of system resources. Specifically, CPU benchmarking analysis on the Android platform using a ZTE V975 device, indicates that the app uses an average of 9% of CPU. Moreover, RAM memory consumption when the app is running fluctuates between 115 and 233 MB depending on the mini-game in use.

B. Effectiveness

Knowledge acquisition effectiveness before and after using CyberAware, is also examined via questionnaires composed of 6 questions that learners answer before and after playing CyberAware. According to our analysis, before playing the game, about 32.6% of the learners were able to recognize all 4 technologies that are required to keep their Internet-connected devices protected. After playing it, this result was improved by almost 15%. An analogous improvement was also perceived for the rest of factors measured by the corresponding questions. For example, before playing the game, 18.6% of the learners were able to recognize at least 3 scenarios out of 6 that an Internet-connected device needs to be protected. After playing CyberAware, this attainment rate has increased to about 32.6%.

VI. CONCLUSION

This paper details on the design of an mDGBL app destined to cybersecurity education for students of primary education. Contrary to other works in the literature, our contribution is not focused on technical implementation only but to the pedagogical factor as well. The latter pertains to the way the ARCS motivation model is embedded in the app to maximize the learning outcomes. We show that CyberAware is simple to use and lightweight in terms of system resources. Also, it is multi-platform enabled making it ideal for the BYOD model. As a future work, we plan to extend app's functionality to integrate adaptive learning elements, and embrace privacy and especially anonymity topics too.

REFERENCES

[1] J. M. Keller, "Development and use of the arcs model of instructional design," *Journal of instructional development*, vol. 10, no. 3, pp. 2–10, 1987.

[2] M. Zechner. (2012) Libgdx documentation initiative.

[3] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching johnny not to fall for phish," *ACM Transactions on Internet Technology (TOIT)*, vol. 10, no. 2, p. 7, 2010.

[4] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish," in *Proceedings of the 3rd symposium on Usable privacy and security*. ACM, 2007, pp. 88–99.

[5] IASE. (2014, February) Information assurance support environment (iase), dod, cyberprotect. [Online]. Available: http://iase.disa.mil/eta/Lists/IA20 Simulations/AllItems.aspx

[6] S. Srikwan and M. Jakobsson, "Using cartoons to teach internet security," *Cryptologia*, vol. 32, no. 2, pp. 137–154, 2008.

[7] N. A. G. Arachchilage and M. Cole, "Design a mobile game for home computer users to prevent from phishing attacks," in *Information Society (i-Society), 2011 International Conference on*. IEEE, 2011, pp. 485–489.

[8] C. B. Hodges, "Designing to motivate: Motivational techniques to incorporate in e-learning experiences," *The Journal of Interactive Online Learning*, vol. 2, no. 3, pp. 1–7, 2004.

[9] A. S. Gibbons, E. Boling, and K. M. Smith, "Instructional design models," in *Handbook of research on educational communications and technology*. Springer, 2014, pp. 607–615.

978-1-4673-8243-4/15/$31.00 ©2015 IEEE 19-20 November 2015, Thessaloniki, Greece