Signature-Based Hybrid Intrusion detection system (HIDS) for Android devices

Avadhoot Pawaskar[1], Vidya More[2], Zain Navrange[3], Hasib Shaikh[4]
[4]Assistant Professor
[1-3]B.E. Students
Department of Computer Engineering,
[1]*aviash024@gmail.com*;[2]*vmore1594@gmail.com*;[3]*zainnavrange@gmail.com*;[4]*shaikh.hasib@rediffmail.com*

***Abstract*—**The goal of this paper is to develop an intrusion detection application for the Android platform. It also strengthens HIDS (Intrusion Detection System Based on the Host) to identify malicious software and toughens the access control on Android system-level. By analyzing the Android security architecture, we proposed a host based intrusion detection application-HIDS which is applied to the Android platform and the active defense is substituted for the conventional passive antivirus.

Keywords*—User Interfaces, pattern of intrusion, android devices.*

*****

I. INTRODUCTION

Android is a mobile device software stack that contains an O.S. (Operating System), a middleware and a key application. Android basis has been established in the technology of Linux and constituted of O.S., U.I. (User Interface) and components of application. It permits developers a free access and allows them to modify the source codes. Based on the raw availability of developed applications and effective controlling issuance, users are most interested to download and install somehow spiteful software coded by hackers. These sorts of users' function make some or all mobile feature vulnerable to working improper. Due to this fact, increasing Android security mechanism will enhance the effectiveness of mobile protection and ability.

This paper will be a significant endeavor in detecting intrusion, especially by proposing a Host-based intrusion detection application for Android platform.

II. LITERATURE SURVEY

In 2007 an open source Linux based mobile Operating System was published by Google called Android. Being Open Source, No Operators Restriction, More Hardware Choice, No Restricted Third-Party Restriction and Google Applications Coherent Integration are five Android advantages. Relating to these advantages Android has conquered much markets share.
Fig. 1 illustrates Android layers.

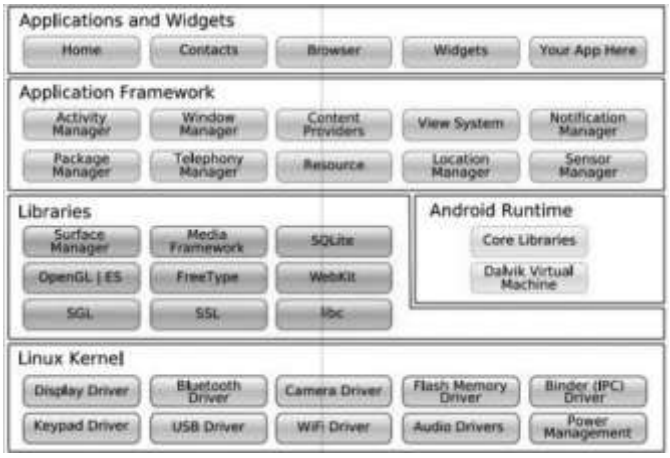

Fig. 1. Android system structure

System kernel services such as memory management, system security, process management and driver model are sufficiently provided in Linux Kernel layer. Alongside Android veils the hardware details to provide uniform services for upper layers; acts as an abstract layer between software and hardware. Android runtime layer is a combination of Android kernel libraries which delivers most functions invoked by Java Class Library. Android libraries layer is a set of C/C++ libraries that is applied by Android components. These libraries are used by developers through Android Application framework. The Android developing platform is Application Platform Layer that contains A.P.Is invoked by kernel applications [5]. Developing different applications by this A.P.Is are provided for developers beside freely hardware using, location information, background service running, clock setting, adding status bar

notes and other function. Android Application Layer is a kernel applications incidental accretion that comprising phone calling, browsing and etc. The developing language of all these mentioned applications is Java [1].

III. EXISTING SYSTEM

An I.D.S. is a security system that detects intrusion made by malicious cracker whose intends to compromise a system. It will display a warning message to the host or server in which intrusion is detected. By using some mechanism, it is possible to halt the intrusion and even block it from a particular resource. The I.D.S. basic activity is to monitor the packet on network traffic and system behavior. Then, it shows a message if abnormal activity occurred in network or host. One of significant parts of information security is intrusion detection system since it is responsible to control the security level of information [2].

Currently, I.D.S. has two types of technique to analysis and detecting an intrusion. Signature-Based Detection is the first method. In this method any intrusion is detected by applying user defined or predefined rules. These rules will indicate patterns which need to be detected. Intrusions are happened if the network packets or recorded system log file match with the predefined patterns. A data base is set up based on these signature rules that can be applied by the I.D.S. to equate all passing packets and check if any pattern recognized. Misuse detection techniques are not effective against novel intrusion which has no matched rules or patterns and it is the prominent disadvantages of this method [2].

Moreover, new or modified attack pattern recognition is also difficult. Detecting well-known attack is the main advantage of this method although.

Second technique is called anomaly detection method when the system will be taught the normal and anomaly activities. It means the mentioned method can perceive malevolent behaviors regarding to log file. It implies the method can also detect modified or unknown intrusion attacks. This technique demands some artificial intelligent algorithms that the normal activities pattern can be taught results decision making for detecting new intrusion attacks can be taken. Detecting unknown attacks is one of the advantages of this method. Being slow regarding to the time consumed to learn new patterns in intrusion detection is counted as one of its drawbacks. Another considered drawback referees in the condition when network has generated all behavior sorts in learning phase of I.D.S. which is hidden from the user, thus it may produce a high number of false positive alerts [2].

Currently, there is an international organize research on I.D.S. that is Common Intrusion Detection Framework (C.I.D.F.). It is the conventional mainstream model of I.D.S. that is categorized into four subsections: E which stands for Event generators, A that is the symbol of Event Analysis, R that represents Response Unit and finally, Event Database that is expressed by D (Fig. 2).

The E Box collects data of events from the overall of computer or network using e.g. sensors, and transfers the gathered data to the other parts. Data received from section E is analyzed in section A besides gives analyzing to some standard. Section R has the responsibility of responding to the analyzed results for instance warning even connection cutting off or manipulating files attributes and actions the same. Data received from the boxed A, E and R is stored in D box how a complex structure or simple text file can be used for.

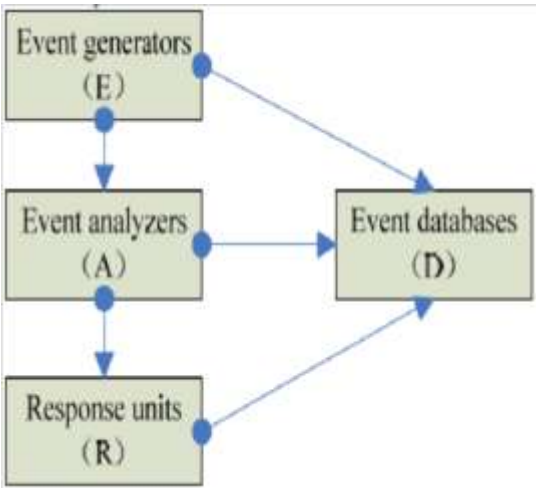

Fig. 2. Structure of CIDF Model

IV. PROPOSED SYSTEM

The log files are fed to the proposed model (as shown in Fig.

3) by logcat command and then Log File Decoder Module is invoked to change the records into a defined format that system is able to analyze them conventionally. In the next step, the Detection Engine is invoked to compare the records with the rule-sets. In case of finding any matched item, a possible intrusion action command is detected and Output Model does proper response such as giving alert, output intrusion behavior or logging it. In case of no matching item, natural action is done and the system goes to get next record to process [1].

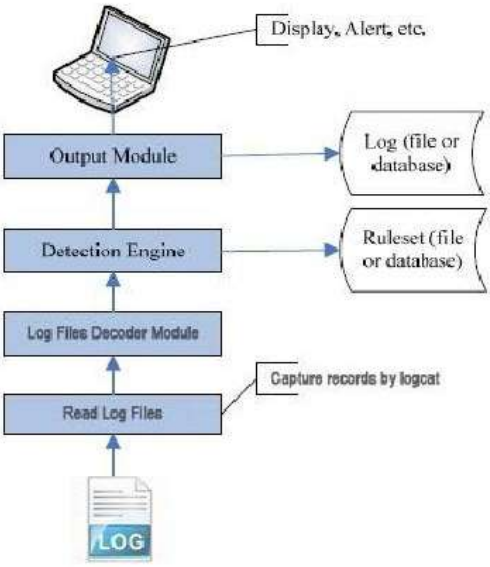

Fig. 3. Structure of Proposed Model

HIDS for Android indicates implementing HIDS to smart phone security that introduces an active defense system in Android security area.

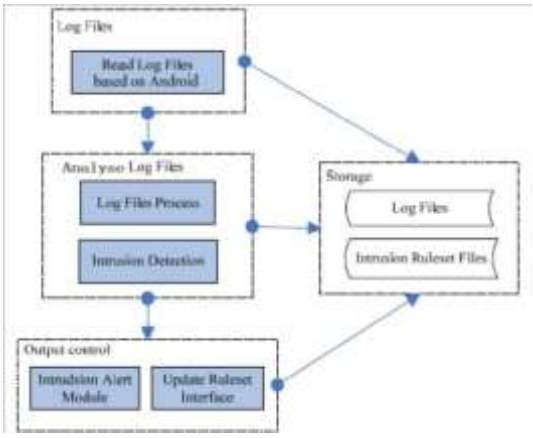

Fig. 4. Structure of HIDS model based on Android

Fig. 4 depicts the system structure clearly. Regarding to C.I.D.F. definition, the proposed H.I.D.S. covers four sections: Log File Reading, Log File Analysis, Controlling Output, and Storage. There is a collecting and viewing system output mechanism which is provided by the Android logging system. The Log Files are inserting by logcat command and are given to Analyzing module. The module decodes and pre-processes the records, and then invokes the matching engine to detect intrusions. At the last step, the matching results are sent to Output Control Module which chooses to alert or record into log files regarding to the results. With the purpose of adapting the changing Internet and new intrusion behavior, the proposed system has Update Rule-set Interface to update rule-set which is enable to detect. The work flow of HIDS based on Android is shown in Fig. 5[1].

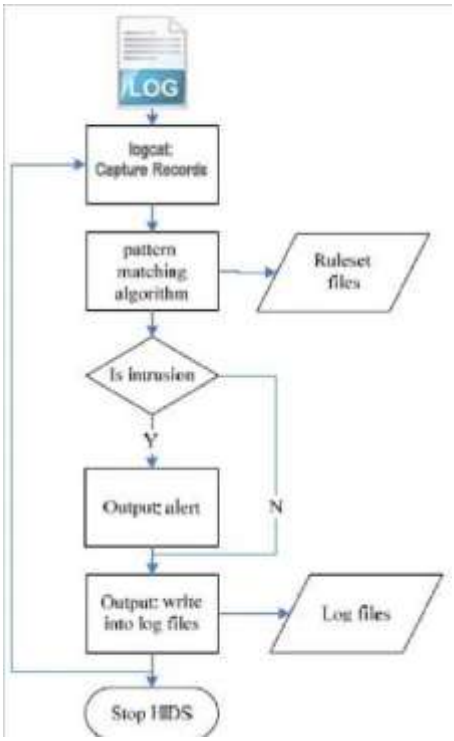

Fig. 5. Work flow of HIDS based on Android

A. Rule-set Design and Log Files

The supposed H.I.D.S. model is just an initiative to enhance the system quickly, it uses a file to store rule-set of intrusion.

Therefore, when it functions properly, a suitable database can surpass the rule-set file to store a lot of intrusion rule-set.

To make the rules, we use a simple method in which each rule has to be in a single line with no crossing lines and includes rule head and rule option. Rule head includes: rule's action, name of classified event (Error, Warn, Info, Debug, and Verbose), name of application. Rule option includes: alert message. For instance, the following is an example:

Rule head: alert D/GTalkService
Rule option: msg (internet access)

This rule means: To detect every access to the internet from the specific application that in this example is Google talk (GTalkService).

On the other hand, the Android log file is relatively simple where each line represents an activity on the host. For example:

Date Time Type/Name of Activity (Code)
10-01 12:25:13.804 D/GTalkService (1567)

B. Application Development

Regarding to R.A.D. (Rapid Application Development), four phases in this research are provided to develop the system thoroughly. This System Analysis phase demands System Design, System Development and Implementation, and System Testing and Evaluation as its

requirements. System Analysis is the first phase which information is gathered as much as needed regarding to the study. System Design is the second phase that proposing Host based I.D.S. according to the study and the project requirements. Then the project user and system requirements are specified and project is analyzed regarding to the requirements demands and system interface and architecture are designed. Structured Methods are applied for modeling system analyzing and design [2].

System Development and Implementation is the further phase that system is implemented regarding to the design of the system. In this phase the system is coded in Java to transforming the system logical form concepts into a useable system. System Testing and Evaluation is the final phase. The system is tested in this phase regarding to test case and the overall functionality of the system [2].

Fig. 6 illustrates how the system recognizes two attacks types and their patterns. If there is a known attack pattern, the system matches the pattern in the database and alerts the host user to take any proper action in response.

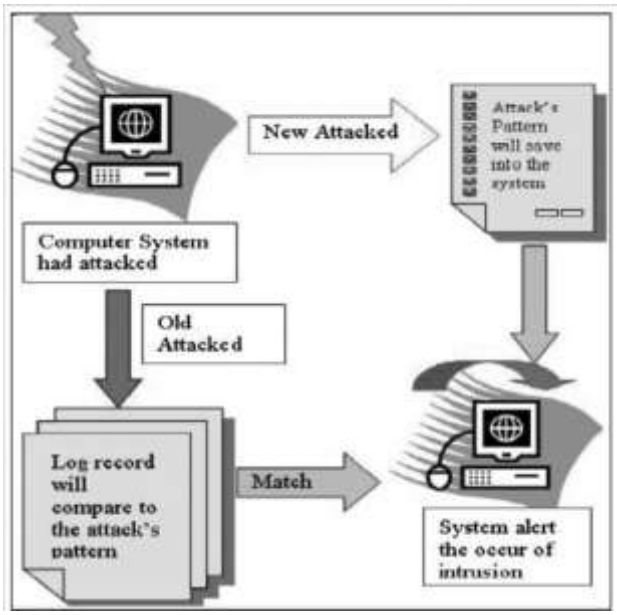

Fig. 6. System Architecture

C. Implementation

Detecting intrusion through log file is the main concern of this Host based I.D.S. providing by Android O.S. Therefore implementation and result of this system (modules and their processes) is the main subject of this section. Table 1 presents the six main models in the system. Before anything else, users are demanded to have an account with regarding login and password provide user access into the system by. A successful authentication prompts the user main interface of the system within the five modules that is explicated briefly in table 1.

Table 1 SYSTEM MODULES

System's Module	**Description**
Login	System Logging in using login and password
LogFile Analysis	Analysis EventLogfile
Pattern Input	Input pattern of intrusion
Pattern Edit	Edit pattern of intrusion
Pattern Delete	Delete pattern of intrusion
Username and Password Edit	Change information of login and password

D. Interface Design of Application

Designing a friendly user interface that is based on Android Application Framework and Applications respecting to look up the detection results and update rule-set pattern easily is the concern of this phase [1].

PATTERN MATCHING ALGORITHM

Currently, two kinds of pattern matching algorithms exist: single-pattern matching algorithm that matches only one pattern a time and the second, multi-pattern matching algorithm that matches many patterns a time [1].

The efficiency of pattern matching algorithm is so important due to the time. One of the efficient pattern matching algorithm is Fuzzy logic that allows for approximate values and inferences as well as ambiguous data (fuzzy data) as opposed to only relying on crisp data (binary yes/no choices). For example, fuzzy logic usually uses IF- THEN rules, or constructs that are equivalent. Rules are usually expressed in the form: IF variable IS property THEN action

Therefore, in the base of analysis of both hardware and software, fuzzy logic algorithm that is a fast multi-pattern matching algorithm is applied [3].

CONLUSION

This paper represents a host based intrusion detection model after analyzing security of smart phone for the Open Android platform on Google. By considering the mobile hardware limitations, we develop a host based intrusion detection application in the area of smart phone security. There are some things that we can do for developing the model. It is possible to combine I.D.S. based software on the host and I.D.S. based packets on the network which will result in intrusion detection from not only host malware but also from the network. Furthermore, the system can be enhanced on how making the systems rule-set up to date by the mean of learning mechanism

as neural network or adaptive neural-fuzzy tools. Eventually, the pattern matching mechanism also demands to be optimized, it is essential to propose a more operative multi-pattern matching algorithm to make most prominent critical security problem adapted along with the rapid smart phone enhancement.

ACKNOWLEDGMENT

The authors would like to thank Research Management Centre, Universiti Teknologi Malaysia for funding this research work through vote number 4D066.

REFERENCES

[1] K. Xiaoming and W. Qiaoyan, “Intrusion detection model based on Android,” in Broadband Network and Multimedia Technology (IC- BNMT), 2011 4th IEEE International Conference on, 2011, pp. 624-628.

[2] F. A. Bin Hamid Ali and L. Yee Yong, “Development of host based intrusion detection system for log files,” in Business, Engineering and Industrial Applications (ISBEIA), 2011 IEEE Symposium on, 2011, pp. 281-285.

[3] J. Fenggen, W. Weiming, G. Ming, and L. Chaoqi, “A real-time rulematching algorithm for the network security audit system,” in Information, Communications and Signal Processing, 2009.ICICS 2009. 7th International Conference on, 2009, pp. 1-4.

[4] T. Liu and Q. Meng, "Research on high-speed Network-based Intrusion Detection System," in System of Systems Engineering (SoSE), 2012 7th International Conference on, pp. 363-365.

[5] B. Han, "Analysis and Research of System Security Based on Android," in Intelligent Computation Technology and Automation (ICICTA), 2012 Fifth International Conference on, 2012, pp. 581-584.

[6] Z. Gu and C. Wang, "Statistic and Analysis for Host-Based Syslog," in Education Technology and Computer Science (ETCS), 2010 Second International Workshop on, pp. 277-280.