Faculty of Information and Communication Technology

AN AUTOMATED APPROACH TO ELICIT AND VALIDATE SECURITY REQUIREMENTS OF MOBILE APPLICATION

Noorrezam bin Yusop

Doctor of Philosophy

2018

DECLARATION

I declare that this thesis entitled "An Automated Approach to Elicit and Validate Security Requirements of Mobile Application" is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : ……

Name : Noorrezam Bin Yusop

Date : ……

APPROVAL

I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in term of scope and quality for the award of Doctor of Philosophy.

Signature	:	……...
Supervisor Name	:	Assoc. Prof. Dr. Massila Binti Kamalrudin
Date	:	……..…….....

DEDICATION

This thesis is dedicated to my beloved parents; Yusop bin Harun, my mother, Asiah binti Daud, siblings and family to support

My warmest appreciation to my beloved wife and daughter, Nur Ezyanie binti Safie and Nawwal Erina binti Noorrezam for all their sacrifices, understanding, love, care, motivation and support.

My appreciation to my mother in laws, Saryati binti Tukimin and father in law, Safie bin Parlan for understanding and support,

who have always loved me unconditionally and whose good examples have taught me to work hard for the things that I aspire to achieve. They have successfully made me the person I am becoming.

ABSTRACT

Mobile phone usage has continued to rise, and it is becoming more convenient for users to use mobile applications for booking hotels, conducting online transaction and online payment. In this case, secured applications are required to increase the confidence among mobile users. In order to achieve correct secure application, a correct security requirements needs to be elicited and defined. Additionally, it is also crucial for security requirements of mobile apps to fulfill basic quality attributes such as correct, consistent and complete (3Cs). However, few problems are found in eliciting security requirements for mobile apps. Firstly, most requirements engineers (RE) are identified to have less knowledge and understanding of security requirements attributes, leading to the failure of implementing the 3Cs of security requirements. Secondly, most of the elicitation and the validation of security requirements are conducted at the later stage of the development and leads to poor quality security requirements implementation which might resulted to project failure. Motivated from these problems, the objectives of this thesis are three-folds; 1) To analyze the security requirements for mobile apps, 2) To propose an approach to elicit and end-to-end validation of security requirement, and 3) To evaluate the efficacy in term of correctness and performance as well as usability of the approach. This thesis proposes a new automated approach to assist the elicitation and validation of security requirements. Here an automated tool support called MobiMEReq is also developed. For this, we have adopted Test Driven Development (TDD) methodology with semi-formalized models: i) Essential Use Cases (EUCs) and ii) Essential User Interface (EUI). We then divided our approach into two parts: 1) Elicitation and 2) End-to-end validation security requirements. Further, we have developed pattern libraries to assist on the correct elicitation and validation. They are mobile Security attributes pattern library and mobile security pattern library. Then, we have constructed a new algorithm using fuzzy logic to assist on the prioritization of the test for better performance of validation. Finally, a comprehensive evaluation of the approach, comprising experiments of correctness test and usability test were conducted. Here, we have also evaluated the feedback from the industry experts especially on the usability of the automated approach and tool support. In summary, the findings of the evaluations show that our approach is able to contribute to the body of knowledge of mobile security requirements engineering especially in enhancing the performance and correctness level of security attribute elicitation and its usability for end-to-end elicitation and validation. It is found that the approach able to enhance the correctness level of the elicited security attribute compared to the manual approach, and produce correct generation of test. Then, the results of the usability test by the novice and experts show that the approach is useful in eliciting and validating security requirements at the early stage of application development and is able to ease the elicitation and validation process of security requirements of mobile apps.

ABSTRAK

Penggunaan telefon mudah alih didapati meningkat dan lebih mudah digunakan oleh pengguna untuk menggunakan aplikasi menempah hotel, menjalankan transaksi dalam talian dan pembayaran dalam talian. Maka, aplikasi yang selamat adalah diperlukan bagi meningkatkan keyakinan pengguna telefon bimbit. Bagi mencapai aplikasi keselamatan yang betul, keperluan keselamatan yang betul perlu dicungkil dan dikenalpasti. Tambahan juga, atribut berkualiti seperti menjadikan ketepatan, konsisten dan lengkap (3Cs) diperlukan oleh keselematan kepada aplikasi telefon. Justeru itu, beberapa masalah dikenalpasti dalam pencungkilan keperluan keselamatan aplikasi telefon. Pertama, kebanyakan Jurutera Keperluan (RE) didapati kurang pengetahuan dan pemahaman atribut keperluan keselamatan yang membawa kepada kegagalan melaksanakan 3Cs keperluan keselamatan. Kedua, kebanyakan pencungkilan dan validasi keperluan keselamatan dikendalikan di peringkat akhir pembangunan dan menyebabkan kualiti keperluan keselamatan lemah dan menyebabkan kegagalan projek. Motivasi kepada masalah ini, objektif tesis ini terdiri tiga perkara;1)Mengenalpasti keperluan keselamatan aplikasi telefon,2)Mencadangkan pendekatan mencungkil dan menvalidasi akhir-ke-akhir keperluan keselamatan dan 3)Menilai keberkesanan dalam ketepatan dan kecepatan pendekatan kebolehgunaan. Tesis ini mencadangkan pendekatan automatik baharu bagi membantu pencungkilan dan validasi keperluan keselamatan. Di sini, sokongan peralatan automatik dipanggil MobiMEReq dibangunkan. Kami mengguna pakai metodologi Ujian Berpandukan Pembangunan (TDD) bersama model separa formal:i)Kes Berguna Penting (EUC) dan ii)Antara-muka Penting (EUI). Kami kemudiannya bahagikan pendekatan kepada dua bahagian:1)Pencungkilan dan 2)Validasi keperluan keselamatan akhir-ke-akhir. Seterusnya, kami membangunkan pangkalan data bagi membantu ketepatan pencungkilan dan validasi yang terdiri daripada pangkalan data keselamatan atribut dan keselamatan telefon. Kami juga membina algoritma baharu menggunakan logik kabur bagi membantu memendekkan tempoh untuk ujian kecepatan validasi. Akhinya, penilaian menyeluruh pendekatan terdiri daripada eksperimen ujian ketepatan dan kebolehgunaan telah dijalankan. Disini, kami juga menilai maklumbalas pakar industri terutamanya dari aspek kebolehgunaan pendekatan automatik dan sokongan peralatan. Kesimpulannya, penemuan penilaian menunjukkan pendekatan kami mampu menyumbang kepada badan pengetahuan kejuruteraan keperluan keselamatan terutamanya dalam menangani paras kecepatan dan ketepatan pencungkilan keselamatan atribut dan kebolehgunaan bagi pencungkilan dan validasi akhir-ke-akhir.Ianya dikenalpasti bahawa pendekatan ini boleh meningkatkan ketepatan keselamatan atribut yang dicungkil berbanding manual dan menghasilkan ketepatan ujian penjanaan. Kemudiannya, keputusan ujian kebolehgunaan pakar dan novis menunjukkan pendekatan ini berguna dalam pencungkilan dan validasi keperluan keselamatan pada peringkat awal pembangunan aplikasi dan memudahkan proses pencungkilan dan validasi keperluan keselamatan aplikasi telefon.

ACKNOWLEDGEMENTS

Foremost, I am deeply grateful for the continuous support, insight and patience of my supervisors, Associate Professor Dr. Massila Kamalrudin and Professor Dr. Mokhtar Mohd Yusof. Thank you for your continuous support of my Ph.D study and research, for their patience, motivation, guidance, enthusiasm, and immense knowledge throughout my candidature. Their guidance helped me in all the time of research and writing of this thesis. Further, special thanks to Associate Professor Dr. Safiah Sidek for your assistance to proofread and to advice on the organisation of my theses. I gratefully acknowledge to Ministry of Higher Education (MOHE), MyBRAIN15 to support scholarships. I also would also like to thank my parents for their love and continuous support – both spiritually and materially. You are always there for me. Last but not least, to those who indirectly contributed in this research, your kindness means a lot to me.

Thank you very much.

TABLE OF CONTENTS

LIST OF TABLES

TABLE **TITLE**

PAGE

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

RE	:	Requirements Engineer
MobiMEReq	:	Mobile Malay English Requirements
3C	:	Correctness, Completeness and Consistency
TDD	:	Test Driven Development
EUC	:	Essential Use Case
EUI	:	Essential User Interface
SecEUC	:	Security Essential Use Case
SecEUI	:	Security Essential User Interface
SecAttributes	:	Security Attributes

LIST OF RELATED PUBLICATIONS

No.	Publications	Related Chapter
	Journal	
1	Yusop, N., Kamalrudin, M., Sakinah, S., & Sidek, S. (2014). Validation of Security Requirements for Mobile Application : A Study. *Science International Lahore*, *2014*(October), 1451–1454.	1, 2
2	Yusop, N., Kamalrudin, M., Mohd Yusof, M., & Sidek, S. (2016). Meeting Real Challenges in Eliciting Security Attributes for Mobile Application Development. *Journal of Internet Computing and Services(JICS)*, *0170*(5), 25–32.	2
3	Yusop, N., Kamalrudin, M., & Sidek, S. (2015). Jurnal Teknologi. Security Requirements Valdation for Mobile Apps: A Systematic Literature Review. *Jurnal Teknologi*, *34*, 123–137.	2, 3, 4, 5
4	Yusop, N., Kamalrudin, M., & Sidek, S. (2017). Capturing Security Requirements of Mobile Apps Using MobiMEReq. *Asia Pacific Journal of Contemporary Education and Communication Technology (APJCECT)*, *3*(1)	4
5	Yusop, N., Kamalrudin, M., & Sidek, S. (2017). Eliciting security requirements for Mobile Apps: A Replication Study Noorrezam Yusop. *Journal of Theoritical and Applied Information Technology*	4,6
	Book Chapter	
1	Yusop, N., Kamalrudin, M., Sidek, S., and Grundy, J., 2016b. *Automated Support to Capture and Validate Security Requirements for Mobile Apps*,Part of the Communications in Computer and Information Science book series (CCIS, volume 671). Springer, Singapore.	5,6

CHAPTER 1

INTRODUCTION

1.1 Introduction

Quality security requirements are important to increase the confidence of mobile users to perform many online transactions, such as banking, booking and payment via mobile devices. Therefore, issues related to security have become a major concern among mobile users as insecure applications may lead to security vulnerabilities that make them to be easily compromised by hackers. Thus, it is important for mobile application developers and requirements engineers to validate security requirements of mobile apps at the earliest stage of the development to prevent potential security problems. Therefore, this research aims to propose an automated approach to elicit and validate security requirements of mobile application at the early stage of development. The automation process is required to automate the process on eliciting security requirements than conducting manually. Most security requirements conducted using natural language. This means that knowledge to elicit security attributes of security requirements must at early stage.

1.2 Research Background

This research focuses on the issues related to the difficulties to elicit and identify relevant and correct security requirements of mobile application during the development of mobile application. In today's world, mobile application is widely used as it facilitates

mobile users to perform online transactions for banking, e-commerce, online booking and payment. The mobile application is considered as useful applications for people to communicate everywhere, anywhere and anytime. Although it has been considered as part of our everyday life, there have been increased concerns among developers as well as users regarding the security of the mobile apps as it opens up some avenues to be attacked by malicious users.

Eliciting security requirements is crucial at the early stage of apps development. One of the reasons is the complexity of the Common Criteria (CC) of the security requirements that makes it difficult to understand, especially to the novice requirements engineers (Paja et al., 2012). Additionally, developers tend to make mistakes when determining the right security requirements and attributes because they need to personally identify the requirements and attributes without any supports, such as the automation or the manual training. Further, there is no predefined instruction provided to the user when using the GUI for dynamic analysis. This leads to various challenges in completing the security identification process. The aforementioned scenarios indicate the need for an automation that can help to elicit security requirements and attributes, especially for novice requirements engineers.

Further, several researchers have highlighted that the process of the quality security requirements for correct, consistent and completeness (3Cs) requirements from client-stakeholders is often difficult, time consuming and error prone (Kamalrudin and Grundy, 2011)(Paja et al., 2012). Fortunately, requirements engineering use natural language with deal client-stakeholder to collecting security requirements. Requirements engineer then use traceability to improve consistency checking by embedded light-weight automated tracing tool in order to allow client-stakeholder to capture their security requirements. According to Zowghi (2003), consistency requires that no two or more requirements in a

specification contradict each other, where there is no case the requirements cannot be compensate at same time. In eliciting a correct and consistency security requirements at traditional approach, they using natural language processing and analysis of textually expressed requirements require the use of complex analysis algorithms and complexity of natural language. The critical translating requirements in semi-formal model e.g: UML use cases to improve structure natural language continued problematic and having to rely using a complex and mathematical models.

More researchers focus on addressing the approach at the later stage of mobile apps because the later stage has been identified by several researchers as being complicated, costly and lack of proper method (Jaalinoja and Oivo, 2004) and (Kotonya and Sommerville, 1998). Therefore, Quality security requirements approaches at early stage are more cost-effective, improve the quality of mobile application and reduce testing efforts to elicit and validate security requirements compared than conducting at the later stage of software development.

Researchers have proposed some technique for improving accuracy of heuristic analysis approach for elicitation. The current proposed approach try to increase the correctness and consistency of security requirements generated method in elicitation of security requirements including the test character (Liu, 2014), security rules (Enck et al., 2009), classifying mobile application both functional and non-functional requirements (Andreou et al., 2005) or classification of context (Afridi and Gul, 2008).

On the other hands, there are researchers use validation to increase the correctness and completeness of security requirements of mobile application separately that it is including the item and method (Rhee et al., 2012), Test Execution (Vivekanandan et al., 2014), Security Assurance (Krishnan and Zeiser, 2011), Testbed Components (Hargassner et al., 2008), Data-centric model (Dezfouli et al., 2013), Risk catalog (Jha, 2007),

automatic event and test case generation (Hu and Neamtiu, 2011), dependency graph (Gilbert et al., 2011), crawling and generate test case (Amalfitano et al., 2012), performance testing for Android components, usage logging and automatic test case generation (Spataru , 2010), adopts a sensitive-event (Bo et al., 2007), cryptography format (Singaraju and Kang, 2008), automatic test case generation (Avancini et al., 2013) or user behavior modelling, GUI test case generation, and post-test analysis and debugging (Li et al., 2014). Despite the various method and approach and tools is proposed by researchers, there is none of work proven to correct and consistency of mobile application at early stage of mobile application. The heuristic analysis focus at the later stage of development, and there is limited technique in heuristic analysis focusing on work at the early stage of development.

To solve the problem in elicitation and validation, several research have been using several technique from heuristic analysis. Yahya et al. (2013) have been developed eliciting Security Requirements Essential Use Case (SecEUC) using semi-formalize model. However, a several studies discuss the elicitation of security requirements of modelling techniques used, but the limited focusing on eliciting security attributes of security requirements of mobile application. On the other hands, heuristic analysis have been used for making decisions (Silver, 2004) to assist in specifying essential process, detecting an exception and taking correction (Maiden and Sutcliffe, 1993) and help to provide the closest right answer (Kokash, 2005). However, this method has challenges on how method to elicit and validate at same time at early stage of requirements engineering of mobile apps.

The two main problem found to elicit and validate correct security requirements: problem late of elicitation such as understanding and fail to eliciting a correct security attributes of related security requirements and problem late of elicit and validate security

requirements such as the difficult to prioritize test case of security requirements during at early requirements engineering.

Respect to the first problem, failure to elicit security attributes of security requirements may lead to inconsistencies and incorrectness of development application for mobile application. Further study reported, developer could not specify the security attributes at the early requirements phase of product development. This phenomena leads to a plethora of mobile applications to be developed especially for online transaction, changing information and storing data. El-hadary and El-Kassas (2014) stated that the main issue emerged in relation to the growth of mobile application is how to ensure the significance of validating mobile security requirements. They emphasized that identifying security requirements is crucial, although it is often neglected or ignored in the context of requirements analysis (El-hadary and El-kassas, 2014) and the collaboration between client-stakeholder and engineer teams.

For second problem, late elicit and validate of security requirements at early stage result the error prone and time consuming. Although, many of the mobile apps projects have been delivered to users with an increasing amount of data or repository (use large of test case), these projects have failed to perform the validation of security requirements at the early stage of requirements analysis. This practice has resulted in the software to be exposed to malware, which subsequently increases the manpower usage of software testers. There are also instances that they were struggling to accomplish the testing process, which requires cost and time efforts to perform the testing. We believe that this practice may lead to a loss of business value and market trends.

To address this problem, the current practice of security guidance and solution, most developers or engineers refer to the Common Criteria (CC), although the CC is complex and difficult to understand by novice. They found that most of the developers