Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Evaluating efficiency of Anti-Malware using Transformation Attacks

[1]Seemadevi M. Shelake*, [2]Prof. Prakash. B. Dhainje, [3]Dr. Deshmukh Pradeep K.
[1]M.E (CSE), Student, SIETC, Paniv CSE Dept., Solapur University, Solapur, Maharashtra, India
[2]MTech, MBA (IT), PhD (CSE) Head of CSE Dept., SIETC, Paniv CSE Dept., Solapur University, Maharashtra, India
[3]M.E., PhD (CSE) Principal, SIETC, Paniv CSE Dept., Solapur University, Solapur, Maharashtra, India

Abstract— In this paper we have reviewed and studied various malware detection tools. There are various attacks are applied on anti-malwares. Such attacks can be detected by anti-malware systems but some of them can't detect unknown and all types of attacks. We have reviewed different techniques of malware samples detection, such as resistance to various common obfuscation techniques are analyzed. The possible solution for improving the current state of malware detection on mobile devices can be found using a larger malware samples.

Keywords— malware, anti-malware, obfuscation techniques, transformation.

I. INTRODUCTION

Day by day the popularity of mobile apps is increasing rapidly. These apps increases ease of access within less time. But with this security must be serious about these devices. Today Android have problems related with security. The Android apps are more vulnerable to malware attackers. There are many anti-malware software's available to protect the android apps against attacks. But with the growth of the android platform, it becomes target for malware authors. Google Play offers different paid and free offerings for anti-malwares. It can be observed that there are many malware threats attempting to break the security chains of android even though there is a huge security provided by different anti-malware softwares. So here, aim is to evaluate the efficiency of anti-malware tools on Android in the face of various techniques. To do so the term 'transformation' which refers to polymorphic changes is done on malware samples. It does not involve code-level changes. These transformed malwares are applied to the anti-malwares to check their efficacy. The technique called Droid Chameleon is used to conduct these common transformations. This technique transforms android applications automatically. That is the reason why we are trying to study the anti-malwares and their capability to defeat the attacks.

Generally, the efficacy of anti-malwares is concerned with following issues:

- Different Malwares and the way they are used for transformation attacks.
- How the anti-malwares are resistant to these transformation attacks.
- The probable ways to improve the efficiency of anti-malwares.

II. LITERATURE SURVEY

MALWARE DETECTION USING VARIOUS TOOLS

a) ADAM

ADAM, an automated and extensible system that can evaluate, the effectiveness of anti-virus using a various malware samples for the Android platform. It automatically transforms an Android malware sample into different variants through various repackaging and obfuscation techniques, while preserving the original malicious behavior
Fig.1. shows the design of ADAM.

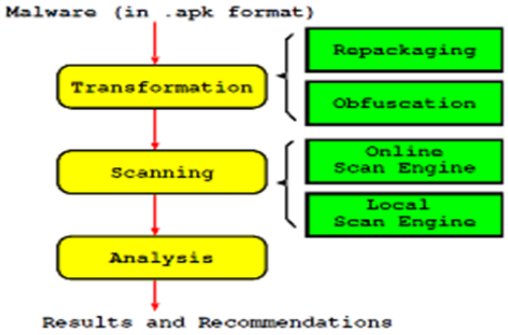

Fig. 1: Design of ADAM

ADAM can automatically transform an original malware sample to different variants via repackaging and obfuscation techniques in order to evaluate the robustness of different anti-virus systems against malware mutation [1]. ADAM is designed by connecting different building blocks. These blocks are used to test different anti-viruses against malware

samples.

1) Advantages-

1. It can be used for studies of very large-scale malware samples.
2. As transformation is done manually there is no need to apply manual modification of malwares. This results less overhead on codes.

ADAM is not always capable to avoid an anti-malware tool. It implements only some of transformations, such as renaming methods, introducing junk methods. It cannot be said that ADAM will always provide the better detection mechanisms and this is main limitation of this system.

b) Obfuscation Techniques

Obfuscation techniques have been the focus of much research due to their relevance. This helps to preserve privacy policies between sender and receiver. Fig.2. shows how obfuscation technique provides the protection of messages between Alice and Bob. The source message is compiled and object code is created which is then obfuscated and passed to the server. Server then passes it to the client i.e. Bob. The obfuscated object code is then deobfuscated to object code which is decompiled to original source. Executer does the actual execution.

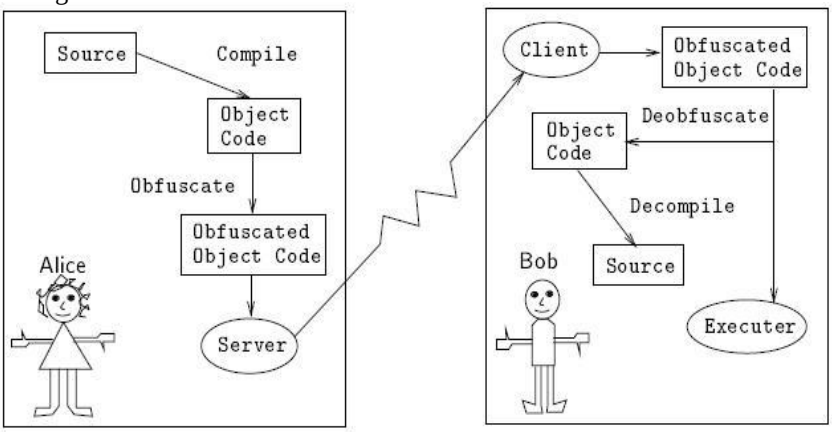

Fig. 2: Protection through obfuscation

1) Advantages-

Obfuscation can be easily used to trace software pirates.

2) Limitations-

The obfuscated software remains secret until the powerful deobfuscator to be built. Therefore, there must be short time period between the releases of obfuscated software versions.

c) Semantics-preserving Malware Detection

M. Christodorescu et al. [3] proposed malware detector that is used to find out the malicious behavior of a program. Most of times hackers use obfuscation to change the malwares. So, here the detectors use pattern-matching technique to search the obfuscations made by hackers. The advantage of this system is that it is totally syntax based technique. So, it is easy to be understood by detectors and it has relatively low run time overhead. Limitation is mandatory to save the patterns of malicious instructions into templates which need to use of large databases.

d) Effective and Efficient Malware Detection at the End Host

Clemens Kolbitsch et al. [4] proposed a novel malware detection approach that is both *effective* and *efficient*, and thus, can be used to replace old anti-virus tool at the end host. This technique analyzes a malware to build a model that characterizes its behavior. Such models describe the information flows between the system calls essential to the malware's mission, and therefore, cannot be easily evaded by simple obfuscation or polymorphic techniques. Then, extract the program slices responsible for such information flows. For detection, execute these slices to match with these models against the runtime behavior of an unknown program.

1) Advantages

1. It can effectively detect running malicious code on an end user's host with a small overhead.
2. It generate effective tool that capture detailed information about the behavior of a malwares variation.
3. Scanner that can efficiently match the activity of an unknown program against this system.

2) Disadvantages

1. It cannot generate system call signatures or find a starting point for the slicing process.
2. The new algorithms should be implemented for above limitation.

e) Scalable and Accurate Zero-day Android Malware Detection

Michael Grace et al.[6] proposed proactive scheme to spot zero-day Android malware, It does not depend on malware samples and their signatures. It is an automated system called RiskRanker to scalable analyze whether a particular app exhibits dangerous behavior (e.g. launching a root exploit or sending background SMS messages).

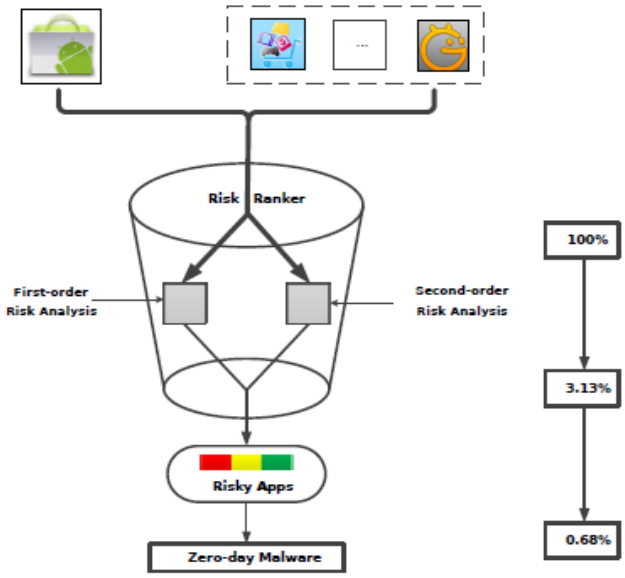

Fig. 3.The RiskRanker Architecture

Fig. 3. Shows the overall architecture of RiskRanker. It checks and translates potential security risks into corresponding detection mod-ules of two orders of complexity. The first-order modules handle non-obfuscated apps by evaluating the risks in a straightforward manner; the second-order modules capture certain behaviors (e.g., encryption and dynamic code loading) to detect malware.

f) Automated Remote Repair for Malware

The malicious network traffic increases because of intruders. The problem can be solved by using Airmid, which is an automated system for remote remediation of mobile malware. After the detection of malicious traffic, the cellular network interacts with the source device to identify its originality of that traffic [5]. Fig 3. Shows this approach

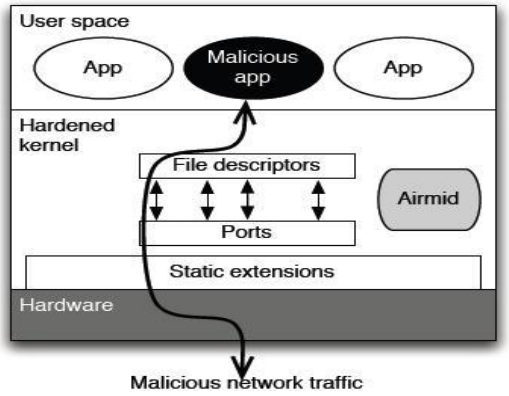

Fig. 4.malicious network traffic

This system has very low overhead as its benefit but having disadvantages as,

1. It does not tie to device and its security.
2. It is not able to characterize the traffic of large amount of malwares.

g) Automated Security Analysis of Smartphone Applications

To do the automation of security analysis the tool Apps Playground is used. It integrates multiple components comprising different detection and automatic exploration techniques for this purpose [7].The system can be evaluated using multiple large and small scale experiments involving real benign and malicious application.

The main advantage of this is it gives effective analysis even with large number of applications, with limitation of less effective at automatically detecting privacy leaks and malicious functionality in application.

h) Detection of malicious apps in official and alternative Android markets

To find out malicious applications related to android permission based behavioral footprinting scheme is used. It is used for known malwares. Then a heuristics-based filtering scheme is applied to unknown malwares. This total system with known and unknown malicious families is called 'DroidRanger' [8].

1) Advantages-

1. It helps to focus on both official and unofficial Android markets for detecting malicious apps.
2. By using known and unknown malicious apps the detection proves to be scalable and efficient.

2) Limitation-

It needs rigorous policing process especially for unofficial marketplaces which is not satisfied by DroidRanger yet.

III. PROPOSED SYSTEM

V. Rastogi et al. [9] DroidChameleon a framework used to check the efficiency of anti-malwares. It does this by using different transformations on malware samples. Figure5. Shows how all these transformations are used.

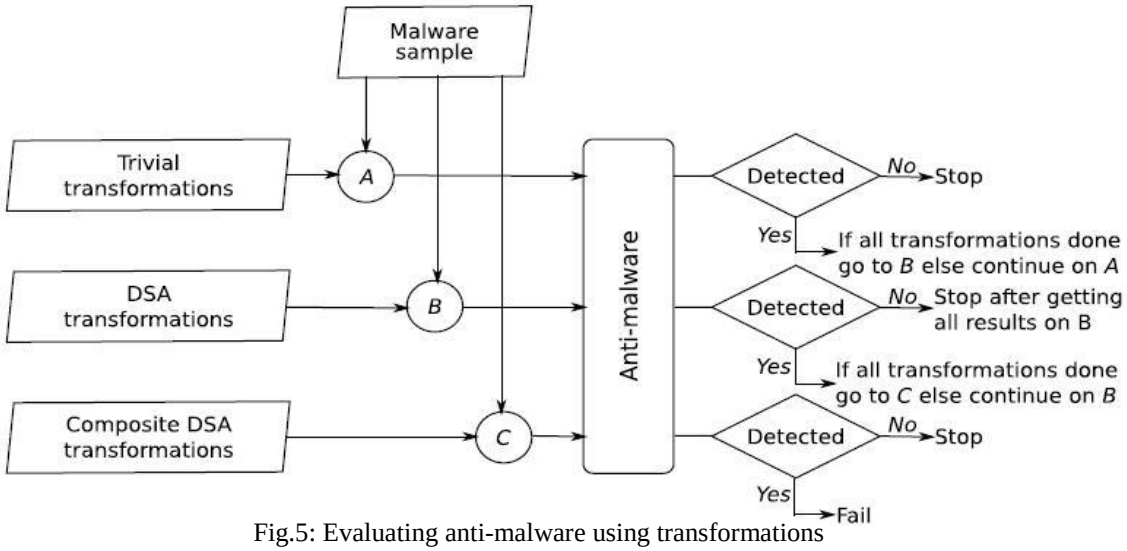

Fig.5: Evaluating anti-malware using transformations

- Trivial Transformations: It uses different transformation categories such as repacking signed jar files, disassembling and reassembling the bytecode, changing package name.
- Transformation Attacks Detectable by Static Analysis: As per the name the transformations done here are can be detected by static analysis. The techniques used here are identifier renaming of class or method, data encoding in dex file, call indirections, code reordering in methods of program and encrypting payloads.
- Transformation Attacks Non-Detectable by Static Analysis: The encryption techniques which are not recognizable by static analysis are used here. Most commonly reflection of API and bytecode encryption is done to make code unavailable for static analysis.

The proposed system first take malware sample, apply trivial transformation and test it in anti-malware software if not detected then stop otherwise apply DSA transformation and test it again. If it is not detected stop it. If it is detected then go for next transformation. In this way by applying various transformations, one stage will be there where malware is detected in every transformation.

Advantages-

1. There is no need to do the code level changes for applying transformations.

IV. CONCLUSION

In this paper, we have analyzed different anti- malwares that can be used for avoidance of different malware attacks. ADAM tool, obfuscation techniques can be used for privacy preserving but with fewer transformations Malware detectors that use obfuscation requires pattern matching techniques. A framework based on DroidChameleon uses even more transformations using which more accurate efficiency of anti-malware tools can be found.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to Dr. Deshmukh Pradeep K for their guidance and to Prof. Prakash. B. Dhainje for their supervision. We would like to express our appreciation to our parents and all the teachers and lecturers who help us to understand the importance of knowledge and show us the best way to gain it.

REFERENCES

[1] M. Zheng, P. Lee, and J. Lui, "*ADAM: An automatic and extensible platform to stress test Android anti-virus systems*," in Proc. DIMVA, Jul. 2012, pp. 1–20.

[2] .C. Collberg, C. Thomborson, and D. Low, "*A taxonomy of obfuscating transformations,"* Dept. Comput. Sci., Univ. Auckland, Auckland, New Zealand, Tech. Rep. 148, 1997.

[3] .M. Christodorescu, S. Jha, S. Seshia, D. Song, and R. Bryant, *"Semantics-aware malware detection,"* in Proc. IEEE Symp. Security Privacy, May 2005, pp. 32-46.

[4] C. Kolbitsch, P. Comparetti, C. Kruegel, E. Kirda, X. Zhou, and X. Wang, *"Effective and efficient malware detection at the end host,"* in Proc. 18th Conf. USENIX Security Symp., 2009,pp. 351–366..

[5] Y. Nadji, J. Giffin, and P. Traynor, *"Automated remote repair for mobile malware,"* in Proc. 27th Annu. Comput. Security Appl. Conf., 2011, pp. 413-422.

[6] M. Grace, Y. Zhou, Q. Zhang, S. Zou, and X. Jiang, *"RiskRanker: Scalable and accurate zero-day android malware detection,"* in Proc.10th Int. Conf. Mobile Syst., Appl., Services, 2012, pp. 281–294.

[7] V.Rastogi, Y.Chen, and W.Enck *,"AppsPlayground: Automatic security analysis of smartphone applications,"* in Proc. ACM CODASPY, Feb. 2013, pp. 209–220.

[8] Y. Zhou, Z. Wang, W. Zhou, and X. Jiang, *"Hey, you, get off of my market: Detecting malicious apps in official and alternative Android markets,"* in Proc. 19th Netw. Distrib. Syst. Security Symp., 2012, pp. 1–13.

[9] Vaibhav Rastogi, Yan Chen, and Xuxian Jiang, *"Catch Me If You Can: Evaluating Android Anti-Malware Against Transformation Attacks"*, IEEE transactions on information forensics and security, VOL. 9, NO. 1, Jan 2014

