Sci.Int.(Lahore),26(4),1451-1454,2014 ISSN 1013-5316; CODEN: SINTE 8

VALIDATION OF SECURITY REQUIREMENTS FOR MOBILE APPLICATION: A STUDY

Noorrezam Yusop[1], Massila Kamalrudin[2], Sharifah Sakinah[2], Safiah Sidek[2]
[1]Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.
[2]Innovative Software System and Services Group, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.
Email: [1]noorrezam@gmail.com, [2]massila@utem.edu.my, [2]sakinah@utem.edu.my, [2]safiahsidek@utem.edu.my

ABSTRACT : *The increased usage of 3G and 4G networks in smartphones has resulted in the need for validating security requirement to ensure safe and secure mobile application experience to users. However, improper validation of security requirements can lead to poor quality of software development. This is also commonly happened while developing software application for mobile. Thus, this paper discusses the gaps found from the existing work on validating the security requirements of mobile application and analyses a few security requirement engineering tools for mobile application that exist in the market for commercial or research purposes. We report our findings from review and analysis of different studies on security requirement engineering for mobile application. The strengths and weaknesses of the features and utility are also presented to provide further understanding of the gaps and weaknesses of each tool. We conclude that these tools are still immature and need further improvements.*

KEYWORDS: security requirements, mobile security testing, security requirements validation, mobile application

1.0 INTRODUCTION

Security requirements are classified as non-Functional Requirements (NFR) and they are related to system confidentiality, integrity and availability. Further, all developed software including the mobile applications need to fulfil the NFR for safe mobile application usage to users. Currently, the widespread development of mobile application particularly the emergence of the 3G and 4G networks smart phones has allowed the conduct of online finance, business and social interactions. Parallel to this development, the validation of security requirement for mobile application has become increasingly important. In this case, it is necessary to conduct security testing as most of the applications carry important data that involve sensitivity and privacy. Further, considering that validating specified and implemented security measures often reveal critical security holes and threats [1], mobile application developers need to ensure safe and secure mobile application experience to their customers. Therefore, mobile security testing is becoming an essential process in the development of mobile application. Here, security requirement elements such as authority, authorization, data bridge, and confidentiality of data are tested between mobile and remote data access with database.

In this paper, a review on existing works and tool support to validate security requirements for mobile application are presented. The paper is organised as follows: Section 2 describes the survey of literature. Section 3 presents a description of selected tools for security requirements validation available in the market together with its comparison analysis. Section 4 is devoted to the discussion of the overall findings and this paper ends with a conclusion section.

2.0 RELATED WORK

There are many works done to validate security requirements. For example, a work by [2] presents a validation technique called the IVT method, which is implemented in MICASA tools. This technique is able to find defects and generate test case within a short period of time. However, this technique is found to be more suitable for senior testers as it generates high level syntacting coverage, which is only understandable by senior testers. Meanwhile, Mee et al. developed an elastic pattern to detect the defect based on the manual tester. However, both of works focus on web-based environment [2][3] rather than for the mobile application. In addition, Gilbert et al. [4] applied the AppInspector, an automated security validation system that analyses applications and generates report for potential security and privacy violations. The authors describes the future need for making a more secured smartphones applications through automated validation and they outline its key challenges such as detecting and analysing security as well as privacy violation through test coverage and scaling to large numbers of application [4]. Nevertheless, the validation for security still has a drawback, which is it does not cover all aspects of security requirements. Meanwhile, Vapen et al. [5] discussed a method for evaluating and designing authentication solutions using mobile phones. The method considers availability, usability and goal to help developers to create secure authentication, considering the users' priorities on security, availability and usability [5]. However, this tool does not propose the validation for authentication and testing mobile application that are locked to phone vendor. Another work is by Syntel [6] who developed a high quality mobile application by creating a secure mobile testing strategy for end-to-end mobile application testing. Here, a Hybrid Script with fewer frameworks is designed to run the test scripts on the devices and to reduce the testing cost and effort to 20-30%. This tool identifies the right set of tools and a framework with devise based the perspective that an access restriction is imperative to effective mobile application testing [6]. However, it is a challenge to develop a high quality tool as it needs to combine two scripts in order to create hybrid framework. Mahmood et al. [7] presented a

ramework for automated security with intelligent fuzz testing for Android applications on the cloud. It provides a fully automated test case generation and iterative feedback loop by providing graphical reporting environment to visually explore the results of the testing. This approach also targets the security issues on android applications but it does not cater validating security requirements before the development stage. Born et al. [8] proposed to define a model driven software construction process, which enables the integration of system development and system test. It includes the provision of a set of supporting tools to increase the level of automation in this process. Then, they implement code generators for the automatic generation of software and test components. They also did verification of the process, the concepts and the generators within the development and implementation of an application system that involves a technology from the mobile computing domain [8]. However, their work did not cover the testing of mobile application. Rhee et al. discussed a methodology to test the Mobile Device Management agent. The authors proposed items and methods to identify security requirements, their processes, and real world test methods for Android devices. They stated that MDM agent can be reused and extended to evaluate the security of other applications on mobile devices [9]. Nevertheless, the security of the MDM agent to strengthen the security of the mobile devices needs improvements and does not support various mobile devices.

In summary, most of the works in validating security requirements discussed have some gaps and limitation. Most of the techniques used are complex, still immature and some do not support mobile application development. Further, most techniques applied for testing security requirements for mobile application only cover specific mobile devices and they do not cover across different platform. Therefore, it is found that further works to validate security requirements for mobile application is in need especially to support application across platforms mobile devices.

3.0 TOOLS SURVEY

There have been several works on developing tools to validate the security requirement for mobile applications. In this section, we present a descriptive review of six security requirements validation tool for mobile applications. Our goal is to investigate and evaluate the usefulness of the automated security requirements validation tools on mobile application use for commercial and research purposes. Perfecto Mobile service [10] provided public services in term of testing the internet connection between different modern hardware and software mobile platforms (Android, iOS, Windows Phone, and Symbian) that can be integrated with HP UFT (QTP). However, this tool requires integration testing techniques for combinational, test generation services and services for automate dynamic security testing. Gilbert et al. [4] proposed AppsInspector tool, an automated security testing and validation system to analyse and generate reports of potential security and privacy violation. However, this tool focuses on the validation of smartphone application at the app-market level to test and verify the security properties of application. Automated validation of application at central

Table 1: Comparison of mobile security testing

Tools Name	**Approach / Methodology and Technique**	**Requirement representation**			**Mobile Security requirements Aspects**						**Support Platforms**		
Features	Support across platform	Formal	Semi-Formal	Informal	Confidentiality	Integrity	Authentication	Authorization	Availability	No-Repudiation	Android	iOS	Windows
Perfecto Mobile	Remote access	x	/	x	x	/	/	/	/	/	/	/	x
Apps Inspector	EDS Test	x	/	x	/	/	/	/	/	/	/	x	x
A^2T^2	Dynamic Analysis	x	/	x	x	x	x	x	x	x	/	/	x
App Twack	Remote access	x	/	x	/	/	/	/	/	/	/	/	x
Applause	Git branch model	x	/	x	/	/	x	/	x	x	/	/	/
Veracode	White box test	x	/	x	/	/	/	/	/	/	/	/	x
Total		0	6	0	4	5	4	5	4	4	6	5	1

distribution points is an important step toward enabling a more secure mobile computing [4].

Amalfitano et al. [11] proposed a tool to overcome the issues of automatic testing of mobile application for Google Android platform. The technique is supported by a tool named A^2T^2 (Android Automatic Testing Tool) and it is used for both crawling the application and generating the test cases for a simple Android application. Yet, this tool is used primarily for finding runtime crashed or user events faults produced through the GUI: It is not a tool to validate the security requirements. Next, AppThwack is a cloud-based real device testing website. This tool can be used to test android, IOS and web application on real device on cloud. AppThwack analyses each screen and maps their app in real time, screen capturing and perform data and any error that occurs. However, this tool has problem to read database file in localhost [12]. Moreover, this tool does not offer validation of security requirement before they produce a final result. Applause brings together the tightly integrated application quality solutions that companies need to earn and measure the loyalty of their users. These tools support across different platforms to ease developers to get coverage across all major mobile devices. Here wild testing is implemented to ensure the application is working well in real environment. Further, these tools also offer the distribution of application as well as bug reporting [13]. However, this tool is still weak for automation scripts errors, scope change and complexity. Next, Veracode is an automated tool that promises to slash the time taken to complete process of identifying and understanding the vulnerability that can be exploited to the code. This tool can check and analyse non-existing source code through API. However, this tool is poor in position automated static analysis (SAST), and it does not offer validation of security requirement [14].

3.1 TOOLS COMPARISON

We compare the six existing tools for validating security requirements of mobile application. Here, we compare the features based on method/approach, requirement representation, mobile security requirements aspects and support platforms as shown in Table 1 below.

DISCUSSION

Security Requirements engineering research has been established for many years and security requirements is a part of the non-functional requirement. Validating security requirements at the early phase contributes to the success of secure software especially the mobile application. However, current works and tools do not provide a proper means to validate security requirements for mobile application and the current techniques are tedious, expensive and time consuming. Thus, it is necessary to have automated validation on security requirement especially on mobile application. We have conducted a review on six types of tools that support the validation of security requirements such as Perfectto Mobile, AppsInspector, A^2T^2, AppTwack, Applause and Veracode. Based on our review as shown on Table 1, we found that there are various approaches or methodologies used by existing security tools for mobile application. We also found that validating security requirement for mobile are based on the specificity and purpose of the respective tools. All of the tools have reperesentation of requirement in the form of semi-formal model. In terms of security requirements, most of the tools cover the aspect of integrity and authorization, followed by the authentication and availability. All of these aspects are the important security elements that need to be considered in the mobile application to ensure the safety, security and privacy of the data to the users. We also found that confidentiality has been ignored by most of the tools although confidentiality is important for mobile application as it is related to authorization and privacy. Based on the analysis, most of the tools support IOS and Android users, but not Windows users. Most also do not support cross platform and only working well in a single platform.

4.0 CONCLUSION AND FUTURE WORKS

Validating security requirements for mobile application during the early phase of software development is important. Due to the rapid development of mobile application, validation of security requirements is seriously needed to ensure the safety, privacy and confidentiality of data. For future works, we plan to develop an approach and tool that is able to support end-to-end validation of security requirements of mobile applications across platforms.

ACKNOWLEDGEMENTS

We would like to thank Universiti Teknikal Malaysia Melaka for its support and Sciencefund grant: 01-01-14-SF0106 for funding this research.

REFERENCES

[1] Capgemini, *Taking Mobile Security to the Next Level*, 2013.

[2] J.H.Hayes, *Input validation testing: A System level, early lifecycle technique*, 1998.

[3] S.Mee, *Testing Mobile Web Applications for W3C Best Practice*, 2012.

[4] P.Gilbert and B.Cun, *Automated Security Validation of Mobile Apps at App Markets*, 2011.

[5] A.Vapen and N.Shahmehri, *Security levels for web authentication using MobilePhones*, 2012.

[6] Syntel, *Secure automated solutions for mobile application testing*, 2012.

[7] R. Mahmood, N. Esfahani, T. Kacem, N. Mirzaei, S. Malek, and A. Stavrou, "A whitebox approach for automated security testing of Android applications on the cloud," in *2012 7th International Workshop on Automation of Software Test (AST)*, pp. 22–28, 2012.

[8] M.Born and I.Schieferdecker, *Model-Driven Development and Testing*, 2014.

[9] K. Rhee, H. Kim and H.Y.Na, *Security Test Methodology for an Agent of a Mobile Device Management System*, 2014.

[10] Perfecto Mobile, http://perfectomobile.com, Accessed from: 2013.
D. Amalfitano, A. R. Fasolino, P. Tramontana, and N. Federico, *A GUI Crawling-based technique for Android Mobile Application Testing*," 2012.
[11] AppThwack, https://appthwack.com/overview, Accessed from: 2014.
[12] Applause, http://www.applause.com/, Accessed from: June 2014.
[13] State of Software security report, *The Intractable Problem Insecure Software*, vol.4, 2011.