COMPREHENSIVE OVERVIEW ON SECURITY SOLUTIONS FOR MOBILE DEVICES

Annie Sujith[1], Chitra S Nair[2], Salonee Mishra[3], Manjusha Kulkarni[4]

[1]*Assistant Professor, Department of CSE, T. John Institute of Technology, Karnataka, India*
[2]*Assistant Professor, Department of CSE, T. John Institute of Technology, Karnataka, India*
[3]*Assistant Professor, Department of CSE, T. John Institute of Technology, Karnataka, India*
[4]*Assistant Professor, Department of CSE, T. John Institute of Technology, Karnataka, India*

Abstract

"A smartphone is a mobile phone with an advanced mobile operating system which combines features of a personal computer and more important is its size, advanced processing capability as well as connectivity capabilities, smaller cost, and their ability to connect multi-purpose third party or devices applications. Smartphone's are in high demands in both office and private work". Use of android permission-based security model makes the application access to device resources very difficult. The main drawback is that users cannot have adequate control over the device and also it does not provide information how third party applications uses personal data of users. While installing applications and getting permission warnings users are unable to take right security decisions.This paper provides the overview about development of a risk assessment method in order to resolve security related issues at Android Smart phone. In this paper authors have given 3 methods:1)"Smartphone risk assessment (SRA) is the design of risk assessment implemented on Android Smartphone". System Usability Scale (SUS) is being used as a questionnaire for the evaluation of SRA and the result is remarkable. The users find SRA very beneficial against the threats of the smartphones or any applications related to sensitive data leakage.2) "WHYPER a framework using Natural Language Processing (NLP) techniques which is basically used to identify sentences that describe the need for a given permission in an application description".3)one more method of risk assessment that authors have discussed in this paper is RiskMon that gives idea about assessing risks based on machine learned ranking sustained by users for applications based on Android.The main advantage of this method is that if there is "any sensitive data leakage users can increase the level of security of the device."

Keywords: *Smartphone's; Android; Risk Assessment*

----------***----------

1. INTRODUCTION

Smartphone are in high demands in recent trends because of their portability, small size, very advanced connectivity and processing capabilities, low cost and most important their capability to host multi-purpose third party applications. Various kindof data such as sensor data, multimedia data, and data created or consumed by applications, communication logs etc are hosted by smart phones. Smartphone users carry the device on different multiple locations throughout day and night and make connections to different networks which is not secure.

Smartphone's contains most valuable information of personal and business data as users use the device for both personal and professional work. In comparison to Smartphone OS market Android share showed a remarkable increase of 85% in Q2 2015. Consumers who own an Android-powered Smartphone are almost as satisfied with their purchases as are iPhone owners, who have been historically extremely happy with their hardware. Of the people who told Change Wave they had an Android handset, 72% said they were "very satisfied;" 77% of those who reported they own an iPhone answered the same way.

But sometimes user's habits and behavior increases the risk level on Android smart phones. So the main aim of this study is to develop a risk assessment method on Android Smartphone whose main aim is to increase the security level of the device basically against sensitive data leakage. There are two approaches used for risk assessment method, one is sensitive data risk assessment which is based on combination of permissions from all applications installed on the device and security configuration level assessment which is based on built-in Android Smartphone configurations. The design of risk assessment implemented on Android Smartphone is SRA whose results help users to determine potential threats of their Smartphone's and any applications that has potential to leak sensitive data. The 2nd method that we are using in the paper is WHYPER which is a framework using Natural Language Processing (NLP) techniques which is basically used to identify sentences that describe the need for a given permission in an application description.

The main aim of the WHYPER framework is to connect the relative gap of user expectations by identifying whypermission is required by an application. The 3rd method that we are using in the paper is RiskMonRiskMon that gives idea about assessing risks based on machine learned ranking sustained by users for applications based on Android. The main job of Riskmon is to combine the runtime behaviors of trusted applications and users' coarse

expectations to generate a risk assessment baseline that captures appropriate behaviors of applications. By the use of baseline, RiskMon assigns a risk score on every access attempt on sensitive information and ranks applications by their cumulative risk scores.

In the following sections authors have given: in Section II related works, Section III illustrates theproblems, which is then followed bydesign and implementation of each method atSection IV. At Section V we explain the evaluation of this work. At last, Section VI discusses some concluding remarks from this work.

2. RELATED WORK

The mobile phone risk assessment is still relatively new and many associated standard and approaches are in practice. Theoharidou et al [1] suggesting a specific risk assessment technique specifically designed for Smartphone's. But specific risk calculation has not delivered reasonable impact estimation tables and applicable case studies, which is significant for smartphone handlers. To calculate smartphone practice risk, one should first find the impact of its resources. Then, resources should be related to smartphone risk benchmarks'. Impact calculation for each resource is evaluated.

The first and the foremost are to involve the user with the primary impression estimate process. Then, the risk expert should achieve clear relations and combinations to compute the whole risk. In classic risk calculation methods, physical resources are appreciated in terms of additional or renewal costs, in a measurable way. For a smartphone this discusses to additional or renovation device cost, in the case of impairment, burglary, or ruin. Though, a smartphone contains, various information types, which need to be relatively measured in terms of impact.

For material resources, a loss of confidentiality, integrity, or availability may be valued via several criteria such as individual evidence disclosure, legislature defilement, predetermined breach, profitable and economic securities, economic loss, unrestricted order, international associations, business procedure and procedures, loss of concern/status, private security, frustration, etc. Due to the smartphone's adaptable environment, these impact kinds vary from morally particular ones, e.g. handler frustration, to typical information arrangements ones, e.g. profitable interests.

Jing et al [4] present a continuous and automated risk assessment framework called RiskMon that uses machine learned grade to measure risks experienced by handlers' mobile uses, particularly Android applications. RiskMon chains users' coarse opportunities and runtime behaviors of trusted applications to produce a risk calculation baseline that detentions suitable performances of applications. This method uses data about data on application market for downloads,rankings and category which gives information regarding application status and main functionalities.

Concerning existing application of RiskMon, it is not addressing third party application communication, Binder connection that is supposed to attack directions that can detour RiskMon.

Pandita et al [5] present WHYPER, a framework using Natural Language Processing (NLP) procedures to recognize sentences that designate the requirement for a given authorization in an application explanation. Their result determine excessive potential in using NLP procedures to link the semantic gap between user anticipations and application functionality, which additional should assistance in the risk calculation of mobile uses. Though, false charges in an application's account can deliver explanation for deletion from the market or hypothetically even criminal prosecution.

WHYPER is based on keywords in the application demonstration.In a platform such as Android, there are many ways to achieve the same application goals. Some application options necessitate authorizations.

The leading objective of this paper is to improve a risk assessment technique for an Android smartphone so it can support to device security bearing that at the end aids developing the security level of device, particularly against subtle data leakage. Design of risk assessment proceeds conducted from two methods, security configuration level assessment and sensitive data risk assessment. Security configuration level assessment exists grounded on built-in Android smartphone configurations, while sensitive data risk assessment is based on authorizations and the combination of all applications connected on the mobile device. The design of risk assessment that is applied on Android smartphone is called SRA (Smartphone Risk Assessment). The effects help users to control possible threats of their smartphones and some applications that have possible to leak subtle information.

3. PROBLEM ANALYSIS

Based on related work that have been done on data-related issues [1] [4] [5] and attack vectors of Smartphone's authors have formed security requirements that must be met by smartphone's users.They have developed Tropos goal model which consists of subgoals which is model security goals and their relationships to risks.The model consists of two layers based on the data usage 1. Asset layer and based on action or event which harms asset 2. Event layer.

This model represented as tree like structure where node is smartphone user and link is goal.Authors have considered different risks which give harm to smartphone users.Thus, the use of applications on the Android connectivity must also go through declaration permission beforeuse. There are on Android API level 21, there are 4 permissions associated with connectivity s/w or h/w application. Data moved or stored on the device to other media or devices by using these permissions making it possible to be saved by malicious developers to disclose sensitive data. Here these four permissions in SRA are called sensitive resource

permissions. The combination of sensitive resource permissions and sensitive data permissions may become potential risk of the leaking of user sensitive data.

4. RISKMON: DESIGN OUTLINE OVERVIEW

Here this section includes framework of risk assessment which reduces the intrusion and refinement in mobile applications where risk assessment will be more."NIST SP 800-30 [35]and CERT OCTAVE [2]," are the IT risk assessment guidelines provides general methodologiesthat provides institutions key to understand, comprehend and notice their information about risks. Such as identifying information assets and how to provide security for them. Identifying activities that can harm security of assets. Defining risk evaluation methodology that can hold information about operational context and sufferance of organization.

With the help of this guidelines given by NIST or CERT OCTAVEcan handle organizational and infrastructure risks by security dealers but this framework designed by authors developed and started the risk assessment methodologies and take care of user's security requirements as well as operational contexts as input.The design framework captures users predicted deportment rather than running rehearsal of user developers. There is a supposed assumption that appropriate behavior of application can be defined by RiskMon. Following section summarizes thedesign objectives which gives uninterrupted framework for risk assessment.

"Continuous and Fine-Grained Behavior Monitoring"*:*
By using APIs calls applications access sensitive resources and communicate with each other as well as with other system services. *For this continuous monitoring of API call is needed* hence Risk Mon places Binder IPC on users device. Because of this intervention the risks determined by API calls that are identified by the caller, the data and calling entity.Various intelligences about applications are captured by schemes opted by RiskMon.

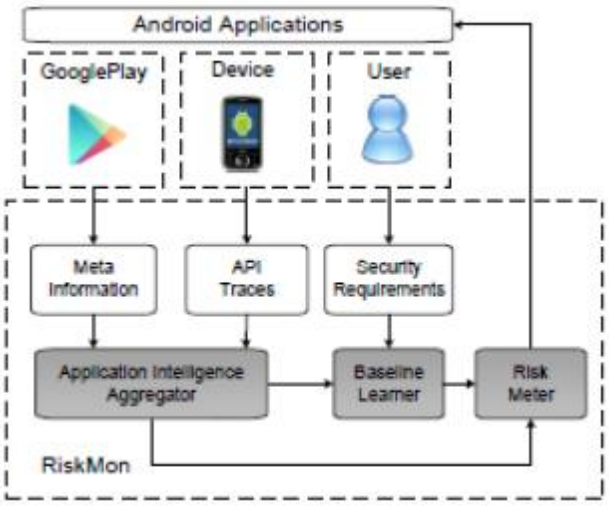

Fig1 [4] "Y. Jing" RiskMon architecture

This framework provides a good base for calculating distance while gap of runtime practices in the middle of 2APIcalls.

Simplified Security Requirement Communication*:*
For specifying security requirements for security tools RiskMon gives a simple technique based on user expectations while communicating their requirements.

"Intuitive Risk Representation*:"*
RiskMon gives a ranking of applications which helps user to differentiate other applications probable loss with their own applications.

"Iterative Risk Management*:"*
Whenever updates are available all the current applications get updated hence the new risk should be measured accordingly. This process of updation is iterative hence risk assessment is too ongoing iterative process. With this updation risk assessment should be monitored on installed applications update it periodically.Users should provide their reactions to RiskMonby including and specifying their security requirements.

The RiskMon framework is presented in following section,Figure1depicts the RiskMon architecture for Android. The framework given by authors consists of three components: an application intelligenceaggregator, a baseline learner, and a risk meter.

The first component compiles the dataset collected on users device based on API traces and gathers data from different application market. The training set is prepared by new learners by merging user's core wishes and collaborative operation of their own trusted applications.The machine-learned ranking algorithm is used by baseline learner to learn a risk assessment baseline. Measurement of deviation in the behavior of application in baseline is done by risk meter. This deviation used to provide risk information, and rank is given by risk measure given by application on mobile devices.

4.1 WHYPER Design

The second study of risk assessment gives the framework called WHYPER for adding the sentenceswhich gives necessity of permission for application descriptions. Figure 2 gives an overview ofour framework. This framework consists of five components:a preprocessor, an NLP Parser, an intermediaterepresentationgenerator, a semantic engine (SE), and an analyzer.

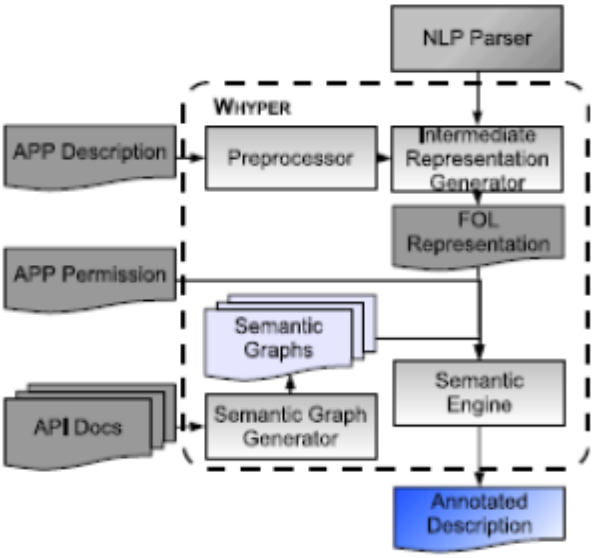

Fig 2 [5] "Pandita" Overview of WHYPER frameworks

Application descriptions are accepted by the preprocessor and it preprocesses the sentences in the descriptions. "The intermediate-representation generator"takes the pre-processed sentences by using NLP parser sentences that can be parsed. The sentencesparsed from the above unit are then convertedinto the first-order-logic representation.FOL representation of a sentence are accepted by SE and gives the graphical representation of semantic permissions.

4.2 Smartphone Risk Assessment (SRA)

Smartphone risk assessment (SRA) is the design of risk assessment implemented on Android. As shown in the goal risk model (Fig.3), there are several sub-goals that can be achieved with Android built-in security configuration for example the use of open wifi by scanning=secure network access point and denoted by G9, G12 denotes the downloading software from trusted sources and so on.

These sub goals gives an assessment for security configuration based on some criteria such as: Network, application, operating system and device. There are five levels for security configuration, levels 1 (very high), 2 (high), 3 (medium), 4 (low), and 5 (very low). Lowest value indicates better level of security configuration of the device.

Author's analysis is based on Android permission and it's a combination of sensitive data permissions and sensitive resource permissions can cause sensitive data leaks from the applications. The leakage may happen when an application request a service that is related to these permissions. These combinations arecategorized based on sensitive data types. Each category has 5 levels, 1 (very low), 2 (low), 3 (medium), 4 (high), and 5 (very high), where highest value indicates higher risk of sensitive data leak of the device.

For all the applications installed on device this assessment can be performed.According to each sensitive data category and assessment criteria each application has 11 values of risk. Results of risk assessment based on sensitive data are obtained from permissions combination of all applications. Authors have shown only those applications that have highest risk in each category to users.

Smartphone Risk Assessment SRA is the risk assessment design implemented by authors specially on android smartphone. This application performs both security configuration level assessment and sensitive data risk assessment.

On devices with Android Ice Cream Sandwich (4.0.3) version or above SRA can be installed and executed. The results of both assessments are displayed on a spider web graph with detailed explanation related to configuration and sensitive data categories. The area of the attack surfaces are described by Spider web graph [see fig. 2 and fig. 3].In each category of sensitive data, they have provided a list of applications and an "Add to Exception List" button which is an additional feature on the SRA application to add one or more applications to exceptions list so that application will not be included in calculation of sensitive data risk assessment.

The result of security configuration and sensitive data risk assessment is shown with the help of spider web graph according to the data categories such as each angular spokes represents location,media,message,phone info, storage data etc. For each category of sensitive data authors have given privilege to add applications as well as button to "Add to Exception List", which is used to include applications in exception list hence that particular application will not be included into sensitive data risk assessment.

5. EVALUATION

In this section evaluation of usability of the application is given. Here usability testing and questionnaire are used as evaluation methods.

5.1 "Usability Testing"

Under Usability testing Task scenarios are used. Task scenarios describe the context in which a user or group is using an application. Number of tasks is limited from 10 to 12 tasks. For this evaluation 10 tasks have been created based on SRA application functions to conduct a risk assessment. Usability is measured based on the success or failure of users performing a single task and time required to complete a task.

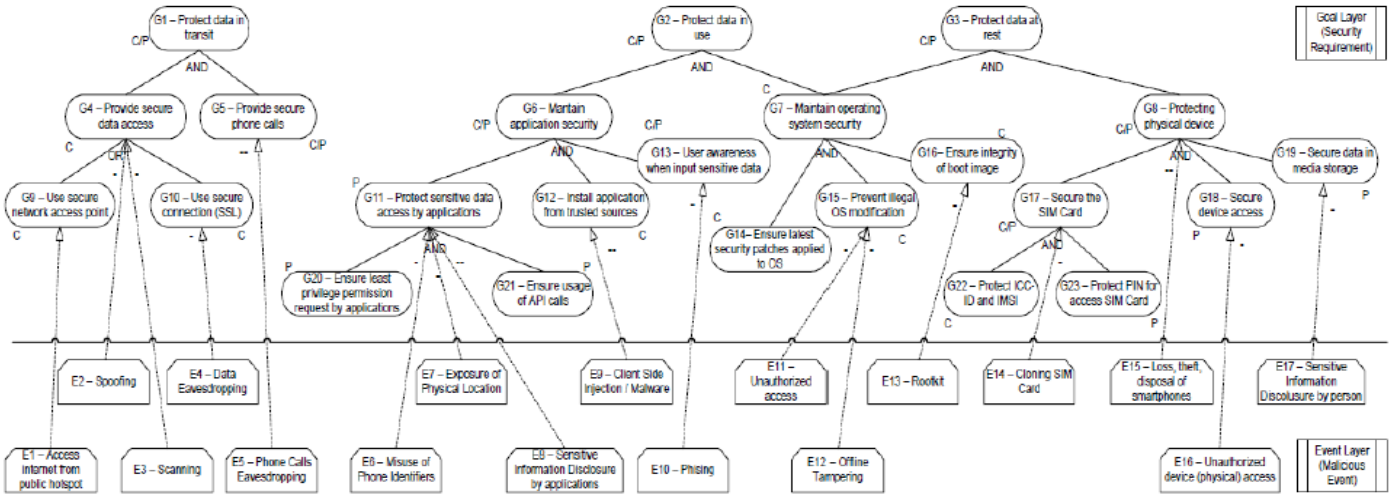

Fig3 [2] "Irwan" goal risk model

5.2 "Questionnaire "

Questionnaire has been used to measure user satisfaction of SRA application. In this study, SUS (System Usability Scale) questionnaire has been used. SUS is a type of survey that can be used to assess the usability of a variety of products or services. As Bangor, Kortum, and Miller [13] have shown, SUS can be applied to a wide range of technologies, many of which hadn't been invented when SUS was first developed.

This Questionnaire contains two parts, the first part contains eight general questions that are related to the user's response and the second part contains 10 statements related to SUS.

SUS questionnaire has a ratio between positive and negative statements 5:5. Each statement is represented using 5-point Likert scale. SUS questionnaire is asked after respondents have done usability testing task. Table III shows SUS questionnaire used in the study.

The results indicate that 83.4% of users are concerned about sensitive data leak when using a smart phone. It shows that smart phone users are generally aware of risks in using smart phones. However out of them there are 25% who did not do anything to protect the security of their smart phone. Based on results of SUS questionnaire, a mean SUS score with a value of 60.2 is obtained which is the average score of each user in SUS questionnaire.

According to the rating scale [12], the score of 60.2 lies in the range of "Good". Hence it shows that SRA application is acceptable. SRA provides information regarding possible threats based on the user's smart phone configuration and also provides a list of applications that has the potential to cause leakage of sensitive data of user. Such information provides better awareness to users about security configuration of their devices and makes users more alert when installing new applications into the device.

Another study was done to evaluate thepracticality and usability of RiskMon. 10 applications that were trusted by users were chosen and downloaded from Google Play depending on their category. The participant's security requirements for the 10 applications and their knowledge about the application were used to generate the baselines. Four target applications were also chosen from the charts of Google Play to compute their risks based on the generated category, including:

a) CNN App for Android Phones (abbreviated as CNN);
b) MXPlayer;
c) Pandora Internet Radio (abbreviated as Pandora); d
d)Walmart.

For both the trusted and target applications, their one-day runtime behaviors was calculated on a Samsung Galaxy Nexus phone. Also a web-based system was developed that feeds a user's security requirements to RiskMon. It also presents the results calculated by RiskMon to the user. A user was given atutorial page that explained how to specify relevancy levels for her security requirements.

After seeing the trusted applications overview on Google Play user would set some relevant levels. Afterwards, Then RiskMon will give a risk assessment report for the participant based on their inputs and runtime practices of the 10 trusted applications. The RiskMon then applied the baseline on each of the 14 applications. It displayed a bar chart that gives a ranking for 14 applications by their measured cumulative risks.

Next is the evaluation of WHYPER. For anyapplication, the WHYPER removes the semanticgap between user expectations and the permissions itrequests. WHYPER removes the gap by findingsentences in the application description that describethe need for a given permission. These sentences are called as permission sentences. To evaluate the effectiveness the permission sentencesidentified by WHYPER are compared with a manual identification of all sentences in the application descriptions. This comparisongives a quantitative assessment of the effectivenessof WHYPER. The WHYPER effectivelyidentifies permission sentences with good precision.It also performs better than keyword-based Search.

6. CONCLUSIONS

This survey paper basically provides developing a risk assessment method in order to resolve security related issues at Android Smart phone. The main advantage of this method is that if there is any sensitive data leakage users can increase the level of security of the device.

There are two approaches used for risk assessment method, one is sensitive data risk assessment which is based on combination of permissions from all applications installed on the device and security configuration level assessment which is based on built-in Android Smartphone configurations. In this paper we are reviewing 3 methods: 1) Smartphone risk assessment (SRA) is the design of risk assessment implemented on Android Smartphone. System Usability Scale (SUS) is being used as a questionnaire for the evaluation of SRA and the result is remarkable which makes it “very good”.

The users find SRA very beneficial against the threats of the Smartphone or any applications related to sensitive data leakage.2) WHYPER a framework using Natural Language Processing (NLP) techniques which is basically used to identify sentences that describe the need for a given permission in an application description. And 3)last method of risk assessment method that we are using in paper is RiskMon which uses machine-learned ranking to assess risks captured by users’ mobile applications installed on Android.

ACKNOWLEDGEMENT

We have great pleasure in expressing our deep sense of gratitude to founder Chairman Dr. Thomas P. John for having provided us with a great infrastructure and constant motivation.We take this opportunity to express our profound gratitude to our Principal, Dr. H. N. Thippeswamy for his constant support and encouragement. We are also grateful to the Head of Computer Science Department, Dr. T.R. Mahesh for his unfailing encouragement and useful suggestions. We are also indebted to all the staff members of the Department of Computer Science and Engineering for their support and encouragement.

REFERENCES

[1]. M. Theoharidou, A. Mylonas and D. Gritzalis, "A Risk Assessment Method for Smartphones," in 27th IFIP TC 11 Information Security and Privacy Conference, Heraklion, Crete, Greece, 2012.

[2]. Irwan, Yudistira Asnar, BayuHendradjaya, ”Confidentiality and Privacy Information Security Risk Assessment for Android-Based Mobile Devices”,2015 International Conference on Data and Software Engineering.

[3]. G. Hogben, "Smartphone security: Information security risks, opportunities and recomendations for users.," ENISA - European Network and Information Security Agency, 2010.

[4]. Y. Jing, G.-J. A. Ahn, Z. Zhao and H. Hu, "RiskMin: Continious and automated risk assessment of mobile applications," in *Proceedings of the 4th ACM conference on Data and application security and privacy* , New York, 2014.

[5]. R. Pandita, X. Xiao, W. Yang, W. Enck and T. Xie, "WHYPER: Towards Automating Risk Assessment of Mobile Applications," in *In Proceedings of the 22nd USENIX Security Symposium (USENIX Security '13)*, Washington DC., 2013.

[6]. IDC, "Smartphone OS Market Share, 2015 Q2," 15 08 2015.[Online].Available:http://www.idc.com/prodserv/smartphone-os-market-share.jsp.

[7]. “N. Li, H. Peng,C. Nita-Rotaru, C. Gates, , B. Sarma, Y. Qi, R. Potharaju, and I. Molloy, "Generating Summary Risk Scores for Mobile Applications," Dependable and Secure Computing, IEEE Transactions on (Volume:11 , Issue: 3) , pp. 238-251, 2014.”

[8]. OWASP, "Projects/OWASP Mobile Security Project - Top Ten Mobile Risks," 26 June 2015. [Online]. Available: https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks.

[9]. G. Hogben, "Smartphone security: Information security risks, opportunities and recomendations for users.," ENISA - European Network and Information Security Agency, 2010.

[10]. Y. Feruza and P. T.-h. Kim, "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security," International Journal of Multimedia and Ubiquitous Engineering, 2007.

[11]. Y. Asnar and P. Giorgini, "Modelling Risk and Identifying Countermeasures in Organizations," in In Proc. of CRITIS '06, LNCS 4347, 2006.

[12]. usability.gov, "Usability Testing," 26 Agustus 2015. [Online]. Available: http://www.usability.gov.

[13] .J. Brooke, "SUS: A Retrospective," Journal of Usability Studies Vol. 8, Issue 2, pp. 29-40, 2013.

[14]. A. Bangor, P. Kortum and J. Miller, "Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale," Journal of Usability Studies Vol. 4, Issue 3, pp. 114-123, 2009.

[15]. J. R. Lewis and J. Sauro, "The Factor Structure of the System Usability Scale," in HCD 09 Proceedings of the 1st International Conference on Human Centered Design: Held as Part of HCI International 2009, 2009.

[16]. H. Lockheimer, “Android and security,” Google Mobile Blog, Feb.2012, http://googlemobile.blogspot.com/2012/02/android-and-security.html.

[17]. W. Enck, D. Octeau, P. McDaniel, and S. Chaudhuri,“A study of Android application security,”in Proc. 20th USENIX Security Symposium, 2011,p. 21.

BIOGRAPHIES

Chitra Nair, Asst. professor T John institute of Technology, Bangalore

Salonee Mishra, Asst. professor T John institute of Technology, Bangalore.

Manjusha Kulkarni, Asst. professor T John institute of Technology, Bangalore.