Assessment of malicious applications using permissions and enhanced user interfaces on Android

Sangho Lee
School of Integrated Technology, Yonsei University
Incheon, South Korea
sangholee@yonsei.ac.kr

Da Young Ju
Yonsei Institute of Convergence Technology
Incheon, South Korea
dyju@yonsei.ac.kr

***Abstract*— Smartphone OS, such as Android, enables us to install third party applications. However, security threats of malicious applications are rapidly increasing due to the nature of the third party applications where only developers can assign required permissions. For this reason, attackers can inject exploits into a normal application with inappropriately acquired permissions. In this paper, we propose a method to distinguish an application by analyzing permissions set and enhanced user interfaces to improve the chance of making right decisions. The proposed methods are intended for users to make better decisions with more information provided by the system.**

Keywords—Android applications, malicious application assessment, enhanced user interfaces

I. INTRODUCTION

Modern smartphone OS, such as Android, enables to install third party applications which everyone can develop and publish. Once the user installs and executes a malicious application, an attacker can transmit the remote server entire activities with agreed permissions. Since the smartphone contains personalized information, such as contact, message and call log, this activity can be dangerous in many aspects. Therefore, this paper proposes the method to prevent from an installation of malicious applications by examining a risk value of required permissions. The method is achieved by two steps; Maximum Severity Rating classification of an application by calculating required permission type of an application, and emphasis of visibility about analyzed maximum severity rating classification based on user experience. Then, these will aggregate into an application installation procedure to improve to assist the users to make a better decision.

II. MAXIMUM SEVERITY RATING(MSR) CLASSIFICATION

To calculate Maximum Severity Rating (MSR), statistical analysis result is employed. Training server analyzes sufficient amount of clean applications, and generates a ranking table of top 20 permissions which is required by applications. Then, the server executes the same operations with malicious applications. Using two different tables, the method calculates a weight of permissions and recognize as a malicious application if the weight value of malicious application is greater than normal application. To implement this, the weight of malicious and normal applications will be stored as a pre-defined vector table. As the second step, generation of permission requests set in an application which is trying to install is desired. If the permissions exist, it is translated into a binary vector table with the value of 1 if requested and 0 if not requested. After assigning a binary vector table, normalized statistical analysis result is multiplied. Then, an average value is calculated as follows:

$$Avg_{xMR} = \frac{\sum_{i=1}^{25} xMR_i}{25}$$

Once risk value calculation is done, comparison of values for malicious and clean applications are performed. If risk value of malicious one is greater than normal, proposed method recognizes an application as a malicious application. Otherwise, an application is indicated as a normal app.

III. ENHANCED VISUALIZATION OF PERMISSIONS SET

To improve difficulties in existing permission-grant screen described above, this paper proposes the user interface which applies enhanced visualization and relocation of an information to provide the users messages more efficiently. When an analysis result of an application is adjudicated as Safe, the color of the background display is represented as blue. In contrast, the color is represented as red if an application is resulted as Malicious. Moreover, a pie graph is provided to show potential risks of each permissions in an application. Once the user presses a particular permission in a graph, a detailed explanation of the permission is displayed in an opposite side.

IV. CONCLUSION

In this paper, we propose the method to indicate a comprehensive assessment of an application, and enhanced visualization. More training date will be necessary to improve an accuracy of MSR classification. Also, more test is needed in further research.

ACKNOWLEDGMENT

This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the "IT Consilience Creative Program" support program supervised by the NIPA (National IT Industry Promotion Agency) (NIPA-2013-H0203-13-1002)