ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

Meeting Real Challenges in Eliciting Security Attributes for Mobile Application Development

Noorrezam Yusop[1] Massila Kamalrudin[2*] Mokhtar Mohd Yusof[2] Safiah Sidek[2]

ABSTRACT

There has been a rapid growth in the development of mobile application resulting from its wide usage for online transaction, data storage and exchange of information. However, an important issue that has been overlooked is the lack of emphasis on the security issues at the early stage of the development. In fact, security issues have been kept until the later stage of the implementation of mobile apps. Requirements engineers frequently ignore and incorrectly elicit security related requirements at the early stage of mobile application development. This scenario has led to the failure of developing secure and safe mobile application based on the needs of the users. As such, this paper intends to provide further understanding of the real challenges in extracting security attributes for mobile application faced by novice requirements engineers. For this purpose, two experiments on eliciting security attributes requirements of textual requirements scenario were conducted. The performance related to the correctness and time taken to elicit the security attributes were measured and recorded. It was found that the process of eliciting correct security attributes for mobile application requires effort, knowledge and skills. The findings indicate that an automated tool for correct elicitation security attributes requirement could help to overcome the challenges in eliciting security attributes requirements, especially among novice requirements engineers.

☞ keyword : Security requirement, security attribute, mobile application development

1. Introduction

In the era of globalization, the use of mobile devices has grown at an exponential rate leading to the development of a plethora of mobile applications, especially for online transaction, data storage and exchange of information. In this case, developing a secure and safe mobile application has become a priority. However, when eliciting requirements from clients, requirements engineers tend to neglect or ignorethe security-related requirements, causing incorrect elicitation of requirements [1][2]. Further, failure to develop a secure mobile application may result in high risk of uncertainty in using the application, and this eventually leads to resistanceamong the end-users to use the applications.

Recognizing the importance of identifying security attributes of mobile application, this study aims to investigate the challenges faced by requirements engineers (REs) to elicit the security attribute of mobile application. For this purpose, an experiment to elicit security requirements and security attributes, involving students of Software Engineering has been conducted.

This paper focuses on describing the challenges faced by requirements engineers to elicit security attributes of specific functional requirements of a mobile application. It is organized into five sections. Subsequent to this section, the Motivation and Background of the Study is presented in Section 2. This is followed by Section 3, which presents the description of our experiment. Next, Section 4 describes the result and discussion and this paper ends with a conclusion section and future work in Section 5.

2. MOTIVATION AND BACKGROUND OF STUDY

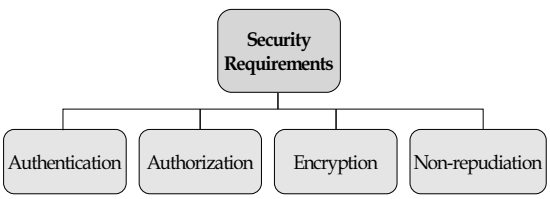
Security requirements are classified as non-Functional Requirements (NFRs) and they are related to system

[1] Faculty of Communication and Information Technology, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia
[2] Innovative and Software System and Services Group, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia
* Corresponding author (massila@utem.edu.my)
[Received 9 May 2016, Reviewed 24 May 2016, Accepted 15 June 2016]
☆ A preliminary version of this paper was presented at ICONI 2015 and was selected as an outstanding paper.

confidentiality, integrity and availability. Security requirements can also be defined as a system specification with required security that includes specifications with the types and levels of protection necessary for the data, information, and application of the system [3].

The most common security related requirements for software are shown in Figure 1. They are [4]:

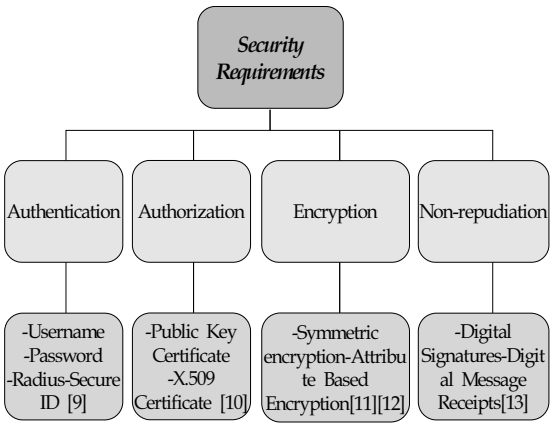
Authentication: Application can verify the identity of their users and other applications with which they communicate. Authorization: Authenticated users and applications have defined access right to the resources of the system. Encryption: The message sent/to /from the application is encrypted. Integrity: This ensures the contents of the message are not altered in transit. Nonrepudiation: The sender of the message has a proof of delivery and the receiver is assured of the sender's identity. This means that neither the sender nor the receiver can subsequently refute their participation in the message exchange.



(Figure 1) TYPE OF SECURITY REQUIREMENTS

Security requirements attribute or security attribute can be defined as any piece of information that may be associated with a controlled implicit entity or user for the purpose of implementing a security policy that is not necessarily implemented directly in data structures [5]. It provides a behavioral attributes such as reliability, availability, safety, confidentiality and exclusivity or more accurately to security and dependability related attributes [6][7][8]. Figure 2 shows the attributes used for each security related requirements.

The main problem faced by the requirements engineers is that they have difficulties to elicit the correct security requirements for mobile application. They also fail to identify relevant security attribute for security requirements. Additionally, most of the elicited security attributes do not match specifically to the purpose of the mobile application. It is also found that very limited work has been conducted to overcome these problems.



(Figure 2) SECURITY REQUIREMENTS AND ITS RELATED SECURITY ATTRIBUTES

At present, most developers or engineers refer to the Common Criteria (CC) for security guidance and solution although CC is a bit complex and difficult to comprehend, especially by the novice [14]. Further, developers tend to make mistakes in detecting or choosing the right security requirements and attributes because they need to identify the requirements and attributes personally without any supports, such as automation or manual training. This is because CC presents the requirements in two distinct categories: the functional requirements and assurance requirements, in which the security behavior is described in both types [15].

Moreover, there is no predefined instruction provided to the user when using the GUI for dynamic analysis. This leads to challenges in completing the security identification process [16][17]. These instances justify the need for an automation that can help to elicit security requirements and attributes, especially for the novice. To overcome this issue, Haley et al. [3] has presented an approach to support security requirements elicitation and analysis. They used a method to construct a system context using a problem oriented notation. However, the complexity of the approach requires a certain level of expertise to construct the setting and analysis.

Likewise, Berger et al. [18] supported the claim that software engineers lack security knowledge although this body of knowledge is easily accessible. The lack of security knowledge among the software engineers and developers makes it difficult for them to extract and make decision on selecting the relevant piece of security knowledge to be applied to their design or

requirements. Yusop et al. [19] found that relevant attributes for security requirements of mobile apps are authentication, confidentiality, authorization, access control and integrity. They also found that the main challenge is to identify the most relevant security attributes for each of the requirements for the mobile apps. Further, it is also found that none of the existing work focusses on eliciting the security at the beginning of the development, but most prefer to consider security at the implementation stage of the mobile apps.

3. OUR STUDY: ELICITING SECURITY ATTRIBUTE FOR MOBILE APPLICATION

As mentioned in the previous section, requirements engineers or software engineers face difficulty to elicit security related requirements and security attributes from the business requirements [20]. Hence, an experiment aiming at gaining a better understanding of the difficulties to elicit security attributes from natural language requirements has been conducted. For this purpose, two experiments have been conducted and novice requirements engineers were considered as the most appropriate sample.

In this study, 50 undergraduate students majoring in Software Engineering and mobile software development have been selected as the sample of the study. They were considered as novice requirements considering that they have very limited exposure in eliciting requirements. However, they have sufficient understanding of the process and methodology of eliciting security attributes from the functional requirements.

Prior to this study, each participant was given a brief explanation and a tutorial on how to elicit security attributes from the functional requirements written in textual requirements scenario. After the explanation, they were asked to extract the security attributes related to the requirements scenario. During the completion of the task, we tracked the time they took to complete the task. The accuracy of the task attempted by the students was also determined.

The participants were instructed to attempt two tasks: The first was a scenario based on a flight booking as shown in Figure 3, and the second was i health patient apps shown in Figure 4. Participants were required to write down the functional requirements based on the two scenarios given in Figure 3 and 4. Then, they were required to extract the relevant security attributes for each of the functional requirements. Students were given an hour to complete the two tasks. It was anticipated that they should be able to identify five functional requirements with a total of 19 relevant security attributes for the first scenario and six functional requirements with the total of 29 relevant security attributes for the second scenario.

> *Users can book a flight ticket using the Fly Air app via online by making online payment through their mobile app to the bank nominated by the flight company. To book the air ticket, users must first register as a member so that they can login to access the page. Once they have access to the page, they can then search for flight journey and its availability. Users can then book the chosen flight journey and then the system will ask them to make payment. Users can make online payment using their credit card. They need to specify the price of the flight booked and confirm to make payment. Fly Air apps provides the TAC code and users need to verify the code. Upon verifying the code, user will be prompted that they have successfully booked the flight ticket with the airline.*

(Figure 3) USER SCENARIO FOR MOBILE FLIGHT BOOKING APPS

> *This mobile application named i health apps could support mobile online application based on patient health monitoring. I health provides highly secure information for patient. For this scenario, patient must register their information as a member so that the system can allow patient to access the application. Patient will login to i health to view patient information and details such as the username, password, identity card no, phone no and email from their console. Patient also can choose the menu selection option to view the patient medical record exercise. Patient is compulsory to do exercise 3 times a week based on the exercise classification and all of these need to be recorded in the patient exercise console provided. Patient can modify certain information related to the mobile apps. This i health provides automatic notification to patient with incomplete exercise. It also provides patient monthly summary report for doctor record.*

(Figure 4) USER SCENARIO FOR MOBILE HEALTH MONITORING APPS

(Table 1) EXPERIMENT 1 AND EXPERIMENT 2 STUDY RESULT

Experiment 1	Experiment 2
430 out of 950 were identified as correct security attributes	611 out of 1450 were identified as correct security attribute
1 out of 50 (2%) of participants extracted almost correct security attributes	1 out 50 (2%) of participants also extracted almost correct security attributes
0.48 accuracy of correctness of experiment 1	0.42 accuracy of correctness of experiment 2

4. RESULT AND DISCUSSION

Table 1 shows the result of the two experiments: Experiment 1 and 2. Based on Table 2, there are five functional requirements, namely i) register, ii) log in, iii) search flight, iv) book flight and v) payment ticket that need to be elicited by the participants. While as presented in Table 3, there are six functional requirements, namely i) register, ii) log in, iii) menu option, iv) patient record v) notification and vi) monthly report. Additionally, there are a total of 29 security attributes associated with the functional requirements. The correct extraction of the security attribute is represented by the sign (/), while the inaccurate extraction is represented by the sign (x). A correct answer (/) means that the answer provided by the participant is exactly the same or very similar to the security attribute pattern provided by us. The following are the results of the study:

These results indicate that participants were more likely to generate incorrect security attributes than the correct ones, and it was very unlikely (4%) that they produced a completely correct security attributes. All except two of the participants failed to identify some of the essential interactions presented in the textual requirements scenario; many failed to assemble these into an appropriate interaction sequence of security attributes; and only one (participant no 47) in Table 2 and one (participant no 5) in Table 3 managed to obtain a solution that is almost the same as or very similar to the model answer of the flight booking and health monitoring scenario. The root cause for most of the problems was that the participants had the tendency to incorrectly determine the required security attribute for their related functional requirements.

The study also demonstrates that the participants consumed quite some time to complete the task with the average of 22.38 minutes as they need to figure out the appropriate security for the application. The results also show that there is a considerable variation in the time taken to identify the security attributes. Further, the longest time taken does not ensure the correct identification of the requirements. For example, the participant who took the longest (25 minutes) time to accomplish the task in experiment 1 and (30 minutes) experiment 2 was able to identify 1 correct functional requirement only. Only 45% accuracy was identified from the experiment and this result has proven that novice requirements engineers have problems to elicit correct security attribute of the mobile application. As shown in Table 2, we also found that the common errors made (in red color) are eliciting the security attributes for the functional requirements of the search flight, book flight ticket and payment of flight ticket. Table 3 also indicates that the same participant has problems to describe the security attributes between Menu Option, Patient Record, Notification and Monthly Report. In this study, we also found that participants did well in identifying the relevant security attributes for log in functional requirements. This is perhaps that they are familiar with the application or system development that usually needs the functions of identifying user or log in.

In summary, these results conforms the anecdotal findings discussed in the previous section.

5. CONCLUSIONS

This paper discussed the challenges and difficulties faced by requirements engineers and software engineers in eliciting security requirements and security attributes. Two experiments, focusing on the manual elicitation of security attributes from a set of requirements scenario have been conducted with novice requirements engineers (REs) and the findings of the experiments have been discussed. It shows that the elicitation of security attributes is very challenging for the novice REs and they require help, especially an automation support. This is because the process requires effort, knowledge and skills to ensure the accuracy of the elicited security attributes. Therefore, our key future work will be focusing on developing an automation support for easy elicitation of the security attributes

from the textual requirements scenario for mobile application development. We will also extend the work with an automated approach to validate the quality of the security requirements for mobile application development.

6. ACKNOWLEDGEMENTS

This research was supported by a research grant from Sciencefund grant: 01-01-14-SF0106, Universiti Teknikal Malaysia Melaka (UTeM) and Ministry of Education (MOE), MyBrain15.

(Table 2) SECURITY ATTRIBUTES STUDY RESULT: EXPERIMENT 1

Functional Requirements	Register				Login		Search flight				Book Flight ticket				Payment Ticket						
Security attributes	Username	Password	Email	PassportIcNo.	Username	Password	Flight code	Destination code	Username	Password	Booking code	Flight No.	Username	Password	Account No.	TACCode	TicketId	Username	Password	Total Correct	Time taken
1	/	/	/	/	/	/	/	/	×	×	/	/	×	×	/	/	×	×	×	12	20.5
2	/	/	/	×	/	/	×	×	/	/	×	×	/	/	/	×	×	×	×	10	22.5
3	/	/	/	/	/	/	/	/	×	×	×	/	×	×	/	/	/	×	×	12	23.5
4	/	/	/	/	/	/	×	×	×	×	×	×	×	×	×	/	×	×	×	7	21.5
5	/	/	/	×	/	/	×	×	×	×	×	×	×	×	×	/	×	×	×	6	23.5
6	×	×	/	×	/	/	×	×	×	×	×	×	×	×	/	/	×	×	×	5	21.5
7	/	/	/	/	/	/	×	×	×	×	×	×	×	×	/	/	/	×	×	9	25
8	×	/	/	×	/	/	×	×	×	×	×	×	×	×	/	/	×	×	×	6	25
9	/	/	/	/	/	/	×	×	×	×	×	×	×	×	/	/	×	×	×	8	23.5
10	×	×	×	×	/	/	×	×	×	×	×	×	×	×	×	/	×	×	×	3	21
11	/	/	×	×	/	/	×	×	×	×	×	×	×	×	×	/	×	×	×	5	21.5
12	×	×	×	/	/	/	×	×	×	×	×	×	×	×	/	/	/	/	/	8	22.5
13	/	×	/	/	/	×	×	×	×	×	×	×	×	×	/	×	×	×	×	5	23.5
14	/	/	/	/	/	/	/	×	×	×	×	×	×	×	/	/	×	×	×	9	22
15	/	×	×	×	/	/	×	×	×	×	×	/	×	×	/	/	×	×	×	6	22.5
16	/	/	/	/	/	/	×	×	×	×	×	×	×	×	/	/	×	×	×	8	21.5
17	/	×	×	/	/	/	×	×	×	×	×	×	/	×	/	/	×	×	×	7	23.5
18	/	/	/	×	/	/	/	/	×	×	×	×	×	×	×	/	×	×	×	8	20
19	/	/	/	/	/	/	/	×	/	/	×	×	×	×	/	/	×	×	×	11	21
20	/	/	×	×	/	/	×	×	×	×	×	×	×	×	/	/	×	×	×	6	24.5
21	/	/	/	/	/	/	×	×	×	×	×	×	×	×	/	/	×	×	×	8	20
22	/	/	/	/	/	/	×	/	×	×	×	×	/	/	/	/	×	/	/	13	19.3
23	/	/	/	/	/	/	/	×	×	×	×	×	×	×	/	/	×	×	×	9	20
24	/	/	/	/	/	/	×	/	×	×	/	×	×	×	/	/	×	×	×	10	20.5
25	/	/	/	/	/	/	/	×	×	×	/	×	/	/	/	/	×	×	×	12	17.5
26	/	/	/	/	/	/	/	/	×	×	×	×	×	×	/	/	/	×	×	11	26
27	/	/	/	/	/	/	×	×	×	×	×	/	×	×	/	/	×	×	×	9	25
28	×	×	/	/	/	/	×	×	×	×	×	×	×	×	/	/	×	×	×	6	26.5
29	/	/	/	×	/	/	×	×	×	×	×	×	×	×	/	/	×	×	×	7	22.5
30	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	/	×	×	×	1	24.5
31	/	/	×	×	/	/	×	×	/	/	×	×	×	×	/	/	×	×	×	8	24.5
32	/	/	/	/	/	/	/	×	×	×	×	×	/	/	/	/	/	×	×	12	24
33	/	/	/	/	/	/	×	×	×	×	×	/	×	×	/	/	×	×	×	9	23.5
34	×	×	/	/	/	/	/	×	×	×	×	×	/	/	/	/	×	×	×	9	23
35	/	/	/	/	/	/	/	/	×	×	/	/	×	×	/	/	×	×	×	12	21
36	/	/	/	/	/	/	×	×	×	×	/	/	×	×	/	/	/	×	×	11	23.5
37	/	/	×	×	/	/	×	×	/	×	×	×	/	/	/	×	×	/	/	10	23
38	×	×	×	×	/	/	/	×	×	×	×	/	×	×	/	/	×	/	×	7	19.5
39	/	/	/	/	/	/	/	×	×	×	×	/	×	×	/	/	×	/	×	11	22.5
40	/	/	×	×	×	×	×	×	×	×	×	×	×	×	/	/	×	×	×	4	27
41	/	/	×	×	/	/	×	×	/	/	×	×	/	/	/	/	×	×	×	10	17.5
42	/	/	/	/	/	/	×	×	/	/	×	×	/	/	/	/	×	/	/	14	18.5
43	/	/	×	×	/	/	/	×	×	×	×	/	×	×	/	/	×	×	×	8	21
44	/	/	/	/	/	/	×	×	/	/	×	×	/	/	/	/	×	/	/	14	25
45	/	/	×	×	/	/	×	×	×	×	/	/	×	×	/	/	×	×	×	8	24
46	/	/	/	/	/	/	/	×	×	×	/	/	×	×	×	/	×	×	×	10	24.5
47	/	/	/	/	/	/	/	/	/	/	×	/	/	/	/	×	/	/	/	17	23.5
48	/	/	×	×	/	/	×	×	×	×	/	×	×	×	/	/	×	×	×	7	22.5
49	/	/	/	/	/	/	/	/	×	×	×	/	×	×	/	/	×	/	/	13	19.5
50	/	/	×	×	/	/	/	/	×	×	/	/	×	×	/	/	×	×	×	10	19.5
Total	42	40	33	30	48	47	17	9	8	7	9	14	11	10	43	47	6	9	7		

(Table 3) SECURITY ATTRIBUTES STUDY RESULT: EXPERIMENT 2

Functional Requirements	Register					Login		Menu Option			Patient record							Notification					Monthly Report								
Security Attributes	Username	Password	Email	PatientId	ContactNo	Username	Password	Username	Password	MenuId	Username	Password	Email	PatientId	ContactNo	RecordId	ExerciseId	Username	Password	NotificationId	RecordId	PatientId	Username	Password	StaffId	PatientId	ReportId	Email	ContactNo	Total Correct	Time Taken
1	/	/	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	/	/	/	/	11	23.00
2	/	/	/	/	/	/	/	x	x	x	/	/	x	x	x	x	x	x	x	x	x	/	/	/	/	x	x	x	x	13	25.00
3	/	/	/	/	/	/	/	x	x	x	/	/	x	/	x	/	/	/	/	x	/	/	/	/	/	/	x	/	/	22	26.00
4	/	/	/	/	/	/	/	x	x	x	x	x	x	x	x	/	/	x	x	x	x	x	x	x	x	x	x	x	x	9	24.00
5	/	/	/	/	/	/	/	/	/	x	/	/	/	/	/	/	/	/	/	x	/	/	/	/	/	/	/	/	/	27	26.00
6	/	/	/	/	/	/	/	/	/	x	/	/	x	x	x	/	/	x	x	x	/	x	x	x	/	/	/	x	x	17	24.00
7	/	/	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	/	/	/	/	/	x	x	/	/	/	x	x	15	30.00
8	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	0	30.00
9	/	/	/	/	/	/	/	/	/	x	x	x	x	x	x	/	/	x	x	x	x	x	x	x	/	/	/	x	x	14	26.00
10	/	/	/	/	/	/	/	x	x	x	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	12	23.50
11	/	/	/	/	/	/	/	x	x	x	/	/	/	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	11	24.00
12	x	x	x	/	x	/	/	x	x	x	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	6	25.00
13	/	/	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	7	26.00
14	/	/	/	/	/	/	/	x	x	x	x	x	x	/	x	x	/	x	x	x	x	x	x	x	/	x	x	x	x	10	24.50
15	x	x	x	/	x	/	/	x	x	x	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	5	25.00
16	/	/	/	/	/	/	/	x	x	x	/	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	13	24.00
17	/	/	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	7	26.00
18	/	/	/	/	/	/	/	x	x	x	x	x	x	/	x	x	x	x	x	x	x	/	x	x	x	/	x	x	x	10	22.50
19	/	/	/	/	/	/	/	/	/	x	/	/	x	x	x	x	x	x	x	/	x	x	/	/	x	x	x	x	x	14	23.50
20	/	/	/	/	/	/	/	x	x	x	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	12	27.00
21	/	/	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	7	22.50
22	/	/	/	/	/	/	/	x	x	x	x	x	x	x	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	8	24.30
23	/	/	/	/	/	/	/	x	x	/	/	/	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	15	22.50
24	/	/	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	7	23.00
25	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	15	20.00
26	/	/	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	7	52.00
27	/	/	/	/	/	/	/	/	/	x	x	x	x	/	x	x	x	x	x	x	x	/	x	x	x	x	/	x	x	12	30.00
28	/	/	/	/	/	/	/	x	x	x	x	x	x	/	x	x	x	x	x	x	x	/	x	x	x	x	/	x	x	10	30.00
29	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	17	25.00
30	x	x	x	x	x	x	x	x	x	x	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	5	27.00
31	/	/	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	7	27.00
32	/	/	/	/	/	/	/	/	/	x	/	/	/	/	/	/	/	x	x	x	x	x	/	/	/	/	/	x	/	22	26.50
33	/	/	/	/	/	/	/	x	x	x	/	/	/	/	/	/	/	x	x	x	x	x	/	/	x	/	x	x	x	17	26.00
34	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	x	x	x	x	x	/	x	/	x	/	x	x	/	/	20	25.50
35	/	/	/	/	/	/	/	x	x	/	/	/	/	/	/	x	x	x	x	x	x	/	/	/	/	/	x	/	x	19	26.00
36	/	/	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	7	26.00
37	/	/	/	/	/	/	/	x	x	x	/	/	/	/	/	x	x	x	x	x	x	/	/	/	/	x	x	x	x	16	25.50
38	/	/	/	/	/	/	/	x	x	x	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	/	x	x	x	13	22.00
39	/	/	/	/	/	/	/	x	x	x	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	/	x	x	x	13	25.00
40	/	/	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	7	29.50
41	/	/	/	/	/	/	/	/	/	x	/	/	x	x	x	x	x	/	/	x	x	x	/	/	x	x	x	x	x	15	20.00
42	/	/	/	/	/	/	/	/	/	x	/	/	x	x	x	x	x	/	/	x	x	x	/	/	x	x	x	x	x	15	21.00
43	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	x	x	x	x	x	x	x	/	/	x	/	/	/	/	20	23.50
44	/	/	/	/	/	/	/	/	/	/	/	/	x	x	x	x	x	/	/	x	x	x	/	/	x	x	x	x	x	16	27.50
45	/	/	/	/	/	/	/	x	x	x	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	12	26.50
46	/	/	/	/	/	/	/	x	x	x	/	/	/	/	/	x	x	x	x	x	x	x	x	x	x	x	x	x	x	12	27.00
47	/	/	/	/	/	/	/	x	x	x	/	/	/	/	x	x	x	x	x	x	x	x	x	x	/	/	x	x	x	13	29.00
48	/	/	/	/	/	/	/	x	x	x	/	/	x	x	x	x	x	x	x	/	x	x	x	x	x	x	x	x	x	10	25.00
49	/	/	/	/	/	/	/	/	/	/	/	/	x	x	x	x	x	/	/	x	x	x	/	/	x	x	x	x	x	16	22.00
50	/	/	x	x	x	/	/	x	x	x	/	/	/	/	x	x	x	/	/	x	x	x	/	/	x	x	/	x	x	13	22.00
Total	46	46	45	47	45	48	48	14	14	8	32	32	22	25	20	10	10	8	8	3	5	9	15	14	12	14	9	6	6		

References

[1] S.Yahya, M.Kamalrudin, S.Sidek, "The Use of Essential Use Cases (EUCs) to enhance the Process of Capturing Security Requirements for Accurate Secure Software," *e-Proceeding of Software Engineering Postgraduates Workshop (SEPoW)*, pp.21-26, 2013. http://ftmk.utem.edu.my/sepow2013/e-proceeding_SEPoW2013.pdf. Access from September 2015

[2] S.Yahya, M.Kamalrudin, S.Sidek, "A Review on Tool Supports for Security Requirements Engineering," Proceedings of the *IEEE Conference on Open Systems*, Sarawak, Malaysia, 2013. http://dx.doi.org/10.1109/ICOS.2013.6735072

[3] C. B. Haley, R. C. Laney, J. D. Moffett, and B. Nuseibeh, "Security Requirements Engineering: A Framework for Representation and Analysis," *IEEE Trans. Software Eng.*, pp.133-153, 2008. http://dx.doi.org/10.1109/TSE.2007.70754

[4] G.Ian, "Essential software architecture," pp.1-283, 2006. http://dx.doi.org/10.1007/978-3-642-19176-3

[5] K.Ivo, E.George, C. Leslie, G. Leana, M. Nenad, "A comprehensive exploration of challenges in architecture-based reliability estimation," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics),"* Vol 202-227, 2009. http://dx.doi.org/10.1007/978-3-642-10248-6_9

[6] I. Kashmala, "Analytical Survey for Assuring and Maintaining Quality of Mobile Applications," Vol 2, pp. 336-345, 2015. www.ijccse.com/april15/RP_0415_5872.pdf. Access from September 2015.

[7] N. Nan, "Extractive Product Line Requirement," 2009. http://dx.doi.org/10.1109/RE.2008.49

[8] N. Ranjbar, M. Abdinejadi, "Authentication and Authorization for Mobile Devices," 2012. http://hdl.handle.net/2077/30043

[9] "User Authentication in Mobile Access," https://sc1.checkpoint.com/documents/R77/CP_R77_Mobile_Access_WebAdmin/41587.htm, Accessed from September 2015.

[10] P. Vilhan, L. Hudec, "Building Public Key Infrastructure for MANET with Help of B.A.T.M.A.N. Advanced," Modelling Symposium (EMS), 2013 European, Manchester, 20-22 Nov., pp. 566 -571, 2013. http://dx.doi.org/10.1109/EMS.2013.94

[11] A.Rekha, P.Anitha, A.S.Subaira, C.Vinothini, "A Survey on Encryption Algorithms for Data Security," *IJRET: International Journal of Research in Engineering and Technology*, pp.131-134. http://dx.doi.org/10.15623/ijret.2014.0312017

[12] C. E.Loftis, T. X. Chen, J. M Cirella, "Attribute-level encryption of data in public Android databases," *(RTI Press publication OP-0016-1309), Research Triangle Park, NC: RTI Press*, 2013. http://dx.doi.org/10.3768/rtipress.2013.op.0016.1309

[13] C.L. Chen , W.C.Tsai, "Using a Stored-Value Card to Provide an Added-Value Service of Payment Protocol in VANET," *Proceedings of the Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference,* Taichung, pp. 660-665, 3-5 July 2013. http://dx.doi.org/10.1109/IMIS.2013.119

[14] E. Paja, F.Dalpiaz, M.Poggianella, P.Roberti, P.Giorgini, "STS-tool: Socio-technical Security Requirements through social commitments," *Proceedings of the 20th IEEE International Requirements Engineering Conference (RE),* IEEE , pp.331-332, 2012. http://dx.doi.org/10.1109/RE.2012.6345830

[15] M.S.Ware, J.B.Bowles, "Using the Common Criteria to Elicit Security Requirements with Use Cases," *Southeast Con, 2006. Proceedings of the IEEE*, pp.273-278, March 31 2005-April 2 2005. http://dx.doi.org/10.1109/second.2006.1629363

[16] P. Aho, N. Menz, and T. Räty, "Enhancing generated Java GUI models with valid test data," *Proceedings of the 2011 IEEE Conf. on Open Systems (ICOS)*, Langkawi, Malaysia, pp. 310-315, 25-28 Sep 2011. http://dx.doi.org/10.1109/ICOS.2011.6079253

[17] A. Kull, "Automatic GUI Model Generation: State of the Art," Proceedings of the. *2012 IEEE 23rd Int. Symposium on Software Reliability Engineering Workshops (ISSREW)*, Dallas, TX, USA, pp. 207-212, 27-30 Nov 2012. http://dx.doi.org/10.1109/ISSREW.2012.23

[18] B.J.Berger, K.Sohr and R.Koschke, "Extracting and Analyzing the Implemented Security Architecture of Business Applications," *Proceedings of the* 2013 17th European Conference on Software Maintenance and Reengineering, 2013.
http://dx.doi.org/10.1109/CSMR.2013.37

[19] N.Yusop, M.Kamalrudin, S.Sidek, "Security Requirements Validation for Mobile Apps: A Systematic Literature Review," *Jurnal Teknologi (Science & Engineering)*, 2015.
http://dx.doi.org/10.11113/jt.v77.7017

[20] S.Yahya, M.Kamalrudin, S.Safiah, J.Grundy, "Capturing Security Requirements Using Essential Use Cases (EUCs)," *Proceedings of the First Asia Pacific Requirements Engineering Symposium, APRES 2014,* New Zealand,April 28-29, pp. 16-30, 2014.
http://dx.doi.org/10.1007/978-3-662-43610-3_2

◐ Authors ◑

Noorrezam Yusop

2004 Diploma in Computer Science from University Technology of Malaysia (UTM).
2011 Bachelor of Science (Hons) in Information and Technology from Kuala Lumpur Metropolitan University College (KLMUC). 2013 Master of Computer Science (Software Engineering and Intelligence) from Universiti Teknikal Malaysia Melaka (UTeM).

Massila Kamalrudin

2003 Bachelor of Science in Computer Science (Software Engineering) from Universiti Putra Malaysia, Malaysia.
2005 Masters in Computing & Software Technology from University of Wales Swansea, United Kingdom.
2011 Philosophy of Doctoral in Electrical and Electronic Engineering from University of Auckland, New Zealand. 2012 Post of doctoral from Swinburne University of Techology, Melbourne Australia.

Mokhtar Mohd Yusof

1976 Bachelor of Economic from Universiti Malaysia (UM).
1984 Masters of Science in Computer Science from National University of Malaysia (1984).
2011 Philosophy of Doctoral in Information Systems from the University of Salford, United Kingdom.

Safiah Sidek

1986 Bachelor of Business Economics from Brock University, Ontario, Canada
1999 Masters of TESL from University Putra Malaysia, Serdang, Malaysia
2012 Philosophy of Doctoral from Deakin University, Melbourne, Australia