INTERNATIONAL
HELLENIC
UNIVERSITY

A mobile application for increasing users' security awareness through gamification

Kefala Aikaterini

SID: 3306170004

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Mobile and Web Computing

DECEMBER 2018

THESSALONIKI – GREECE

INTERNATIONAL
HELLENIC
UNIVERSITY

A mobile application for increasing users' security awareness through gamification

Kefala Aikaterini

SID: 3306170004

Supervisor: Prof. C. Kalloniatis

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Mobile and Web Computing

DECEMBER 2018

THESSALONIKI – GREECE

Abstract

This dissertation was written as a part of the MSc in Mobile and Web Computing at the International Hellenic University.

The first component incorporates a short introduction of the present thesis, which will be presented methodically, briefly including the fundamental configuration and rationale of this study.

In the second part of the dissertation the term “gamification” will be defined while its advantages are going to be collocated.

In the third part, the significance of the increasing requirement for satisfying users’ security awareness in information systems will be offered.

In the fourth part, a way will be cited in which applications that exploit game elements can have the potential of assisting in the amplification of the users’ security awareness, as these emerge to be additionally appealing to users.

In the fifth part a mobile application running in an iOS environment will be explained aiming to augment users’ security awareness with the employment of gamification principles.

At this point I would like to show gratitude to my supervisor Dr. Christos Kalloniatis, for the significant guidance, the targeted pieces of advice he offered, the incessant support and the spirited motivation that he has provided me with during the continual time of research and development of this dissertation. His devoted attitude was fundamentally decisive for the successful accomplishment of the work presented in this thesis.

Kefala Aikaterini

07/12/2018

Contents

1 Introduction

The intricacy statement, the goals of the dissertation and the dissertation outline are going to be presented in this section.

1.1 Background

The setting of this dissertation incorporates the study on the expression of gamification, its contribution to applications, its denotation of security awareness and the grave magnitude of its enhancement nowadays in modern business companies and corporate organizations. Finally, the confluence of gamification in the field of information security systems is going to be further analysed.

1.2 Problem

The predicament defined in this dissertation is the dearth of users' awareness concerning information systems security. One of the main reasons is that a great number of the existing methods and programs are designed solely focusing on the content of the training and not on the final user. The majority of users do not bear in mind that the traditional training bears any extraordinary concern while the results regarding the knowledge property they gain after erudition are not extremely encouraging. The human factor could comprise serious vulnerabilities within a business company or a corporate organization. Therefore, it is deemed crucially essential that higher levels of attention should be paid on investing in the quantitative acquaintance of the users regarding possible digital threats and cyber-attack risks.

1.3 Goals

The core objective of this dissertation is to devise and fabricate a prototype iOS application that could be effortlessly adaptable and extendable by a large range of business companies. Not only will the use of game elements convert the experience of the users' training into an agreeable modus operandi, but it will boost their awareness concerning security issues as well.

1.4 Conclusion

As a wrapping up outcome, the model application will be clearly outlined along with some future judgments for improvement.

2 Gamification background

This section is going to deal with the **gamification** term, its description, its history and how it is applied worldwide. The profits of gamification will be listed along with the chief discrepancies between game development and gamification.

2.1 Definition

Gamification is an expression that deeply concerns a lot of scientific researchers. Even though a great number of them have attempted to define it in the past, it is obviously clear that there is a level of complicatedness as regards that. Thus, in point of fact, nearly every single one of them initially delimitated the meaning of the *game,* which comprises the first lexical part of the word.

Avedon and Sutton-Smith in [1] were the first who addressed the term, claiming that *game* is a voluntary activity which is delimited by rules. Crawford in [1] mentioned that games should represent some kind of reality, which means to depend on the interaction between the system and the user, presenting the user with the ability to come into direct collision with the provided environment. As for Huizinga in [1] game is not a serious but an intensively voluntary activity, which is based on rules and social limits. Salen and Zimmerman in [1] classified the game as a system which is determined by rules. During the interaction with the given system, the users are actively involved into a conflict whose result can be evidently quantified. Juul in [1] suggested that all the games should have six basic characteristics: a) rules, b) variety, c) countable results, d) result with meaning, e) effort of the user, f) investment of the user and negotiable consequences with respect to the real life.

The progressive advent of technology has led to a revolutionised modification of the techniques with which the games are enjoyed. Nowadays, all manner of videogames have replaced games, where the users are enthusiastically involved in a dissimilar way, resulting in a change of users' enjoyment level during their involvement with them

(Brumels et al., 2008). Furthermore, nowadays, modern society more and more utilizes social media, while digital entertainment currently constitutes a customary pleasurable activity [2]. Jesse Schell in [2] presented a future where videogames comprise a part of contemporary human reality. Mora, Riera et al. in [2], explained that owing to the presence of the games in society's daily life, gamification is rising nearly automatically as a means of extracting the features of the games and their integration into other environments.

As mentioned above, there is no specific definition for the term *gamification*. The first approach was made by Nick Pelling in [2], who defined gamification as an application where the user is provided with an interface, which is comparable to a game in order to make electronic transactions quick and easy to apply. Since then, this definition has been altered by combining some elements of the games and their design.

Seaborn and Fels in [2] during their research, have established that before the birth of the term gamification, diverse terms had been applied for this process. There was a range of prose that had been projected for this term, like "funware" (Azadegan and Riegel, 2012), "funology" (Malone, 1982), "productivity games", "surveillance entertainment", "behavioral games", "game layers", "applied gaming" and "serious games" [1]. McGonigal in [1] also forwarded some other requisites, like "alternate reality games", "games with a purpose" and "augmented reality games". Nevertheless, the term *gamification* has prevailed these past recent years and is entirely acceptable by everyone who deals with this methodology.

Even though the employment of this phrase is quite fresh, the attitude has been habituated a lot during the last decades in dissimilar forms of systems. Zichermann and Linder in [1] defined gamification as a tool that is employed for the compliance of branding through application. Deterding et al. [1,3] also defined the method of gamification. It is regarded as the most famed definition and is heavily practiced in diverse investigations concerning this specific scheme. According to Deterding et al. [1,3] gamification is the function of game elements in applications that do not represent a game.

Simultaneously, Huotari and Hamari in [1] based on the definition of Deterding et al. [1,3], accepted as true that the experience of the user should be the most imperative factor while the final result should be left aside. As a result, the purporting constitutes that gamification personifies the practice to strengthen a service that along with the experiential perspective of the game can utterly support the overall experience of a user.

Werbach and Hunter in perceived gamification as a function of game elements and design techniques of a game in terms of a non-game. In general, as Seaborn and Fels also concurred in [1], according to all of the above mentioned definitions, the ending conclusion is that gamification is the international manipulation of game elements for the experience of the game itself in the terms of a non-game having a sizeable increase in users' motivation as a main purpose.

2.2 Design of applications with game elements

In this division the essential design guidelines regarding the applications that employ game elements will be abundantly demonstrated. Firstly, the accompanying graph represents the key results of Google by each year, categorized by keywords habituated at the principal searches. It is obviously clear that the primary concentration is focused on the designing of applications bearing game elements.

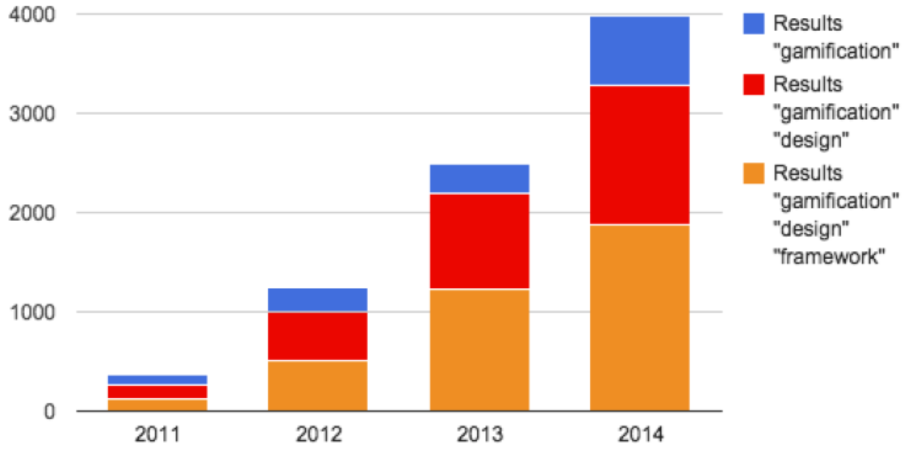


Figure 1. "Results of academic searches about gamification", Mora A., Riera D., Gonzalez C. & Arnedo-Moreno J. (2015), A literature review of gamification design frameworks, Spain.

At the same time, in another graph, it is noted that the dates that documents regarding gamification were published are quite recent. As it obviously turns out, 2013 was the year when the most articles were published at a percentage of 66.7%.

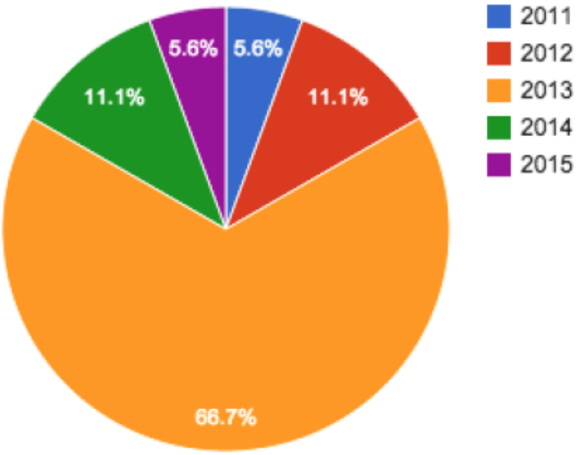


Figure 2. "Gamification design framework publish date", Mora A., Riera D., Gonzalez C. & Arnedo-Moreno J. (2015), A literature review of gamification design frameworks, Spain

The purpose of designing an application with game elements compared to the rationale of designing a game application is indeed rather dissimilar. The first one deals with fully accomplishing its targets in an added pleasurable way, while the second one has to directly answer only to entertainment requirements. Marczewski in [2] markedly distinguished the games and the applications with game elements, by declaring the first intend of the games, which is the proposal of amusement and the first aim of the applications with game elements which is the proposal of a business objective. Designing a system that reminds of a game setting compared to designing an actual game personifies a wholly variable procedure. There is a fine line that separates these two worlds, which is actually what the game elements represent. The principal concepts of gamification are based on key conceptions of games. Salen and Zimmerman in [2] defined a set of indispensable principles in order to design a game, which are the following:

1. The understanding of the designing of a system, the considerations of the interactivity, as well as of the selection of a player, the action and the result.

2. The construction of the rules, the complexity, the appearance, the experience of the game, its representation and its reaction with the users and finally
3. The strong connection between the rules of a game and the game that the rules create, the entertainment that is offered by the games, the concept that they are building, the way of thinking that they incorporate, and the stories that they are indeed describing.

After studying all these principles, Brathwaite and Schreiber in [2], claimed that after the recognition of the chief game elements, it is compulsory for a research to be carried out regarding the interrelationship between them and their appliance. They distinguished the parts of a game as minor components that may be isolated and studied separately. According to this approach, the process of scheming a game with several elements gets much clearer. This idea was used by Reeves and Red in [2], which presented the ten basic components for the designing of a game:

1. Self-representation
2. Three-dimensional environment
3. Narrative
4. Feedback
5. Reputations ranks and levels
6. Marketplaces and economies
7. Competition under rules
8. Teams
9. Communication
10. Time pressure

A structure for the content of game elements named “Mechanics, Dynamics and Aesthetics (MDA)” was developed by Hunicke in [2]. This approach attempts to fill the gap between the design and the development of a game and according to that, the games are constituted by three principal elements:

1. Rules
2. System
3. Entertainment

Cavillo–Gamez in [2] at “Core elements of gaming experience (CEGE)” exacted that model as just a part of the experience of a game. He suggested several compacts for the provision of a sufficiently positive feeling during the gaming progression, which should definitely be included during the designing stage.

Gamification is a subject that concerns quite dissimilar scientific fields, such as psychologists, sociologists, software engineers to name just a few. Every bit of such attention is focused on the procedure of designing itself, allotting separate roles for each professional brand.

The pyramid of gamification elements indicates the following three steps: mechanics, dynamics and components. This pyramid is considered as the basis of assorted other theories regarding the theory for the design of gamification.

A complete methodology regarding gamification is called Octalysis in [2] and is defined by Yu-kai Chou. According to this approach, gamification is the kind of design which focuses more on the human motivation during its process. Essentially, he claimed an anthropocentric design based on an octagonal shape with eight core drivers. Each core represents a side of the octagonal shape. More specifically:

1. Epic meaning and calling
2. Development and accomplishment
3. Creativity and feedback
4. Ownership and possession
5. Social influence and relatedness
6. Scarcity and impatience
7. Unpredictability and curiosity
8. Loss and avoidance

Cunningham and Zichermann in [1] created a list of elements of the game, with mechanisms based on examples. These mechanisms are the following:

1. Feedback and reinforcement
2. Pattern recognition
3. Collecting
4. Organizing
5. Surprise and unexpected delight

6. Gifting
7. Flirtation and romance
8. Recognition for achievement
9. Leading others
10. Fame and getting attention
11. Being a hero
12. Gaining status
13. Nurturing and growing

Werback and Hunter in [1] defined the game elements as the parts that identify a game: mechanics, dynamics and components, just like Deterding et al. in [1,3]. Besides that, they deem that the systems with game elements are not essentially games. They just take advantage of the human psychology in the same way that games do. They have confirmed that gamification bears the ability to develop into a more effectual one, rewarding in a completely changed way from what the traditional games do, because the shared game element itself is rewarding. They are of the same opinion that gamification is an expedient manner to assist existing plainly designed applications so as to be converted into more interactive and meaningful ones bearing confirmed affirmative elements.

According to a number of surveys, the broad rudiments that aid in the implementation of gamification are competent to being clearly distinct. The most vital of them appearing in the majority of the elements lists are the following:

1. Points
2. Leaderboard
3. Badges
4. Levels
5. Rewards
6. Theme/story
7. Clear goals
8. Feedback
9. Challenges
10. Progress

11. Roles

The first three of them are those in which all researchers agree on [4].

There are a few steps that need to be abided by in order for an application that employs game elements to be developed effectively. Morschheuser B., Werder K., Hamari J. and Abe J. in [5] published such gamification states of design. They accomplished a survey based on bibliography and interviews to both specialists and game designers as well. They concluded in seven basic stages that should be strictly followed during the designing process. Those states are the following:

1. Project preparation
2. Analysis
3. Ideation
4. Design
5. Implementation
6. Evaluation
7. Monitoring

During the preparation process, all of the above activities that should be carefully executed must be thoroughly checked before launching the project. While on the second stage, an analysis of those activities ought to take place in order for the compulsory acquaintance of the users to be crystallised. During ideation, the activities of the design are summarized and during design the prototypes are to be created. During the fifth state, the implementation of the project occurs, in order for the project to be further tested and additionally evaluated at the sixth state. Finally, at the seventh state the route of the use of the project is wholly monitored while several acts may be found necessary to be interposed.

If all the above principles are faithfully observed, researchers claim that someone will be able to formulate a winning application utilizing game elements as fundamental parameters.

2.3 Gamification in education

In the third and last part of this chapter, the sectors where the method of gamification has been applied are going to be analyzed, mentioning some examples of such applications.

Gamification in the field of education has been greatly developed these past few years. These applications utilise game elements in order to design a system for educational purposes. Gamification in education is used in digital game-based learning (DGBL) according to Kapp in [1,6]. He defined gamification as the employment of mechanisms based on games and the way of thinking aiming to furnish users with confidence to exploit the applications so as to render their knowledge wealthier and firmer.

The use of gamification in education as a research topic has been increasingly observed in recent years. Caponetto, Earp and Ott published a document in 2014 [6]   recording the number of documents that were published from 2011 to 2014. The following figure reveals in great detail the number of documents based on the year of its publication.

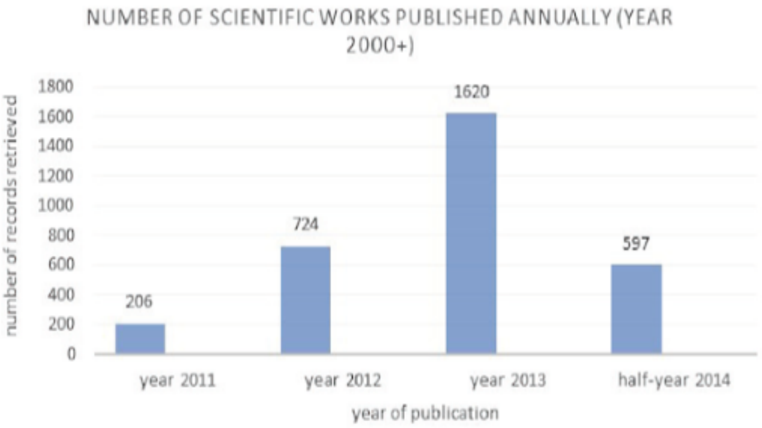


Figure 3: The number of scientific articles that were published from 2011 to 2014 regarding gamification in education, Caponetto I., Earp J. and Ott M. (2014), Gamification and Education: A Literature Review, Germany: Research and Training Center for Culture and Computer Science (FKI), University of Applied Sciences HTW Berlin, Proceeding of the 8th European Conference on Games Based Learning ECGBL 2014

In the same research, the percentage of the documents that is related to gamification in education depending on the educational level has been methodically established. In the following figure, the percentages of the researches are demonstrated, making it clearly apparent that most of the articles evidently target the use of gamification at a university level, while 48% of these documents plainly direct towards other educational levels.

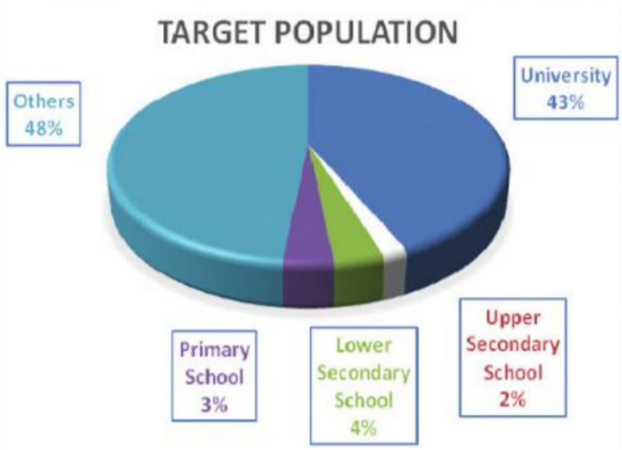


Figure 4: Percentages of research documents that have been written depending on their target group, Caponetto I., Earp J. and Ott M. (2014), Gamification and Education: A Literature Review, Germany: Research and Training Center for Culture and Computer Science (FKI), University of Applied Sciences HTW Berlin, Proceeding of the 8th European Conference on Games Based Learning ECGBL 2014

Yu-kai Chu [7] suggests several applications of gamification in education. Through games, not only is the interest of the students increased but the communication with their teachers and the contact between the students themselves is augmented as well. Duolingo, which is an application that relates to the learning of foreign languages, can be taken as an example of gamification. This application is quite user friendly providing ample entertainment as well as sufficient knowledge, which is its main objective.

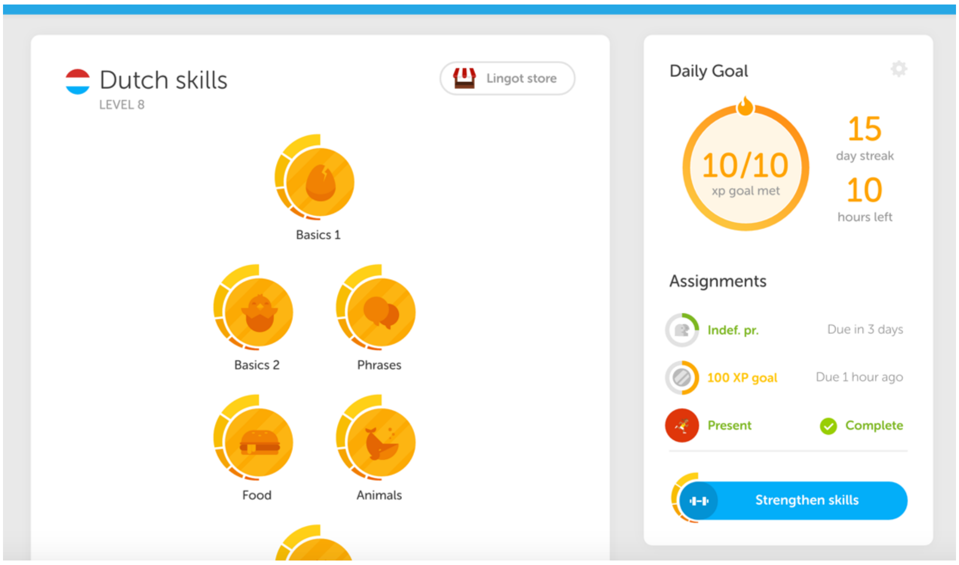


Figure 5: Duolingo, figure available at https://support.duolingo.com/hc/en-us/articles/208191253-How-do-I-find-an-assignment-

ClassDojo is one more application that is suggested by Yu-kai Chu [7]. This is a tool of class management, assisting educators to control student behaviours within any given classroom environment.

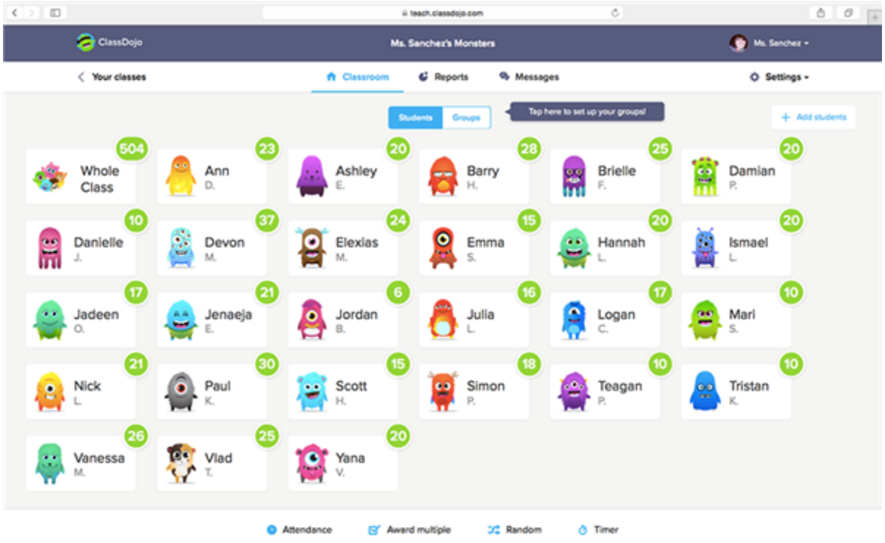
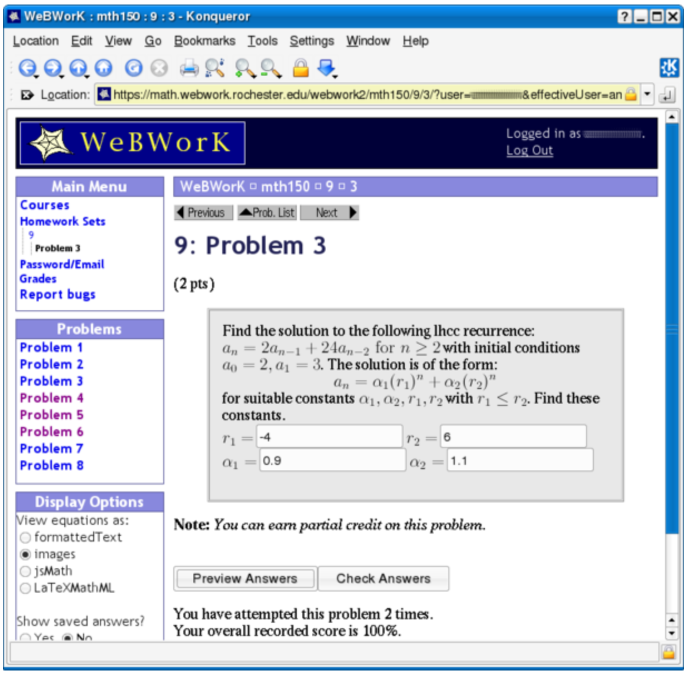


Figure 6: ClassDojo available at https://www.cusd200.org/Page/14503

Webwork is a platform that concerns the completion of homework regarding maths and physics. Goehle in [1] added several game elements. Results prove that learners' efforts are justly recognized.



View equations as:
○ formattedText
● images
○ jsMath
○ LaTeXMathML

Show saved answers?
○ Yes ● No

9: Problem 3

(2 pts)

Find the solution to the following lhcc recurrence: $a_n = 2a_{n-1} + 24a_{n-2}$ for $n \geq 2$ with initial conditions $a_0 = 2, a_1 = 3$. The solution is of the form:

$$a_n = \alpha_1(r_1)^n + \alpha_2(r_2)^n$$

for suitable constants $\alpha_1, \alpha_2, r_1, r_2$ with $r_1 \leq r_2$. Find these constants.

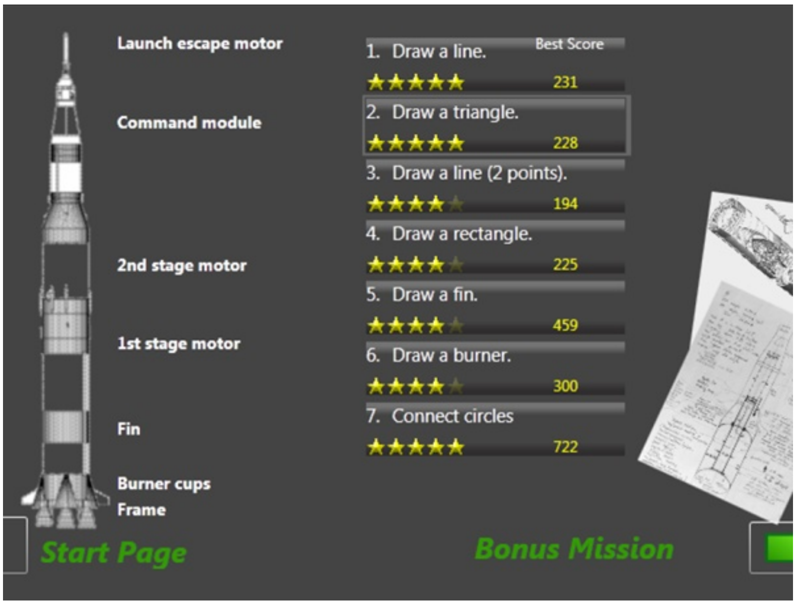
$r_1 =$ -4 $r_2 =$ 6
$\alpha_1 =$ 0.9 $\alpha_2 =$ 1.1

Note: *You can earn partial credit on this problem.*

You have attempted this problem 2 times.
Your overall recorded score is 100%.

Figure 7: WebWork available at https://en.wikipedia.org/wiki/WeBWorK

Li et al. in [1] developed GamiCAD, an educational system which aids new users in familiarising themselves with AutoCAD. Results show that more and more users can actively participate and markedly improve their overall performance.



	Best Score
1. Draw a line.	
★★★★★	231
2. Draw a triangle.	
★★★★★	228
3. Draw a line (2 points).	
★★★★☆	194
4. Draw a rectangle.	
★★★★☆	225
5. Draw a fin.	
★★★★☆	459
6. Draw a burner.	
★★★★☆	300
7. Connect circles	
★★★★★	722

Figure 8: GamiCAD available at https://www.autodeskresearch.com/publications/gamicad

3 Security awareness

In this chapter the issue of **security awareness** is going to be studied, mentioning the particulars of its magnitude regarding a system and its protection. Additionally, the role of increased security awareness in minimizing security incidents induced by users will be openly addressed.

3.1 Security awareness of information systems

This chapter will directly demonstrate all the crucial information regarding security awareness that deals with information systems.

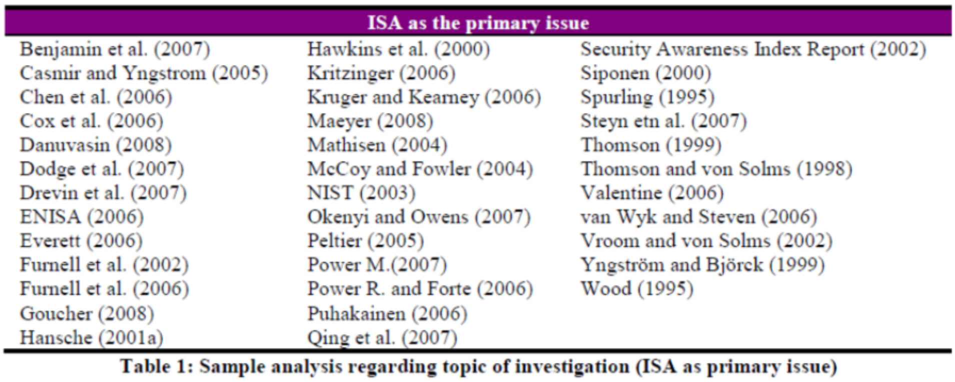
Security awareness is a huge topic. In fact, it is so imperative that security of information should concern everyone. Jeager in [8] makes an honest effort to clearly comprehend the meaning of awareness. As a concept it is able to be correlated with the mental state of a person, since a specific interpretation of this connotation may be for someone to own consciousness or to be familiar with something. Some definitions include the procedures that transpire in order for a person to gain valuable knowledge. Nevertheless, a number of definitions are also in existence that cannot distinguish awareness from a specific kind of conduct [8].

Rhee et al. define the security awareness of information as a vigilant understanding of the various threats towards security information and the perceptions of each person regarding these threats [8].

Ernst and Young in [9] recognized the lack of security awareness from the users as an obstacle to the effective security of information. They also recognized security awareness as a considerable topic that is responsible to fill the gap between the increasing risks of the information systems and the actions that should be taken in order to face those risks. They also deem awareness as a procedure that should be globally taken seriously into consideration and careful thought should be devoted as a key priority concerning the security of information, which will have accelerating effects into the ability of the organizations to handle their trade perils.

Most definitions imply that security awareness is the fundamental level of the security knowledge targeting to lead the users of information systems towards interpreting the grandness of the security of information and their obligations towards security. Training should be targeted in advancing familiarity and relational capabilities, while education should be directed towards the creation of resolute specialization upon security issues [9].

Tsohou et al. in [9] presented a table with all the researchers who conducted investigations on the definition of security awareness.



ISA as the primary issue

Benjamin et al. (2007)
Casmir and Yngstrom (2005)
Chen et al. (2006)
Cox et al. (2006)
Danuvasin (2008)
Dodge et al. (2007)
Drevin et al. (2007)
ENISA (2006)
Everett (2006)
Furnell et al. (2002)
Furnell et al. (2006)
Goucher (2008)
Hansche (2001a)

Hawkins et al. (2000)
Kritzinger (2006)
Kruger and Kearney (2006)
Maeyer (2008)
Mathisen (2004)
McCoy and Fowler (2004)
NIST (2003)
Okenyi and Owens (2007)
Peltier (2005)
Power M.(2007)
Power R. and Forte (2006)
Puhakainen (2006)
Qing et al. (2007)

Security Awareness Index Report (2002)
Siponen (2000)
Spurling (1995)
Steyn etn al. (2007)
Thomson (1999)
Thomson and von Solms (1998)
Valentine (2006)
van Wyk and Steven (2006)
Vroom and von Solms (2002)
Yngström and Björck (1999)
Wood (1995)

Table 1: Sample analysis regarding topic of investigation (ISA as primary issue)

Table 1: Sample analysis regarding topic of investigation, Tsohou A., Kokolakis S., Karyda M. and Kiountouzis E. (2008), Investing Information Security Awareness: Research and Practice Gaps, Greece: Information Security Journal A Global Perspective, December 2008

Hanshee in [9] distinguished the difference of security awareness and training absolutely claiming that it is not considered as identical as training. The European Union Agency for Network and Information Security (ENISA) is an organization that faces issues concerning the security of network and information. ENISA in [9] distinguished the concepts of awareness, training and education affording the prospect to corporate organizations to come to a decision of whether the program should focus exclusively on awareness or on training and education as well. Krintzinger in [9] recognized the existing terminology defining those three concepts. Mathisen in [9] also differentiated those three meanings as well, while Chen et al. in [19] agreed with the definitions that were provided by The National Institute of Standards and Technology (NIST) in [9] apprehended the differentiation between training and education. The same perspectives were adopted by Okenyi and Owens in [9], who distinguished the three concepts supporting at the same time a procedure of learning, which starts with awareness, continues with training and finally passes through education, the meaning of which is termed as a learning process. However, at the beginning of their examination they had declared that the purpose of the program of security awareness is to amplify awareness, which can indeed facilitate comprehension through training. Notwithstanding, they ended up differentiating explicitly all the above meanings.

Drevin et al. in [9] investigated extensively the targets of security awareness considering them as key objectives towards bringing down probabilities of human errors, stealing, fraud and appalling manipulation of computer data. The fundamental functions of information security awareness should be related with the indispensable purposes of security, which, in point of fact, means confidentiality, integrity as well as availability [9].

3.2 Awareness, training and education

The staple definitions for these requisites will be entirely delivered and analyzed below. NIST in [10] published a document with rules and techniques for the creation of programs regarding security information and training. According to NIST, a productive program of information security consists of a foundation of information security policy, which may fluctuate depending on the desires of each organization affording the possibility to be dully moderated according to the existing perils of users' knowledge regarding their obligations towards information security, as they are explicitly listed on the security policy of each organization. Finally, certain procedures should be established so that any kind of monitoring and reviewing of programs can be fruitfully accomplished.

Security awareness and training should be resolute on the totality of the users' population of any given organization. The executive management of an organization should drive their attention towards the security of information. A program of awareness ought to be effortlessly adaptable and extendable depending on the analogous requirements as well as the target groups. The effectiveness of this collective effort will designate the effectiveness of the program itself concerning awareness and training. The above parameters are measured extremely indispensable for a victorious information security program to be implemented [10].

A program of awareness and training in any corporate organization is deemed fundamentally elemental since it is viewed as a way of adequately disseminating information, including even managerial positions. Ergo, it is considered critically rudimental in order for them to complete their day-to-day duties safely. In the case of the information security program, it is measured as the means of acknowledging security requirements in a whole corporate organization [10].

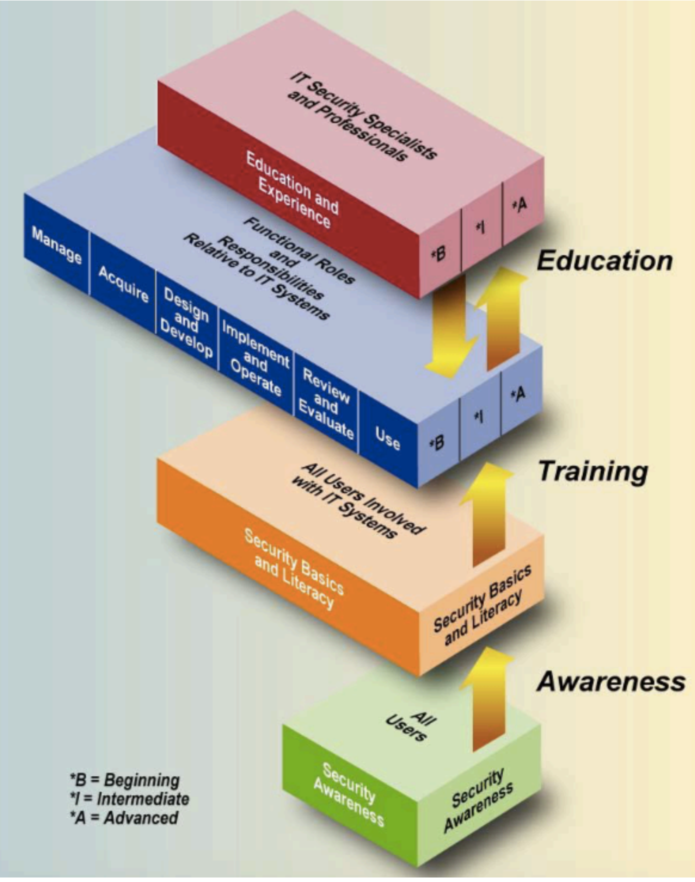


Figure 9: The continuous learning of security of information technologies, Wilson M. and Hash J., (2003, October), Building an Information Technology Security Awareness and Training Program, Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8933

Laborious efforts regarding security awareness had better be carefully considered in order for users to convert their contemporary updating methods so as to be superiorly capable of diminishing error instances. Corporate companies, as well, ought to reinforce their high-quality security practices. NIST [10] defines awareness as a kind of non-training, since its sole principle is to pay focused consideration on security alone. Their chief objective is to direct persons towards recognizing the vexations regarding security matters so that they can respond instantly. Training is universally deemed as an official approach to gaining knowledge and skills bearing the possibility of expediting work performances.

NIST defines training as a level of continuous erudition targeting on the fabrication of relevant security skills for the users, who ought to possess varying degrees of knowledge relevant to fields other than just security. The core disparity of this awareness is that training is directed towards teaching skills that permit a person to handle specific operations while, on the other hand, awareness aims at the attention of a person on any given concern. The skills that are required during training are fashioned based on the awareness and the basic familiarity of the security. A training program does not automatically denote that has to be certified by a university. Nonetheless, a training course could comprise identical content elements taught within a course at a university [10].

Education is the stage level where all manner of skills and security capacities of various functionalities can be encapsulated. A universal sagacity of knowledge adds to an interdisciplinary study of concepts, of issues and of technological and social principles. It intensively attempts to bring specialists and professionals into being highly competent of vision and proactive response [10].

Professional growth is dominantly central in the context of user tutoring. Thus, it can be ensured that all levels of users, ranging from beginners to professionals regarding security, boast the required level of acquaintance and professional aptitude that is held obligatory for their role.

A lot of business companies and corporate organizations focus their recruitment attentions on information technology security professionals, who own accredited certifications as core qualifications. In addition to this, there are companies that proffer increments on salaries and bonuses ensuring that the users with certifications will also urge colleagues to come by certifications on security sectors as well [10].

4 Security awareness through gamification

In this chapter a description concerning the way gamification could assist towards incrementing users' security awareness following the aforementioned analysis in chapters 2 and 3 is going to be thoroughly presented.

While researching the present thesis, a serious piece of evidence came to my attention: Although there are programs in existence relevant to security awareness, most of them do not accomplish their full potential. The main explanation may be that these programs are not attractive enough to the users. Their creators have concentrated mainly on the awareness and training regarding security issues and failed to pay any serious attention on whether they are user friendly and pleasant to the users to spend time with. It follows that an intelligently clever way of profitably resolving this issue is to implement game elements on these programs. Through gamification, the security awareness programs could grow into becoming more appealing, so that the user can face them as something entertaining and pleasurable and not as an obligation that merely demands to be accomplished. By utilizing game elements, any particular program instantly acquires an entertaining substance meaning that the user can straightforwardly comprehend its content.

The inspiration of gamification in security awareness programs is not something illusory. Thornton and Francia in [11,12] presented a research regarding a tower defence game, whose goal was the instructing of students to respect the strength of passwords. Nevertheless, it has never been clear which practices of gamification were used in this case.

Many a research have sought to prove the effectiveness of gamification. Hamari et al. in [11] composed a review derived from 24 studies in order to investigate how gamification works. The outcome visibly depicted that gamification has optimistically contributed to the melioration of the education in multiple occasions. Nevertheless, it was mentioned that the grades may depend on both the users' ability and the content of the programs. It was also remarked that there are very few high-grade researches regarding the actual results of gamification.

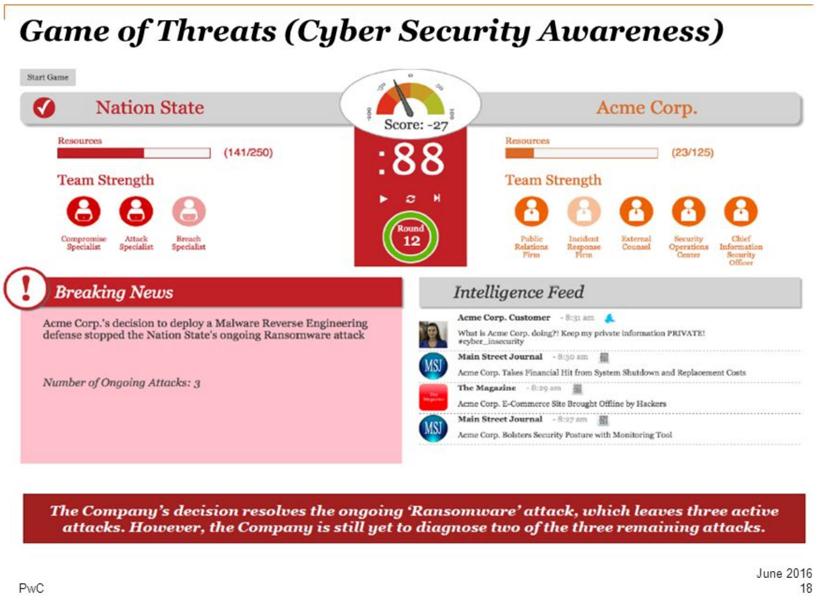
Gjertsen, Gjaere et al. in [11,13] throughout their research studied the use of gamification in programs of security awareness and training. The existing programs were not productive enough in providing the obligatory knowledge to the employees, so a novel scenario and prototype needed to be re-developed. Several interviews with experts in security were conducted in order to investigate the appropriateness of this prototype. During this research, it was established that most of the trouble of the existing programs of security awareness could effectively be resolved with the use of game elements [11]. The process of designing game elements needs to effectively aim the user. The writers support that knowledge and progress are the two most essential motivational factors. It is indispensable that competitiveness be used when the principal function is the training of all users. It is globally accepted that wherever any form of recompense is involved human antagonism prevails. Corporate rewards should tap into this convention and instigate repayments for those who excel noticeably within any given marketable environment. Gamification extends a lot of possibilities to deliver more than a few varieties of content depending on the skills and the position each user holds within any specified company ranks. The developed prototype was grounded on the fact that the existent courses were heavily time-consuming [11]. A key factor that should be taken into solemn consideration is the utilization of petite tasks during a course. It has been acknowledged that this characteristic may bear two imperative consequences: it may well supply the users with a kind of autonomy when it comes to training and it may advance their educational grades as well.

Thornton David and Francia in [12], presented the results of a project regarding education in security issuances through the function of gamification. They examined the brunt on both teachers and students while the outcomes encouraged the exploitation of game elements. Positive feedback was provided towards these elements by the students while their overall participation percentage was positively enlarged.

Wood in [14] exacted that it is not a trouble-free duty to persuade employees of any given corporate company to take hold of serious consideration the security issues. Hence, in this mission the use of gamification possibly will facilitate the process. The game elements may be used for the upgrading of users' security awareness, who may positively modify their corresponding actions. The rewards of the users with points and a leaderboard with users' ratings can be viewed as game elements. A representative example of the results of security training is that before a training is addressed to the users with a program regarding security, 30% up to 60% of the users could become without doubt victims of a malformed email, while after a six-month to one-year training period this percentage can be diminished to 5%.

Additionally, in this chapter some noteworthy examples with applications that habituate game elements will be presented.

Game of threats [15] is an application example regarding security awareness with the use of gamification. The PwC company created a digital application, which was designed in order to simulate the speed and complexness of an authentic cyber-attack. The procedure of the solution lets in game elements in order to endow users with an interactive experience. The environment of the application creates a factual experience for the users. It was designed to remunerate the users who make the finest critical decisions, while it punishes the users who arrive to wrong conclusions. The application assists users to comprehend more beneficially the steps that they require to trail towards a more improved security environment of their company.



Game of Threats (Cyber Security Awareness)

Acme Corp.'s decision to deploy a Malware Reverse Engineering defense stopped the Nation State's ongoing Ransomware attack

Number of Ongoing Attacks: 3

Acme Corp. Customer - 8:31 am
What is Acme Corp. doing?! Keep my private information PRIVATE! #cyber_insecurity

Main Street Journal - 8:30 am
Acme Corp. Takes Financial Hit from System Shutdown and Replacement Costs

The Magazine - 8:29 am
Acme Corp. E-Commerce Site Brought Offline by Hackers

Main Street Journal - 8:27 am
Acme Corp. Bolsters Security Posture with Monitoring Tool

The Company's decision resolves the ongoing 'Ransomware' attack, which leaves three active attacks. However, the Company is still yet to diagnose two of the three remaining attacks.

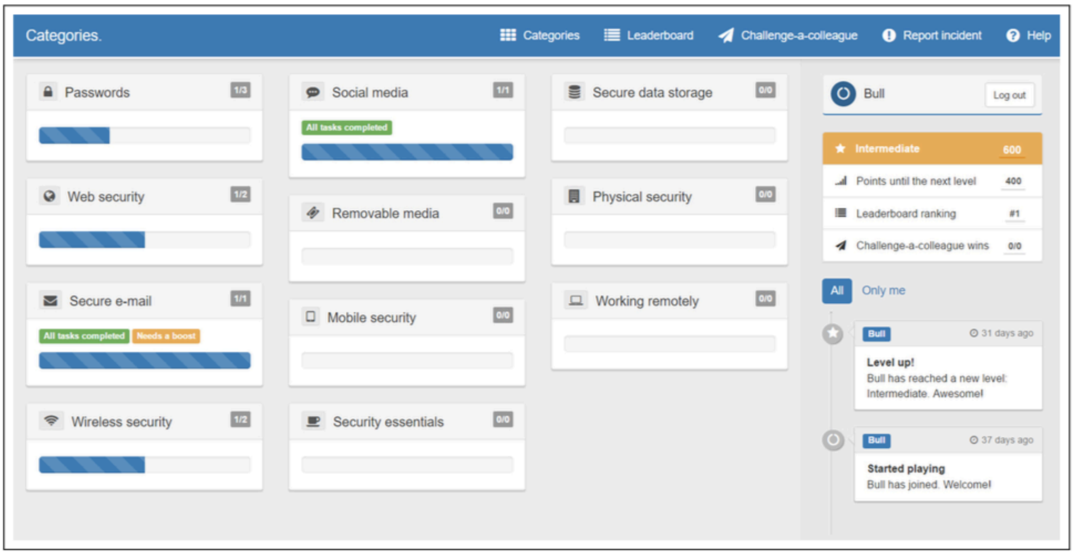
PwC

June 2016
18

Figure 10: Game of threats, available at https://slideplayer.com/slide/10788466/

Cyber Security Challenge UK [16] company created a series of national competitions as well educational programs designed to inspire more persons to turn professionals in the cyber security field. These competitions were designed for a range of ages of the people who participate.

An example of an application that employs game elements targeting security awareness was developed [13]. This application is contributed from several categories relevant to security such as passwords, security in web and so on and so forth. The user is rendered free to opt for a category and respond to all relevant questions. Depending on their right or wrong answers points are collected. They are also able to adjust their level replying to more tricky questions. Furthermore, the user bears the right to spot the users that stand at the same level as they are while they can also invite other users to compete with them. A program employing game elements contains more possibilities of use than an undemanding program does.



Intermediate 600

Points until the next level 400

Leaderboard ranking #1

Challenge-a-colleague wins 0/0

Bull 31 days ago

Level up!
Bull has reached a new level: Intermediate. Awesome!

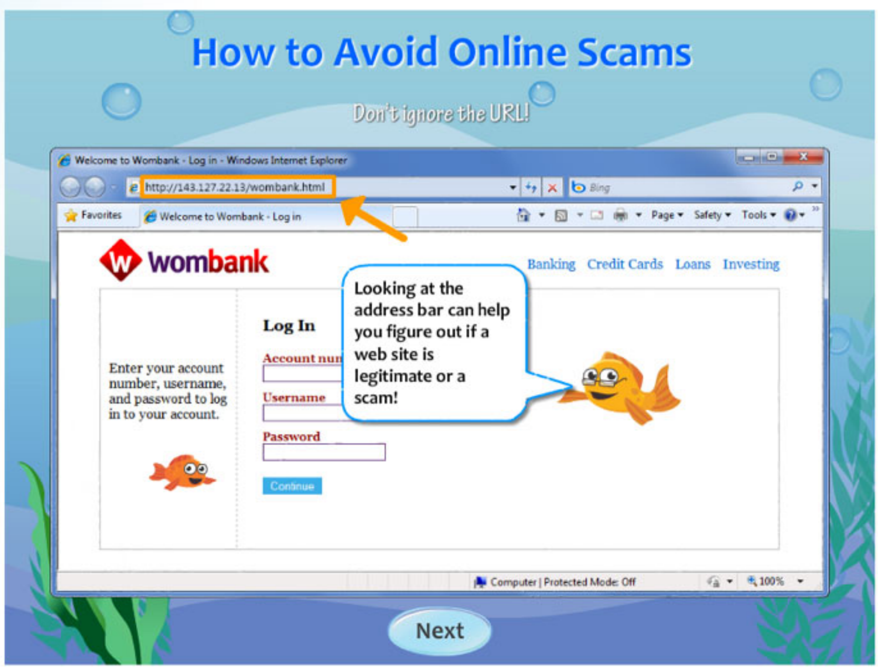
Bull 37 days ago

Started playing
Bull has joined. Welcome!

Figure 11: A Gamified Security Awareness and Training Program, Gjertsen B Eyvind Garder, 2016, Use of Gamification in Security Awareness and Training Programs, Norwegian University of Science and Technology

Wombat Security company [17] has equipped us with another noteworthy example of application regarding security awareness training courses. Security Awareness Training Modules heavily targets the training of employees in order for them to be rightfully equipped with the exact approach towards addressing security dangers. The game rudiments and their incorporated techniques significantly improve users' knowledge heartening them towards an affirmative behavioural transformation through the decisions that they need to take.

Furthermore, Anti-phishing Phil [18] was developed by CMU Usable Privacy and Security Laboratory in Carnegie Mellon University accepting as a sole purpose the schooling of the users regarding malformed web pages.



How to Avoid Online Scams

Don't ignore the URL!

Enter your account number, username, and password to log in to your account.

Looking at the address bar can help you figure out if a web site is legitimate or a scam!

Welcome to Wombank - Log in - Windows Internet Explorer
http://143.127.22.13/wombank.html
Favorites
Welcome to Wombank - Log in
Page
Safety
Tools
wombank
Banking
Credit Cards
Loans
Investing
Log In
Account nur
Username
Password
Continue
Computer | Protected Mode: Off
100%
Next

Figure 12: Anti-Physing Phil available at https://www.helpnetsecurity.com/2013/02/08/learn-by-doing-phishing-and-other-online-tests/

5 Developed project

In this chapter, the developed mobile application is going to be thoroughly presented and described in detail.

5.1 Introduction

iOS is a mobile operating system created and developed by Apple Inc for its hardware devices. The iPhone entered into the market in 2007, since then Apple has greatly changed the mobile device market and to some extent, has caused the emergence of new operating systems for mobile platforms. In November 2007, Google announced the creation of the Android operating system. With the launch of Google's operating system, the smartphone market has full-fledged appreciably. This has led consumers to develop into becoming fully acquainted with diverse operating systems and manufacturers. Telecommunications companies embarked into advertising the benefits of each operating system, as well. Nowadays, all new operating systems are accompanied by their own application development software, so anyone who wishes to deal with and expand applications regarding a certain operating system is offered the possibility to perform so.

iOS was originally developed for iPhone devices only. Later, however, it was expanded to support other Apple mobile devices such as iPod Touch, iPad and Apple TV. Unlike Microsoft's Windows Phone and Google Android, Apple does not license the installation of iOS software on non-Apple devices.

Its user interface is founded on direct user interaction with the touch screen of the device. The controls that make up the graphic environment are basically switches, buttons and sliders. For example, the user through the multi-touch touchscreen can exercise various finger movements and obtain instantaneous results on the screen.

Focusing on a text page is enabled by enlarging it through widening the index and the thumb fingers or photos can be changed with a simple finger movement from right to left. This straightforward way of use has enabled the operating system to stand out from the competition, especially at the time it was introduced in early 2007. It is based on the operating system Mac OS X which is based on UNIX.

By altering the way that mobile platforms and mobile devices perform, new operating systems have been introduced in recent years, one of the most vital effects they have accomplished is creating through them many innovative and imposing applications for such systems. Mobile platform applications are a core ingredient of the global mobile market that grows rapidly year by year. They are consisted of software that runs on a mobile platform performing explicit functions for their users. These mobile applications are used in a variety of mobile phone models, even at low cost devices that can be found on the market. Almost all new operating systems can be fully and legally obtained by means of downloading them from specific online application stores. Their widespread use is due to the countless functions they can perform, including simple user environments for basic telephony and messaging services, advanced services such as video games, multimedia applications and much more. There are loads of categories of such applications in existence. Applications such as those that are used to send and receive SMS / MMS, applications as web browsers and media players such as mp3 players are installed in the device operating systems while the rest can be installed after the device is purchased. For example, any user can download applications over a wireless network installing them on their devices themselves or, alternatively, they can download and install apps from the online store that comes with the operating system.

Applications can be divided in a technical point of view into categories depending on the programming environment they are running:

- Applications running on an operating system environment such as applications running on iOS, Android, Symbian OS, Windows Phone and Blackberry OS
- Applications running on an Internet browsing environment such as Webkit, Mozilla Firefox, Opera Mini, and RIM
- Other platforms and virtual systems such as Java / J2ME, BREW, Flash Lite and Silverlight

They can also be separated according to their mobile platform functions:

- Communications applications such as email, messaging, web browsing, information, and social networks

- Derivative applications such as calculators, calendars, reminders, notes, word processing, spreadsheets, GPS services and banking services
- Multimedia applications such as audio playback, audio and video data, graphics and video, video playback and presentation
- Game applications such as strategy, decks and casinos, action and adventure, puzzles, sports and hobbies.

In recent years, mobile platform applications have been greatly evolved to the point of extending a copious and high-speed experience to any user. In this context, such applications boast dissimilar features than navigating on mobile web sites does, where users still experience access tribulations and low speeds on their mobile network.

5.2 Motivation

The motivation of this dissertation was the development of a modern and functional iOS application that could be effortlessly parameterized and ready to be adapted by various projects.

In recent years more and more business companies and corporate organizations invest in digital protection directed towards security issues and the most fundamental action that they choose to take is to endow their employees with knowledge regarding this topic.

Regrettably, most of the existing programs do not grapple to raise the interest of the users so they keep on trying and making superfluous efforts in order for their human resources to acquire more cognition so as to develop into a better workforce. As it was mentioned in the previous chapters, gamification is, indeed, a smart way to trigger and keep the interest of the users alive.

By and large, one of the goals of this dissertation was to develop a prototype application that would implement several game elements and endeavor to convert the experience of the users into a more engaging one. Hopefully, through this application their awareness regarding security can be heightened.

One of the most central goals of this dissertation was also to deal with iOS development and go through what any user can experience. It was challenging enough to ascertain all the technologies that should be combined in order to fabricate a concluding product for the users.

Native code implementation was an undemanding resolution to follow and the chief motive was to ensure that all the iOS characteristics would be taken full advantage of and by extension to the users. Moreover, native code is deemed faster than the cross-platform one. When developing on a native programming language, complete access to the features of the device is gained.

5.3 Basic functionality

The basic functionality of the application will be presented at this part.

The users see the icon of the application called **SecureIT**.

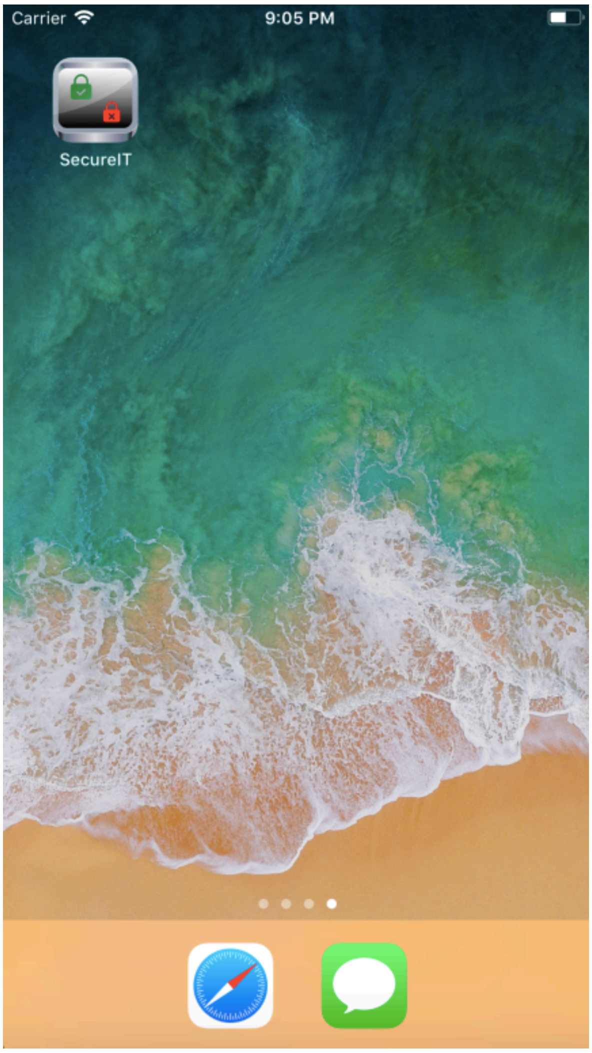


Figure 13: Application icon of SecureIT

The users tap on the application icon and observe the *launching screen* while the application is being loaded.

Figure 14: Launching screen of SecureIT

When the application has loaded, the users are able to observe the *Welcome* page of SecureIT. There, they may distinguish the two options that exist:

1. Register
2. Log in

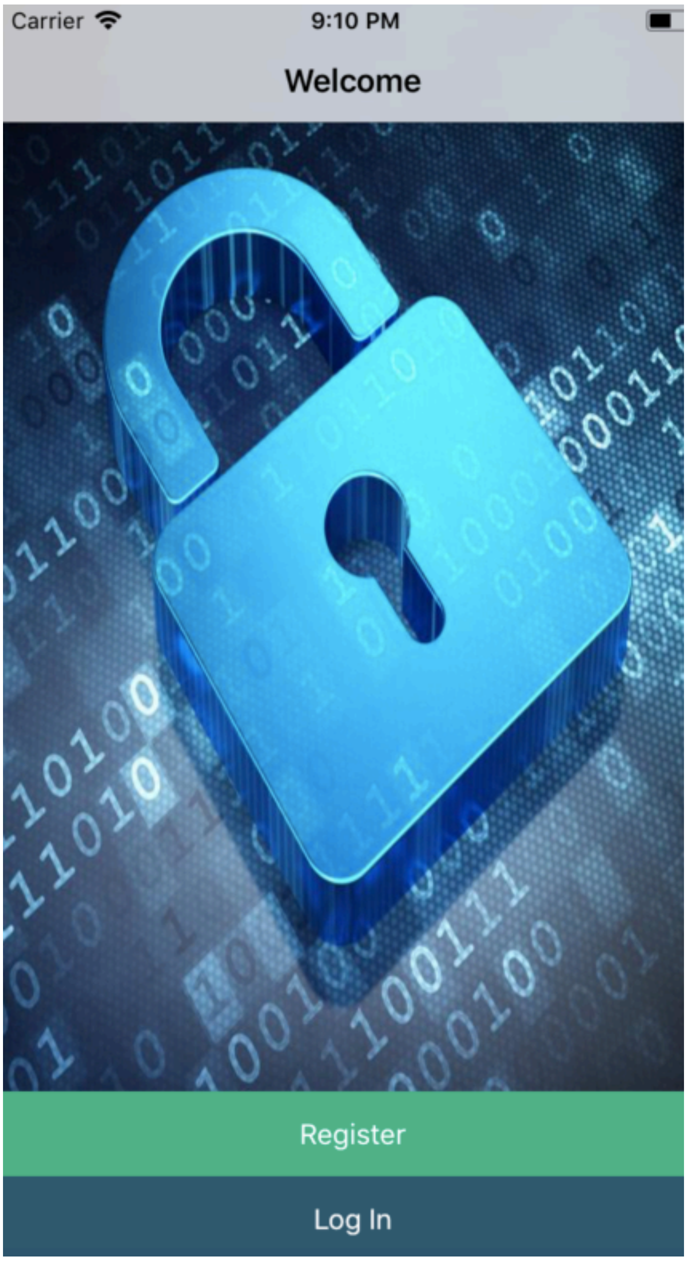


Figure 15: Welcome page of SecureIT

Firstly, the users have to register into the application.

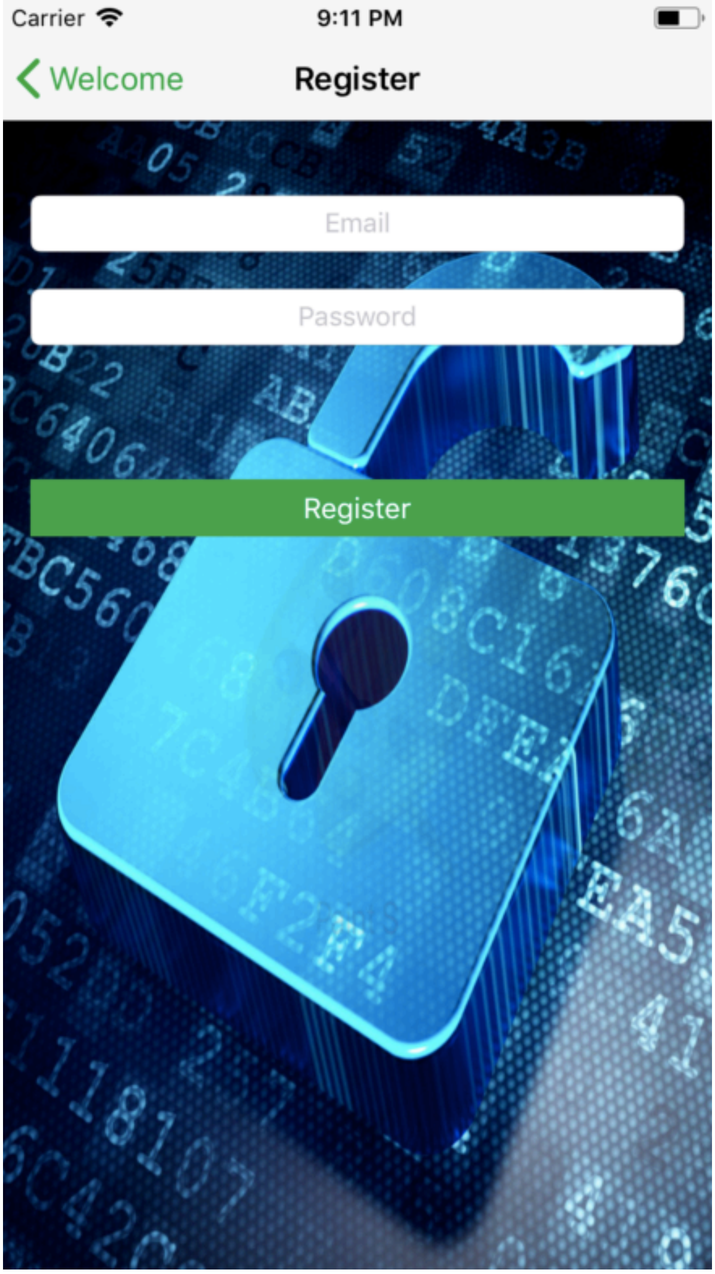
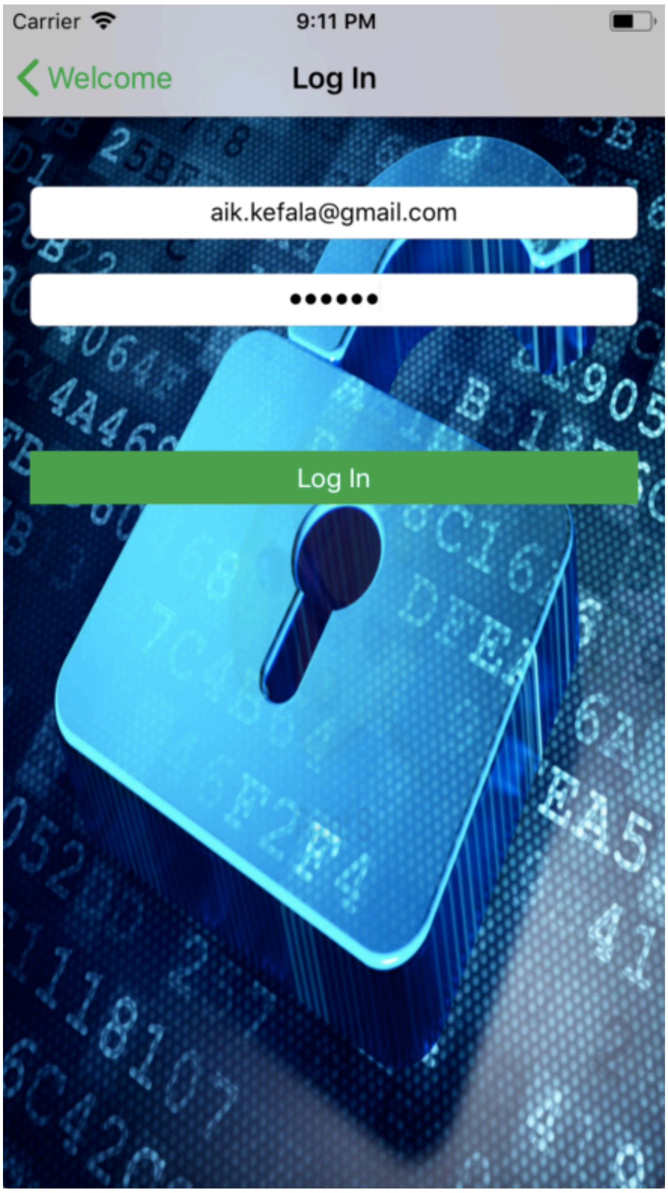


Figure 15: Register page of SecureIT

If the users are already registered, they can select the *Log in* button. For the password in both *Register* and *Log In* screens there is a secure text entry that has to be filled in.

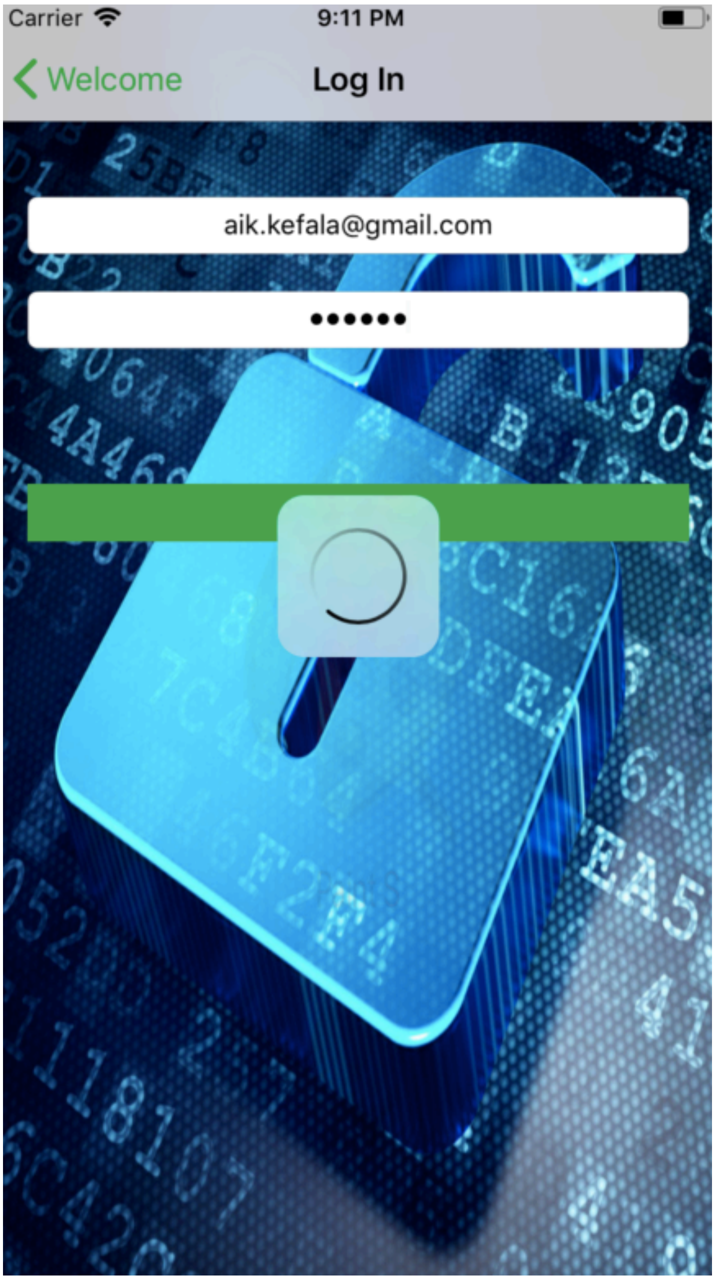


aik.kefala@gmail.com

••••••

Figure 16: Log In page of SecureIT

When the users press the *Log In* button or the *Register* button, a loading icon appears.



aik.kefala@gmail.com

••••••

Figure 17: Loading page of SecureIT after Log In pressed

After the registration or the log in process on the part of the user, they are led to the main page of the application. At this page they are able to select the *level* that they wish to launch:

1. Level 1
2. Level 2
3. Level 3

Or they may select the *Leaderboard* button in order to see the leaderboard of all the players of the application in detail.

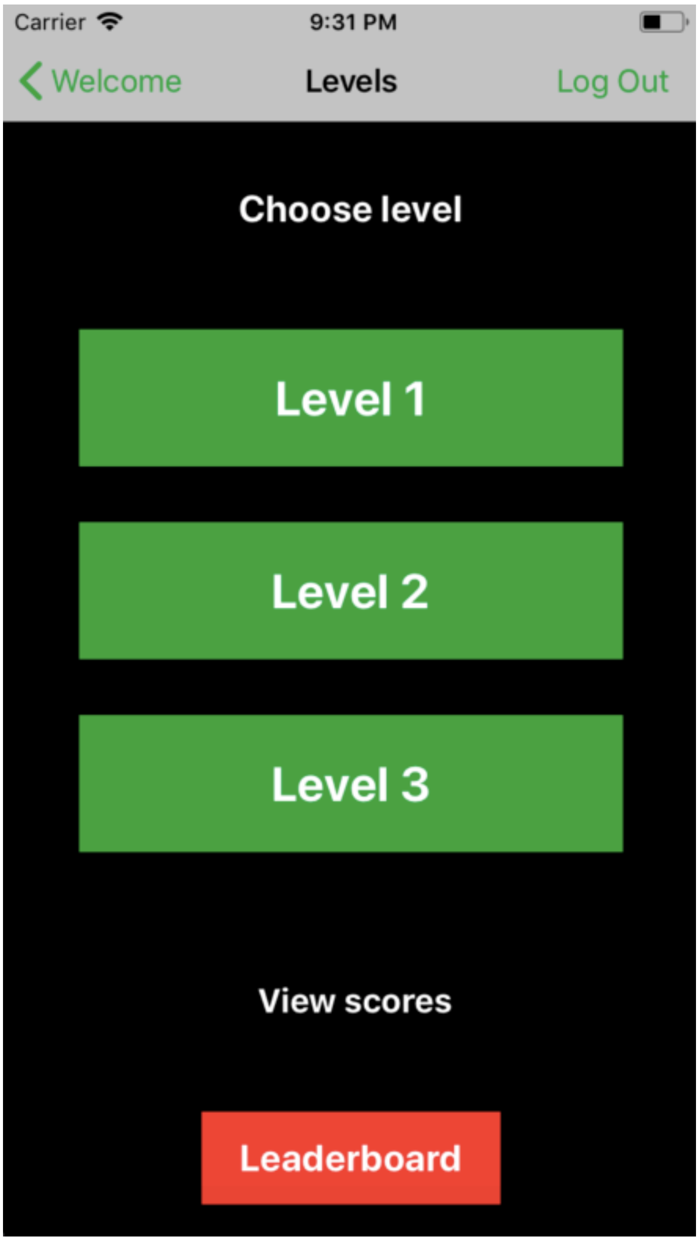
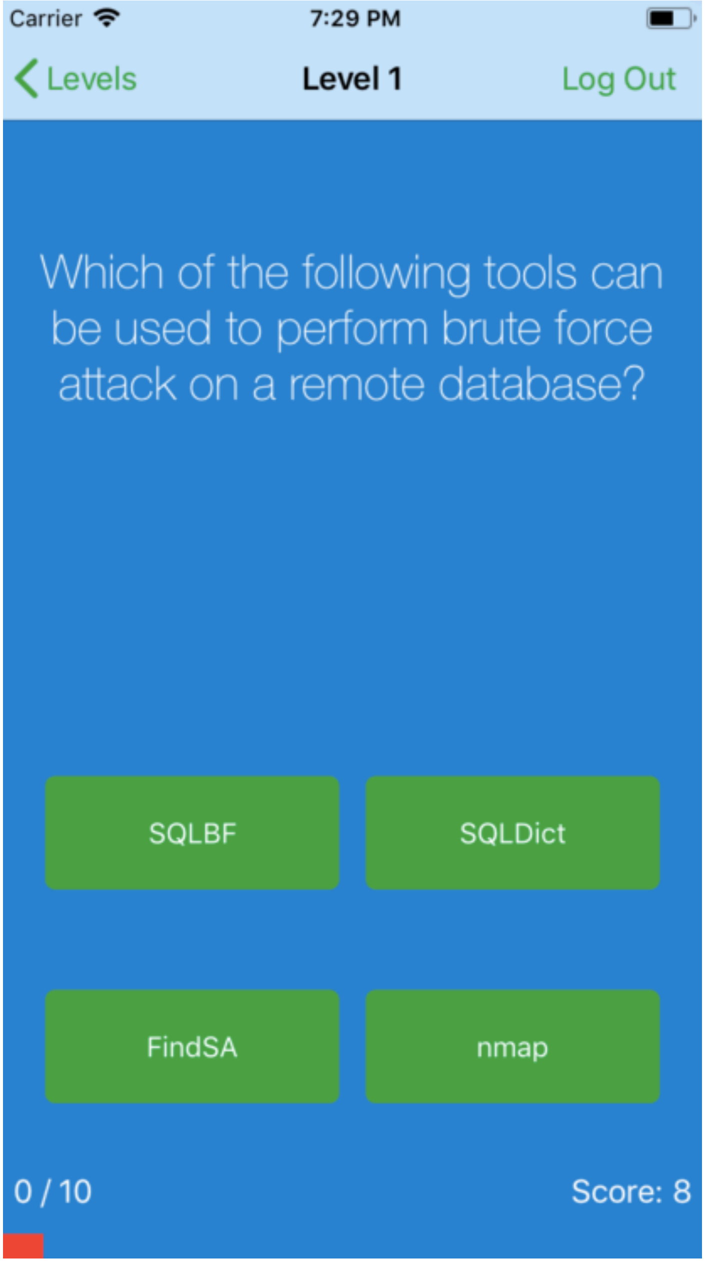


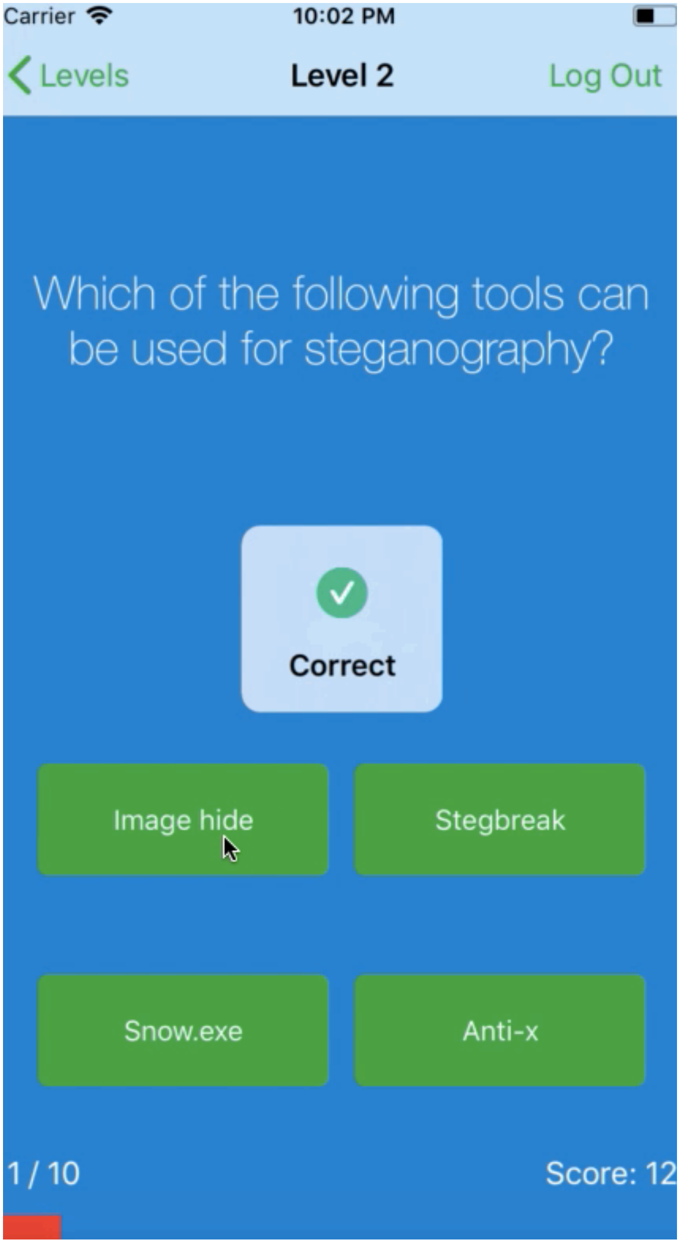
Figure 18: Main page of SecureIT

Each level of the application leads to another set of questions that the users have to respond. The second level is more complicated than the first one while the third one is even more intricate than the second one. For each correct answer the users earn one point at the first level, two points at the second and three at the third. Not only are they able to notice their score live but the number of answers that they have already produced as well. After every one answer is specified, immediate feedback for all correct or wrong responses is visually provided. Each level consists of 10 questions with 4 possible correct answers. When the users complete the level, they have the right to start over at that level.



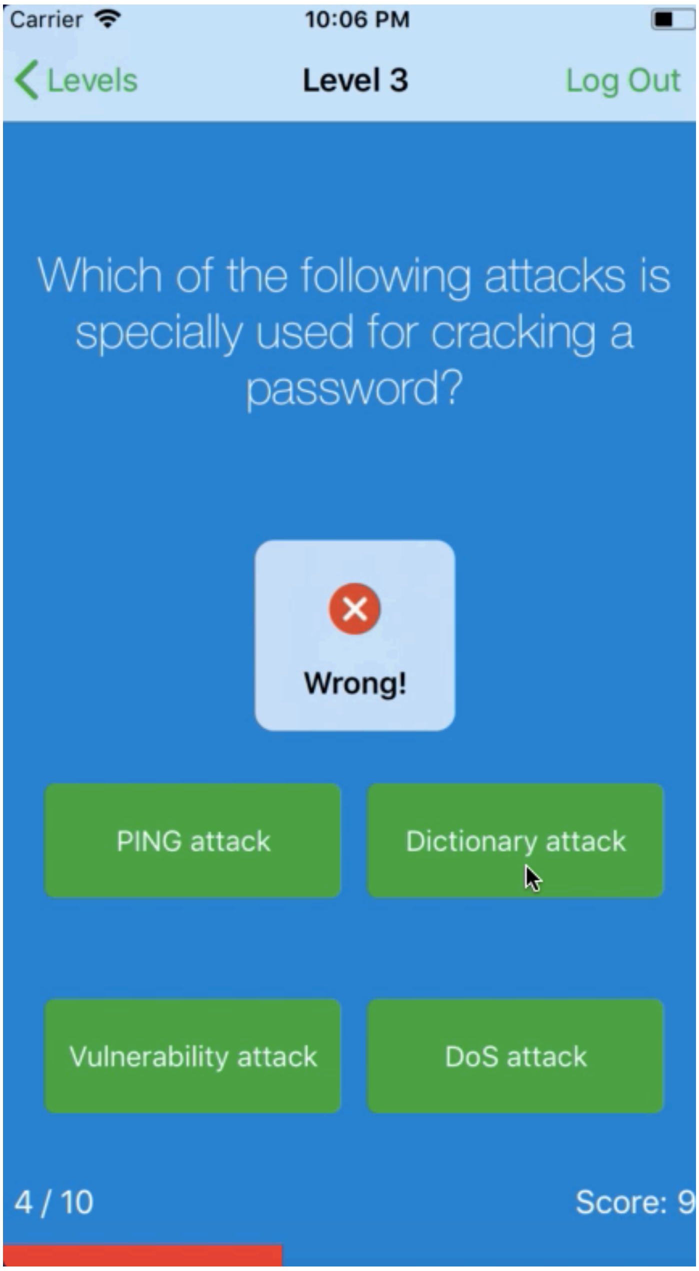
Which of the following tools can be used to perform brute force attack on a remote database?

Figure 19: Level 1 page of SecureIT



Which of the following tools can be used for steganography?

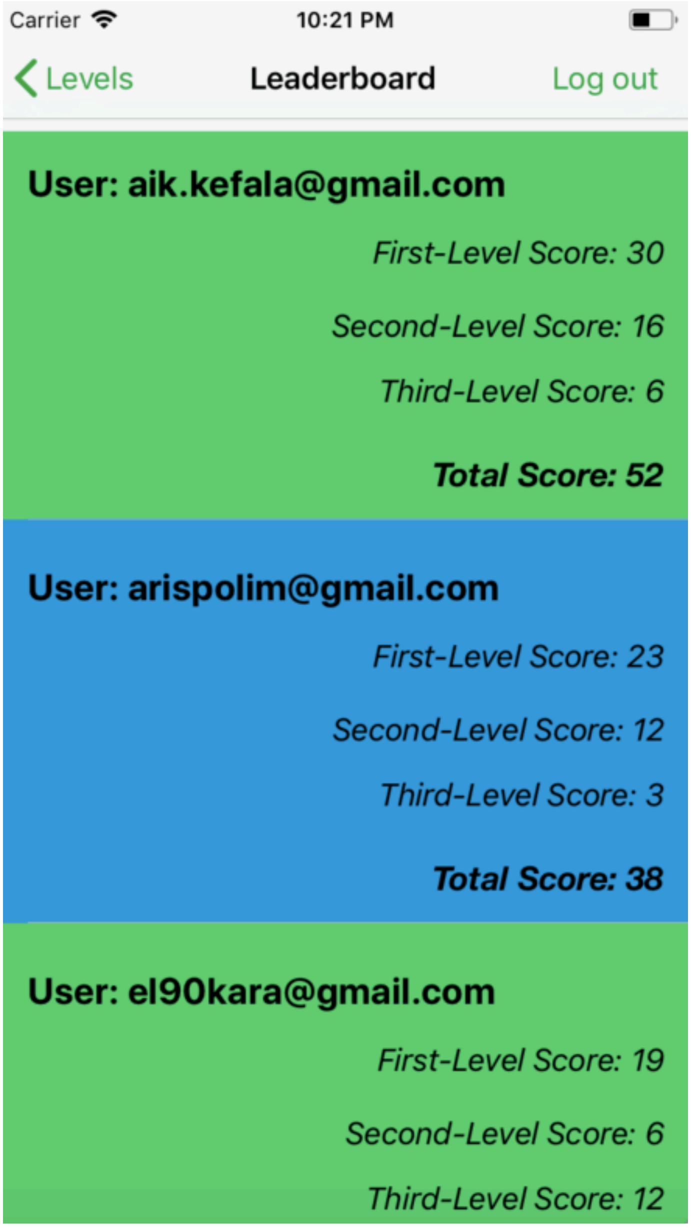
Figure 20: Feedback for correct answer at Level 2 page of SecureIT



Which of the following attacks is specially used for cracking a password?

Figure 20: Feedback for wrong answer at Level 3 page of SecureIT

On the leaderboard page the users can observe all the analytical scores of all players categorized by each level and in a descending order depending on the total score from the sum of all levels.



User: aik.kefala@gmail.com

First-Level Score: 30

Second-Level Score: 16

Third-Level Score: 6

Total Score: 52

User: arispolim@gmail.com

First-Level Score: 23

Second-Level Score: 12

Third-Level Score: 3

Total Score: 38

User: el90kara@gmail.com

First-Level Score: 19

Second-Level Score: 6

Third-Level Score: 12

Figure 21: All users' scores at Leaderboard page of SecureIT

In all screens the users can exercise the right to *Log Out* from the application and return to the initial *Welcome* page.

5.4 Architecture and Technologies used

In this chapter, the information of the project and its parameters will be clearly presented and thoroughly analyzed.

For the implementation of this application **Xcode IDE**, **Firebase Database** and the **Swift** programming language were used.

5.4.1 Xcode

The *Xcode* application development software was developed by Apple, so as to present developers with the prospect to set their undertakings in action. Developers hold the capacity to construct applications testing them in an emulator called *iPhone Simulator*. In order to install an application on a factual device as well as to sell it through the App Store, every developer must be enrolled in the Apple iPhone developer program at a cost of 99 Euros per year. Xcode both includes the iPhone Simulator and the iPad Simulator, a program that the developer could possibly utilize in order to simulate how applications would appear and how they would function if they were running on the iPhone or iPad.

Figure 22: Xcode available at https://developer.apple.com/xcode/

The most significant tools extended by Xcode are:

1. Source Editor
2. Asset Catalog
3. Simulator
4. Interface Builder

Source Editor is a professional editor with syntax highlighting warnings and errors regarding coding.

Asset Catalog is the place where all the photos of the application are stored and grouped.

Simulator is actually an iconic iPhone with which the application may run in various versions of iPhone.

Interface Builder is where the whole design of the application is implemented with an assortment of multiple choices.

5.4.2 Swift Programming Language

The programming language that was widely used in the past was *Objective-C*, which is an object-oriented programming language based on C. It was the fundamental programming language used to expand applications in iOS and OS X operating systems. Since it is an object-oriented programming language, it makes use of objects, classes, inheritance, and other object-oriented language features. There likelihood is also offered of utilizing libraries in C, as it is a superset of the programming language C.

Swift is the following programming language developed by Apple. Its purpose was to replace Objective-C with Swift that was created in order to design applications for iOS, OS X and Watch OS and was released in 2014. Apple sought to get less complicated programming elements reminiscent of Python to manufacture a language which is more prosperous to handle. It is designed to work with the Cocoa and Cocoa Touch frameworks as well as with Objective-C code. Apple claims that Swift is a more dependable programming language, as well as more comprehensive. It is built with the LLVM framework compiler and allows the use of Objective-C, C, C++ and Swift, in the equivalent program.

Figure 23: Swift Programming Language available at https://developer.apple.com/swift/

5.4.3 Firebase Database

Firebase is a cloud hosted NoSQL database acquired by Google in 2014 that stores data in JSON format. For this application the Firebase Realtime Database has been selected as data can be stored and synced in real time.

Firebase tenders any handling of users in a rapid and secure manner. There are multiple modes that the users can be authenticated, like email, Google and Facebook accounts to name but a few. The user passwords are saved encrypted and are humanly impossible to be revealed.

Analytics about the applications can also be provided, so that it becomes easy for daily active users to monitor the route of their application usage.

Figure 24: Firebase Realtime Database available at https://cloud.google.com/storage-options/

5.5 Project set-up

In the fifth part of this chapter, the project set-up is to be entirely demonstrated.

5.5.1 Model – View – Controller (MVC)

To begin with, **Model-View-Controller** pattern was used for the implementation of this application.

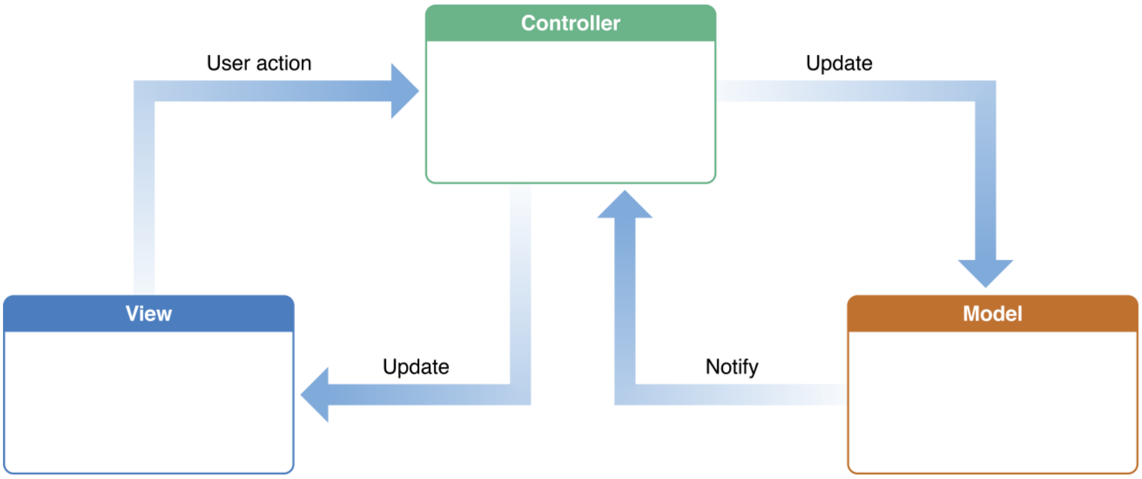


Figure 25: Model – View – Controller pattern connection available at https://developer.apple.com/library/archive/documentation/General/Conceptual/DevPedia-CocoaCore/MVC.html

Model – View – Controller is an architectural pattern that is broadly used for applications including three parts connected with each other.

Model is responsible for handling the application data and is largely independent on the user interface.

View is the component that represents the information of the application; it interacts directly with the user as it is data self-regulating.

Controller is the liaison between the view and the model. Its core function is to collect feedback from the users. It then decides what to do with it constructing the corresponding interactions by forwarding the transactions to the model and then updating the information in view.

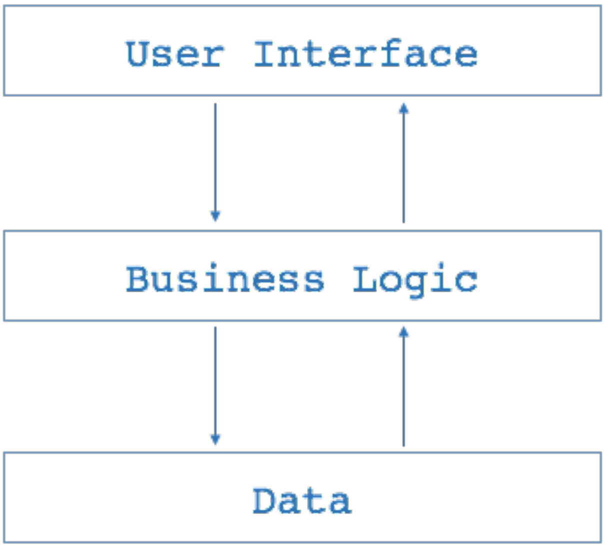


Figure 26: Model – View – Controller, Layered Application Architecture available at https://medium.com/ios-os-x-development/modern-mvc-39042a9097ca

5.5.2 Realtime Database set-up

In Firebase the *Realtime Database* was selected so that the application could read and write data in an JSON format.

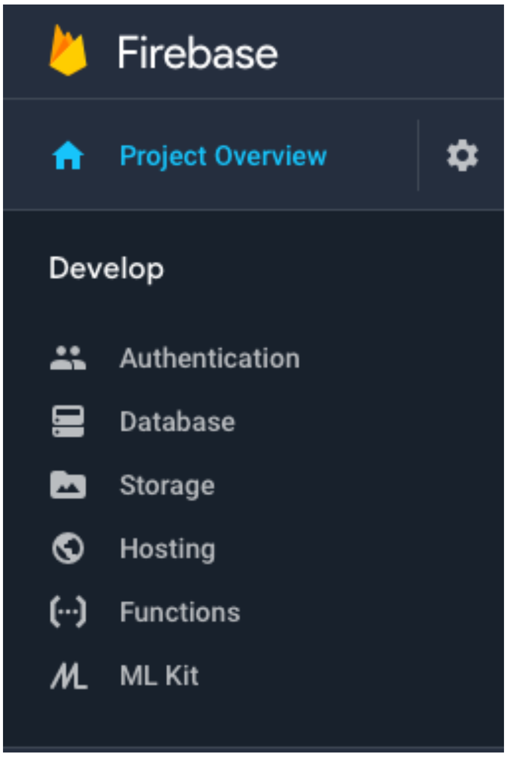
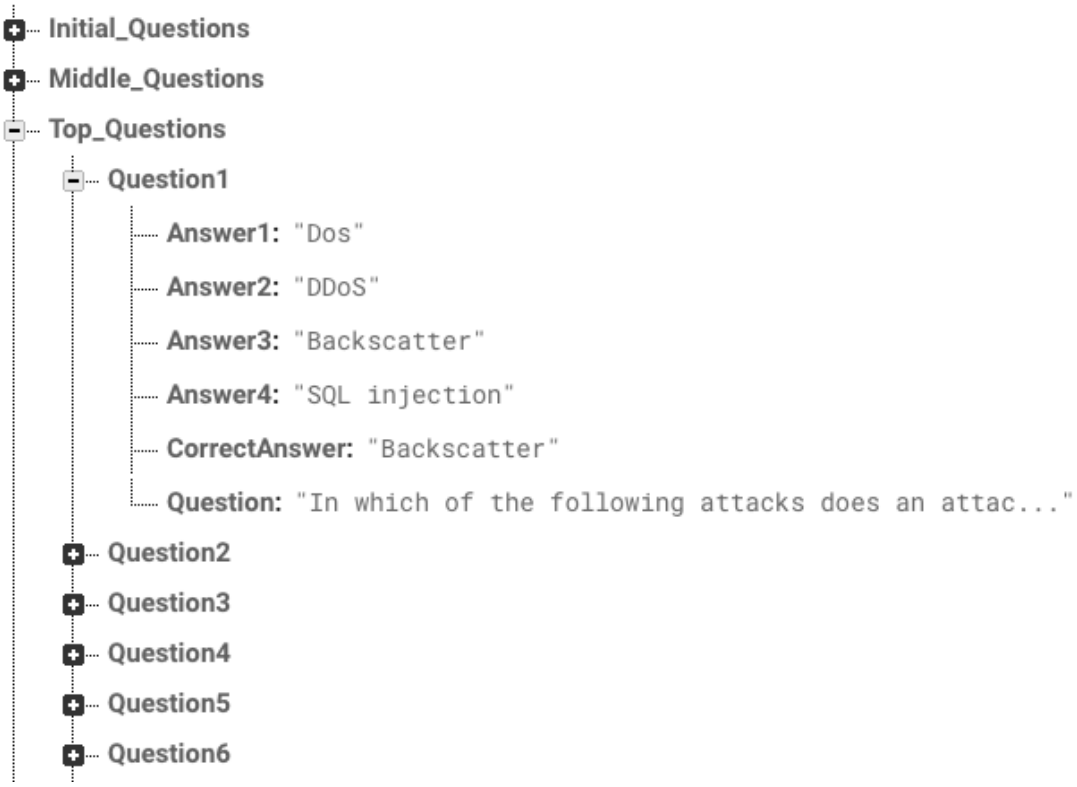


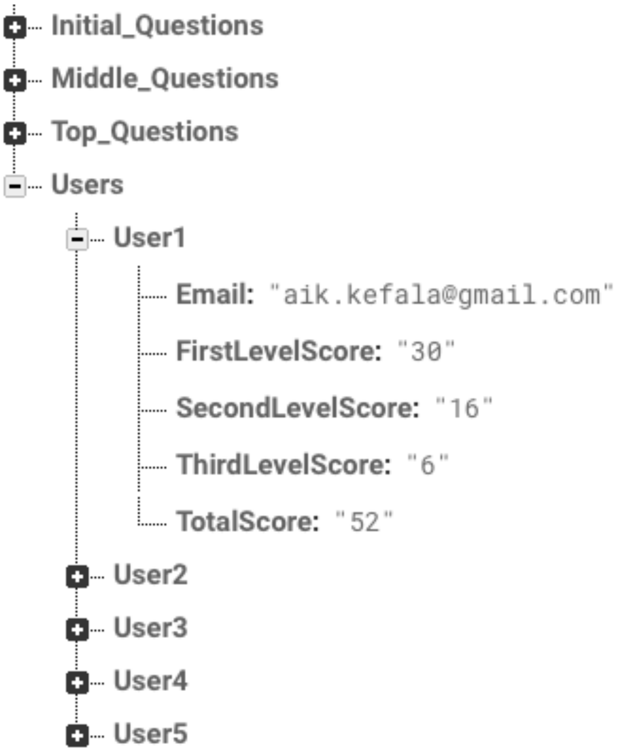
Figure 27: Firebase menu of SecureIT

The questions and answers of the application for all three levels are stored in the database, as well as the users' emails, and their analytical scores for each level. For the users' authentication the email method is preferred.



```
Initial_Questions
Middle_Questions
Top_Questions
    Question1
        Answer1: "Dos"
        Answer2: "DDoS"
        Answer3: "Backscatter"
        Answer4: "SQL injection"
        CorrectAnswer: "Backscatter"
        Question: "In which of the following attacks does an attac..."
    Question2
    Question3
    Question4
    Question5
    Question6
```

Figure 28: Firebase questions' data in JSON format for SecureIT



```
Initial_Questions
Middle_Questions
Top_Questions
Users
    User1
        Email: "aik.kefala@gmail.com"
        FirstLevelScore: "30"
        SecondLevelScore: "16"
        ThirdLevelScore: "6"
        TotalScore: "52"
    User2
    User3
    User4
    User5
```

Figure 29: Firebase users' score data in JSON format for SecureIT

5.5.3 Xcode set-up

On the left side of Xcode the basic MVC structure of the application can be distinctly observed.

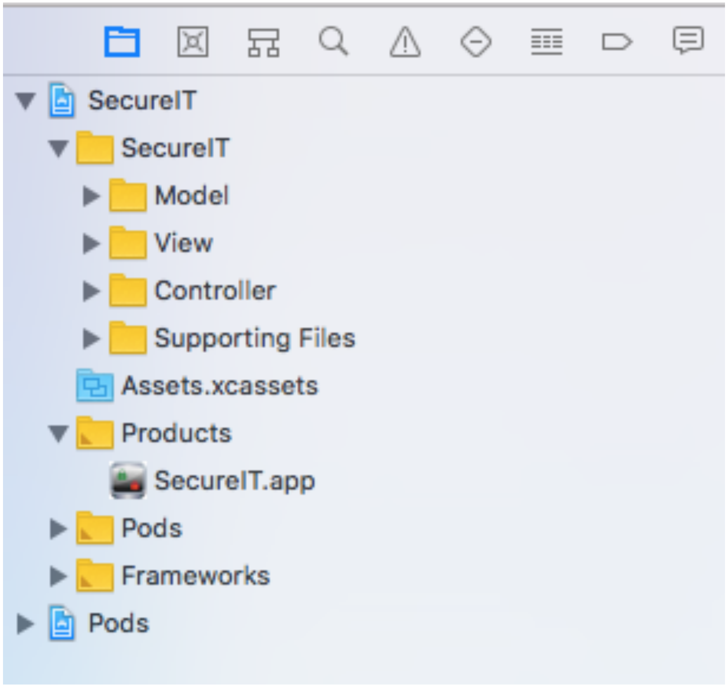
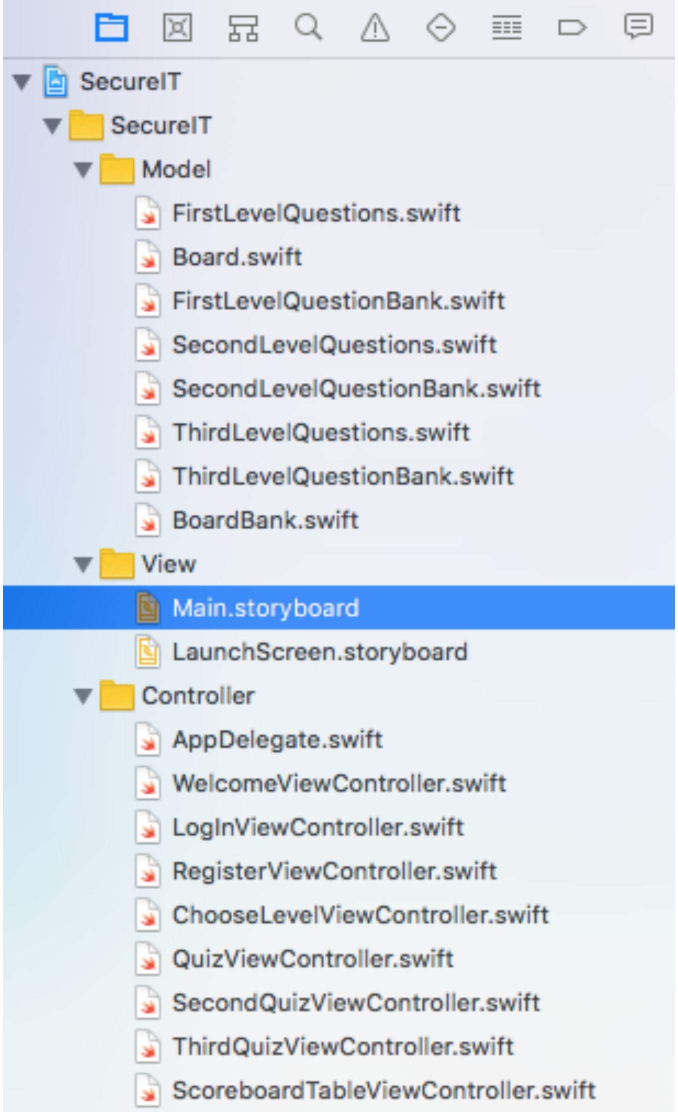


Figure 30: MVC Structure of SecureIT

If the files are extended, all the details contained inside each file can be carefully noticed.



```
▼ SecureIT
  ▼ SecureIT
    ▼ Model
        FirstLevelQuestions.swift
        Board.swift
        FirstLevelQuestionBank.swift
        SecondLevelQuestions.swift
        SecondLevelQuestionBank.swift
        ThirdLevelQuestions.swift
        ThirdLevelQuestionBank.swift
        BoardBank.swift
    ▼ View
        Main.storyboard
        LaunchScreen.storyboard
    ▼ Controller
        AppDelegate.swift
        WelcomeViewController.swift
        LogInViewController.swift
        RegisterViewController.swift
        ChooseLevelViewController.swift
        QuizViewController.swift
        SecondQuizViewController.swift
        ThirdQuizViewController.swift
        ScoreboardTableViewController.swift
```

Figure 31: MVC files of SecureIT

At *Main.storyboard* the design of the application with all the screens can be discovered.

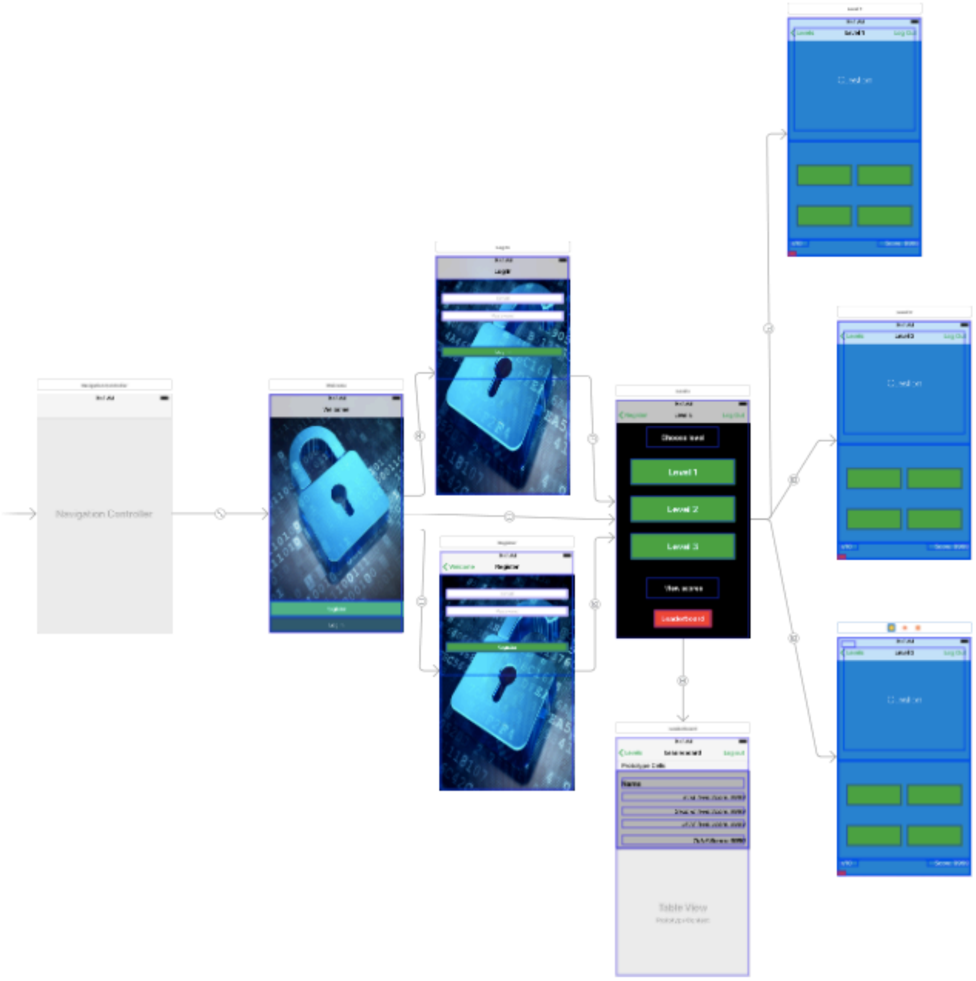
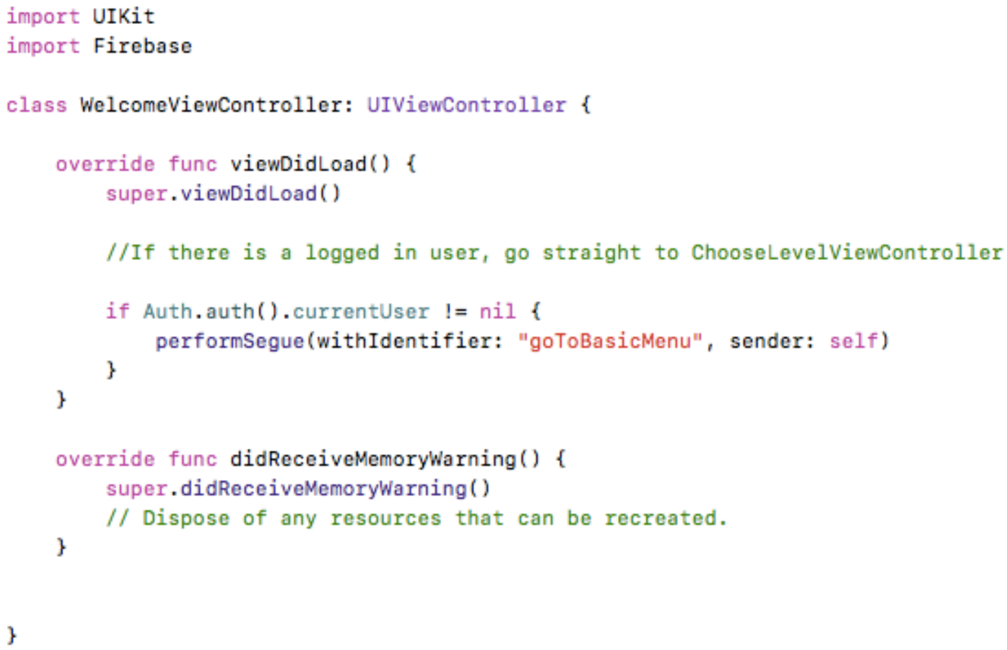


Figure 32: MVC files of SecureIT

Several examples of code are going to follow:

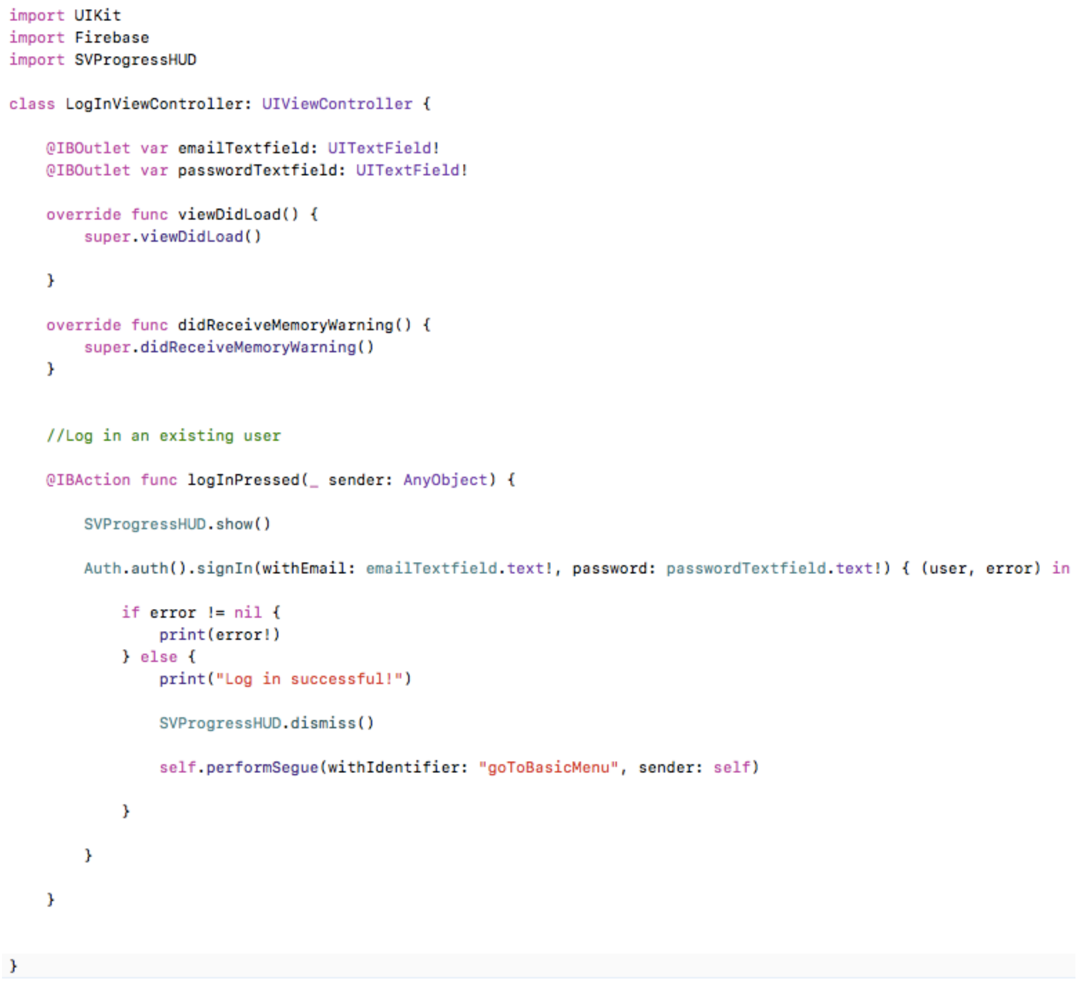
In the next screen the swift code regarding *Welcome* screen is available, where the Firebase is imported in order to use its data and actually move directly to *ChooseLevelViewController* if the user is already logged in.



```swift
import UIKit
import Firebase

class WelcomeViewController: UIViewController {

    override func viewDidLoad() {
        super.viewDidLoad()

        //If there is a logged in user, go straight to ChooseLevelViewController

        if Auth.auth().currentUser != nil {
            performSegue(withIdentifier: "goToBasicMenu", sender: self)
        }
    }

    override func didReceiveMemoryWarning() {
        super.didReceiveMemoryWarning()
        // Dispose of any resources that can be recreated.
    }


}
```

Figure 33 : ChooseLevelViewController of SecureIT

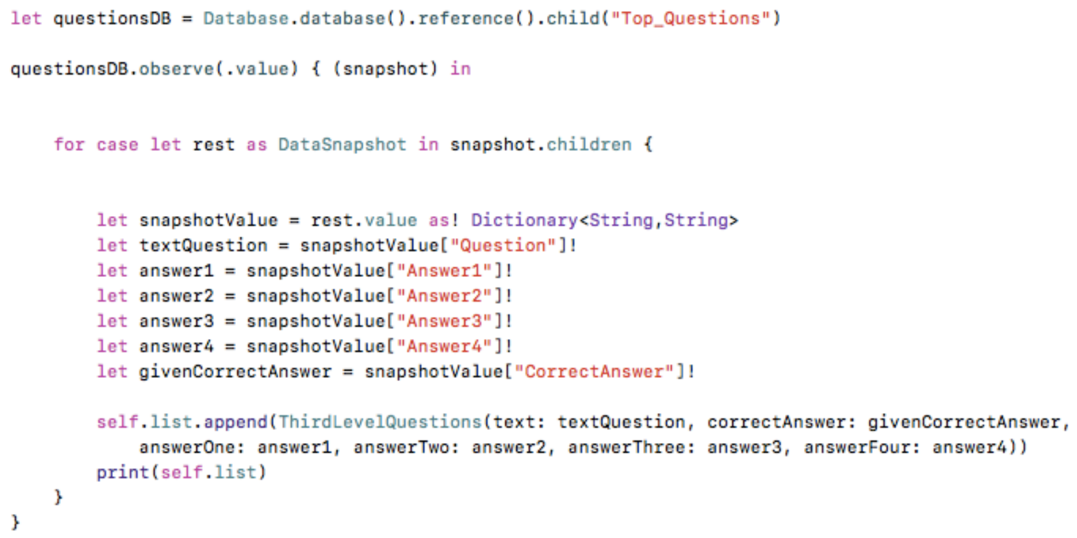
Login authentication of the user should take place at *LogInViewController* and use of *SVProgressHUD* while the authentication process is underway, and the screen is loading.



```
import UIKit
import Firebase
import SVProgressHUD

class LogInViewController: UIViewController {

    @IBOutlet var emailTextfield: UITextField!
    @IBOutlet var passwordTextfield: UITextField!

    override func viewDidLoad() {
        super.viewDidLoad()

    }

    override func didReceiveMemoryWarning() {
        super.didReceiveMemoryWarning()
    }


    //Log in an existing user

    @IBAction func logInPressed(_ sender: AnyObject) {

        SVProgressHUD.show()

        Auth.auth().signIn(withEmail: emailTextfield.text!, password: passwordTextfield.text!) { (user, error) in

            if error != nil {
                print(error!)
            } else {
                print("Log in successful!")

                SVProgressHUD.dismiss()

                self.performSegue(withIdentifier: "goToBasicMenu", sender: self)

            }

        }

    }


}
```

Figure 34 : LogInlViewController of SecureIT

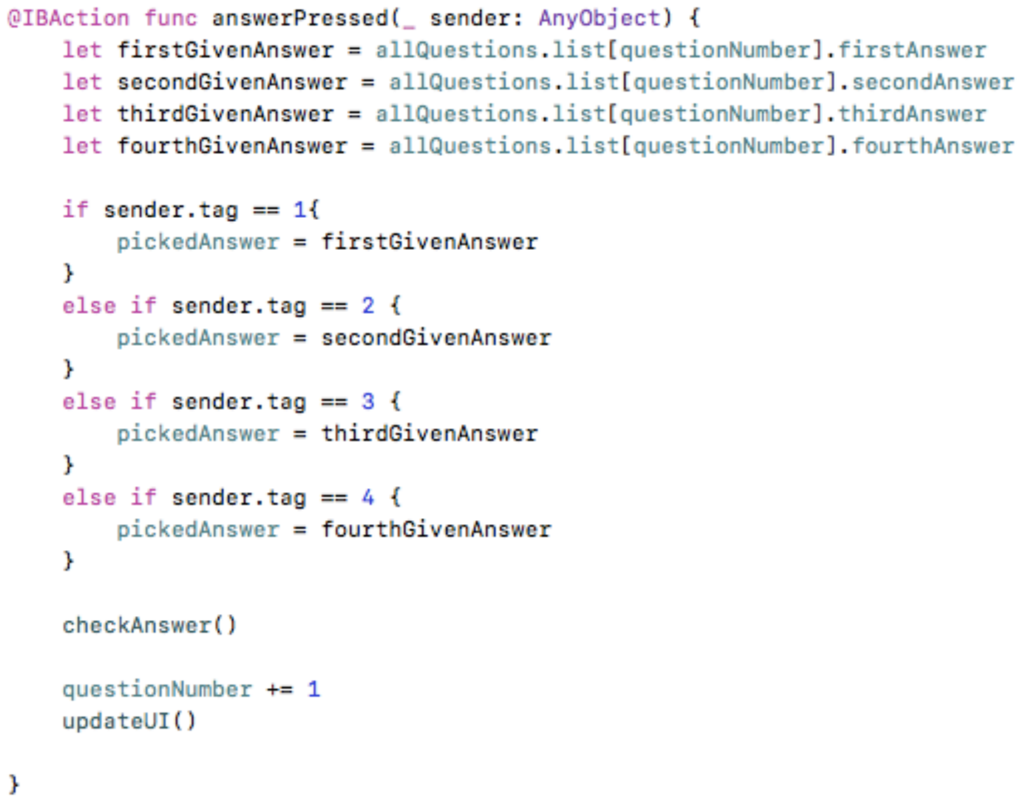
In model *ThirdLevelQuestionBank* users can read data of *Firebase* and update the list with the questions and answers for the Level three of the application and finally they hold the ability to print them.



```
let questionsDB = Database.database().reference().child("Top_Questions")

questionsDB.observe(.value) { (snapshot) in


    for case let rest as DataSnapshot in snapshot.children {


        let snapshotValue = rest.value as! Dictionary<String,String>
        let textQuestion = snapshotValue["Question"]!
        let answer1 = snapshotValue["Answer1"]!
        let answer2 = snapshotValue["Answer2"]!
        let answer3 = snapshotValue["Answer3"]!
        let answer4 = snapshotValue["Answer4"]!
        let givenCorrectAnswer = snapshotValue["CorrectAnswer"]!

        self.list.append(ThirdLevelQuestions(text: textQuestion, correctAnswer: givenCorrectAnswer,
            answerOne: answer1, answerTwo: answer2, answerThree: answer3, answerFour: answer4))
        print(self.list)
    }
}
```

Figure 35 : ThirdLevelQuestionBank of SecureIT

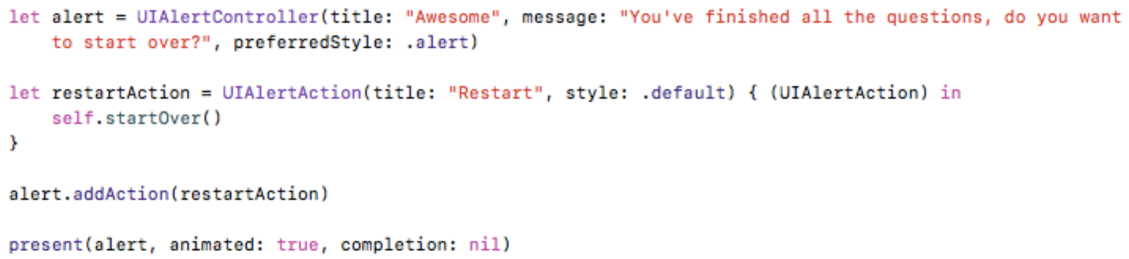
Check the user’s answer and update the user interface by showing the next question.



```
@IBAction func answerPressed(_ sender: AnyObject) {
    let firstGivenAnswer = allQuestions.list[questionNumber].firstAnswer
    let secondGivenAnswer = allQuestions.list[questionNumber].secondAnswer
    let thirdGivenAnswer = allQuestions.list[questionNumber].thirdAnswer
    let fourthGivenAnswer = allQuestions.list[questionNumber].fourthAnswer

    if sender.tag == 1{
        pickedAnswer = firstGivenAnswer
    }
    else if sender.tag == 2 {
        pickedAnswer = secondGivenAnswer
    }
    else if sender.tag == 3 {
        pickedAnswer = thirdGivenAnswer
    }
    else if sender.tag == 4 {
        pickedAnswer = fourthGivenAnswer
    }

    checkAnswer()

    questionNumber += 1
    updateUI()

}
```

Figure 36: QuizViewController of SecureIT

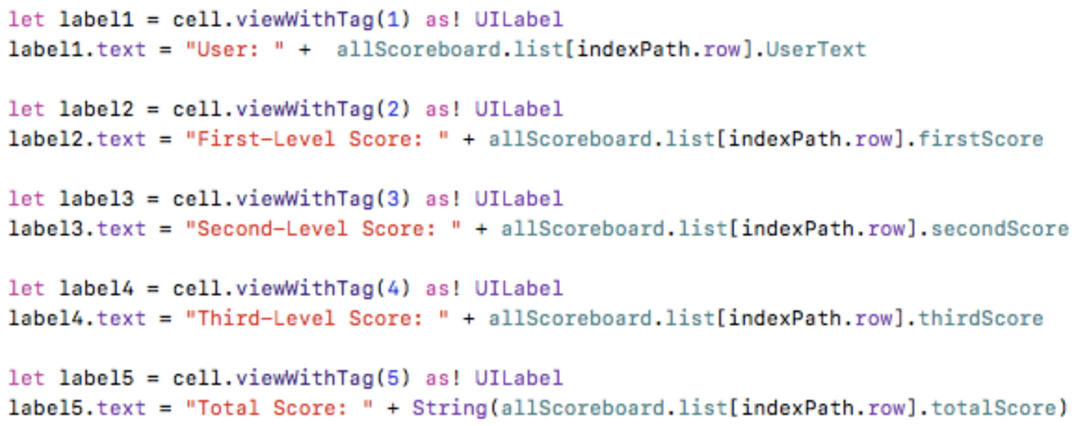
When the user answers all the questions of the current level there appears an alert icon asking them if they want to start over the level.



```
let alert = UIAlertController(title: "Awesome", message: "You've finished all the questions, do you want
    to start over?", preferredStyle: .alert)

let restartAction = UIAlertAction(title: "Restart", style: .default) { (UIAlertAction) in
    self.startOver()
}

alert.addAction(restartAction)

present(alert, animated: true, completion: nil)
```

Figure 37: QuizViewController alert for restart of SecureIT

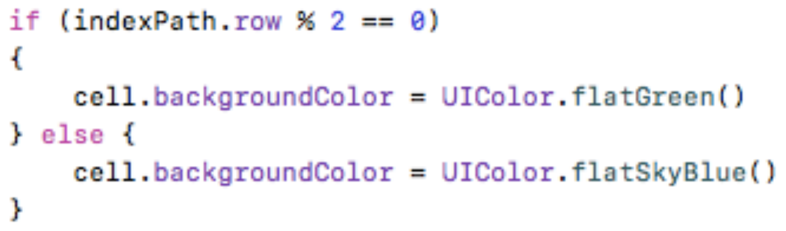
In *ScoreboardTableViewControler* all scores are displayed in detail for each user, each level and the total score can also be taken.



```
let label1 = cell.viewWithTag(1) as! UILabel
label1.text = "User: " +  allScoreboard.list[indexPath.row].UserText

let label2 = cell.viewWithTag(2) as! UILabel
label2.text = "First-Level Score: " + allScoreboard.list[indexPath.row].firstScore

let label3 = cell.viewWithTag(3) as! UILabel
label3.text = "Second-Level Score: " + allScoreboard.list[indexPath.row].secondScore

let label4 = cell.viewWithTag(4) as! UILabel
label4.text = "Third-Level Score: " + allScoreboard.list[indexPath.row].thirdScore

let label5 = cell.viewWithTag(5) as! UILabel
label5.text = "Total Score: " + String(allScoreboard.list[indexPath.row].totalScore)
```

Figure 38: ScoreboardTableViewController alert for restart of SecureIT

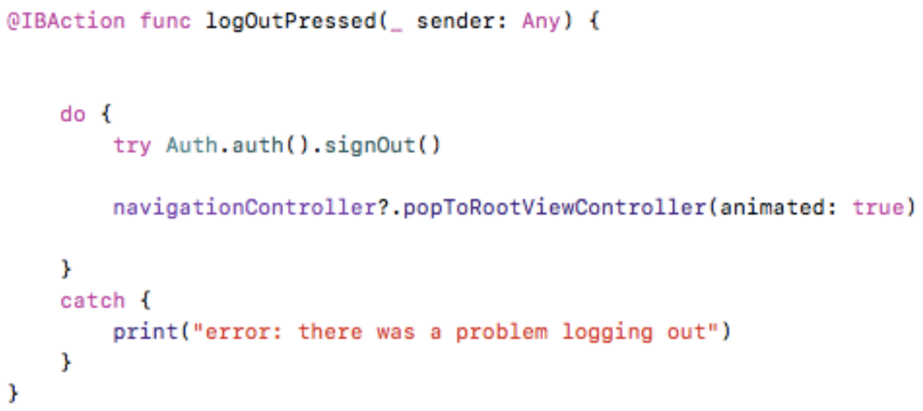
Additionally, import *ChameleonFramework* and manage the colors of the *Scoreboard-TableViewControler,* so that each row will have different color, green – blue – green – blue – green etc.



```
if (indexPath.row % 2 == 0)
{
    cell.backgroundColor = UIColor.flatGreen()
} else {
    cell.backgroundColor = UIColor.flatSkyBlue()
}
```

Figure 39: ScoreboardTableViewController green and blue for each row of SecureIT

Finally, there is the *Log Out* option in all screens.



```
@IBAction func logOutPressed(_ sender: Any) {


    do {
        try Auth.auth().signOut()

        navigationController?.popToRootViewController(animated: true)

    }
    catch {
        print("error: there was a problem logging out")
    }
}
```

Figure 40: Log Out function of SecureIT

6 Conclusions

In this final chapter, the conclusions of all the facts that were copiously described in this dissertation are going to be profusely presented.

In all the above chapters, every single one of the potential aspects of the designed iOS application as well as the background research in terms of gamification, security awareness and the positive impact of gamification in security topics were abundantly described and richly analyzed.

Security is indeed deemed as a considerable subject that all business companies and corporate organizations should seriously take into account nowadays, as technology constantly continues to advance speedily surprising users with its original innovations.

Consequently, all serious companies should take immediate action and invest in security, by initially investing in their own human resources. It is vitally essential that employees receive updated training so as to heighten their overall awareness regarding information security systems.

Applying gamification in modern programs, all promising possibilities are widely broadened. Therefore, it follows that the users can experience a more entertaining know-how in their learning modus operandi than the traditional one and their wish to apply it in more productive instances will be on the rise. When designing an application, more focus should be concentrated on the end user since actually they are the ones who would have the ultimate say in this attempt. Through these programs, the users can be superiorly competent in being acquainted with the paramount significance of the issue wishing still to further ameliorate it.

The proposed method of gamification honestly bears the unsurpassed vantage of capturing any users' earnest interest tutoring them via a uniquely recreational way, without burdening their everyday lives with any added someway dreary activities.

For the purposes of the present thesis, a bibliographic review has been prolifically undertaken regarding gamification and security awareness, a prototype iOS application was amply developed as well.

Gamification is a novel term that has been in use for only a few years now so for this reason, no exact scientific definition can be found. However, most extensively concur on some specific characteristics that could match this term. During the designing stage of applications, several elements from games are typically used.

Judging from various researches that have been conducted lately concerning information system security, most scientific researchers place enormous emphasis on the significant call for awareness on such a somber topic. User's sufficient and updated tutoring as well is viewed as critically noteworthy. Ultimately, their knowledge can be augmented upon that so as to productively accomplish their professional duties depending on the employment position they hold in their company.

The iOS application that was developed for the purposes of the current dissertation has employed a number of game elements, like a live score, immediate feedback, a progress bar and a leaderboard to name only a few. All these were applied in a bidding effort to render this application a pleasant tool for the users that would simultaneously furnish them with knowledge achieving its initial goal. This is a straightforwardly adaptable and extendable application assuming the privilege to be able to be parameterized for other purposes and uses as well only by just managing the data in the secure Realtime database.

By and large, there is a mounting necessitation for raising interest in security awareness issues as well as investing on the exploration of such a sober topic. Gamification is indeed a grand method to encapsulate in order to effusively seize this admirably commendable goal.

Bibliography

1. Seaborn K. & Fels D. (2014), *Gamification in theory and action: A survey*, Int. J. Human-Computer Studies 74 (2015) 14-31
2. Mora A., Riera D., Gonzalez C. & Arnedo-Moreno J. (2015), *A literature review of gamification design frameworks*, Spain
3. Deterding S., Dixon D., Khaled R. & Nacke L. (2011), *From game design elements to gamefulness: defining 'Gamification'*, Finland: In Proceeding of the 15th International Academic MindTrek Conference, Tampere, ACM
4. Hamari J., Koivisto J., Sarsa H. (2014), *Does Gamification Work? – A Literature Review of Empirical Studies on Gamification*, Hawaii: 47th Hawaii International Conference on System Science
5. Morschheuser B., Werder K. Hamari J. & Abe J. (2017), *How to gamify? A method for designing gamification,* Hawaii: Published in Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS 2017) (pp. 1298-1307). University of Hawaii at Manoa. ISBN: 978-0-9981331-0-2., available at https://scholarspace.manoa.hawaii.edu/handle/10125/41308
6. Caponetto I., Earp J. & Ott M. (2014), *Gamification and Education: A Literature Review*, Germany: Research and Training Center for Culture and Computer Science (FKI), University of Applied Sciences HTW Berlin, Proceedings of the 8th European Conference on Games Based Learning ECGBL 2014
7. Yu-kai Chou, Top 10 education gamification examples, available at https://yukaichou.com/gamification-examples/top-10-education-gamification-examples/
8. Jaeger L., (2018), *Information Security Awareness: Literature Review and Integrative Framework*, Hawaii: Proceedings of the 51st Hawaii International Conference on System Sciences, p. 4703-4712
9. Tsohou A., Kokolakis S., Karyda M. & Kiountouzis E. (2008), *Investing Information Security Awareness: Research and Practice Gaps*, Greece: Information Security Journal A Global Perspective, December 2008
10. Wilson M. & Hash J. (2003, October), *Building an Information Technology Security Awareness and Training Program*, Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8933
11. Gjersen Eyvind Garder B., Gjaere Erlend Andreas, Barthnes Maria & Flores Waldo Rocha (2017), *Gamification of Information Security Awareness and Training*, Proceedings of the 3rd International Conference on Information Systems Security and Privacy, Porto, Portugal, 19 - 21 February 2017, p. 59-70
12. Thornton David & Francia Guillermo III (2014), *Gamification of Information Systems and Security Training: Issues and Case Studies*, United States: Information Security Education Journal, Volume 1, number 1, June 2014, p. 16-29
13. Gjertsen Eyvind Garder B. (2016), *Use of Gamification in Security Awareness and Training Programs*, Norwegian University of Science and Technology, Master of Science in Communication Technology

14. Wood Lamont (2014), *Boost your security training with gamification*, available at https://www.computerworld.com/article/2489977/security0/boost-your-security-training-with-gamification-really.html (Accessed 10 November 2018)
15. PwC, *Game of Threats - A cyber threat simulation*, United States, available at https://www.pwc.co.uk/issues/cyber-security-data-privacy/services/game-of-threats.html (Accessed 10 November 2018)
16. Cyber Security Challenge UK, available at https://www.cybersecuritychallenge.org.uk/about
17. Wombat Security, *Security Awareness Training Modules*, available at https://www.wombatsecurity.com/security-education/security-awareness-training-modules (Accessed 10 November 2018)
18. CMU Usable Privacy and Security Laboratory, *Anti-Phishing Phil*, Carnegie Mellon University, available at https://www.ucl.ac.uk/cert/antiphishing/ (Accessed 10 November 2018)
19. Online available at https://web.archive.org/web/20100721013724/http:/library.stanford.edu/mac/primary/docs/pip83.html (Accessed 20 November 2018)
20. Online available at https://en.wikipedia.org/wiki/IOS (Accessed 3 November 2018)
21. Online available at https://en.wikipedia.org/wiki/Apple_Inc. (Accessed 3 November 2018)
22. Online available at https://developer.apple.com/documentation (Accessed 20 August 2018)
23. Online available at https://developer.apple.com/library/archive/documentation/Cocoa/Conceptual/ProgrammingWithObjectiveC/Introduction/Introduction.html (Accessed 17 August 2018)
24. Online available at https://developer.apple.com/swift/ (Accessed 17 August 2018)
25. Online available at https://developer.apple.com/documentation/swift/imported_c_and_objective-c_apis/importing_objective-c_into_swift (Accessed 15 September 2018)
26. Online available at https://docs.swift.org/swift-book/LanguageGuide/TheBasics.html#//apple_ref/doc/uid/TP40014097-CH5-ID309 (Accessed 17 September 2018)
27. Online available at https://firebase.google.com/products/ (Accessed 2 October 2018)
28. Online available at https://firebase.google.com/docs/ios/setup (Accessed 2 October 2018)
29. Online available at https://developer.apple.com/xcode/features/ (Accessed 17 August 2018)
30. Online available at https://stackoverflow.com (Accessed 17 August 2018)
31. Online available at https://www.udacity.com (Accessed 17 August 2018)
32. Online available at https://www.udemy.com (Accessed 17 August 2018)
33. Online available at https://github.com/SVProgressHUD/SVProgressHUD (Accessed 13 September 2018)
34. Online available at https://github.com/viccalexander/Chameleon (Accessed 13 September 2018)
35. Online available at https://medium.com/ios-os-x-development/modern-mvc-39042a9097ca (Accessed 10 November 2018)
36. Online available at https://www.gratisexam.com/vce-to-pdf/sans/sec504/SANS.Prepaway.SEC504.v2018-07-17.by.Edward.170q.pdf/ (Accessed 10 October 2018)