Proposed security by IDS-AM in Android system

Chaimae SAADI[1], ibtissame kandrouch[2] and Habiba CHAOUI[3]
Systems Engineering Laboratory, Data Analysis and Security Team National School of Applied Sciences, Campus Universitaire, B.P 241, Kénitra14000, Morocco
chaimaesaadi900@gmail.com[1] ibtissame.kandrouch@uit.ac.ma[2] ,mejhed90@gmail.com[3]

Abstract— mobile systems are always growing, automatically they need enough resources to secure them. Indeed, traditional techniques for protecting the mobile environment are no longer effective. We need to look for new mechanisms to protect the mobile environment from malicious behavior. In this paper, we examine one of the most popular systems, Android OS. Next, we will propose a distributed architecture based on IDS-AM to detect intrusions by mobile agents (IDS-AM).

***Keywords*— Android, IDS, IDS-AM, mobile agents, attacks.**

1. INTRODUCTION

With the advent of the mobile operating system, including Android devices, the security threat is increasing and mobile security enhancement solutions that can mitigate the associated risk are lacking [1]. So android devices have serious problems with malwares, in 2016 according to a recent report from Kaspersky Lab and INTERPOL, Android users would be prime targets for malware. Indeed, over 98% of detections Kaspersky Lab to Android [13]. On an open market such as that of Android, the quality of applications is moderated by the user reviews [2]. If an application is reported by some users as malware, Google removes this malicious application. Security is primarily based on the user should not install an application with a small number of comments or requesting not required permissions for the application [3]. This paper proposes a methodology to automatically detect an intrusion (malware, virus, bug…) using IDS, that is an integral part of any complete security package of a modern. An IDS is used to detect the intrusions by supervising a network or a system and analyzes collected flows of audit [4].

This paper is organized as follows: Section 2 presents some security issues in android environment, and we provide background overview information about the current status of security solutions in this platform. Then in section 3 we propose a solution that enables an Androphone to detect an intrusion using IDS based on new architecture that have three agents: monitoring, analyzing and reporting. And finally in section 4 we will show the test and result of implementation of this architecture in real environment.

2. RELATED WORK

The use of intrusion detection techniques has been attempted by many researchers to detect malware on Android devices.

[9] used DroidBox, the Android application sandbox, to generate behavioral graphs to help analyze runtime activities and establish functional patterns. The patterns were then used in cross-examining naming classification of malware families by known antivirus vendors. But the test that was made is not efficient with all types of malwares. [10] proposed a solution based on monitoring events happening, on kernel level. [10] used kernel system calls, network activity events and file system logs to detect anomalies in the system. At that time, there were no real Android devices available, so they failed to test their operating system properly. [11] developed abnormally a framework for anomaly detection on Android Smartphones. The framework monitored the information obtained from the Smartphone. Then, it applied machine learning to classify the collected data as normal or malicious. Yet they could not find real malware to test their solution. [12] proposed a methodology to automatically detect the use of a considered permission and to warn the user about its use when this occurs. [12] proposed to achieve this goal without modifying the Android operating system a methodology that decompiles the application and injects a small patch into the Bytecode before repackaging the application. The introduced patch sends notification to a third party application that can be used as a monitoring application or an authorization service. But this solution detected just

978-1-7281-1482-8/19/$31.00 ©2019 IEEE

66% of malwares that try to steal private data such as contact, SMS.

2.1. Android Overview

Google Android is an open source Linux Based operating System, which allows modification on kernel level. Android consists of five layers of services [5]:

1) **Kernel layer** based on Linux, it is closest to hardware.

2) **Runtime layer** contains a Dalvik Virtual Machine (DVM) and each app operates in its own DVM.

3) **Libraries** are specific to hardware architecture on the device,

4) **Framework layer** implements application level services such as Inter-Process Communication (IPC).

5) **The Application** framework defines the creation and working of apps.

The following figure summarizes all this five layers[5].

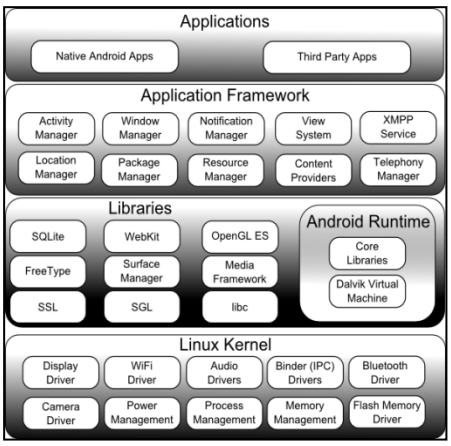

Fig 2. Android architecture [14]

2.2. Android security

Android security depends on different parts of the OS. It is built on top of a Linux kernel. Then, as each application runs as an independent process, isolation is guaranteed by the UNIX permissions of standard user processes. Each process contains an instance of the DVM that also provides some isolation between the application and the OS. Nevertheless, Android gives the ability to run native libraries that could endanger the system [6].

Attacking android

Figure 3 shows the evolution of many types of malware, and in figure 4 we can find the Top 20 malicious mobile programs as reported in [15].

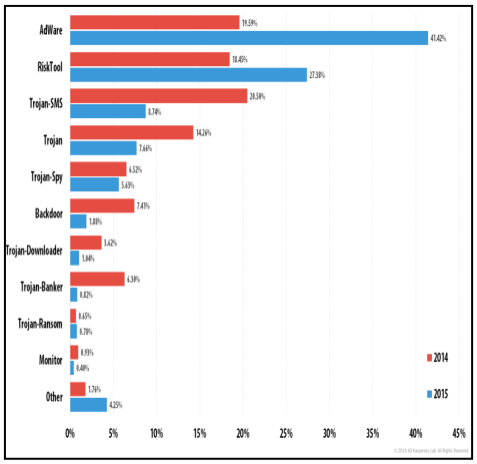

Fig 3. *Distribution of new mobile malware by type in 2014 and 2015*[15]

	Name	% of all attacked users*
1	DangerousObject.Multi.Generic	44.2
2	Trojan-SMS.AndroidOS.Podec.a	11.2
3	Trojan-Downloader.AndroidOS.Leech.a	8.0
4	Trojan.AndroidOS.Ztorg.a	7.6
5	Trojan.AndroidOS.Rootnik.d	6.9
6	Exploit.AndroidOS.Lotoor.be	6.1
7	Trojan-SMS.AndroidOS.OpFake.a	5.6
8	Trojan-Spy.AndroidOS.Agent.el	4.0
9	Trojan.AndroidOS.Guerrilla.a	3.7
10	Trojan.AndroidOS.Mobtes.b	3.6
11	Trojan-Dropper.AndroidOS.Gorpo.a	3.6
12	Trojan.AndroidOS.Rootnik.a	3.5
13	Trojan.AndroidOS.Fadeb.a	3.2
14	Trojan.AndroidOS.Ztorg.pac	2.8
15	Backdoor.AndroidOS.Obad.f	2.7
16	Backdoor.AndroidOS.Ztorg.c	2.2
17	Exploit.AndroidOS.Lotoor.a	2.2
18	Backdoor.AndroidOS.Ztorg.a	2.0
19	Trojan-Ransom.AndroidOS.Small.o	1.9
20	Trojan.AndroidOS.Guerrilla.b	1.8

Fig 4. Top 20 malicious mobile programs [15]

In the following paragraph, we discuss the results of the classification and the characteristics of Android malwares given in [8].

- Trojans look like a normal app, but they perform harmful behavior without knowledge of the users.
- Spyware may present itself as good applications, but has a hidden agenda to silently monitor contacts, messages, location etc. that leads to steal private data.
- Worm app can create similar copies of itself and spreads them through network and media.
- Backdoor authorize other malware to enter the system facilitating them the bypass of the normal security procedures.
- Botnet apps compromise the device to create a Bot, so that the device is controlled by Botmaster (remote server), called, through specific commands.
- Ransomware can lock the user device to make it inaccessible until some ransom amount is paid through online payment service.

As mentioned before, the approaches proved valuable in protecting Smartphones but they have lot of restrictions. Most of the existing methods learn from traditional IDS. The special character of the Smartphone is not fully taken into account. Our presented approaches allow us to extract as many features as we would like. This makes the detection capability becomes more efficient. The intrusion detection system we proposed not only can find abnormality but also can locate the malware, and send reporting log to the system for taking appropriate measures , that are predefined .The main role of this solution is to detect a suspicious behavior in the system caused by a malicious applications particularly malwares.

3. PROPOSED IDS ARCHITECTURE

In order to cope against abnormality particularly malwares, we proposed a new architecture of intrusion detection system. It is used to help users find the suspicious behavior on the Smartphones. The architecture of intrusion detection system based on the android platform can be seen on Figure 5.

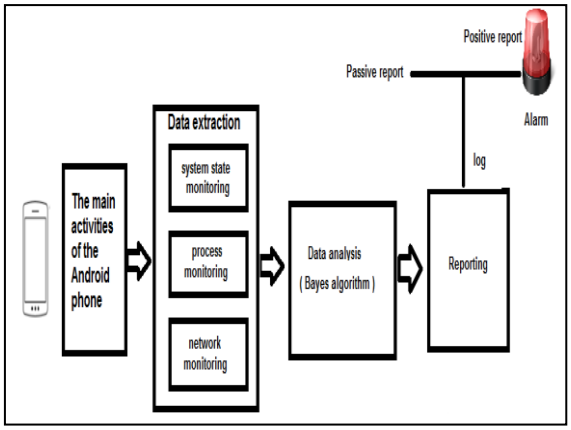

Fig 5. The architecture of intrusion detection system

The architecture of the intrusion detection system is based on three basic elements that are used by mobile agents:

1. Extracting data that allows us to extract activated features from our Android smartphone and more precisely processes, system status and network traffic.
2. the data analysis which allows to analyze the different traffic of our system by the use of bayesian algorithm
3. Reporting that allows us to make the right decision according to dataset extracted from the data analysis

a. Agents of Data Extraction

Data Extraction Agents aim to extract and record the main activities on the smartphone. When a normal smartphone work, the Android system keeps a steady state. Once the smartphone was attacked by malware, the system state defined different levels of abnormality.

for this, we discover smartphone anomalies in real time, efficient selection and extraction of features are essential.

As shown in Figure 5, the data extraction has three functional modules, namely, system status monitoring, network monitoring, and process monitoring. The system status monitoring module monitors real-time system behaviors, such as CPU usage, battery consumption, memory usage. We find indeed malware that can consume a lot of loads and traffic. The main work of the process monitoring module is extracting

the characteristics of all processes running on the phone. This means information about applications running in real time so that we can find malicious applications that can damage the system or steal private data such as SMS, contacts, location, etc. The network monitoring module analyzes the incoming and outgoing network traffic On the smartphone, we can get the source IP address, the destination IP address, the protocol type (TCP / UDP / ICMP), the port number source and the destination port number. All this information is used to identify the creator of each network connection,

Data analysis uses a detection algorithm to determine if the Android system is an invasion. However, it is not enough to find the anomaly of the Android system. In order to further analyze the anomalies of the Android system and to locate malware, we also need to monitor the process and network traffic, providing data analysis for a more detailed data source.

b. Agents of Data Analysis

The data analysis agent is the main element of the intrusion detection system. It analyzes the extracted data provided by the data extraction agents. it uses the Bayes algorithm to analyze and determine if there is abnormal behavior. First, based on the behavioral characteristics of the set of learning samples, we establish the normal behavior profile of the Android system. We then extract the behavior characteristics from the data needed to test and establish the current profile. and afterwards we make a comparison of the retained profile with the contour of the normal behavior. If it exceeds the established threshold, it is thought that there has been abnormal behavior. The intrusion detection system generates an alarm. The reporting process further, otherwise it is considered normal behavior. Indeed, this element can compare a normal behavior that is extracted by the Android system and an abnormal behavior that is extracted by one of the three elements of the extraction of data.

We have therefore used a Naïve Bayes classifier which can affect the most likely class to a given example described by its feature vector.

- C: have two possible values namely c1 = "normal" and *c2* = "abnormal".
- $X = (X_1, X_2, ..., X_n)$: characteristics of the behavior of the Android system. Each element refer to feature of android system (Xi→ i= 1,2…,n).

TABLE I. ANDROID SYSTEM FEATURES

Element	Feature
CPU	Usage of CPU
Battery	Consumption of battery
Memory	Usage of memory
Process	Amount of running processes
Inflow	Inflow of network traffic
Outflow	Outflow of network traffic

This classifier can calculate the maximum of two probabilities which are:

- ***P(C =c1 | X =x):*** the probability x of occurrence of c1
- ***P(C =c2 | X =x):*** the probability x of occurrence of c2

It means that will use this expression:

Max{P(C =c1 | X =x), P(C=c2 | X=x)}

c. Agents of Reporting

The reporting agent's main purpose is to present a report on the security of the Android system. There are two ways to report the positive and the passive relationship. Passive reports to present the normal behavior of the Android system. In the event of a serious threat, the alarm information is saved as a log file. Then the administrator analyzes the log and takes the appropriate measures. It means that we take a positive reporting approach and take the appropriate measures based on predefined rules, such as uninstall the application, terminate the process, cut off all wireless connections, encrypt the data, change the Firewall Policy etc.

In this paper, the intrusion detection system divides the reporting into two levels. We set log file according to the behavior of the android system. Once the phone was found to be invaded, the intrusion detection system alerts the user which would take the appropriate correction measures.

4. TEST AND RESULTS

4.1. Test environment

JADE (Java Agent DEvelopment Framework) is a software Framework fully implemented in the Java language. JADE system supports coordination between several agents FIPA and provides a standard implementation of the communication language FIPA-ACL. In this section we will show how to start JADE platform and we will make agents communicate between them. Indeed in this test we will create five agents for each element of architecture.

4.2. Network monitoring Agent

Network monitoring agent (Netm) captures packets from different network interfaces and prepares these packets to send to the other agent, which can analyses information about the network such IP address to locate the source of malware. This figure shows the result of extraction some information about network

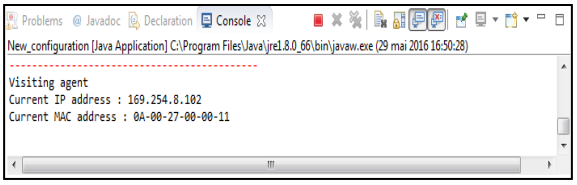

Fig 6. Result of extraction IP adress and Mac adress

4.3. System state monitoring agent

System state monitoring agent (Sym) extracts features of physiques elements from the system of Smartphone, such as CPU usage and memory usage and prepares these features to send to the other agent. This figure shows the result of extraction some information about system state.

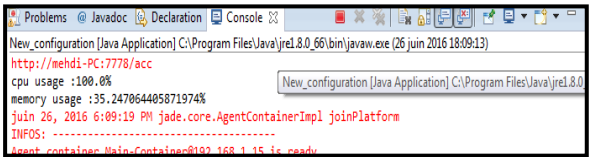

Fig 7. Result of extraction CPU and Memory usage

4.5. Process monitoring agent

Process monitoring agent (Prm) extracts some information about processes such as ID, name, and prepares these data to send to the other agent, and to locate the source of malware. This figure shows the result of extraction some information about process.

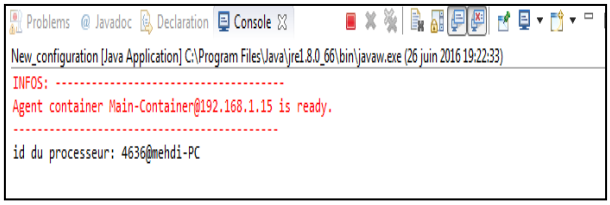

Fig 8. Result of extraction ID process

4.6. Data analysis agent

Data analysis agent (AnalysisBNC) analyses the data which are sending by (Sym) using the Bayes naïve classifier, to detect anomalies in the system.

4.7. Reporting agent

Reporting agent (Report) alert the user of Smartphone using a message that a malicious application is running, so the user must take some correctives measures such as delete the malicious application or end a process …

4.8. Communication between mobile agents

In this proposed architecture, after the creation of agents, (Netm, Prm, Sym, AnalysisBNC, and Report) we must assure the communication between them, so JADE proposes ACL messages which are very simple to use .This figure show the architecture of the proposed solution using agents and ACL messages for communication.

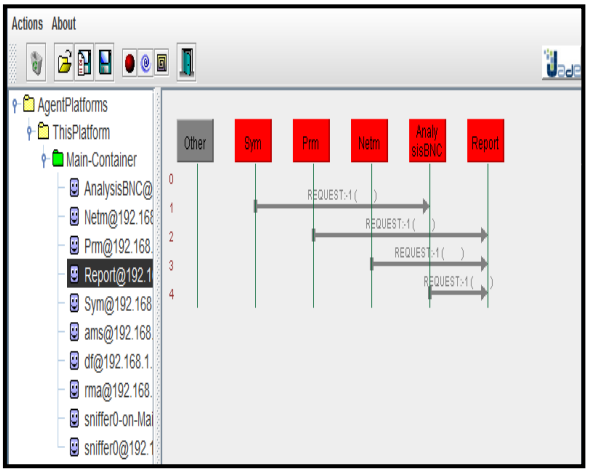

Figure 9: Exchange of message between mobile agents

The ACLMessage class represents messages which can be exchanged by the agents. When an agent wants to send a message, it must create a new object ACLMessage, and then call the send () method, which can send the message to the receiver. When agent wants to receive a message, it must use the receive () method. The content of the messages is an interaction between mobile agents and their environments. In this case the content is about traffic network, particularly IP address and the Mac address, system state such as CPU and memory usage, process such as ID process, and ACL message for displaying the result of analyze. The following figure shows the result of this test.

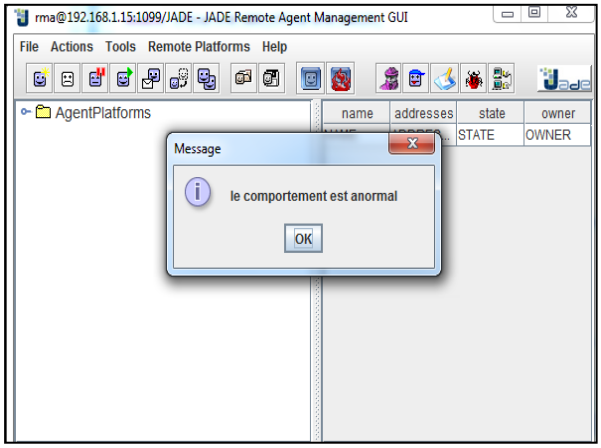

Figure 10: Result of analyze

After analyzing Data which are from system state monitoring (Sym), the result of this analyze is sending to (Report) agent, in this case it displays that the comportment of system is abnormal.

5. CONCLUSION AND FUTURE WORK

Smartphone security is becoming more and more serious. Intrusion detection systems for smartphones will become one of the interesting points of future research. In particular, malware for the Android system is also experiencing abnormal growth. Our future work using this architecture consists to complete the implementation by integrating the solution in Android System. And finally we mentioned that the implementation of this work is in progress. Indeed the finale version of this paper will be done after we finish the evaluation of this solution

REFERENCES :

[1] Smartphone, "smartphone OS and market share," [Online].Available://www.idc.com/prodserv/smartphone-os- marketshare.jsp

[2] C. Miller, “Mobile Attacks and Defense,” IEEE Security & Privacy Magazine, vol. 9, pp. 68–70, Jul. 2011.

[3] C. Orthacker, P. Teufl, S. Kraxberger, A. Marsalek, J. Leibetseder, and O. Prevenhueber, “Android Security Permission Can we trust them?” in 3rd International ICST Conferenc on Security and Privacy in Mobile Information and Communication Systems, vol. 3, 2011,p.12.

[4] C. Saadi, H. Chaoui, H. Erguig” Security Analysis Using IDs Based on Mobile Agents and Data Mining Algorithms” (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1), 2015, pp.597-602.

[5] "Android Open Source Project," [Online]. Available: https://code.google.com/p/android/.

[6] D. Barrera and P. Van Oorschot, “Secure Software Installation on Smartphones,” IEEE Security & Privacy Magazine, vol. 9 ,pp. 42–48 ,May 2011.

[7] G. Delac, M. Silic, and J. Krolo, “Emerging security threats for mobile platforms,” in 34th International Convention, 2011, pp. 1468–1473.

[8] P. Faruki, A. Bharmal, V.Laxmi, V.Ganmoor, M.S. Gaur, M.Conti and M. Rajarajan “Android Security: A Survey of Issues, Malware Penetration and Defenses” IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, vol.00, January 2015

[9] M. Alazab, V. Monsamy, L. Batten, P. Lantz, and R. Tian, “Analysis of malicious and benign Android applications,” in Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on, 2012, pp. 608–616.

[10] A. Schmidt, H. Schmidt, J. Clausen, K.Y¨uksel, O. Kiraz, A. Camtepe,

and S.Albayrak. “Enhancing security of linux-based android devices”. in Proceedings of 15th International Linux Kongress. Lehmann, October.2008.
[11] A. Shabtai, U. Kanonov, Y. Elovici, C.Glezer, and Y. Weiss. “Andromaly: a behavioral malware detection framework for android devices”. Journal of Intelligent Information Systems, , 2011. Pages 1–30
[12] P. Berthomé, T. Fécherolle, N. Guilloteau and J.-F. Lalande” Repackaging Android Applications for Auditing Access to Private Data ”IEEE Seventh International Conference on Availability, Reliability and Security , 2012
[13] Statistiques, "android la cible de 98.05 des malwares sur smartphones," [Online].Available : http://nokians.fr/2014/10/statistiques-android-la-cible-de- 9805-des- malwares-sur-smartphones/
[14] Android, "android OS archiecture," [Online]. Available: http://www.c4learn.com/android/android-os-architecture/
[15] Mobile, "mobile malware evolution 2015," [Online].Available: https://securelist.com/analysis/kaspersky-security-bulletin/73839/mobile-malware-evolution-2015/