ISSN 1870-4069

Security Validation with Owasp Mobile for the Data Protection in Oral Health

Katerine Márceles[1], Clara L. Burbano[2], Gustavo Uribe[3], Diana Burbano[4]

[1,2,3] Grupo TIC-Unicomfacauca, Corporación Universitaria de Comfacauca, Popayán, Colombia
[4] Universidad Cooperativa de Colombia, Popayán, Colombia
{[1]kmarceles, [2]cburbano, [3]guribe}@unicomfacauca.edu.co
[4]caritoburg@yahoo.com

Abstract. The paper presents an analysis of requirements of information security in mobile applications focused on oral health. We studied the security of a mobile application developed in Android, referring to national and international standards, legislation and the Owasp Mobile recommendations. The current increasing use of mobile devices and the ubiquity of information through Internet allows the unauthorized access to information. Also, oral health mobile applications face this problem. Therefore, they usually don't include private information required in some health processes. This paper faces the problem of the information reliability and security in health mobile applications, performing security tests aligned with the risks identified for the Owasp mobile.

Keywords: security, data protection, mobile applications, mHealth, legislation, OWASP.

1 Introduction

Guaranteeing security of mobile applications is an imperative due to diverse at- tacks on their integrity, confidentiality, and availability. The current problem with mobile applications is lack of protection and not treating information according to standards and legislation of the country of origin. In order to mitigate this problem, good practices of mobile application programming have been developed, documented in the Open Web

Application Security Project (OWASP) Top Ten of Most Critical Web Application Security Risks [1]. It addresses problems like information leakage, missing or broken authentication of the application user, enabling phishing, attacks through cross-site scripting and/or SQL injection, among others. The technological development presented in this article guides to generate an application that at least complies with the legal data protection requirements of the country of origin and is built under safe development methodologies aligned with OWASP for mobile phones. The country of origin for this study is Colombia. However, the principles followed can be applied to other countries as well. The current study was performed on a mobile application named OralHealth with the function of calculate the O'Leary index based on the stored information. Therefore, appropriate measures to protect users' security and privacy are inevitable.

2 Mobile Applications in the Field of Oral Health

In recent years, the term "mobile health" [2] has been used for referring to the use of mobile devices in the health care. Currently, there is a variety of apps (mobile applications) in the area of oral health, where users are dentists, but also children and adults, who intend to take care of their teeth and to have fun while deploying their mobile. A list of apps is shown in Table 1.

Table. 1. List of mobile applications for the Oral Health [3,4].

Application	Description
Brush Dj	Application offering a play-list during two minutes while tooth brushing is performed
Brush	This application teaches the correct tooth brushing trough different games
Dental Expert	Application that respond to the frequent asked questions of the users and give advices about topics related with the oral health as: Teeth whitening, oral self-care and emergencies.
Tooth protection tips	This application offers tips for keeping a perfect smile
BrushyTime	Application for children teaching the tooth brush trough draws, games and a digital clock
Dental Care Aid	Application that describe procedures related with the oral health using illustrations
Philips Zoom	This app allows the virtual teeth whitening

The Food and Drug Administration [5], define that the software executable in a mobile platform can be used as medical device. In the mHealth App Developer Economics [6], the 3% of the apps are published in the health category in the Google Play, iTunes and Microsoft Phone stores.

Also, is highlighted the presence of smart mobile devices in countries as: Venezuela (20%), Chile (18%), Argentina (17%), Brazil (16%), Mexico (15%), Perú (9%) and Colombia (8%). For the 2013 year, researchers discovered the fact that Android have a 45% of participation in the market [6][7].

According to the 2015 statistics in Colombia, mobile devices were used by 95.6% of the population [8]. It is important to note that around 700,000 apps are available for download [9].

On other hand, 3% of them are apps related to health, which have reached about 44 million downloads a year [10] [11]; In 2018, it is estimated that about 50% of the 3.4 trillion mobile devices will use health apps [12].

2.1 Information Security in Mobile Applications

Information security is defined as preservation of confidentiality, integrity, authenticity and availability of information managed by, e.g., mobile applications. It requires technical measures to guarantee authenticity, reliability and non-repudiation of access to hardware (e.g. tablets and/or smart phones) and the software (data entered, stored, processed and communicated by OralHealth application.

When talking about information security on mobiles, it is necessary to identify their vulnerabilities (possible attacks) as well as the risks (probability of occurrence and resulting damages) when using the devices. Possible security risks are the infection of the device by malware, or unauthorized access to, theft or modification of information. Bad practices in the development of the applications increase the aforementioned risks. In order to minimize vulnerabilities and risks it is important to consider the operating system, technologies and communication networks, and to deploy good development practices and related standards [13].

OWASP Mobile Security Model is a tool intended to give developers the resources they need to build and maintain secure mobile applications. Furthermore, it allows the classification of mobile se curity risks providing necessary development controls to reduce the risk of attacks against the applications [1]. For a secure development of the OralHealth application based on the Android operating system, the OWASP Mobile Top Ten guidelines [14] as well as the NowSecure Chapter 7 Mobile Applications Development Manual for Android systems have been used [15]. Furthermore, the national and international leg- islation safeguarding data stored by the user was considered. The Android platform was used because of its significant growth in the last years with respect to the other platforms. For example, in 2016 Android could score an increase of use by 10.3% in relation to IOS and others [16].

Additionally, it was required that the OralHealth application complies with the legal guidelines of the Colombian government and inter- national standards. In Colombia, the Online Government Manual requires for 2018 that every application must guarantee the four dimensions making up security and privacy of information measures designed to protect information against unauthorized access, unintended use, unauthorized or illegal disclosure, interruption or unauthorized destruction [7].

Fig. 1. The top ten information security risks for mobile apps [1].

The top ten information security risks for mobile apps was published in 2014 by OWASP, based on the statistics of vulnerabilities. The Fig. 1 shown this top ten security

risks. Furthermore, the apps should follow the next steps in order to analyze its level of information security [18]:

1. Compilation of information: The scope of the application is defined.
2. Static analysis: The security in the source code of the application is verified.
3. Dynamic analysis: The security of the application is analyzed in execution over a device or an emulator [19].

2.2 Legal and Regulatory Aspects in the Area of Health

Internationally, the health entities responsible for the proper management of patients' medical information align their processes to regulations and standards such as HIPAA, COBIT 5, ISO 27002, CALDICOTT, ITU-T, and HL7. They provide guidelines for regulating the exchange of personal data. Another relevant regulation is the Organic Law 15/1999 of Spain related to the automated processing of personal data LOPD [20]. Following, the selected standards implemented in OralHealth are briefly described. HIPAA [21] (Health Insurance Portability and Accountability Act), this law defines the policies for protecting the confidentiality, integrity and availability of the patient information. ISO / IEC 27002:2013 defines good information security practices, addressing confidentiality, integrity, authenticity and availability of information as well as the security of information systems involved [22].

Similarly, there is a related national legislation on data protection in place in Colombia to guarantee confidentiality, integrity and availability. Examples are: Law 1273 from 2009, article 269F, on violation of personal data by entities who, without being entitled to do so, for their own benefit or for a third party, obtain, compile, subtract, offer, sell, exchange, send, purchase, intercept, disclose, modify or use personal codes, personal data contained in files and/or databases [23].

In Article 10 of Decree 1377 from 2013, which regulates Law 1581 from 2012, the National Health Institute, as handler of personal data obtained through a website and / or any other type of device, requests its users' authorization when deploying personal data in accordance with the privacy policies that have been established under the terms of Law 1581 from 2012 on Protection of Personal Data in Colombia. It should be noted that personal data provided may be processed, collected, stored, used, deleted and / or updated in accordance with terms and conditions of the privacy policies established by the National Health Institute [24].

On the other hand, the congress of the Republic of Colombia promulgates in the 599 law of July 24 of 2000 [25] the crimes against individual liberty and other guarantees, including the violation of the privacy, reservation and interception of communications. The violation of the privacy in the Colombian communication enforce the data protection declared in the 192 articles.

3 Methods

The work realized is the type descriptive and experimental performing tests of dynamic analysis for identify the vulnerabilities of the mobile applications based on the OWASP mobile recommendations.

Taking into account the different aforementioned concepts, we continued verifying for the designed OralHealth application the compliance with Colombian minimum

legal and regulatory requirements and international standards. Furthermore, we ensured that the development process followed good practice in safeguarding personal data.
The application was verified using the checklist structured under article 269f of Law 1273 from 2009 and Decree 1377 from 2013 of Law 1571 from 2012 about the policies of use, i.e. terms and conditions the application follows at the time of registration. Furthermore, computer security software tools such as zAnti, YSO Mobile Security Framework, ZAP OWASP and Wireshark have been applied.

Those tools enabled the performance of intrusion tests, allowing the verification of some controls of ISO / IEC 27002: 2013 related to Clause 9 Access Control, Clause 10 Cryptography, Clause 14 Acquisition, Development and Maintenance of Information Systems, and Clause 18 Compliance with Regard to the Legal Part. It should be noted that the YSO Mobile Security Framework as a hybrid tool generated several false positives and negatives which were manually verified to corroborate them. The Top Ten of the OWASP Mobile Security Project [9] have been checked for each of the 10 risks identified in the 2014 list: *Weakness in the server-side controls of the application, Insufficient storage in the transport layer, Insufficient transport layer protection, Unintentional data leak, Poor authentication and authorization, Broken cryptography, Client-side injection, Security decisions via untrusted entries, Handling of inappropriate sessions, and Lack of protection of binaries.* The YSO Mobile Security Framework have been complemented by social engineering techniques.

4 Results

Verifying the risks determined by OWASP, by widely used information security standards, and by the data protection legislation in Colombia, the following evaluation results were obtained for the OralHealth application:

M1 Weakness in the server-side controls of the application: For the exploitation of this vulnerability SQL injections were made, allowing the validation of the corresponding text fields. It is evident that the mobile device connects to the server application remotely, which has sufficient security controls, since the application can man- age non-validated or malicious data preventing the SQL injection.

M2 insufficient storage in the transport layer: The application stores the data in a secure way, i.e., it does not store them in the device but in the server, and it does not store temporary data. The stored data was encrypted with the AES 256 encryption standard, and the PBKDF2 function allowed the generation of strong keys.

M3 ***insufficient protection in the transport layer***: The application in the device is connected to the server, transmitting information over an encrypted connection. The SSLSocketFactory for secure SSL/TLS channels is used to validate the server identity, so reducing the interception risk for the stored data.

M4 ***unintentional data leakage***: When updating the operating system, software frameworks and application did not change the behavior. Furthermore, the status of the back doors was checked.

M5 ***poor authentication and authorization***: The application provides adequate and necessary levels of authorization and authentication by implementing secure pass-

words of at least 6 digits with alphanumeric and numeric characters. Furthermore, the location of the memory storing the password for hash calculation is deleted.

M6 ***cryptographic weakness***: The application performs an adequate encryption of the information stored and transmitted (from or to the device), as evidenced above. Additionally, the executable code is obfuscated by randomization of the design address space (ASLR).

M7 ***injection from the client side***: The mobile device application has security controls for data entry and for sending data to the server. It should be noted that this is one of the risks that took a little longer time for assurance, as black and white box tests (Sql injection attacks, Java Script injection (XSS), Fuzzing and inclusion of local files) had to be performed. Those tests allow verifying the integrity, confidentiality and availability of the information. The queries were parameterized and validated to mitigate the risk of Sql and Fuzzing attacks, deactivation for any WebViews of the File System Access and JavaScript.

M8 ***security decisions via untrusted inputs***: The application receives only validated data, given the different controls previously implemented.

M9 ***inappropriate session management***: The application has adequate security levels, so that the user session cannot be intercepted and / or overridden. This is done by implementing security mechanisms, among them a check at the beginning of each activity.

M10 Regarding the ***lack of binary protection***: It could be verified that there were no changes of the binaries of the application and no modification of the behavior of the binaries during the different training tests, including checks regarding SU (superuser) command as well as certificate verification. In this same sense, the checklist de- signed under Colombian legislation and aligned with the selected international standards was applied, and its compliance was verified, in addition to the safe development related to the controls defined in the ISO/IEC 27002:2013 and the policies of se cure development defined by OWASP, which allowed the assurance of the data stored by the user. On the other hand, it was verified that the OralHealth application can be- come vulnerable through inadequate configuration of social engineering techniques. Therefore, it is suggested to follow good practices and the recommended installation guide.

Finally, the application OralHealth is in line with the guidelines for mobile insurance development, the specific risks by the Owasp, standards of information security and protection legislation of data in Colombia. Many of the security flaws are not due to operative system updates, but non-implementation of secure application development. Dice to the above the mobile application developers for Android should start using methodologies aligned to standards to provide a degree of computer security to users of the platform.

5 Discussion

It is important to note that the alteration of information stored in the application can impact the integrity of the user, leading to fraud and / or impersonation through the application. It may involve the alteration and disclosure of personal and clinical data on the user's oral health, e.g.: name, email, login, password, and the O'Leary clinical

records. These are protected by Law 1581 on data protection from 2012, Law 1266 on Habeas Data from 2008 and Law 1273 on cybercrimes from 2009. The legal repercussions of that bring the compulsory of secure development in mobile phones and in any type of application.

6 Conclusions

During the process of implementing the Colombian data protection standards and legislation, aligned with the e-Government Manual with its fourth information security dimensions, it was determined that in order to comply with these challenges, it is necessary to implement a secure development process. That process must be parameterized according to the latest identified risks, further mitigating the risk for the stored information. In summary, the model shown in Fig. 2:

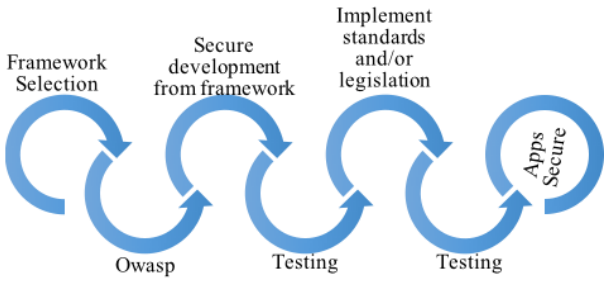

Fig. 2. Safe agile mobile development.

The model presented in Fig. 2 intends a mobile application with the minimum-security parameters able to safeguard the information in accordance with legal guidelines.

References

1. Owasp Mobile Security (2016)
2. Fiordelli, M., Diviani, N., Schulz, P.: Mobile Health Research Mapping: A Decade of Evolution. Journal of Medical Internet Research (2013)
3. Conozca 5 aplicaciones móviles para cuidar de la salud bucal (2016)
4. Aplicaciones móviles para cuidar tu salud dental (2016)
5. U.S. Food and Drug Administration: CDRH-CBER (2015)
6. Research2guidance: mHealth App Developer Economics (2015)
7. Ramos, S.: Android amplió su dominio a nivel mundial mientras iOS cae. Social Geek (2016)
8. Population using mobile devices in Colombia (2015)
9. Administrativo Estadístico Nacional de Estadística: Indicadores básicos de tenencia y uso de tecnologías de la información y comunicación. Boletín Técnico, Colombia (2016)
10. Ifrach, B., Johari, R.: Pricing a bestseller: sales and visibility in the marketplace for mobile apps. ACM SIGMETRICS Performance Evaluation Review (2014)

11. Fox, R., Cooley, J., McGrath, M., Hauswirth, M.: Mobile health apps - from singular to collaborative. Stud Health Technol Inform (2012)
12. Santamaría-Puerto, G., Hernández-Rincón, E., Suárez- Obando, F.: Use of mobile health applications with Internal Medicine patients at the Regional Hospital of Duitama, Boyacá, Colombia. Cuban Journal of Information in Health Sciences (2016)
13. Shuren, J.: FDA's role in the development of medical mobile applications. Clinical Pharmacology & Therapeutics (2014)
14. Villegas, G.: La seguridad en aplicaciones móviles: estrategias en el mundo actual (2016)
15. OWASP Mobile Security Project: Top 10 mobile risks (2016)
16. nowsecure.com: Android: Secure mobile development (2016)
17. Sergio, R.: Android expanded its dominance globally while iOS drops. http://socialgeek.co/moviles/android-amplia-dominio-nivel-worldwide-ios-cae [Last Accessed: 22 11 2016]
18. Ministerio de Tecnologías de la Información y las Comunicaciones: Decreto 2573 de 2014, Colombia (2014)
19. Leonardo-Ramírez, L.: Estrategia de validación para aplicaciones móviles de salud. IAI, Actas de Ingeniería, vol. 2, pp. 325–333 (2016)
20. Díaz, S.: Mejores prácticas en las pruebas de aplicaciones móviles, ATSistemas, España (2013)
21. Informáticos Europeos Expertos: Protección de datos de carácter personal (2016)
22. Ayuda Legal: Ley Hipaa y la confidencialidad de la información médica (2016)
23. International Standards Organization, ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security controls (2013)
24. Congreso de Colombia: Ley 1273 de 2009 - Legislación de Delitos Informáticos, Bogotá
25. Gobierno de Clombia: Authorization for the Processing of Personal Data National Institute of Health (2016)
26. Secretaría del Senado de Colombia: Ley 599 de 2000