Hierarchical expert system for security evaluation and its implementation on an Android smartphone

Anushree Sitaram Das
Department of Computer Science
Golisano College of Computing and Information Sciences
Rochester Institute of Technology
Rochester, NY 14586
ad1707@rit.edu

***Abstract*— The goal of this paper is to build an application to be used for evaluating the security of android smartphones. Based on the analysis of two different methodologies a hierarchical security metric system is defined and implementation of an expert system using fuzzy logic is described. An approach to improve efficiency of the expert system using machine learning is discussed at the end.**

I. Introduction

Smartphones are the most widely used gadgets in the world and Android is the most popular operating system on smartphones. In 2019, 86 percent[4] share of the global market of smartphones are running on Android operating system and it is expected to increase in the coming years. The main reason for this popularity is the availability of Android SDK (Software Development Kit) for free download which provides the basic platform for the developer community and offers them the right tools for creating the apps and the APIs. All these apps require a set of permissions to be granted, for example, permission to read data about contacts stored on your phone or permission to get your exact location. Android applications run in a sandbox, an isolated area of the system that does not have access to the rest of the system's resources, unless access permissions are explicitly granted by the user when the application is installed.

Granting these permissions could lead to various privacy issues. There are intelligence agencies which try to intercept personal information transmitted across the Internet by social networks and other popular applications. They collect personal information about the users and bother them with unwanted and intrusive advertisements on their devices, or send their personal information to unauthorized third parties. Due to these concerns, the need to address android security has become of paramount importance.

This paper describes an approach to evaluate an android device's security with the help of security metrics. Metrics helps us understand quality and consistency. Security metrics for software systems provide quantitative measurement for the degree of trustworthiness for software systems. These measures can be used to facilitate decision making and improve performance and accountability through the collection, analysis, and reporting of relevant performance-related data. The process of evaluating security of an android device can be automated using a Rule-based Expert System. The Expert System will extract device details or take user's answers on auditing questions, analyze them, and output a result in form of an integer on a scale of 0-10 and give the user some advice on what needs improvement. The rest of this paper is organized into the following sections. In section 2, we analyze research on Development of security metrics for a distributed messaging system[1], by Reijo M. Savola and Habtamu Abie, and Software security risk analysis using fuzzy expert system[2], by Sodiya A. S, Lonhe H. O. D. and Fasan O. M. In section 3, a hierarchical security metrics developed for the security evaluation of android is defined; in section 4, implementation of a rule-based expert system is mentioned based on the security metrics developed..

II. Analysis of methodologies

A. Development of security metrics for a distributed messaging system[1]

The study investigates a practical development of security metrics for a distributed messaging system based on threat and vulnerability analysis and security requirements. The original security metrics development process [3] is updated in accordance with the results of their study whose steps that are relevant for this project can be summarized as follows:

1. Threat and vulnerability analysis is per formed in which known or suspected vulnerabilities are identified and impact and risk exposure of those vulnerabilities are analyzed.
2. Security requirements are prioritized.
3. Basic Measurable Components(BMCs) from the higher-level requirements are identified using a decomposition approach. When the decomposition terminates, all leaf nodes should be measurable components.
4. BMCs based on feasibility and importance are selected.

As a result, a methodology for practical security metrics development based on the identification of basic measurable components in the system was developed. This methodology can be applied to develop security metrics for various systems, services and products which will help in improving their security performance.

B. Software security risk analysis using fuzzy expert system[2]

This work presents a technique for analyzing software security using fuzzy expert system in which the inputs to the system are suitable fuzzy sets representing linguistic values for software security goals of confidentiality, integrity and availability. The expert rules are constructed using the Mamdani fuzzy reasoning in order to adequately analyze the inputs. The de-fuzzification technique is done using Centroid technique. Procedure for building the initial fuzzy inference system mentioned in the research paper is:

1. Determining the input variables.
2. Defining the input variables.
3. Defining the output variable membership function.
4. Formulating the rules and populating the rule base.

As a result, a process to design a system that can be used to evaluate the security risk associated with the production of secure software systems was developed. This methodology can be applied to develop an expert system using fuzzy logic to evaluate security of a software or system.

B. Conclusion

As a conclusion, the above analysis of two different methodologies can be helpful in building our hierarchical expert system for security evaluation. The process mentioned in paper can be used for developing hierarchical security metrics for an android system and the process mentioned in paper can be used to build an expert system using fuzzy logic to evaluate security of an android system using the hierarchical security metrics developed.

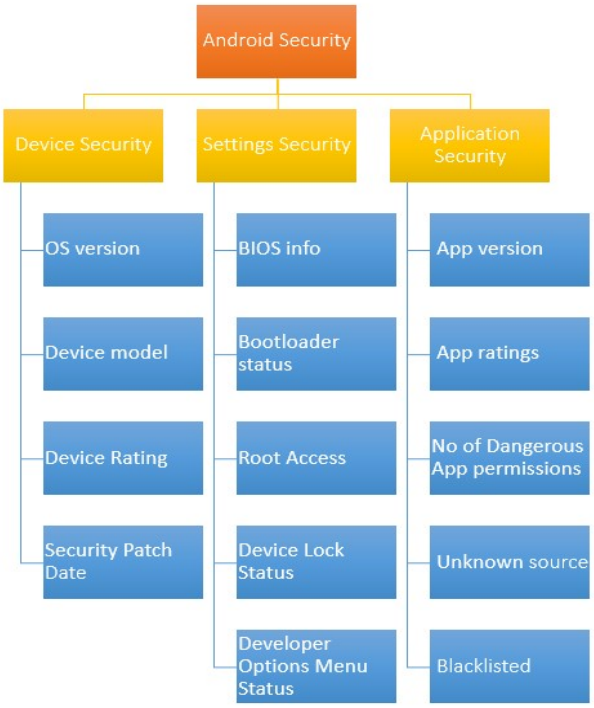
III. Design of the hierarchical metric system

In this section we find out the metrics that should be measured in order to evaluate the security of an android system. The core activity in the security metrics development process is in the decomposition of the security threats. Then the high-level security threats can be expressed in terms of lower-level measurable components applying a decomposition approach. In this way we can develop a hierarchical security metric. The high-level security threats can be divided into three categories: Device Security, Settings Security and Application Security. These three categories can be subdivided into smaller components.

Device Security: This category contains components that are related to the android device information like Android version, Device model, Device Rating and Security Patch Version.

Settings Security: This category contains components that are related to the android device settings like Bootloader status, Root Access and Device Lock Status.

Application Security: This category contains components that are related to the android applications installed in the device like if the application is from an unknown source, if application a blacklisted application and how many out of the following nine dangerous



permissions are granted to an application: Call logs, Camera, Contacts, Body sensors, Microphone, SMS, Memory, Location and Telephone.

IV. Implementation

To build a rule-based expert system, the knowledge can be expressed in the form of rules. A rule consists of two parts: the IF part, called the antecedent (premise or condition) and the THEN part called the consequent (conclusion or action). The rules for this project can be developed using the security metrics defined in the section before. Due to shortage of time, we will be considering only few or the metrics described in the hierarchical metric system presented in the above section for this project. The security metrics evaluated in this project are shown in table 1.

Table 1

Metric	Category	Value
OS Version	Software Security	Latest version or not
Security Patch Date	Software Security	Latest date or not

Table 1

Metric	Category	Value
Bootloader Status	Hardware Security	Locked or Unlocked
Device Lock Status	Hardware Security	True or false
Number of Dangerous App Permissions	Application Security	Scale 0-9

Example of rule for the expert system build based on the metrics mentioned in table 1:

IF bootloader is unlocked
THEN bootloaderStatus = unlocked

System shell used to fill the expert system with knowledge in this project is JESS. JESS is rich in feature and highly portable. It is a rule engine for Java platform, developed by Ernest Friedman-Hill at Sandia National Laboratories in Livermore, CA. on. The second methodology mentioned in section 2 can be used to incorporate fuzzy logic into our expert system to evaluate android security.

While an expert system design has many advantages, its implementation requires a high computational power. To overcome this shortcoming, machine learning techniques can be used. A supervised machine learning can be employed to improve performance. The dataset needed to train can be obtained by generating all possible combinations (permutations) of all inputs and apply them to the Expert System built.

References

1. Development of security metrics for a distributed messaging system, by Reijo M. Savola and Habtamu Abie.
2. Software security risk analysis using fuzzy expert system[2], by Sodiya A. S, Lonfe H. O. D. and Fasan O. M.
3. Identification of basic measurable security components for a distributed messaging system by Reijo M. Savola and Habtamu Abie
4. Smartphone Market Share https://www.idc.com/promo/smartphone-market-share/os