ijecs
open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 1 Jan 2013 Page No. 226-228

Malware Attacks on Smart Phone, Its Limitation & Evolution to Detect New Techniques

Miss Nita B. Thakkar Miss Dhara N. Darji

Assistant Professor, DCS,Ganpat University.
nbt01@ganpatuniversity.ac.in dnd01@ganpatuniversity.ac.in

Abstract

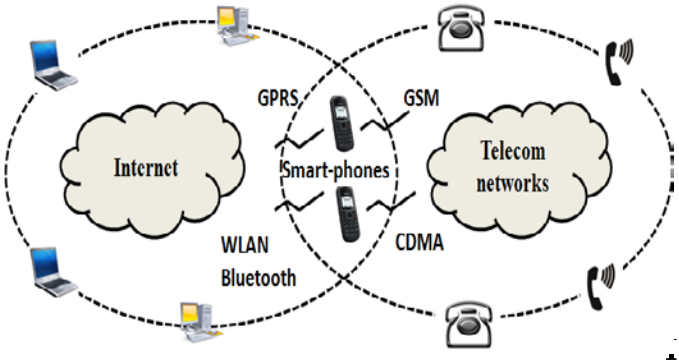
We are currently moving from the Internet society to a mobile society where more and more access to information is done by previously dumb phones. As a result, mobile security is no longer immanent, but imperative. In this paper it shows the various ordinary attacks on Smartphone & the drawback of the techniques at the it show one way to detect the various kind of attacks

Keywords:
Mobile Viruses, Mobile Worms, Cabir, ComWar, CardTrap, Proactive Security

I. INTRODUCTION

Problem with smartphone

"A Mobile device containing both cellular components and Internet access, with powerful computing components similar to those found on desktop PC's."[2]



II. CURRENT THREATS BY MALWARE

Causing financial loss to the user[3]

- Initiate unnecessary calls, send SMS or MMS[3 eg /Trojan
- Qdial/ANDROIDOS_DROIDSMS/ Comwar sybian worm) [4,8]
- Send private information (such as contacts or address book information) to a prede-fined phone

Spread via Bluetooth, causing drainage of battery. [3]
Cause the devices to work slowly or to crash. [3] (eg Cardtrap windows CE virus)[4]
Infect files (attach its code to the application sis files)[3]
Modify or replace icons or system applications. [3]
Wipe out information (such as address books) on the infected devices [3] (eg trojan)
Install bogus or false applications on the device [3]
Allow remote control of the device [3]
Remote control of the phone (eg any eavesdropping attack)

.II. VARIOUS DETECTION TECHNIQUES

Signature Based Detection:

This is the classic approach when a malware is identified and its characteristics are known. A signature may be generated and can thereafter be used to detect this special type. Classical AV software is signature based and works exactly this way on almost all computers. Next to the "classical signatures" for AV scanners, static function call analysis may provide clues about the intents of the corresponding program. This is typically done once at installation time for new programs. The used function calls. may be classified and, if necessary, appropriate actions can be taken. This has been tested for the Android and the Symbian platform.

A proactive way to detect malware before it even gets the chance to perform its malice intent is the way how Apple's App Store application vetting works. Each application that is uploaded by its developers is checked before it can be downloaded. [1]

Anomaly Detection:

In contrast to signature based detection approaches, anomaly detection techniques attempt to detect malware with unknown behavior.

Able to detect unknown malware based on its communication behavior through Bluetooth and SMS. It's providing a way to detect new types of attacks.

A completely different approach is evaluated, Since mobile devices have comparatively small batteries, malware should be detectable by the amount of battery power consumed by their conducted instructions. If the running applications, the user behavior, and the state of the battery is well known and precisely defined, additional hidden (malicious) activity can be detected. [1]

Root Kit Detection:

Malware with high privileges may attempt to hide itself at kernel level. The rootkit techniques do not differ from ordinary computers and, hence, their detection is to a certain extent identical—and therefore very hard. A first rootkit for Android has already been presented and evaluated rootkit detection on mobile devices[1]

Software based Attestation:

it is suited to detect malicious software that wants to hide its presence on mobile devices such as spyware.

In this technique it uses the idea light-weight cryptographic constructions with the property that it takes notably longer to compute a given function when the performing algorithm is given less usable RAM than for which it was configured.[1]

IV. LIMITATION OF CURRENT DETECTION TECHNIQUES

Signature Based Detection: [1]

The matching algorithm must be regularly active to scan all processes for suspicious code. This puts a heavy burden on the CPU and might even be noticeable by the user. Signature based approaches are doomed to fail given the large number of newly emerging threats.

In Proactive way, It is hard to detect malicious code hidden somewhere deep in the code path, some unwanted software slips through this mechanism from time to time.

Anomaly Detection:

It requires expensive computation to much more powerful processing capacity in the cloud then signature based approach. The privacy of user can be injured & some time provides the false results.

Root Kit Detection:

The rootkit techniques do not differ from ordinary computers and, hence, their detection is to a certain extent identical and therefore very hard. It is an open question how rootkits on smartphones can be detected effectively and efficiently.

V. A NEW APPROACH TO DETECTS MALWARE BASED ON THEIR BEHAVIORS

Unfortunately, current techniques(or tools) do not scale well and frequently fail to generalize the observed activity well enough to recognize related malware. [7]

A clustering technique that helps to identify samples that exhibit similar behavior.

In this approach to identify and group malware samples that contain similar behavior & for that Clustering technique will be applied.

Because of the growing need for automated techniques to examine malware, dynamic malware analysis tools.

These systems execute the malware sample in a controlled environment and mon itor its actions. Based on the execution traces, reports are generated that aim to support an analyst in reaching a conclusion about the type and severity of the threat imposed by a malware sample. However, while automating the analysis of the behavior of a single malware sample is a first step, it is not sufficient. The reason is that the analyst is now facing thousands of reports every day that need to be examined.

Thus, there is a need to prioritize these reports and guide an analyst in the selection of those samples that require most attention. One approach to process reports is to cluster them into sets of malware that exhibit similar behavior. The ability to automatically and effectively cluster analyzed malware samples into families with similar characteristics is beneficial for the following reasons: First, every time a new malware sample is found in the wild, an analyst can quickly determine whether it is a new malware instance or a variant of a well-known family. Moreover, given sets of malware samples that belong to different malware families, it becomes significantly easier to derive generalized signatures, implement removal procedures, and create new mitigation strategies that work for a whole class of programs. Grouping individual malware samples into malware families is not a new idea, and clustering and classification methods have already been proposed

VI. References

1. Research Paper on "Mobile Security Catching Up Revealing the Nuts and Bolts of the Security of Mobile Devices" Published By: Michael Becher, Felix C. Freiling, Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, Christopher Wolf, Published In: IEEE Symposium on Security and Privacy in 2011.

Available At:
http://www.ieeesecurity.org/TC/SP2011/PAPERS/2011/paper007.pdf

2. Research Paper on "Smart-Phone Attacks and Defenses" By Chuanxiong Guo, Helen J. Wang, Wenwu Zhu

Available At:
http://research.microsoft.com/en-us/umpeople/helenw/papers/smartphone.pdf

3. A Project Report on "Mobile Worms and Viruses" By: Amit Kumar Jain Submitted at : Indian Institute of Technology, Bombay in 2010

Available At:
http://www.sans.org/reading_room/whitepapers/incident/wireless-mobile-security_33548

4. A Paper on "Wireless Mobile Security" From SANS Institute InfoSec Reading Room

Available At:
http://www.it.iitb.ac.in/~jeevan/courses/sem1/Mobile_Viruses_and_Worms_Report_IT653.pdf

5. An Article on "Mobile device security – what's coming next?" From Sophos in 2011

Available At:
http://resources.idgenterprise.com/original/AST-0056070Accellion8CritialRequirements Mobile_Whitepaper.pdf

6. A Paper on "Smartphone Security Evaluation The Malware Attack Case" By: Alexios Mylonas, Stelios Dritsas, Bill Tsoumas, Dimitris Gritzalis in 2010

Available At:
http://www.aueb.gr/users/amylonas/docs/secryptShort.pdf

7. A Paper on "Paladin: Automated Detection and Containment of Rootkit Attacks" By: Arati Baliga1, Xiaoxin Chen2, and Liviu Iftode1 in 2010

Available At :
http://www.docstoc.com/docs/38779239/Paladin-Automated-Detection-and#

8. An Article on "A Brief History of Mobile Malware" From Trend Micro in 2010

AvailableAt:
http://countermeasures.trendmicro.eu/wp-content/uploads/2012/02/History-of-Mobile-Malware.pdf

9. A paper on "Scalable, Behavior-Based Malware Clustering" by Ulrich Bayer_,Paolo Milani Comparetti_,Clemens Hlauschek_,Christopher Kruegel§, and Engin Kirda in 2009

Available at :