The Security of Adaptive Ubiquitous/Mobile Learning Systems

Andreea-Cristina STROE
Bucharest University of Economic Studies, Romania
stroeandreea96@gmail.com

The purpose of this paper is to examine the security vulnerabilities that may appear in an adaptive mobile learning system, as well as to present ways to prevent security breaches in this type of learning systems. Moreover, this paper has the objective to present a possible solution consisting of an adaptive ubiquitous learning system that can bypass the most frequent security issues that may appear in mobile learning systems. This paper relies on a study of the three most used mobile applications in learning foreign languages, considered also being the best on the market. Those applications were submitted to security scan in order to identify their vulnerabilities. After this analysis, several categories of vulnerabilities have been identified, in addition to their cause. Besides scanning against OWASP Mobile Top 10 vulnerabilities, the study determines that it may exist some security breaches in relation with the external communication the application has. Based on the results from the security scan, a new solution that has the objective to prevent as many discovered vulnerabilities as possible is to be implemented. Overall, this paper contributes to the literature by revealing security questions that appear in some of the most used mobile application for learning a foreign language at the moment. Moreover, it will describe a prototype of a possible first adaptive ubiquitous learning systems, free from security threats, that allow Romanian users to obtain basic knowledge for speaking Swedish.

Keywords: m-learning, u-learning, security, ubiquitous learning, adaptive mobile learning system, learning experience, vulnerability scan

1 Introduction

At the present time, the development of mobile technologies has reached a peak in which they have become indispensable in people’s life. Smartphones gained control over people’s behaviour, influencing both their personal way of being and their professional life [1]. Therefore, the way people learn, work, communicate has changed considerably over the last decades. Any needed information is just a click away, as well as sharing any type of content with anyone and anywhere.

As a response to the changes that occurred in people’s way of being due to the development of mobile technologies, the institutions also needed to embrace the use of smartphones in their processes in order to prevent a breach between their activity and society. Educational institutions are not an exception as the development of mobile technologies has imposed several important changes in the learning process. Thus, the variation of mobile learning systems has become a favourite topic for analysis. Since the learning process evolved into gaining knowledge anywhere and anytime [2][5], the concept of m-learning represents a central issue in the learning management systems sphere. E-learning management systems are not considered sufficient anymore and mobile learning systems are viewed as an evolution of them because of their availability [1] and their informal nature [6]. Moreover, of particular interest is also a learner-centred, adaptive learning system [7], that the literature presents as ubiquitous learning system [8] [5].

So far, investigations have been confined to presenting the differences between the three types of learning management systems, as well as their advantages and disadvantages. Nevertheless, few studies have been dedicated to analysing the security issues that appeared in these new forms of the learning process and understanding the security breaches that can appear still remains a major challenge.

Thus, the primary focus of this paper is to examine and understand the security threats of a mobile learning system that considers learner's preferences and rhythm of learning. For this purpose, a series of the most used applications for learning a foreign language will be closely studied from the security point of view. Based on the conclusions discovered from this research, this paper aims to present a securely safe solution of a mobile learning system.

2 Evolution of mobile learning systems

The changes that the development of mobile technologies has brought into people's life have raised specialists' attention and interest. Therefore, a considerable amount of literature has focused on describing the concepts of m-learning and u-learning, as well as their advantages and disadvantages. Since in recent years the interest in cyber security has increased, a growing body of literature has also investigated the security of mobile learning systems. This section will focus on a brief overview on mobile and ubiquitous learning systems, including their security implications.

2.1. M-learning: advantages, disadvantages, security questions

M-learning, the short form for mobile learning, is defined as being "learning across multiple contexts, through social and content interactions, using personal electronic devices" [9]. On a simpler approach, m-learning is the process of acquiring new knowledge using a mobile technology. One remark should be done here for the reader's proper understanding of what "mobile technology" signifies since many will reduce the meaning to only "mobile phone". Apart from the usual synonymy that exists between mobile learning and smartphones, one should also consider that other devices, such as iPods or tablets, supports mobile technologies [1]. J. Lam, Y. Yau and S.K.S Cheung [1] go further and even include laptops and PDAs (Personal Digital Assistants) to the category of mobile devices due to their portability and their possibility to support wireless connections, but this study will not embrace this theory in the following exposure.

As the definition states, mobile learning is not so restrictive [3], it can be represented by any type of learning process in which the student is not reduced to a place in a classroom at a certain moment in time and with a certain group of colleagues [3]. It is above all else a new type of learning activity that is independent of student's time and location, but also from being connected to a certain network infrastructure [10]. This approach by all means has several advantages, but also some disadvantages.

The most evident advantage is undoubtedly the flexibility that m-learning offers to its users [1]. Thus, the learners are not conditioned to be at a specific time to a specific location with a specific group of people in order for the educative process to take place [11]. In addition, m-learning can be a powerful tool both when talking about distance education and improving the traditional learning approach by becoming a part of it [1]. It means that the pedagogical methods used in m-learning can be of almost any type [8], observing therefore an evolution of the learning environment. In terms of materials, m-learning allows the possibility to use a variety of materials (including more interactive ones such as pictures, videos), which are a plus in the educational process [12]. Another benefit of m-learning is that users have more control on the topics they want to cover and how much time they want to spend [8] in order to acquire knowledge and the teams they want to be part of, improving then the quality of process and transforming the educational activity from a formal approach to a more informal one [1]. Moreover, since the control is in user's hands, the process is more centred on learner [13], adapting better to their desires.

Nevertheless, m-learning implies a series of disadvantages. In the first place, neither teachers nor students express a strong confidence regarding this new approach in terms of educational method [13]. There is still a huge number of people who prefer traditional learning, considering that pedagogical methods can be better implemented in this kind of approach. In addition to this, educational institutions share the same amount of trust into mobile technologies used in teaching [13], giving more credits to traditional learning rather than supporting the new approach. Moreover, it seems that m-learning is not suitable for all ages [14], all the advantages presented above being annulated when talking about children who are less than ten years old. They cannot, indeed, benefit from the flexibility, since they need clear assistance in the educational process [14] and they most likely do not possess a mobile device. Another drawback is caused by the limitations a mobile device comes with: little memory and little battery autonomy [3], that reduce the flexibility and availability. Additionally, these limitations make the device susceptible to security threats [10].

It has demonstrated that designing a mobile learning system centred on preventing security breaches, especially related to data security, has not been a priority [15]. But security issues must undoubtedly be considered when developing such a system because they can appear both on application level and communication level [16]. A poor security perspective is a menace for integrity, confidentiality and privacy [15], data privacy vulnerabilities being the most encountered security risk [15]. One may wonder about the reason why mobile technologies are so vulnerable and the answer is their portability that makes them sensitive to both physical and digital attacks [15]. When it comes to security risks at communication level, the transaction security is the one to highlight [16]. A mobile learning system should be extremely careful about how data that is used in a communication (with a server, a database) is handled. There should not be used any sensitive information and everything should be encrypted. In the case of security vulnerabilities at application level, one may distinguish two categories of risks: at user level and at content level [15]. Using and storing passwords and personal information without any security measure (such as encryption) can threaten the privacy and the confidentiality [15]. In addition to this, the learning content is also to be taken care of because its integrity can also be compromised [12]. However, all the security issues can be bypassed through several measures such as encryption, handling permissions [17] or by a security safe approach when developing the application.

2.2. U-learning: advantages, disadvantages, security questions

A new educational trend has appeared due to the need to create an adaptive educational process with individualized content and interface [18] whose main focus is to be aware of the learning context [19] and it carries the name ubiquitous learning, in short u-learning. Thus, one can call ubiquitous learning system a system that is capable to adapt to the context in terms of both learner and environment [20]. In the case of this systems, the learners have the benefit to receive learning recommendations depending on their habits [21], for instance the hour of day the users prefer to learn or for how much time they spend in the learning process or if there are any activities that take longer than others. Moreover, they can also benefit from what the smartphones come equipped with in terms of sensors [21] because an u-learning system can offer material content depending on location, device speed or temperature [21]. Therefore, the activities proposed by such a learning system are very varied [22]. Since the main device used in an ubiquitous system is the smartphone by virtue of the embedded equipment it has and can be used in support of the learning process, u-learning is considered an extension or evolution of m-learning [5]. There are some similarities between the two types of learning systems, but, however, they also differ in certain aspects.

The main resemblance between m-learning and u-learning is the fact that both of them are used on portable devices. Therefore, both benefit from all the advantages and support for spontaneous and informal education a mobile phone offers [6] in aid of the training process, that becomes accessible from anywhere and anytime for anybody who dispose of a device [5]. The immediacy and accessibility of the process is accompanied by its flexibility since learners are not constrained by a location or a time to learn [5]. Nevertheless, u-learning systems are based on the notion of “context” [22] [20], which is not the case for m-learning. The characteristic of adaptability remains a key factor in the case of u-learning [5], providing the possibility that learners apply the notions they acquire in a certain situation [23]. The adaptability is however built on a series of factors that have a huge impact on the usage of an u-learning application: the capabilities of the device (in terms of display or memory limitations), solution’s architecture, the communication capabilities of the protocol that is used [4]. All these characteristics represent the premises for the advantages and disadvantages of ubiquitous systems.

Being an extension of m-learning, u-learning has also its advantages and disadvantages. Even so, taking into consideration the particularities that ubiquitous systems have, there are several benefits that are worth to be mentioned. The first one is situation awareness [8] as the application perceives elements from learner’s environment related to time and space and offers learning material based on this in terms of form and content. Thus, the learner’s learning conditions change and adapt to their need. For instance, the application can perceive that in the room there is too much light and adapt the screen light to be less. Going even further, the adaptability can also be associated with the application taking into consideration learner’s real behaviour [8] in the form of time spent in the application or preferred moment of the day to study. Another advantage is that an u-learning system offers content that can be applied into real world situations. The solution can even be design by integrating a location awareness system [4], in a way that the learner benefits from the surroundings to study a certain topic. (G.-Z. Liu and G.-J. Hwang [8] present a solution designed for a biology lesson in which students learn about some plants from an ecology garden by the use of RFID sensors). The most important aspect is still the integration of device’s sensor (for example, RFID sensors or GPS) in the educational process [8]. In this way, the learner has the ability to learn via interaction with the surroundings by exploring the capabilities the device comes equipped with [24]. Lastly, an ubiquitous systems is centred on learner’s needs [7] and always tries to present the information in such a form that the learner is actively engaged [25], helping therefore to the transformation of learning process from formal and rigid as the traditional approach to a more informal and flexible one.

Nonetheless, u-learning comes also with a series of own disadvantages, apart from the ones proper to m-learning. First of all, there is the difficulty to build an environment to be used for such an approach in a school or university, thus the use is restricted [22]. The educational institutions are not endowed with environments that dispose of sensors such as classes equipped with RFID sensors and obtaining this kind of equipment can get to a huge cost. Since the trust manifested towards integrating m-learning in the teaching process is not very high [13], it seems that the costs to transform even a classroom into a proper environment for u-learning is even more difficult to sustain. Another infrastructural limitation is in terms of learner’s devices. The educational institution should also provide devices for learners and, once more, the costs can be huge. Moreover, there is the question of security and the possibility of several attacks because of hardware’s scalability and confidentiality [7].

Paradoxically, the most important security vulnerability is related to sensors’ integration. In case of Android-based u-learning systems, neither the access to sensors nor the information transmitted are protected [26]. Thus, the problem of received data integrity, as well as stored data is raised [27]. Moreover, user’s privacy might be threatened because the sensors can be used without user’s knowledge, being thus possible to record several habits the learners have and may not want to reveal. In addition, an ubiquitous solution may be susceptible of network attacks, since it uses wireless connection to the internet [25].

3 Study of mobile learning application security scanning

A number of studies has interested in exploring mobile technologies and their security vulnerabilities. This study focuses on the security perspective of m-learning applications for learning a foreign language. Each of the followings sections explains the steps that were conducted in the present approach.

3.1. Research design

This section has the objective to examine the top three most recommended applications of mobile learning for foreign languages. One may ask why the study turns its attention towards the field of foreign languages and there are several reasons to be mentioned. First of all, the necessity to be able to speak at least one foreign language has appeared recently, due to the globalisation of our society. Thus, this is one of the mandatory conditions any job description contains and everyone who is willing to obtain a new job may face a problem in the case of not knowing a foreign language [28]. Since most of the people do not have a lot of time that can be invested into learning, they need a rapid solution that can help them acquire new linguistic abilities [29]. Mobile learning applications come to their assistance, being a method to obtain quick information and in an engaging way [29]. Second of all, in order for m-learning and u-learning solutions to have any results, learners may be able to apply their new knowledge in real world situations and there are plenty of scenarios in which one may need to speak a foreign language (for instance, on the street asking or giving directions, while travelling or when eating in a restaurant) [28].

Moreover, this approach has a very clear procedure by which the applications to be studied were selected and they were meticulously analysed from security perspective by scanning them against OWASP Mobile Top 10 vulnerabilities, as well as against external communication. The following sections will present the selection process as well as the analysis.

3.2. Selection of applications

Choosing a mobile application for learning a foreign language is a real challenge. The offer is so large that can sometimes be overwhelming for someone who has just decided to gain a new linguistic skill. Not only offers each of them diversified materials in order to make the learning process more and more enhancing and attractive, but also their presentation forms are varied [29], they being presented even under the form of “serious games” [29]. Therefore, one may need guidance in their choice. Over the internet, there are numerous articles, written by specialists in m-learning, that analyse the most used applications and boast the leadings of the field. This study has chosen seven such articles [28], [30], [31], [32], [33], [34], [35], all of them being available on the Internet. After having skimmed each of them, more than twenty options to consider were found, for instance Memrise, Duolingo, Lingualift or Tandem. The number of found applications being so huge even for a small number of articles, the decision to make a list with all of them came naturally. Since some of the applications appeared recursively, we have decided to count the number of appearances and to make a top depending on how many occurrences each application has. The next step was to select the three applications that were the most present. In Table 1, the reader is able to see the list of applications and their occurrences.

Table 1. Selection of mobile applications

Mobile Application	Number of occurrences
Duolingo	7
Memrise	7
Bussu	7

Mobile Application	Number of occurrences
AccellaStudy	1
RosettaStone	4
Google Translate	1
Pimsleur	2
Tandem	2
Babbel	6
Drops	2
Beelinguapp	2
Mondly	2
HelloTalks	3
Mindsnacks	2
Lingua.ly	1
TripLingo	2
MosaLingua	2
HiNative	2
Lingualift	1
Clozemaster	1
Lirica	1

According to the provided table, the choice for the top three most used mobile applications for learning a foreign language was simple. Therefore, in the following section, the applications that will be studied for security vulnerabilities will be Duolingo, Memrise and Bussu.

3.3. Security scanning

The most important reference point in terms of mobile security is undoubtedly OWASP Mobile Top 10, another project provided by The OWASP Foundation [36]. Its main focus is to provide security advice to mobile developers in order for them to develop secure applications. Thus, in 2016 [36] there was released the most recent top 10 mobile vulnerabilities that will represent the base of this study. In order to scan the three applications against the OWASP vulnerabilities, this study has used ImmuniWeb AI Platform [37], a product from the Swiss company High-Tech Bridge SA [38]. This product was chosen due to its compatibility to CVE (Common Vulnerabilities and Exposures) and CWE (Common Weakness Enumeration) [38], therefore the accuracy of the scans cannot be doubtful. It is also very simple to use, the only needed resource is the link from GooglePlay or the apk file.

The first application that was submitted to the scan was Duolingo, probably the most famous mobile application for learning a foreign language. The success of Duolingo is certainly due to its presentation form as a serious game: it gives the user the impression of playing a game while developing a skill [30] [31]. Moreover, the combination of images, audio material and text [28] increases user's interest into completing more and more lessons.

According to the security scan, Duolingo is susceptible to 0 high risk vulnerabilities, 6 medium risks, 8 low risks and 7 warnings. Among the top 10 Mobile Vulnerabilities, the scan shows that this application is vulnerable to M1 (Improper Platform Usage [36]), M2 (Insecure Data Storage [36]), M3 (Insecure Communication [36]), M5 (Insufficient Cryptography [36]), M7 (Client Code Quality [36]) and M10 (Extraneous Functionality [36]), having the following distribution: 5 risks related to M1, 5 to M2, 1 to M3, 3 to M5, 2 to M7, 2 to M10, to which is added the temporary file creation risk. Thus, a total of 19 risks were identified. As one can see, this application is most vulnerable to M1 and M2. Therefore, an attacker can, for instance, exploit the way the data is stored or the way the Android platform is used.

One of the M1 risks is represented by the fact that this application can be displayed over other user interfaces of other applications that run on the device and, in the case in which the attacker has installed a malicious application on the device, the touch event can be redirected, because of this vulnerability, to the malicious application and the attacker can be able to fool the user to make an undesired act, such as a payment that the malicious application requires at touch event. Nevertheless, this is a low risk, the medium ones being mostly related to data storage (the application contains hardcoded sensitive data and has the possibility to access external data storage, such as the SD card), insufficient cryptography (using the java Random() function, which is demonstrated to be a threat to encryption tokens due to its predictable behaviour) or insecure communication (the application uses the HTTP protocol through HttpURLConnection class as communication for sending or receiving data).

The low risks are related only to M1 and M2 vulnerabilities. This proves once more that the security of data in a mobile application is always a priority, the developer must always be cautious about exposure of sensitive data that can represent an aim for the attackers. The internal storage, as well as the external one should respect several platform rules in order to enhance security, in addition to which one should always consider data encryption [39].

The second application that was analysed from the security point of view is Memrise. This application utilises a different learning technique than Duolingo, its focus being on learning words in contexts [28]. In addition, it uses the learner's mother tongue in order to help memorise the words in the target language [28].

As a result of the scan, it was identified that Memrise has 0 high risks, 4 medium risks, 6 low risks and 6 warnings. It counts a total of 16 vulnerabilities, which makes it more secure compared to Duolingo. Moreover, its medium risks number is lower than in the case of Duolingo. Nonetheless, it shares the same vulnerabilities, being vulnerable to M1, M2, M3, M5, M7 and M10. The distribution is as follows: 4 risks related to M1, 5 to M2, 1 to M3, 1 to M5, 3 to M7 and 1 to M10. The main risk of this learning application seems to be the way it handles stored data (M2 vulnerability), counting 5 out of 16 risks.

According to the scan, there is a medium risk related to data storage and four low risks. The medium one is represented by the fact that this application uses an unencrypted SQLite database and, in case the attackers access this database, they can get important information that can be used in a malicious way. Another data related issue is the fact that the application contains hardcoded debugging or technical information that can be extracted by an attacker, Moreover, the scan has found hardcoded URLs from development, staging or preproduction hosts, issue that can increase the potential of external attacks. Another risk is the fact that the application is enabled for backup, using the Android default one. By doing a backup, sensitive information can be stored and if the stored location is, for instance, a Gmail account and it is compromised, an attacker will have access to that data that, in addition, is not encrypted.

This application is also susceptible to code injection through various methods, as there are 3 risks related to M7. SQL injection is one of them. As determined by the scan, SQL queries use concatenation operator and are hardcoded (this is an identified example: db.rawQuery("SELECT username FROM users_table WHERE id = '"+ input_id +"'")). Another one is the use of dynamic load of executable code, that, in some situations, can lead to code injection that can be inserted in order to access victim's device.

The last application that will be covered by this study is Bussu, that has an approach based on flashcards and grammar and pronunciation exercises [31]. Its main advantage is the design for travellers, providing courses that tackles the topics one may need while travelling in a foreign country [31].

After the security scan, it was found that Bussu has 0 high risks, 5 medium risks, 6 low risks and 8 warnings, with a total of 19 risks. Moreover, the scan states that this application is vulnerable to M1, M2, M3, M5, M7 and M10, having the following distribution: 5 risks related to M1, 4 to M2, 1 to M3, 3 to M5, 3 to M7, 1 to M10, to which is added the temporary file creation risk. Therefore, Bussu is most susceptible to M1 vulnerability, nevertheless being only categorised as low risk and warnings.

Among the risks included in M1 that were detected for Bussu application, there is the same issue encountered in Duolingo: the fact that this application can be displayed over other user interfaces of other applications that run on the device. This is called missing tapjacking protection. In addition to this, there is a risk related to both exported broadcast receivers and services. By default, in Android, the services are not exported. Thus, in the case of this application, the manifest file contains some services defined without certain restriction. This behaviour makes possible the situation of services being invoked unmanageably by other applications, some of them possibly malicious ones. The same possibility is enabled in the case of exported broadcast receivers, other applications being able to send intents without restrictions.

The medium risks are nonetheless related mostly to M5 (2 out of 5), the application being vulnerable because of insufficient cryptography. One that should certainly be taken into consideration is the presence of hardcoded encryption keys. Since the attacker has access to encryption keys, the encryption process is in vain and, in case of an attack, the security measures that depend on those encryptions are annulated.

4 Results

4.1. Security scans results

The security scans to which the three applications for learning a foreign language were submitted revealed a series of conclusions. They were scanned against OWASP Mobile Top 10 and the occurrence frequency can be consulted in the following graph.

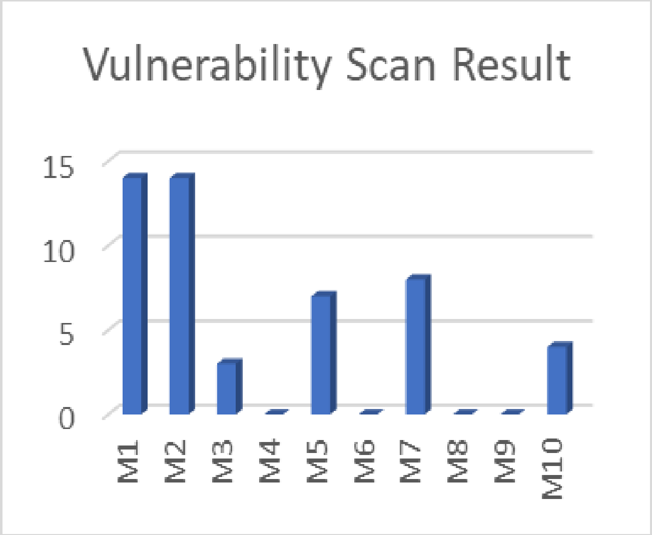


Fig. 1. Occurrences of OWASP Mobile Top 10

As one can see in Fig.1., there were no risks found related to M4 (Insecure Authentication [36]), M6 (Insecure Authorisation [36]), M8 (Code Tampering [36]) or M9 (Reverse Engineering [36]). However, the number of risks related to M1 is equal to the number of risks M2. Thus, one may claim that the way data is handled in an Android application has the same importance as the way the developer uses the benefits the Android platform boasts. Code injection vulnerability (M7) occupies the next position, really close to the insufficiency of cryptography (the use of Random() function, as well as having hard-coded encryption keys).

M10, the next in the top of occurrences, offers the possibility to the attacker to get access to the extraneous components without the need of end-users. This can have a really sever impact on the security of an applications since in this way, the attacker can figure out how the backend works or can get privileges that are unauthorised. All three applications are exposed to JavaScript enabled in WebWiew, thus being susceptible to Cross-Site Scripting attacks.

The last position is occupied by M3, with only 3 occurrences in total, one per each application. This vulnerability is related to external communication. The three applications use the HTTP protocol for sending and receiving data, through HttpUrlConnection class and, as it is already known, HTTP is a protocol that does not encrypt data and, if sensitive information is sent, the attacker can see it without any problem.

4.2. Solution implementation proposal

Taking into consideration the results stated above, this study proposes an adaptive application for Romanian learners to acquire basic skills in Swedish that will handle all the security issues discussed in section 4.1. This application has the objective to bypass the security issues that were proved to be a major challenge in the development of mobile and ubiquitous applications.

The application will have the structure of a serious game, since it was highlighted the need to enhance user's interest into learning and this presentation form seems to be the most suitable. The users will deal with concepts of Swedish vocabulary and culture that can be used in daily life (for instance, going to the doctor, going into a store). Each module will consist in an introduction, followed by a series of quizzes through which the user will learn some words. At the end of each module, the user will save some relevant words in a local database. The first adaptive functionality will be the display of the introduction. It will take into consideration the speed of user's phone. If the user is on the move, the introduction will be displayed as an audio file. If user's position is still, the user will have the option to choose if the introduction will be audio or text based. Another adaptive functionality will be that the application accesses users' location and, when they are nearby a place where they can use any of the words from the local database, they will receive a notification. This functionality will be at user's choice, since it will be active only when the user will enable it.

This short description of the adaptive application raises, however, some serious security problems, that the developer should cautiously consider. First of all, there is the authentication problem. The chosen method will be a biometric one and the username will be based on a pseudonym. In order to get the pseudonym, secure cryptographic solutions will be used. Second of all, the code injection vulnerability needs careful attention, as the results showed that is the third most encountered problem. To this, the encryption of data stored in the database must be taken into consideration since data storage seemed to be a serious problem in the studied m-learning applications. All the communication channels (sending or receiving data) will also be encrypted. In addition to this, the copyright of the materials from the quizzes will be also a focus, this vulnerability being covered by different ways of watermarking.

5 Conclusions

The development of mobile technologies has undoubtedly gained more and more users that prefer this approach in opposition to having a desktop and being close to a desk. People's life is more dynamic due to mobile technologies, which offer the possibility to communicate or to learn more easily [1]. Therefore, mobile learning has also brought some changes into the educational system, introducing two concepts, mobile learning (m-learning) and ubiquitous learning (u-learning), which made the learning process more flexible and more enhancing [1]. Nevertheless, the educational parties are not very willing to introduce these new concepts into the educational process [13].

This paper firstly offered to its readers a brief introduction into the concepts of m-learning and u-learning, focusing on their advantages and disadvantages. Since security is the main topic of this paper, a first step was to provide several security issues related to these two new learning concepts. Many of the security concerns revealed in this part were linked to the way the application handles data, whether it is stored data or data that is used in communication with other applications or simply data used by the application in the learning process.

Nevertheless, this paper wanted to offer more concrete information, therefore there were selected the three most used and recommended mobile applications for learning a foreign language and they were scanned against OWASP Mobile Top 10 vulnerabilities. On one hand, the results reinforced the conclusion drained from the literature study, showing that insecure data manipulation is, indeed, a serious problem in mobile and ubiquitous security. Nonetheless, a rather surprising result places the improper usage of the Android platform on the same position that manipulating data storage. This shows that Android developers should consider more the benefits and the drawbacks the platform boasts and be more cautious in terms of security.

Moreover, the study highlights the fact that code injection is another serious vulnerability for mobile security, as well as not paying sufficient attention to the cryptography elements that are used in the development process. The external communication can also offer attackers the possibility to gain access to sensitive data, as the usage of HttpUrlConnection class has proven to be insecure because of lack of data encryption.

This study has however some limitations. The first one is, indeed, the small number of scanned applications. The results may change in the case of a bigger number of applications that offer even more options to their users. In this case, the statistics may change, as other applications might offer the option of creating an account, for instance and, in this way, other security breaches can be opened. But the objective was to analyse the most recommended applications and to give an overview on these three applications from the security point of view.

Based on these results, this paper proposes another adaptive solution for learning a foreign language that tries to cover all the security vulnerabilities mobile applications are susceptible to. This can be a valuable contribution to the educational process of acquiring new linguistic skills with the aid of mobile technologies in a more secure manner.

Acknowledgement

Results presented in this paper has been obtained conducting my dissertation research project at the IT&C Security Master program from Bucharest University of Economic Studies.

References

[1] J. Lam, J. Yau and S. K. Cheung, “A Review of Mobile Learning in the Mobile Age,” in ICHL: International Conference on Hybrid Learning. Lecture Notes in Computer Science, vol 6248, Hong Kong, China, 2011.

[2] S. A. Shonola and M. Joy, “Enhancing Mobile Learning Security,” International Journal on Integrating Technology in Education, vol. 5, no. 3, pp. 1-15, 2016.

[3] O. Popović, M. S. Markovic and R. Popović, “ mTester-Mobile learning system,” Computer Applications in Engineering Education, vol. 24, no. 3, pp. 412-420, 2016.

[4] D. Dochev and I. Hristov, “Mobile Learning Applications - Ubiquitous Characteristics and Technological Solutions,” Cybernetics and Information Technologies, vol. 6, no. 3, pp. 63-74, 2006.

[5] M. A. Virtanen, E. Haavisto, E. Liikanen and M. Kääriäinen, “Ubiquitous learning environments in higher education: A scoping literature review,” in International Journal of Educational and Pedagogical Sciences, Vol. 4, No. 5, London, Great Britain, 2017.

[6] T. D. Jong, M. Specht and R. Koper, "Contextualized Media for Learning," Educational Technology & Society, vol. 11, no. 2, pp. 41-53, 2008.

[7] C. de Witt and C. Gloerfeld, "Mobile Learning and Higher Education," in The Digital Turn in Higher Education, Wiesbaden: Springer VS, 2018, pp. 61-79.

[8] G. Z. Liu and G. J. Hwang, "A key step to understanding paradigm shifts in e-learning: towards context-aware ubiquitous learning," British Journal of Educational Technology, vol. 41, no. 2, pp. E1-E9, 2010.

[9] Wikipedia, "M-learning," 11 March 2020. [Online]. Available: https://en.wikipedia.org/wiki/M-learning. [Accessed 14 March 2020].

[10] Z. Ugray, "Security and privacy issues in mobile learning," International Journal of Mobile Learning and Organisation, vol. 3, no. 2, pp. 202-2018, 2009.

[11] J. M. Moneo, S. Caballé and J. Prieto-Blazquez, "Information Security in Support for Mobile Collaborative Learning," in 2013 Seventh International Conference on Complex, Intelligent, and Software Intensive Systems, CISIS 2013, Taichung, Taiwan, 2013.

[12] A. Martin and G. J. A. Jose, "M-Learning Effectiveness Factors," International Journal of Engineering Associates, vol. 6, no. 1, pp. 1-8, 2017.

[13] M. Kaiiali, A. Ozkaya, H. Altun, H. Haddad and M. Alier, "Designing a Secure Exam Management System," IEEE TRANSACTIONS ON LEARNING TECHNOLOGIES, vol. 9, no. 3, pp. 258-271, 2016.

[14] R. Shadiev, W. -Y. Hwang, Y. -M. Huang and T. -Y. Liu, "Facilitating application of language skills in authentic environments with a mobile learning system," Journal of Computer Assisted Learning, vol. 34, no. 1, pp. 42-52, 2017.

[15] S. A. Shonola and M. Joy, "Mobile Learning Security Issues From LECTURERS' PERSPECTIVES (NIGERIAN UNIVERSITIES CASE STUDY)," in 6th International Conference on Education and New Learning Technologies, Barcelona, Spain, 2014.

[16] A. Zamfiroiu, "Security Management for Mobile Learning Systems," in eLearning and Software for Education, Bucharest, Romania, 2018.

[17] W. Enck, M. Ongtang and P. McDaniel, "Understanding Android Security," IEEE Security & Privacy, vol. 7, no. 1, pp. 50-57, 2009.

[18] Wikipedia, "Educational technology," 11 March 2020. [Online]. Available: https://en.wikipedia.org/wiki/Educational_technology. [Accessed 14 March 2020].

[19] S. Hallsteinsen, K. Geihs, N. Paspallis, F. Eliassen, G. Horn, J. Lorenzo, A. Mamelli and G. A. Papadopoulos, "A development framework and methodology for self-adapting applications in ubiquitous computing environments," The Journal of Systems and Software, vol. 85, no. 12, pp. 2840-2859, 2012.

[20] I. El Guabassi, Z. Bousalemb,, M. Al Achhabc, I. JELLOULI and B. E. EL Mohajir, "Personalized adaptive content system for context-aware ubiquitous learning," Procedia Computer Science, vol. 127, pp. 444-453, 2018.

[21] M. Li, H. Ogata, B. Hou, N. Uosaki and Y. Yano, "Personalization in Context-aware Ubiquitous Learning-Log System," in 2012 IEEE Seventh International Conference on Wireless, Mobile and Ubiquitous Technology in Education, Takamatsu, Japan, 2012.

[22] C. Pimmer, M. Mateescu and U. Gröhbiel, "Mobile and ubiquitous learning in higher education settings. A," Computers in Human Behavior, vol. 63, pp. 490-501, 2016.

[23] D. Frohberg, G. Christoph and G. Schwabe, "Mobile Learning projects - a critical analysis of the state of the art," J. Comp. Assisted Learning, vol. 25, no. 4, pp. 307-331, 2009.

[24] G. Kambourakis, "Security and Privacy in m-Learning and Beyond: Challenges and State-of-the-art," International Journal of u- and e- Service, Science and

Technology, vol. 6, no. 3, pp. 67-84, 2013.

[25] L. M. Powell, H. Wimmer, C. Rebman and C. Abdul al, “LEARNER SECURITY & PRIVACY RISKS: HOW USAGE OF ONLINE SOCIAL MEDIA OUTSIDE A LEARNING MANAGEMENT SYSTEM AFFECTS LEARNERS’ DIGITAL IDENTITY,” Issues in Information Systems, vol. 20, no. 4, pp. 1-7, 2019.

[26] Q. Do, B. Martini and K.-K. R. Choo, “Is the data on your wearable device secure? An Android Wear,” Software: Practice and Experience, vol. 47, no. 3, pp. 391-403, 2017.

[27] S. Farid, M. Alam, J. Itmazi and G. Qaisar, “Security Threats and Measures in E-learning in Pakistan: A Review,” Technical Journal, University of Engineering and Technology (UET), vol. 22, no. 3, pp. 98-107, 2017.

[28] S. Fisher, “The 6 Best Free Language Learning Apps of 2020,” 13 March 2020. [Online]. Available: https://www.lifewire.com/the-7-best-free-language-learning-apps-1357060. [Accessed 26 March 2020].

[29] A. Zamfiroiu , M. Anghel and C. E. Cîrnu, “USING GRAPHIC LIBRARIES FOR FOREIGN LANGUAGES EDUCATIONAL GAMES,” in eLearning and Software for Education, Bucharest, Romania, 2015.

[30] S. L. King, “The Best Language Learning Apps,” 25 March 2020. [Online]. Available: https://www.oprahmag.com/life/g28468651/best-language-learning-apps/?slide=11. [Accessed 26 March 2020].

[31] S. Hill, “The best language-learning apps for Android and iOS,” 4 April 2018. [Online]. Available: https://www.digitaltrends.com/mobile/best-language-learning-apps/. [Accessed 26 March 2020].

[32] V. I. Oloo, “10 best apps for learning a new language,” 24 September 2018. [Online]. Available: https://www.dignited.com/35310/10-best-apps-for-learning-a-new-language/. [Accessed 26 March 2020].

[33] Lingualift, “10 best language learning apps 2020,” January 2020. [Online]. Available: https://www.lingualift.com/blog/best-language-learning-apps/. [Accessed 26 March 2020].

[34] S. Writtenhouse, “The 8 Best Language Learning Apps That Really Work,” 5 December 2019. [Online]. Available: https://www.makeuseof.com/tag/five-free-apps-help-learn-foreign-language/. [Accessed 26 March 2020].

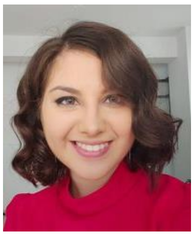
[35] S. Brown , “Best language learning apps of 2020,” 23 March 2020. [Online]. Available: https://www.cnet.com/news/best-language-learning-apps-of-2020/. [Accessed 26 March 2020].

[36] T. O. Foundation, “OWASP Mobile Security Project,” OWASP , 2020. [Online]. Available: https://owasp.org/www-project-mobile-security/. [Accessed 2020 May 4].

[37] H.-T. B. SA, “ImmuniWeb AI for Application Security,” High-Tech Bridge SA, 2020. [Online]. Available: https://www.immuniweb.com/. [Accessed 6 May 2020].

[38] Wikipedia, “ImmuniWeb,” 22 January 2020. [Online]. Available: https://en.wikipedia.org/wiki/ImmuniWeb. [Accessed May 4 2020].

[39] The Android public API documentation, “Security tips,” 27 December 2019. [Online]. Available: https://developer.android.com/training/articles/security-tips. [Accessed 14 March 2020].



Andreea-Cristina STROE has graduated the Faculty of Cybernetics, Statistics and Economic Informatics from Bucharest University of Economic Studies in 2018. She holds a Master diploma in Economics Informatics from 2020. Currently, she is a PhD candidate student of Economic Informatics at Faculty of Cybernetics, Statistics and Economic Informatics from the Bucharest University of Economic Studies. Her work focuses on the digitalization of education system and security of m-learning and u-learning solutions.