“Malicious Applications in Android Devices”

Dr. Shivaji Mundhe
Director-MCA, SIMCA ,Pune
drshivaji.mundhe@gmail.com

Mr. Prashant Wadkar
Associate Professor ASM’s IBMR, Chinchwad, Pune (MCA)
pnwadkar@gmail.com

Abstract :

Android is a Linux-based operating system designed primarily for touch screen mobile devices such as smart phones and tablet computers This study throws the light that how user are utilizing the Android phone without knowing it’s impact on the privacy and security. Here user need to educate at many levels, e. g. at what extent their confidentiality is maintained in these Android smartphones and what type of security these Android smartphones failed to give. Andromaly is framework for detecting malware on Android mobile devices. Host-based Malware Detection System that continuously monitors various features and events obtained from the mobile device and then applies Machine Learning anomaly detectors to classify the collected data as normal (benign) or abnormal (malicious). Since no malicious applications are yet available for Android, we developed four malicious applications, and evaluated Andromaly’s ability to detect new malware based on samples of known malware. The Andromaly framework is effective in detecting malware on mobile devices in general and on Android in particular.

The paper also highlight the how to educate Android users from security aspects and provide more security and privacy for their Android Device and maintain the privacy. In this research we focused on the malware issues which are more necessary for the security and privacy of Android smartphones.

Keywords : **Android, Malware, PDA, Apps,**

1. **Introduction**

1.1 **Information and Communication technology (ICT)**

It is the integration of telecommunications (telephone lines and wireless signals), computers as well as necessary enterprise software, middleware, storage, and audio-visual systems, which enable users to access, store, transmit, and manipulate information.

Day by day the technological changes giving best services to the users. And hence number of users are increasing worldwide due to fastest and cheapest communication.

1.2 Mobile Communication

Now a days the mobile devices like Android are utilized by tremendous users worldwide for calling, SMS, MMS, Internet, creating Access Points, mobile banking, booking and many more. These communications include all types of advanced features which make 5G technology most dominant technology in near future.[13]

1.3 Android Communication

The Android operating system uses the Linux kernel at its core, and also provides an application framework that developers incorporate into their applications. In addition, Android provides a middleware layer including libraries that provide services such as data storage, screen display, multimedia, and web browsing. Because the middleware libraries are compiled to machine language, services execute quickly. Middleware libraries also implement device-specific functions, so applications and the application framework need not concern themselves with variations between various Android devices.

Android is a Linux-based operating system designed primarily for touch screen mobile devices such as smart phones and tablet computers. Google releases the Android code as open source. Android 4.2 includes a variety of new and enhanced platform technologies to support innovative communications use-cases across a broad range of hardware devices. Every Android release includes dozens of security enhancements to protect users. Application of the operating system has also moved beyond mobile phones and tablets; amongst others, television, smart books and cameras have been released running Android. The Android platform includes support for the Bluetooth network stack, which allows a device to wirelessly exchange data with other Bluetooth devices. The application framework provides access to the Bluetooth functionality through the Android Bluetooth APIs. Our goal is to extend and analyze, based on abstract interpretation, to perform formally correct analysis of Android programs. Android 4.0 introduces support for the Bluetooth Health Device Profile (HDP). This lets you create applications that use Bluetooth to communicate with health devices that support Bluetooth, such as heart-rate monitors, blood meters, thermometers, scales and so on. A role defined in HDP. A *source* is a health device such as an Android phone or tablet.

For Global communication with communication devices like mobile phones, tablets & PDA's, we find this sector is booming and every day is new day and to match with the times introduction of new application becomes mandatory. So with the advent of this new technology called 'Android'. It is felt that this technology should be explored and the need of the hour. It has more than 7,00000 apps today and more are releasing daily. It is used in the smart phones, tablets, ipad, watch, TV, MP3 etc. Android technology has been introduced very recently and people are talking about it. But do not know how to use it to a great extent.

2.Choice of the topic with Reason

The security in Android Phones. A compromised smartphone can inflict severe damages to both users and the cellular service provider. Malware on a smartphone can make the phone partially or fully unusable; cause unwanted billing; steal private information (possibly by Phishing and Social Engineering); or infect every name in a user's phonebook. This may cause socio-economical problem to Smartphone user.

3.Significance of Study :

The Significance is mainly important for the popularity of Android devices and its security aspects in the communication. Many of the smartphone users are unaware about the malware which are attacking their smartphones and stealing their confidential information and disclosing privacy like internet banking passwords, sms, mobile banking passwords, personal details etc. Recent study shows that 99.9% of new mobile malware targets Android.[11] So it is necessary to educate them from security aspects and provide more security and privacy for their financial transactions and maintain privacy.

4.Objective of this study:

To study and analyze the impact of malwares on Android smartphones and the role of Andromaly for malware detection.

The main objective is to do study of malwares in Android smartphones

1. The Anomaly detection in Android Smartphone.
2. To Study the Impact of Anomaly on various hardware features of Android Phones.
3. Study of Andromaly to solve the malware issues.

5.Study

The challenges for smartphone security are becoming very similar to those that personal computers encounter and common desktop security solutions are often being downsized to mobile devices. As a case in point, analyzed common desktop security solutions and evaluated their applicability to mobile devices. However, some of the desktop solutions (i.e.,antivirus software) are inadequate for use on smartphones as they consume too much CPU and memory and might result in rapid draining of the power source. In addition, most antivirus detection capabilities depend on the existence of an updated malware signature repository, therefore the antivirus users are not protected whenever an attacker spreads previously un-encountered malware. Since the response time of antivirus vendors may vary between several hours to several days to identify the new malware, generate a signature, and update their clients' signature database, hackers have a substantial window of opportunity. Some malware instances may target a specific and relatively small number of mobile devices. (e.g., for extracted confidential information or track owner's location)

The Andromaly describe a generic and modular framework for detecting malware on Android mobile devices. This is accomplished by continuously monitoring mobile devices to detect suspicious and abnormal activities using a supervised anomaly detection technique. The framework relies on a light-weight application, installed on the mobile device that samples various system metrics and analyzes them in order to make inferences about the well-being state of the device. The main assumption is that system metrics such as CPU consumption, number of sent packets through the Wi-Fi, number of running processes, battery level etc. can be employed for detection of previously un-encountered malware by examining similarities with patterns of system metrics induced by known malware.

Modern computer and communication infrastructures are highly susceptible to various types of attack. A common way of launching these attacks is by means of malicious software (malware) such as worms, viruses, and Trojan horses, which, when spread, can cause severe damage to private users, commercial companies and governments. The recent growth in high-speed Internet connections has led to an increase in the creation of new malware.

The anomalies which happen in the smart phone might be as below

1. Fraudulent use of the operator services (e.g. registration with a false identity and using the phone to high tariff destinations).
2. Location-based detection (a user active in two different locations at the same time); traffic anomaly detection (an area having normally low network activity, suddenly experiencing high network activity); and detecting anomalous behavior of individual mobile-phone users.
3. Trojan attempting to use the message server component without authorization to create an SMS message.

6. Benefits

Every Android user is benefiting with its use, that might be for communication, education or entertainment. It also satisfying customers of all the category. It is fulfilling need of mobile users. Recent release includes dozens of security enhancements to protect users. Applications of these mobile phones moved to tablets, television, smart books and cameras. If every Android user is free from malware attacks then their personal information, transactions, location etc will be more secure and will maintain the confidential information.

7. Drawbacks and Limitations

There is no as such limitation to this emerging Android technology. Because it has come up with a open source platform. Whatever limitations we found in future will get resolved or overcome in next versions. In spite of this there are some security aspects and drawbacks of malware attack on these Android Phones. The both might get resolved by the framework like Andromaly.

8. Concluding Remark:

This Review study throws the light that how user are utilizing the Android phone without knowing it's impact on the privacy and security. Here user need to educate at many levels, e. g. at what extent their confidentiality is maintained in these Android smartphones and what type of security these Android smartphones failed to give. The Android developers are developing different types of apps and uploading apps on google store. There is no any best authenticated/standard procedure which will avoid the possibility of downloading and installing the malicious apps on Android smartphones. Recent study shows that 99.9% of new mobile malware targets Android. Also the Email, SMS stealing virus targeting Android users in India. The app which is published on Google Playstore might content the malware also. So it is necessary to set and follow certain guide lines for these apps before download and installing from Google Playstore to smartphones, By this the chances of malicious apps on Android devices will get reduced.

References:

1. **Books**
   a) Android.Application.Development.for.For.Dummies by Donn Felker published by Wiley Publishing, Inc. ISBN: 978-0-470-77018-4.

b) Professional Android Application Development by Reto Meier published by Wiley Publishing, Inc. ISBN: 978-0-470-34471-2.

2. Journals, Articles and News.

[1] "Andromaly: a behavioral malware detection framework for android devices" by Asaf Shabtai · Uri Kanonov · Yuval Elovici · Chanan Glezer · Yael Weiss Published online: 6 January 2011 © Springer Science+Business Media, LLC 2011

[2] "A Systematic Review of Healthcare Applications for Smartphones" a research article by Abu Saleh Mohammad Mosa, Illhoi Yoo and Lincoln Sheets, Medical Informatics and Decision Making 2012.

[3] "Diversity in Smartphone Usage" authored by Hossein Falaki, Ratul Mahajan, Srikanth Kandula, Dimitrios Lymberopoulos, Ramesh Govindan,Deborah Estr in journal MobiSys'10, June 15–18, 2010, San Francisco, California, USA.

[4] Daily news paper "Pudhari"(Marathi) in Belgaum edition (Karnataka-INDIA) dated 3rd Sept 2013

[5] Design and Implementation of Mobile Forensic Tool for Android Smart Phone through Cloud Computing" authored by Yenting Lai1, Chunghuang Yang, Chihhung Lin, and TaeNam Ahn G. Lee, D. Howard, and D. Ślęzak (Eds.): ICHIT 2011, CCIS 206, pp. 196–203, 2011. © Springer-Verlag Berlin Heidelberg 2011

[6] Research article "5 Ways to Boost Your Android Phone's Performance" authored by Kenneth Butler, LAPTOP Web Producer/Writer in blog. Dt. Apr 9, 2012

[7] "The Potential Impact Of Android On The Mobile Application Development Industry" article by Phil Byrne" in the journal "articlebase"

[8] "U.K. Government Bans Drivers From Using Google Glass Behind The Wheel" by "Killian Bell" in "Cult of Android" a daily news website.

[9] "Email, SMS stealing virus targeting Android users in India" published in Daily news paper "Times of India" dated 8th Sept 2013(NEW DELHI)

[10] "How Samsung plans to tackle Android malware issues" published in Daily news paper "Times of India" dated 5th Sept 2013 (LONDON)

[11] "99.9% of new mobile malware targets Android: Kaspersky" published in Daily news paper "Times of India" dated 3th Sept 2013 (WELLINGTON)

[12] "UK Porn Ban: Prime Minister Declares War on Adult Content" published on web news "www.webpronews.com" dated 22nd July 2013 authored by Sarah Parrott

[13] 5G technology of mobile communication: A survey, Published in: Intelligent

Systems and Signal Processing (ISSP), 2013 International Conference by: Gohil, A. ; Charotar Univ. of Sci. & Technol., Changa, India ; Modi, H. ; Patel, S.K. dt 1-2 March

2013, ISBN: 978-1-4799-0316-0