JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Mobile Malware Evolution, Detection and Defence

Mithilesh M Nimbalkar

Guide: Asst.prof.Prajakta Chowk

Keraleeya Samajam's Model College,Khambalpada Road,Thakurli,Dombivli (East),Maharastra

Abstract

The use of smartphones has increased exponentially and we have online information,payments, gaming, useful applications, etc. We rely on smartphones for functions such as these tasks have only been performed by computers once. The above functions in addition to storing contact information, correspondence and other personal and business information in the address book. We live in a new era where many devices are exchanging data with each other and new security concerns are emerging. The massive increase in smartphone usage has made it a target for malicious attackers to spread malware and carry out other malicious attacks. This research article provides an overview of mobile malware in its infancy, attack vectors, detection methods, and protection mechanisms. This case study highlights the unique nature of mobile malware compared to computer security and research implications for malware mitigation. Also, given the popularity of some mobile phones among users, this article will focus on the security mechanisms used to prevent attacks on iPhone and Android devices.

Keywords

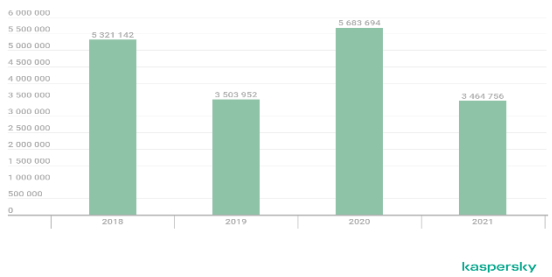
Smartphones, Mobile, Malware, Android, iPhone, Threats, SMS, MMS, Antivirus (AV), IMEI

1.Introduction

Smartphone adoption is growing rapidly, directly linked to advances in computing power and other factors.According to Garter, mobile phone sales increased by 5.6% in the third quarter of 2011, while mobile phone sales increased by 42%. Interestingly, the Android operating system accounts for more than 50% of smartphone sales. Nowadays mobile phones primarily have three functions: communication, calculation and measurement.McAfee's 2011 Q3 Threat Report also adds to this view, stating that 2011 was the busiest year for malware in the operating history. As smartphone sales have increased worldwide, it has paved the way for the spread of mobile malware. Mobile malware can perform malicious tasks such as stealing data, sending credentials to attackers, sending malicious messages, and more. Section 4.2.3 provides a detailed description of the mobile threat model.Services such as mobile payments and transfers used as mobile banking services can be useful for

malware writing, and attacks on these servic es cause serious damage. The total number o f malware is increasing every quarter. Conce rn that the amount of Android malware is rap idly increasing.Mobile
malware has continued to evolve over the pa st decade, and various
types of malware have been released, such as worms, Trojans, other viruses, and spyware that target mobile phone numbers.Damopoul os et al. created an airborne malware called i SAM that spreads wirelessly and delivers its elf to iPhone
devices. The purpose of this malware is to ex pose potential vulnerabilities in modern mob ile devices and processes. In addition to supp orting the six malware strategies shown belo w, iSAM malware also connects to the iSAM bot host and alters programming logic or ex ecutes commands for synchronized attacks. i SAM architecture
includes the following malware technologies :
a) Propagation: spreads wirelessly to other iPhone devices
b) Botnet updates: updates and checks for new versions of malware

> c) Data storage: secret confidential information
d) leak: secretly sending a large number of texts e) Availability: denial of application service on iPhone
f) Availability: deny Internet Service for iPh one.Advanced malware like iSAM demonstr ates the challenges of designing to secure mo bile devices and the evolving need for malwa re detection and protection systems. Similarl y, Android devices are also the target of mali cious attacks.Recently, in January 2012, Sym ante discovered Android.Counterclank, a da ta
stealing Trojan targeting Android devices. Thi s Trojan is included in many applications in t he official Android Market. Download data f or all malicious apps shows that Android.Co unterclank has the highest distribution rate of all malware detected so far this year. A class ic example of authentication malware.Zitmo is a heterogeneous Trojan that infects Symbi an, BlackBerry, Windows Mobile and Andro id devices. The huge popularity of Android, f ree availability of data on the Android platfo rm and poor scanning process in the Android market are the reasons for the increase in ma lware attacks. The report predicts an increase in malware placed on app stores, particularl y the Android Market. The report also envisi ons cell phone surveillance, including stealin g cell phone data and tracking people throug h geolocation services.



2.Related Works

Mobile malware attacks continue to evolve, and more and more researchers are studying malw are attacks specifically aimed at mobile device s. In 2005, Shevchenko presented the evolutio n of mobile malware, which is considered the f irst work. In 2011, It has been

in development since 2005 and explains the details of security operations.The

mainly focus on software centric attacks. In 2011, It detected 46 iOS, Android and Symbian malware circulating between 2009 and 2011.provided a systematic and comprehensive survey of device security solutions.However, in our Extended Summary we did not mention for the first time the survey by La Polla et al. whose research we later included in this article. Defense technology technical discussion.

3.Initial Definition

Defines a mobile phone as a device that can make or receive calls using a smart card controlled by a mobile phone user. Smartphones are mobile devices designed to use a more mobile computer that has functionality and can install third party applications. Initially, Windows Mobile, Blackberry OS and Symbian operating systems were popular, but now iOS and Linux based Android operating systems have rapidly gained popularity and commercial value. These two operating systems are expected to dominate the smartphone space for a while. Smartphones allow users to install software apps from sources other than the user's mobile phone; this requires some control to minimize attacks.In this article, smartphones are sometimes r

Windows Mobile to the latest Android operating system. Various types of malware including file viruses (Virus.WinCE.Duts), backdoors (Backdoor.WinCE.Brador) and Trojans have begun t

attack mobile phones. Malware is often delivered via Bluetooth, Multimedia Messaging Service (MMS) and Short Message Service (SMS) s

above research focuses on different types of security, but in this article

eferred as simply mobile devices or cell phones. Do not run programs, modify files,etc. These are also Trojans, bots, viruses, backdoors, worms, rootkits, etc. It is classified as.

4.Discussion

First, we will briefly introduce the history of mobile malware in Section 4.1, then discuss the aspects of mobile security compared to computer security in Section 4.2, and then analyze various Attack vectors and attack models. Specifically, we will look at various findings related to mobile devices in Section 4.3. In Section 4.4, we will examine methods to block mobile malware. Finally, in Section 5, we estimate regional trends of mobile malware and draw conclusions.

4.1.History of Mobile Malware

The first malware targeting smartphones appeared in 2004. Overview of software history. The first virus was called "Caribe" or Cabir and was written for the Symbian operating system. Cabir spreads via Bluetooth and takes advantage of the limited resources of mobile devices. It shortens the battery life of the device by constantly scanningBluetooth enabled devices. Malware is then written into other operating syste

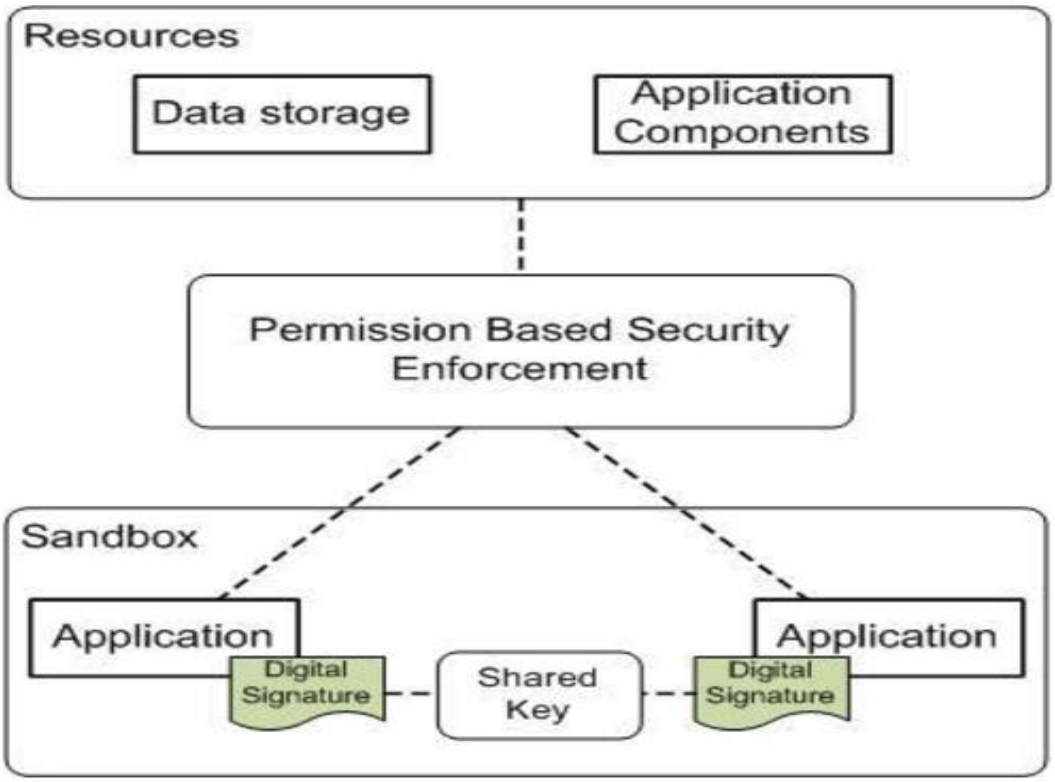
ervices.
When the article was published it was predicted that the amount of malware would increase and therefore we are currently facing this trend. In 2004, describes the damage caused by infected smartphones and prevention solutions. The article reports specific attacks on mobile devices, including privacy breaches, identity theft, emergency p

hone DDoS, and domestic violence. This docu ment is the first to propose anti-traffic solutions such as hardening methods, In ternet protection, and intercoms.

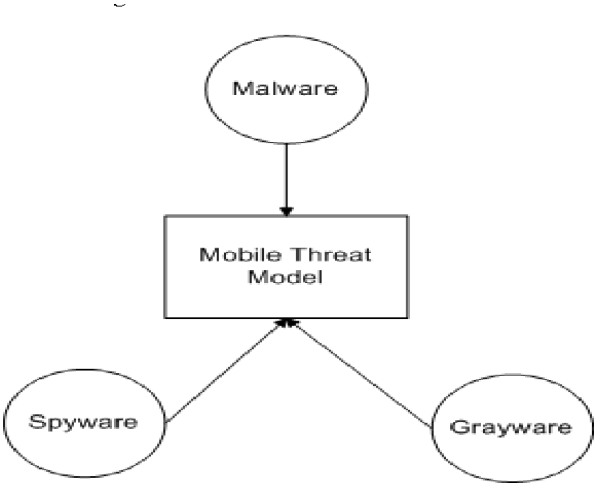
4.2.Mobile Specific Security

Desktop computers and mobile devices run sim ilar hardware and software. Therefore, comput er and smartphone security share many charact eristics; However, there are some features spec ific to mobile devices.In 2011, describes certai n features of the security function. Figure 3 sh ows the details of the security process.

Fig 3 Mobile Specific Security



4.3.Attacker centric Mobile Threat Model



Mobile Threat Model

Malware: As discussed earlier, malware gain unauthorized access to the device either by Driveby download techniques like luring users to install an application or exploiting vulnerabilities in the system like flaws in SMS parser. Personal Spyware: Personal spyware collects personal information like location, contacts, call history etc. of a user. The attack is carried by gaining physical access to the device and installing the spyware. This attack is more targeted and the data collected is of interest to the person who installed it. Unlike malware, spyware does not send the data to the application developer.Grayware: Grayware are applications that collect data to be used for marketing and user profiling. The intention behind grayware might not be to harm users. However, sometimes they may behave in a manner that is annoying or undesirable to users.

4.4.Detection

In this section, we analyze various mobile mal ware detection methods listed in various docu ments.The technology that works on mobile p hones is called proprietary technology. Howev er, to improve performance, heavy calculations are offloaded to separate servers; In 2009,com pared the detection methods of images and mo bile devices to highlight the power constraints inherent in the mobile environment and propos ed a robust malware detection method. Attitud e analysis and honesty testing are some of the research methods used. Scanning is a process t hat examines specific lines of bytes based on malware types and reports vulnerabilities befor e they are executed on the computer.Unlike sc anning, Behavior Checking does not look for malware signatures in every file, but monitors the application for malicious behavio r and detects it. Integrity check checks the file size, t imestamp, checksum, etc. of all files on the co mputer. Creates a diary with details. Although these methods are widely used in malware dete ction, each method has its own advantages and disadvantages.Because resources are limited in the mobile environme nt, the discovery process must be robust.propo sed a solution that works with the coordination of mobile devices and dual control servers. Si milar technology is also used by the desktop v ersion. As a result, they provide limited detecti on with significant resources and have proven to be ineffective. On the other hand, cloud-based detection enables resource-intensive threat detection.

4.5.Application Permission Analysis

Applications run in a sandbox environment but they need permission to access certain data. During installation, the Android platform requires the user to allow or deny permission t o the application, depending on the functions t he application can perform. Section 4.4.2 expl ains permission-based security on Android devices in more det ail. In 2009, proposed the Kirin security servic e to allow sensitive applications for the Androi d platform. The purpose of this is to overcome the limitation on the Android platform where d evelopers can deliberately hide device licenses . If there is no list, there are no restrictions as it has predetermined leave rights. Kirin security services are related to Android app installer an d also Kirin security policy. The code represen ts the default model and is compared with the configuration of installed applications. Research shows five steps to identify risk: (1) Check assets at hand,(2) Work need is not a monster, (3) Analyze securi ty objectives and threats (4) Clarify security requirements (5) D etermine security constraints.

4.6.Cloud Based Detection

As mentioned earlier, mobile devices are less a vailable and there are good detection methods on mobile devices that take a capital overhead. To overcome this problem, cloudbased approa ch will be a good solution. In this case, the use r's light application monitors the device's syste m calls and sends them to the server in the clo ud to detect malicious behavior. Therefore, off loading powerful computing to the cloud will help find the best of heterogeneous devices. O berheide et al.demonstrated the advantages of using bandwidth resources and reducing equip ment. In the proposed architecture, the host's a gent runs on the mobile phone and transfers da ta to the server. All data access is captured and the data is checked for availability or update i n the local cache. If the form changes or a new form appears, it will be sent to the server. The second component is the server used to analyz e the data. Servers may have more than one an tivirus system; This is something that mobile p hones cannot do. The inspection may use static inspection, dynamic inspection, or both. Thes erver may contain an emulatorthat replays logi n information to detect malicious.Centralized s ervers can maintain blacklists of malware and check new files for similar patterns.The advantages of having cloud based detection system are:

a) Efficient detection system through dedicated specialized servers

b) Less usage of device resources

c) Less software complexity at the device

4.7.Controlling Malware in ios:

Publish a list of attacks and defenseson iOS a nd Android devices. One way to control the s pread of malware is to provide a public doma in
and perform an approval process before hosti ng the application. All apps must comply wit h Apple's requirements before being made av ailable on the App Store.Apple
verifies applications by signing their code usi ng an encryption key. Accessing apps from t he App Store is the only way to install apps o n iPhone devices. This ensures that only apps that are Apple
approved and compliant with Apple's Terms of Use can be installed on the iPhone. The bu siness center can also help uninstall applicati ons if suspicious behavior is detected behind the hosting process. Apple may also
remove apps from your device.Second, all ap plications run in a sandbox environment with limited operating rights. Al

applications will run on a non-privileged other than root. iOS also distinguishes betwe en numbers and files. This minimizes attacks where a particular process becomes active a nd is then killed. Finally, iOS only installs so ftware from Apple's authorized services. But software mods are designed to bypass basic permissions and overcome all restrictions. T his process is called jailbreaking
and is explained below. br> Available for use . The main purpose of jailbreaking is to bypa ss the mobile operator's SIM card lock and u nlock the device.Malware writers use these t o control phones.Phone owners use them to c ustomize their phones the way they want. Un like PCs, mobile devices (especially iOS) are designed for messaging and jailbreaking. An y flaw could facilitate an attack.reported thre ats from smartphone rootkits. A rootkit is a t ype of malware that resides in a system or se rvice that has access to a system. Rootkits ha ve been a problem for PCs for a long time, a

nd due to the features and functions of smart phones, rootkits also pose a serious threat to smartphones. This article analyzes three root kit examples to show that smartphones are as vulnerable to rootkit attacks as desktop oper ating systems. But smartphones' special effec ts, such as voice, GPS, and messaging, provi de malware authors with new attacks that ca n cause serious harm to the security and priv acy of the end. In the first example, a remote attacker used arootkit atta ck to eavesdrop on GSM conversations. In th e second example,causes the smartphone to send messages containing the current locat ion, compromising the user's privacy. The thi rd example takes advantage of the high energ y services provided by GPS and Bluetooth accessories.

4.8.Controlling Malware in Android

Android has been a huge success since its lau nch. Popularity comes with the price of bein g a target for malware app developers.The pr ocess for determining how to exploit undocu mented features of Android to create initial malware for the Android platform.By creatin g a native Linux application, they bypassed the Android authorization system.

Android security features include:
a) Sandbox
b) Allow
c) Malware removal

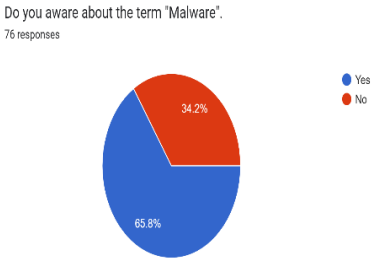
Android system architecture includes customized embedded Linux system. The platform interacts with the phone's hardware. Middleware and application APIs r un on top of this Linux environment.All appl ications use APIs to interact with the phone. These applications were developed using Jav a and executed on the Dalvik virtual machine running under the UNIX specification .This sandbox prevents apps from accessing data fr om other parts of the phone by placing a virt ual wall between apps. However, unlike App le, Android apps can be self signed. Android uses crowdsourcing to evalu ate user applications. As users complain, app s can be removed from the market and remov ed from devices. This differs from Apple's si gnature mechanism.The reason behind Goog le's self-signing mechanism Speeds up the process of getting apps created by commercial developerSecondly, the Andr oid platform provides authorization as a secu rity function [22] to protect the device's reso urces and data.Access to resources and infor mation is controlled during configuration. The permissions requir ed to access the application's resources are sp ecified in the manifest file. During app instal lation users receive or deny permission,thus transfe rring control of permissions to users.developer accounts were removed. By removing the app remotely,Google cleans the app from viruses and releases security updat es to protect the device from such attacks. As recently as February 2012, Google [24] rele ased a service codenamed “Bouncer” that sca ns the Android Market and developer accoun ts for applications.After adding an app the service will immediately scan for known malware. The Bouncer service analyzes an a

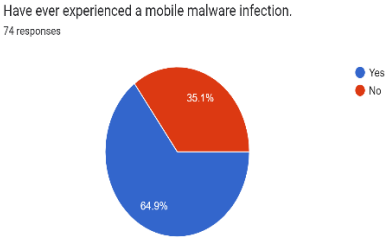
pplication's behavior and compares it to kno wn malware. Analysis
is performed by running the application in a simulated
Android configuration on Google Cloud Infr astructure. Violation
Developers suspended. According to Google, the Android market has seen a 40% decrease in potential malicious downloads.

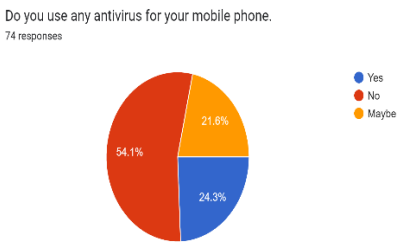
4.9.Preventive measures:

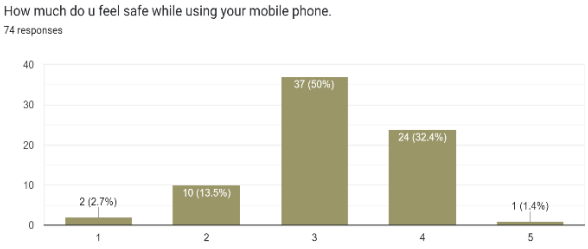
To control and mitigate malware, complete an d comprehensive protection needs to be impl emented at all levels and for all parties invol ved. Via Secure Coding and follow the Priva cy Policy. Unnecessary information should n ot be entered.For example, manufacturers ma y use unique identifiers instead of using the I EI number. Encrypt all sensitive data stored l ocally or sent to a server. For example,use a salted hash to encrypt the IMEI number.Anal ysis, reporting, etc. used in practice. There sh ould be a review for third party.App stores sh ould include a proper review process to elimi nate questionable questions.Have a good sec urity policy and proble
solving plan.Adopt a zero tolerance policy. D ownload mobile applications from reliable m arketplaces. Before installing an app, check i ts reviews, ratings, etc. should be researched by reading. Turn off additional services such as WiFi and Bluetooth when not in use. User s should not hesitate to “jailbreak” their syste ms as they are more vulnerable to attack patt erns.d) Device level: Mobile operating syste ms must be protected at the device level. Sec urity policies such as limited permissions an d exclusions will limit breached applications. Improve operation using technologies such a s address space layout randomizan,cluster protection, and the ability to complete writes t o memory.
In addition to implementing strong defenses, all stakeholders need to develop appropriate response strategies.He demonstrated how sm artphones can be used as a denial of service a ttack against critical public services (e.g., 91 1).

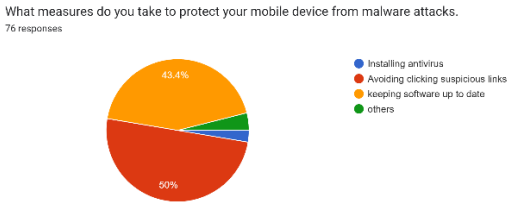
5.Survey

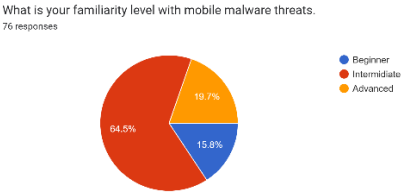


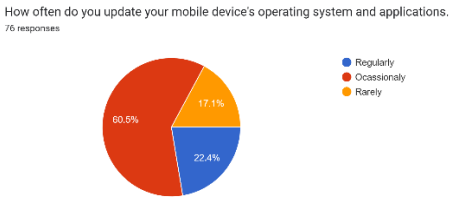


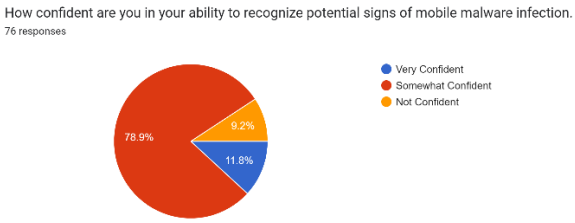


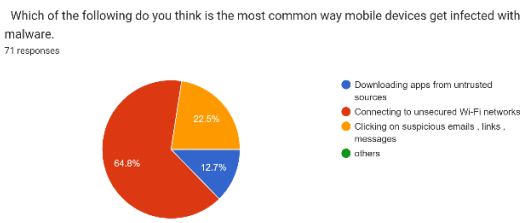


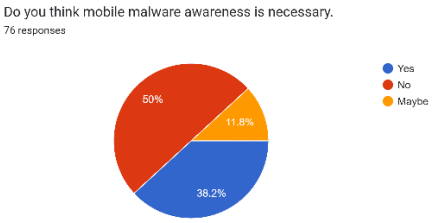












6.Conclusion

The use of smartphones has increased rapidly and devices have become increasingly complex. Their growing popularity makes them perfect targets for attackers. Smartphones are increasingly equipped with complex hardware and software, which paves the way for malware attacks.Since 2004, smartphones have been the target of malware attacks and their numbers are increasing rapidly. This survey primarily describes the evolution of mobile malware and provides examples of malware that can be used on various platforms. We also provide an overview of mobile threat models and attack vectors. Second, we describe various findings from different researchers. Finally, we focus on security systems designed to mitigate malware attacks on mobile devices. Althou

gh the mobile malware category bears some similarities to computer malware, mobile devices have unique characteristics that can make them targets for attackers. Malware attacks, data theft, privacy, denial of service, etc. may cause harm to users.Given the serious impact that malware can cause, it is necessary to have a strategy to deal with mobile malware. This article examines the nature of threats to users and organizations.Like mobile malware, mitigation technology continues to evolve to control attacks. In this article, we will talk aboutprocess based detection and process-based protection. We present various findings such as static analysis, phenomenon or behavior analysis, cloud usage and more. The inspection tool detected cover signatures and system failures. To manage malware and develop interventions, it is necessary to understand the security systems currently available on various platforms (Android, iPhone, etc.). Examining data
centric security systems. Finally, this article lists some mobile malware predictions for 2012.The importance of protecting your phone from mobile malware. We are interested in various studies proposed by many researchers and propose to create a synthesis that includes the best results of all the methods discussed in this article. Intrusion detection systems should have separate signature-
based antivirus systems on mobile devices and servers in the cloud to perform various research such as behavior, data mining techniques, etc. In addition to checking the system, efforts should also be made to improve the protection system, such as strengthening and reviewing the functioning of business practices.The truth is that mobile malware is ubiquitous and will continue to be so.

References:

[1] Gartner Press Release, Egham, UK, November 15, 2011 http://www.gartner.com/it/page.jsp?id=1848514

[2] McAfee Labs Q3 2011 Threats Report Press Release, 2011 http://www.mcafee.com/us/about/news/2011/q4/20111121 -01.aspx

[3] McAfee Labls Q3 2011 Threats Report, US, 2011 http://www.mcafee.com/au/resources/reports/rp-quarterlythreat-q3-2011.pdf

[4] Damopoulos, D., Kambourakis, G., and Gritzalis, S. 2011. iSAM: An iPhone Stealth Airborne Malware. In Future Challenges in Security and Privacy for Academia and Industry, J. Camenisch, S. Fischer-H• ubner, Y. Murayama, A. Portmann, and C. Rieder, Eds. IFIP Advances in Information and Communication Technology, vol. 354. Springer Boston, Chapter 2, 17-28

[5] Android.Counterclank Found in Official Android Market http://www.symantec.com/connect/fr/blogs/androidcounter clank-found-official-android-market , 2012

[6] A. Shevchenko, “An Overview of Mobile Device Security” Sep. 2005,

[7] Becher, M.; Freiling, F.C.; Hoffmann, J.; Holz, T.; Uellenbeck, S.; Wolf, C.; , “Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices,” Security and Privacy (SP), 2011 IEEE Symposium on , vol., no., pp.96-111, 22-25 May 2011

[8] Adrienne Porter Felt , Matthew Finifter , Erika Chin , Steve Hanna , David Wagner, “A survey of mobile malware in the wild”, Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, October 17-17, 2011, Chicago, Illinois, USA

[9] La Polla, M.; Martinelli, F.; Sgandurra, D.; "A Survey on Security for Mobile Devices" Communications Surveys & Tutorials, IEEE Volume: PP , Issue: 99, 2012 , Page(s): 1 - 26

[10] Jazilah Jamaluddin, Nikoletta Zotou, Reuben Edwards. Member, IEEE, and Paul Coulton, Member, IEEE; "Mobile Phone Vulnerabilities: A New Generation of Malware" 10 January 2005

[11] Chandramohan, M.; Tan, H.;"Detection of Mobile Malware in the Wild", Volume: PP , Issue: 99, IEEE Early Access, 2012

[12] Jong-seok Lee; Tae-Hyung Kim; Jong Kim; "Energyefficient Run-time Detection of Malware-infected Executables and Dynamic Libraries on Mobile Devices", Future Dependable Distributed Systems, 2009

[13] Egele, M., Kruegel, C., Kirda, E., Vigna, G.: PiOS: Detecting Privacy Leaks in iOS Applications. In: Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS), Feb 2011

[14] Enck, W., Octeau, D., McDaniel, P., Chaudhuri, S.: A Study of Android Application Security. In: Proceedings of the 20th USENIX Security Symposium. August 2011

[15] Batyuk, L.; Herpich, M.; Camtepe, S.A.; Raddatz, K.; Schmidt, A.; Albayrak, S.; "Using Static Analysis for Automatic Assessment and Mitigation of Unwanted and Malicious ActivitiesWithin Android Applications" Malicious and Unwanted Software (MALWARE), 2011 6th International Conference, 2011

[16] Isohara, T.; Takemori, K.; Kubota, A.; "Kernel-based Behavior Analysis for Android Malware Detection", Computational Intelligence and Security (CIS), 2011 Seventh International Conference, 2011 , Page(s): 1011 - 1015

[17] Yang, Liu; Ganapathy, Vinod; Iftode, Liviu; "Enhancing Mobile Malware Detection with Social Collaboration" Privacy, Security, Risk and Trust (PASSAT), 2011 IEEE Third International Conference, 2011

[18] Hsiu-Sen Chiang; Woei-Jiunn Tsaur; "Identifying Smartphone Malware Using Data Mining Technology", Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference, 2011

[19] Shabtai, Asaf; "Malware Detection on Mobile Devices", Mobile Data Management (MDM), 2010 Eleventh International Conference, 2010

[20] Miller, C.; "Mobile Attacks and Defense" Security & Privacy, IEEE, 2011

[21] Rich Cannings, Android Security Lead, “An Update on Android Market Security” Google Mobile blog, 2011 @ http://googlemobile.blogspot.ca/2011/03/update-onandroid-market-security.html [24] Hiroshi Lockheimer, VP of Engineering, Android, “Android and Security” Google Mobile blog, 2011 @ http://googlemobile.blogspot.ca/2012/02/android-andsecurity.html

[22] Zyba, G.; Voelker, G.M.; Liljenstam, M.; Mehes, A.; Johansson, P.; "Defending Mobile Phones from Proximity Malware" INFOCOM 2009, IEEE , 2009

[23] Yong Li; Pan Hui; Depeng Jin; Li Su; Lieguang Zeng; "An Optimal Distributed Malware Defense System for Mobile Networks with Heterogeneous Devices"; Mesh and Ad Hoc Communications and Networks (SECON), 2011 8th Annual IEEE Communications Society Conference, 2011

[24] Liang Cai , Sridhar Machiraju , Hao Chen, Defending against sensor-sniffing attacks on mobile phones, Proceedings of the 1st ACM workshop on Networking, systems, and applications for mobile handhelds, August 17-17, 2009, Barcelona, Spain

[25] Axelle Apvrille, Senior antivirus analyst and researcher, “Zitmo hits Android”, July, 2011

[26] William Enck , Machigar Ongtang , Patrick McDaniel, "On lightweight mobile phone application certification", Proceedings of the 16th ACM conference on Computer and communications security, November 09-13, 2009, Chicago, Illinois, USA

[27] Jon Oberheide , Kaushik Veeraraghavan , Evan Cooke , Jason Flinn , Farnam Jahanian, Virtualized in-cloud security services for mobile devices, Proceedings of the First Workshop on Virtualization in Mobile Computing, June 17-17, 2008, Breckenridge, Colorado.