

“Android Technology and It’s Challenges”

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

Prof. Prashant Wadkar
Associate Professor ASM’s IBMR Chinchwad, Pune
(MCA)
E-Mail: pnwadkar@gmail.com
Mobile: 9422419386

1. Introduction

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. The various challenges to this Android Technology is the study of this research.

2.1 Review of Literature :

In the research article **“Andromaly”: a behavioral malware detection framework for android devices** authored by **Asaf Shabtai · Uri Kanonov · Yuval Elovici · Chanan Glezer · Yael Weiss** in the journal “Springer” Highlighted the security aspects for Android smartphones. Since Android has been introduced, it has been (and still is) explored for its inherent security mechanisms, and several targeted security solutions were proposed to augment these mechanisms. From our assessment of Android’s we believe that additional security mechanisms should be applied to Android. Furthermore, similar to the PC platform, there is no “silver-bullet” when dealing with security. A security suite for mobile devices or smartphones (especially open-source) such as Android includes a collection of tools operating in collaboration. This includes: signature-based anti-virus, firewalling capabilities, better access-control mechanism and also a malware/intrusion detection platform.

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.

The Significance of this research paper 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.

The Objective of this study is to 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.

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 smartphone 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.

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.

2.2 Review of Literature :

In the research article “**A Systematic Review of Healthcare Applications for Smartphones**” authored by **Abu Saleh Mohammad Mosa1, Illhoi Yoo and Lincoln Sheets** in the Research Article/journal BMC Medical Informatics and Decision Making 2012 Highlighted the popularity of Android smartphones in the world market. This Android platform is becoming prominent in the U.S. as well as globally . Android U.S. market share increased from 9% to 38.1% within a 15-month period during 2010–2011, placing this platform in the top position. Android is predicted to be the global market leader in smartphones, acquiring nearly 50% market share by 2015. This platform supports all the features , but some features (storage-area encryption, video calling, and multi-core processor support) are available in selected smartphone devices only. The system bar provides a software navigation button in addition to system status and notifications. Of the six major OS platforms, only Android 4.0 has built-in support for connecting to Bluetooth Health Device Profile (HDP) devices. So here we conclude the popularity of Android smartphones as well as the potential for Android smartphones.

2.3 Review of Literature :

In the research article “**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** mentioned The data was collected using a custom logging tool that he developed and deployed on the smartphones. The logger runs in the background and records a highly detailed view of smartphone use, including the state of the smartphone screen, start and end of incoming and outgoing voice calls, the time the user spends interacting with each application, the network traffic sent and received per application, and the battery level. The Android OS provides mechanisms to access this information. The logger keeps data records in a local SQLite database on the phone and uploads them only when the phone is plugged to the charger, to minimize the impact on the phone battery. This logging utility can be made available to other researchers by request. Here we conclude that logging utility can be helpful to track and monitor activities of Android smarphone users.

2.4 Review of Literature :

In the Daily news paper “Pudhari”(Marathi) in Belgaum edition (Karnataka-INDIA) dated 3rd Sept 2013 the editor published news that two youngsters Dr. Amit Patil and Dr. Prakash Diwan developed a Android apps specially for women. In any trouble or difficulty, the women, can use to shake the handset. By this, the SMS and the location will be sent to five relatives or friends whose mobile numbers are registered. By this immediate help can be reached to women who is in trouble. It seems that many type of android apps can be developed by developers or company. These type of apps are facilitating, supporting, communicating, monitoring the users, and it is also playing role of social service. Also the developer earns lot of money if these are paid apps. This news highlights and motivates to write Android apps, and how it is contributing to social security services. The open source feature made this thing easier to developers.

2.5 Review of Literature :

In the research journal “**Design and Implementation of Mobile Forensic Tool for Android Smart Phone through Cloud Computing**” authored by **Yenting Lai1, Chunhuang Yang, Chihhung Lin, and TaeNam Ahn** in the journal “Springer-Verlag Berlin Heidelberg 2011” presented that- Most of commercial forensic software process the acquisition when mobile turns off making it fail acquiring volatile data in the memory. In this study, researcher processes acquisition when mobile turns on and successfully acquires volatile evidence in mobile, meanwhile, instantly uploads the data onto the cloud. Without excess instrument, it provides forensic examiners process acquisition anytime, anywhere as long as examiners are able to upload the data through the Internet and browser. Instantly viewing reporting reduces extra time of installation of third appellation or operation system, and provides a more efficient acquisition. In the future, the aim will be the combination of cloud computing platform and mobile forensic that only requires browser to process mobile forensic. Here we conclude that the Android phones and cloud computing together can be used for computer Forensic.

2.6 Review of Literature :

In the research article “**5 Ways to Boost Your Android Phone’s Performance**” authored by Kenneth Butler, LAPTOP Web Producer/Writer in his blog suggested the 5 ways to increase the performance of Android smartphones. He suggested

1. Kill Background Apps, for this he suggested a separate apps “Advanced Task Killer app” (free).
2. Keep Apps Up to Date by using “Android Market” for an update.
3. Turn Off Background Data like Facebook, Twitter or WeatherBug which constantly download data.
4. Manage Google Services -An Android device automatically includes access to Google services including Books, Contacts, Currents, Gmail and Google+. If you don't need these services, turn them off.
5. Defrag your Smartphone's Memory
Just like a PC, your Android phone's internal RAM gets a performance boost after undergoing defragmentation.

So the author suggested how the performance of Android can be increased by above simple steps.

Many of the android users are unaware of this, that how to increase the performance of android phones. This article guides to billions of android users.

2.7 Review of Literature :

In the research article “**The Potential Impact Of Android On The Mobile Application Development Industry**” authored **Phil Byrne** in the journal “articlebase” included that the The open source property of Android is Google's unique selling point. Google recognised that the mobile experience on the most part is inferior to the desktop experience due to the restrictions placed on mobile application developers. Apple, the manufacturers of the iPhone have been known to refuse to approve third party programs because they replace integrated features of the iPhone. Android is a completely open platform that will allow developers to create applications that call upon the use of any of a handset's core features. Android also aims to give developers the tools to innovate by allowing applications to combine information from a variety of sources such as the internet or other mobile device users. This article throws light on Impact Of Android On The Mobile Application Development Industry.

2.8 Review of Literature :

In the article “**U.K. Government Bans Drivers From Using Google Glass Behind The Wheel**” authored by “Killian Bell in “Cult of Android” a daily news website highlighted on the

Google glass where android come in to picture. He says one of the best things about Google Glass is the ability to view maps and get directions while you're driving without ever having to take your eyes off the road ahead. But that's not the case for those in the U.K., where using Google Glass behind the wheel is banned by the government. It is important that drivers give their full attention to the road when they are behind the wheel and do not behave in a way that stops them from observing what is happening on the road. Glass doesn't just give you directions; you can also use it to watch videos, see the latest news headlines, check Twitter, and lots more. Considering the severity; that is possibility of accidents due to failing to focus on road, U.K has banned for this Google Glass. Here we conclude that android technology is best for fulfilling users needs but user has to decide whether to use it or not.

2.8 Review of Literature :

In the news article "**Email, SMS stealing virus targeting Android users in India**" published in Daily news paper "**Times of India**" dated 8th Sept 2013(NEW DELHI) mentioned that the- A potentially damaging virus, which steals SMS and personal details of an Android-enabled gadget-user, has been detected in Indian cyberspace and internet security detectives have asked mobile phone and tablet users to exercise caution while operating. The malware is affecting all the versions of Android prior to version 4.2.2 (Jelly Bean). According to this article we conclude that the Android users has to take special precautions while using the Android smartphones.

2.9 Review of Literature :

In the news article "**How Samsung plans to tackle Android malware issues**" published in Daily news paper "**Times of India**" dated 5th Sept 2013 (LONDON) mentioned that-Samsung has reportedly joined hands with San-Francisco based Lookout's software to tackle the increased vulnerability of Android powered handsets to malware threats. As Samsung holds a major share in the smartphone market, it will receive improved protection to its Galaxy-branded Android devices apart from tablets. **Recently security analysts found a bug in the Google powered Android OS making it vulnerable to malware attacks and attributed it vulnerability to the system's popularity which is used in maximum share of smartphones.** Android manufacturer Google itself has taken steps to address the malware issue and banned apps from its Play store which were embedded with viruses and made changes to device without the owner's knowledge or consent. Samsung began offering its Knox product

to selected Galaxy S4 handsets in May and has promised it would be extended to other devices. According to this news by Samsung, Android users has hopes to get protection by this bug fixing.

2.10 Review of Literature :

In the news article “**99.9% of new mobile malware targets Android: Kaspersky**” published in Daily news paper “**Times of India**” dated 3th Sept 2013 (WELLINGTON) mentioned that Google's popular operating system Android is reportedly also the most prone to malware attacks as found by security firms who claim that the number of malware programmes attacking the OS have only risen this year. Security firm Kaspersky Lab's analyst Christian Funk said that 99.9% of all new phone malware targets Android and one year ago the firm recorded 30,000 versions of malware targeting mobiles. According to stuff.co.nz, the malware attacks Android due to its wide availability making it a big target as its market share has risen about 80% in recent times. Funk said that since the system is open, anyone can download the necessary documentation and write software which can be used as a mask for the viruses, targeting people looking for popular apps, thereby making them download apps with viruses hidden in them. Another IT security firm, Trend Micro has found that Australia was the prime target for malware attack designed to steal online banking information because the country is an 'early adopter' of technology. According to this statement by Kaspersky and Trend Micro we conclude that hackers are targeting the Android users. So it is necessary to have Android technological changes which will give protected and safe service to Android users.

2.10 Review of Literature :

In the news article “**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** wrote that Mr .David Cameron, the Prime Minister of the UK, has announced today that he plans to crack down on internet pornography and focus on making the internet a safer place for children and families. Regulations include “family-friendly filters” that would automatically block pornography and other adult material in millions of people’s homes, filtering material from all land lines, WiFi connected devices, and even in public areas where children are likely to be present.

3.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. Also the drawback is that the many android apps are facilitating for pornography. And this has adverse effects on children and families children and tend to increase in crimes and rape.

4.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. Here we also conclude that the Android phones and cloud computing together can be used for computer Forensic. Here we also would like to focus the significant role played by Android in Health Device Profile (HDP). These are various challenges to this Android Technology and many more challenges we, the user and developer has to face.

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, Ilhoi 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. Ślezak (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) [11]

[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

[14] **“Analytical study of Android Technology”** by Dr. Shivaji Mundhe, Mr. Prashant Wadkar, ISBN:- 978-93-5158-007-3, Vol 2, Jan 2014, ASM Group of Institutes, Pune, India.

[15] **“Malicious Applications in Android Devices”** by Dr. Shivaji Mundhe, Mr. Prashant Wadkar, ISBN: 978-81-927230-0-6, SIMCA, Feb 2014, Pune, India.

[16] **“Filtering of Pornographic Images Using Skin Detection Technique”** by Dr. Shivaji Mundhe, Mr. Prashant Wadkar, Prof Shashidhar Sugur eISSN:- -2320-0065, Jan 2015, ASM Group of Institutes, Pune, India.