Smart Devices Threats, Vulnerabilities and Malware Detection Approaches: A Survey

BalaGanesh D, Amlan Chakrabarti, and Divya Midhunchakkaravarthy

***Abstract*—In recent times, malware detection mechanism systems of mobile smart devices are getting growing concentration from researchers. With the quick expansion of malwares found in mobile devices, preventing the secrecy of mobile users is incredibly imperative and necessary. Intrusion detection systems are programming devices that consequently assemble information, dissect it and recognize such occurrences. These systems advanced to intrusion aversion systems (IPS) including extra counteractive action capacities. The accuracy plays an important role in the Intrusion Detection Systems and the methods efficiency is measured based on this metric evaluation.**

***Index Terms*—Botnets; Bluetooth; Attacker; Malware; Vulnerabilities.**

I. Introduction

Android is the commonly infected Open source OS contrasted with the various mobile device operating systems [1]. For example, SlideME is one of the exterior business sector, an informal market that is selling the clients many applications [2]. The users can download and install these applications from exterior market from these Android markets. Besides, all these application contents are not even controlled by these official Android markets also. Mobile devices provide the achievable exercises such as games, videos and social get-togethers at anyplace and whatever time with the devices. Likewise, different malicious applications are created by malware authors with the chances to attack the rising number of users [3]. Symantec reported that, in 2012, Mobile platforms was regularly attacked and targeted device platform, In 2013, Malware attacked climbed 58% high compared to that of 2011 [4]. In regards to the developing ransomware, that is to affect the whole Android OS in September 2013 was distributed by Symantec.

DroidDream Malware affected up to the 50 applications Android market was found in 2011 and containment was consequently done [5]. Researchers working on mobile malwares with the Google Play detected in April, 2013, that there are 35 types of applications infecting in 10 months. Around 2 and 9 million times, the infected applications are downloaded and it is revealed by Google [6]. F-Secure exhibited the report that in 2010 scarcely 11.25%, in 2011 up from 66.7% and in 2012 79% of malwares are represented [7]. In 2013, Trend Micro anticipated that the multiply of 185% malware Android applications was found propagating. Among such malicious applications, adware and the data theft are the most abundant malware application [8].

Likewise, in the form of ransomware, the Android and the mobile malwares are stealing and accessing the user's information. The mobile bots are importantly working on these samples and they are network-controlled bots [9]. The most utilized and infecting attacks are bots and malwares. In rest of the paper various threat types are discussed in section 2. Section 3 gives the different mobile threats models and section 4 provides the preventive measures. The various vulnerabilities found in the devices are explained in section 5 and section 6 briefed the different existing malware detection techniques. Finally, section 6 is conclusion.

II. Various Threat Types

The different types of threats faced by the Smart devices currently are listed in the figure below.

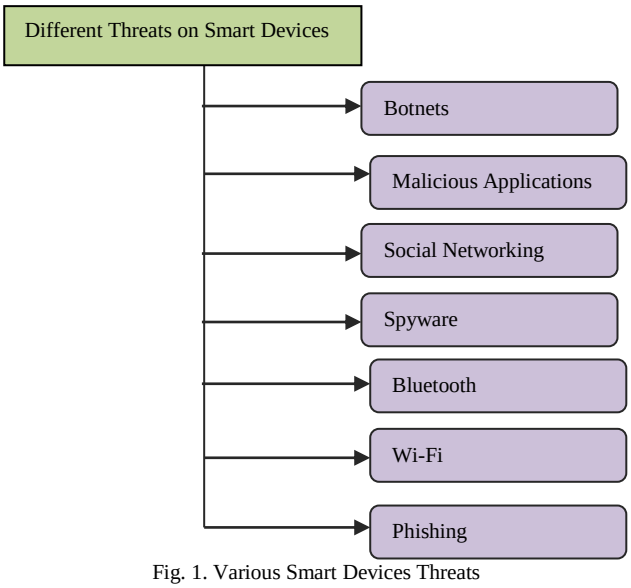

Fig. 1. Various Smart Devices Threats

A. Botnets

Through mail attachments or internet websites, the attackers frame the botnet attacks. Then they contaminate the different vulnerable devices with the malicious attacks. Zombie systems are provided to the malware authors to perform the harmful activities through the remote controls. One of the Mobile botnet targeted Dutch Online Bank, focusing on European clients of a Dutch online bank. The

Published on February 6, 2018.

Mr.Balaganesh is with the Lincoln University College, Klena Jaya, 47301, Petaling Jaya, Selangor, Malaysia (e-mail: *baga_indian@yahoo.co.in*).

Dr. Amlan Chakrabarti is with the Lincoln University College, Klena Jaya, 47301, Petaling Jaya, Selangor, Malaysia (e-mail: *achakra12@yahoo.com*).

Dr.Divya is with the Lincoln University College, Klena Jaya, 47301, Petaling Jaya, Selangor, Malaysia (e-mail:divya.phd.research@gmail.com).

attacking programmers were provided remote control of the Smart device users with the command logic to attack. The denial of Service attack was performed by these zombies that reside in the botnet. The hacker will utilize these zombies with the PCs. However, so far, no such real versatile have been occurred.

B. *Malicious applications*

Google's Android devices and the Apple iPhone users have generally made them accessible on the Internet, in that case, now and again; attackers have transferred malicious attacks in the form of games or software recreations to the smart device clients. Pierluigi stated that "These malicious apps are usually free and get on a phone because users voluntarily install them" Internet security vendor Network Box USA, Chief Technology Officer. For example, the attackers on a handset are hacking the login name and their passwords and replying to the malware authors. Moreover, the different issues that can be caused are the additional application installation, opening the backdoor for the communication channels and so on.

C. *Social networking*

Malicious attacks like malware are rapidly spreading through the malicious connections on social networks. M86's Antsis said that connecting to the friends in the social networking sites and participating in the trust systems also connects them to the unknown attackers and infections occurs to their network from them.

D. *Spyware*

Through GPS updates, the malware authors are utilizing spyware accessible online to seize a telephone, to see instant messages and messages, permitting them to hear calls and also tracking their GPS information. Juniper Networks' Vennon said that, majority of the business on smart device spyware applications collects the area information to a site and identify the spy logs for viewing the information or transfers an overhaul of captured interchanges. The updated and received new information are conveyed to the spy through the SMS correspondences.

E. *Bluetooth*

Bluetooth refers to the sharing of information and the communication among smart devices. Cabir worm is one of the mobile malware propagates into the devices through Bluetooth and infects the devices. Bluetooth in the wireless devices permits spontaneous connections, communicates their nearest and transfers the executables with these attacks, even though the users allow or configure their operations properly.

F. *Wi-Fi*

Interception of connection between the Wi-Fi hotspots and smart devices can be performed by the Malware Attackers. There is no proper encryption for secure data transmission in the architecture and it is the key vulnerable spot for the attackers. Through the man-in-the-middle attack, the attacker enters between the hotspot provider and the client and spreads the attack. In this attack, hacker allows to create a set up between the shared systems that mirrors like the Wi-Fi hotspot providing new qualified connections that tempts the clients to get connected. The transmissions of the victims are hacked by the hackers without their knowledge.

G. *Phishing*

Phishing performs the similar attacks or risks that they performed on desktop systems on to the smart devices also. Therefore, phishing is making subsequently the mobile users helpless as it did in the computer systems. Phishers are making the platforms to its control through vulnerable telephone connections that are joined with portability combination; phishing filters lack of developers and mobile browsers services like reputation based. Similar cases of wireless connections like e-mails, MMS and SMS are empowering phishing to enter and cause damage in the Smart device as Mobile Phishing.

III. MOBILE THREAT MODEL

The attackers spread malware and infect the mobile devices examining their Operating System through device interfaces [10],[11]. With the accessible SDK and different interfaces, the operating system standard works on the Smart devices. Parent interface sort and arranges the interfaces that are Connectivity Interface, External Memory Interface, User Interface and Device Interface. The mobile devices face the threats from different interfaces, such as to control the compass the attacker may impact the magnetic field or else through aggravating the GPS, attacker may bring impedance in the signal.

A. *Attacker is in Possession of the Device -*

During the situation of the smart devices in the attacker's hand, for example, when the device is lost or stolen or the calls are unattended, the another characteristic have to be done in order to depict the threats to occur, that is, neither the attacker is not going to infer the infection on the OS of the device nor that can be accessible by user Interfaces.

Personal Identification Number (PIN) or difficult unpredictable password can be set for the Windows Mobile and iPhone devices. For protecting the SIM card and provide secured access by the mobile phones, PIN authentification feature is done. The purpose of using this PIN is that it confirms the International Mobile Subscriber Identity (IMSI) in the Home Location Registry of its equivalent network provider. The access allowance is provided once if the successful verification is done. The limitation of this technique is that, the data or the information in the mobile devices cannot be controlled only the network access control can be performed by the PIN. To get complete access of the mobile device SIM card can be replaced.

For securing the information and data from the attacks, it is more important to set up the legitimate authentication. Proper authentication to devices helps the users to get targeted by attackers through user interfaces. Utilizing the cyber forensic specialization, some of the attackers apply the techniques to access those devices set with authentication techniques. The security goals such as integrity and confidentiality will be damaged in much of the cases, when the stored information is not encrypted and their information can be altered and accessed. Since the mobile devices are in the hands of the attackers, the

availability feature also gets damaged. These attackers not only read the contents in the memory card but also tries to spread malware using these cards such as WinCE. Cxover.A, a malware found in Windows Mobile devices [10].

In the case of the attacks through Device Interfaces, some of the extra tools are used to utilize the required functionalities as Oxygen Forensic Suite [11] used for examining the major OS in the mobile devices or Universal Subscriber Identification Module (USIM) card infection. To perform the Device Interface infection through these tools, a connector cable and software are sufficient. They recover or access the information like, contacts, web browser cache, emails, message, attachments, IMEI, IMSI, and even erased documents also. Data extraction feature is applied in these tools, so that the security goal, integrity is not damaged.

B. *Attacker is not in Possession of the Device*

The attacker can infect the devices through the existing interfaces that are open to him if cannot find the control of the device. There are two types of connectivity Interfaces namely the wired and wireless connection with the long or shorter range of communication interfaces. Whether the direct infection can be performed by the attackers or else they are used for malicious data transmission process such as phishing or email malwares. Some of the well-known attacks are:

- BlueSnarfing
- BleuBugging
- BlueJacking
- BlueSnarfing

BlueSnarfing infects the devices through the misuse of the immature Bluetooth execution into the smartdevices or the mobile phones. Here, vCards attack is performed and this performs the exchange technique of stealing the file information without user's knowledge, similar to that of the documents for the calendar or the phonebook.

BlueBugging infects the mobile devices by passing the Hayes AT Commands into the phones deposit. Through this installation, the attacker can make different types of activities like passing SMS, Call initiation or the access to dial history of the devices.

BlueJacking is not actually the attack infecting the device, but it simply portrays the Bluetooth specific utilization for transmission of messages to those devices in its range. Here the messages are surrounded with the unpleasant content and make a view to the new users as a threat.

Bluesmacking infects the devices and creates the denial of service attack in the moile devices like the "ping of death" attack. The vulnerable device will be targeted here by this attack and the device will be sending the payload packets with the predefined length that are typically utilized as the part of request to decide the Round Trip Time (RTT).

This attack is making the device that is attacked to be constrained into a state exclusively attempting to respond the send payload packets finishing with a Denial of Service. Caribe is the first malware that infected the smartphone through the Bluetooth transmission using the Bluetooth protocol [12].

BlueBugging is the most terrible attacker contrasting the quantities of registration in every line, malware and input done manually by an attacker. The attacks specified in this section are incorporated with every possible risk. Thus, the more dangerous threats infecting the smart devices are discussed here. The various categories of threat models in the smart devices are figured below.

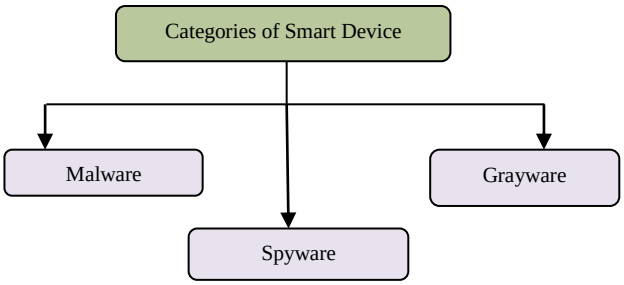

Fig. 2. Smart Devices Threat Model

A. *Malware*

The malware attackers perform its attack through the unauthorized access on the mobile devices either through vulnerability exploitation by SMS parser utilizing the flaws in the system or by Drive by download methods like tricking the end users to set u the installation of application in the system.

B. *Personal Spyware*

The individual's personal information is gathered by the personal spyware such as the contacts, location, call history and so on of the end user of the device. The physical access of the device is conveyed and carried out by the attacker and the spyware is installed. The attacker who installed this attack will access his needs from the injected device. No information will be passed to the application developer.

C. *Grayware*

Here the attacker uses these Grayware applications for gathering the information for user profiling and marketing. The users are not affected in this grayware. The behavior of this attack will be like irritating or unwanted for the end users.

IV. Preventive Measures

For the malware control and mitigation, there should be comprehensive and complete basic preventive measures to be applied by every stakeholder at each level [13]-[15]. Some of the preventive measures applied at each level are shown in the figure below and explained.

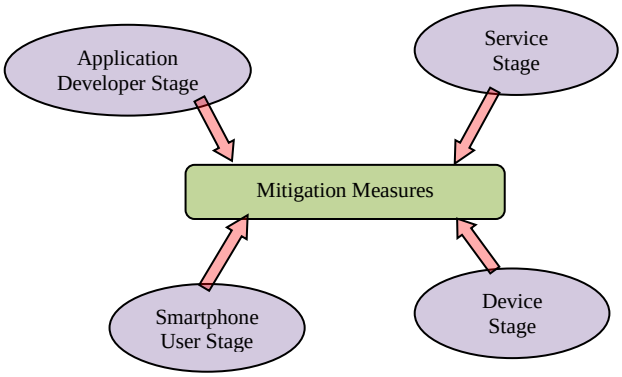

Fig. 3. Measures to Prevent Malwares at each level

A. *Application Developers*

The Application Developer has to guarantee that the privacy policies and the security coding [13] are compiled. Irrelevant access of data should not be performed. Unique identifier should be used by the application developers rather than the use of IMEI number. The data to be passed to the server or to the local delicate should be encrypted. IMEI number must be encrypted utilizing the Hash with salt technique.

B. *Service Level*

To expel the malicious applications, appropriate vetting mechanism should be incorporated at the platform level. Regular response planning and proper good security policies must be maintained. Zero-tolerance policy is better to be followed.

C. *Smartphone User Level*

To overcome the distrustful occasions occurring in the mobile devices, the end user must install the good security solutions in the mobile device. The downloading should be done from the original marketers. The application before it is installed in the mobile device; the user has to read the complete document states such as the rates, reviews and so on. The request sent by the applications to the end user must be properly studied by the users. When the accomplished services are not used by the user, then it should be turned off such as Bluetooth, Wi-Fi and so on. If the devices are found vulnerable, the client must not enjoy the "Jailbreak" in his/her device [14].

D. *Device Level:*

The basic requirement of the device level is to protect the mobile operating system. The violating applications will be limited by the security principles such as process isolation and partial privileges. The methods used for hardening the operating system are stack protection, Address Space Layout Randomization and so on. The strong default settings are ought to be applied in the mobile devices [15].

V. VARIOUS MOBILE VULNERABILITIES

The smart devices have different vulnerabilities existence and the network environment will be getting the attacks or threats entered into these vulnerabilities.
The mobile device networks are harmed by those different vulnerabilities and a portion of those vulnerabilities that are found and operating in the Android devices are explained below in detail.

A. *Virus Vulnerabilities*

The social engineering methods are used by the mobile virus attackers to attract the click on those applications and click on those infected video, picture or the audio attachments. ARM based mobile devices are infected by WinCE.Duts(2005), the principally proofed virus. For the execution of payload into the system, it first essentially attaches itself to executable (*.EXE) files in the mobile device main folder. Further it alters the execution header of the program. To execute and replicate the virus itself in the "coredll" API of Windows CE, the infection exploits through the Windows CE.

B. *Bluetooth Vulnerabilities*

In 1998, Bluetooth Special Interest Group (SIG) [16] was established, then further various updates are performed, for example formation of piconet, voice synchronous modes and data rates enhancement. In 2005, it was stated that almost 300 million mobile devices will be shipped by one of the industrial research report. In the year of 2008, the Bluetooth enabled devices will be more than 922 million and that was reported by IDC. For the synchronization of the mobile or hand-held devices, wireless customers and mobile users are provided with the headsets, hands-free control, mobile phones, computer pheripherals, and so on in the Bluetooth's primary application. For the transmission of data in superior quality rate like USB and fireware, ultra wideband (UWB) radio [17] is attached with the Bluetooth SIG. This radio permits the spread of high quality video, clear digital music to other mobile devices effectively.

The Bluetooth devices are further damaged by various potential vulnerabilities. Probabilistic Queuing model [18] was proposed for identifying the malwares spread in the Bluetooth environment. This model is one of the analytical models that help to evaluate the epidemic infection size that is included by the mobile virus through Bluetooth. The existing vulnerabilities of Bluetooth software stacks are reported and recorded by the Common Vulnerabilities Exploits (CVE) and National Vulnerability Database [19]. Most of the subsequent exploitation is done because of the flaws in programming procedures and wrong Bluetooth execution for matching, device discovery and transfer of data.

C. *SMS/MMS Vulnerabilities*

The mobile device viruses propagating through the Short Messaging Services or Multimedia Messaging Services (MMS) [20],[21] are different to that of proximity scanning, these viruses create danger and damage around the world as like the attacks occurring on the Internet. One of the examples of MMS virus is Commwarrior with 27KB, which can be easily transmitted to other devices. Denial of Service attack happens here during the store-forward stage. The vulnerabilities of the mobile devices are SMS gateway errors, Software errors and SMS spoofing attacks.

VI. MALWARE DETECTION TECHNIQUES

For the detection of mobile malware, the techniques are broadly classified into three types namely: Signature based detection, Anomaly based detection and Virtual based detection [24]-[29]. The relationship between the different categorized malware detection techniques are shown below in the figure.

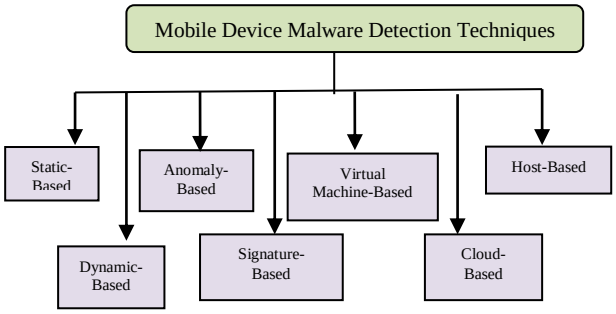

Fig. 5. A Classification of Mobile Malware Detection Techniques

Moreover, the detection techniques will be utilizing three diverse methodologies namely static, dynamic and hybrid approaches. In the Anomaly based detection technique, the training phase will be establishing the normality model earlier for the device action. The benign behavior is initially trained in this detection method, or the target device is monitored first.

The mobile device detection mechanisms are classified into two categories namely host-based detection and cloud-based detection. Host-based detection mechanism refers to the method that executes in the mobile devices. Cloud-based detection mechanism refers to the offloaded serious computation enhanced in the different server. In mobile environment, the detection techniques should be energy efficient because of the nature of limited device resource. Lee et al. [22] proposed such a solution that works under collaboration between mobile and a binary inspection server.

The major classification of detection systems is shown below:

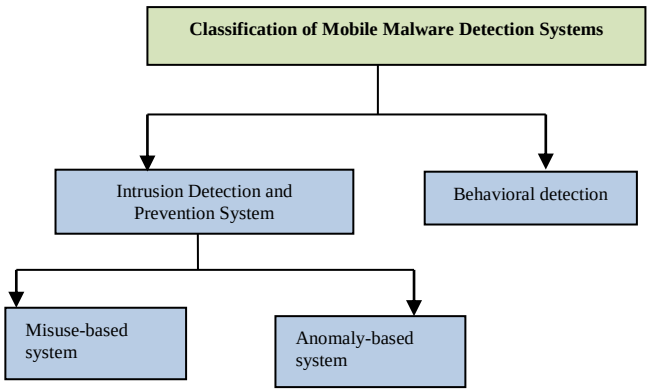

Fig. 6. Mobile Malware Detection Systems Classification

A. *Intrusion Detection System*

Intrusion Detection System is the effective technique for malware detection. Scarfone et al. [23] referred the Intrusion Detection as a procedure of identifying and checking the predefined mechanisms similar to the networks and systems. They define the state of the identified systems information. To find out the malicious events and indicate its incidents these data are analyzed. The malwares initiate these malicious activities. Incidents can perceive the incorrect IP addresses that are wrongly indicated to the servers, when the client forgets the access authorization. This is referred as Nonmalicious activity.

The software tool which is capable of automatically collecting the information, identifying and detecting the malicious occurrence is referred as Intrusion detection system. Some of the prevention capabilities of the intrusion prevention system(IPS) is developed with the intrusion detection system.

Preventive system provides the prevention measures to prevent the system from the malicious attacks infecting the detached and blocked systems. Intrusion Detection and Prevention System (IDPS) has three main stages:

1. System characteristics monitoring such as network, application, operating system behavior, etc.
2. Monitored data re analyzed for identifying malicious occurrences such as misbehavior of application or the security policy breaches.
3. Collect the detected malicious data and initiate the measures to action such as lock systems, report generation, blocking the unauthorized entities.

Further the Intrusion Detection System is classified into two types namely [24]:

- Misuse-based system
- Anomaly-based system

1) *Misuse-based system*

In the misuse detection system, the database is maintained with the collection of predefined patterns in them, and then they are coordinated with the data monitored data. The signatures will be existing in different structures such as, execution stacks, strings, binary information and so on. If any data identified as the malicious during the signature matching, then those records will be predefined as malicious by the IDPS.

2) *Anomaly-based system*

The anomalous activities detected by the system are defined as malicious in the anomaly based detection system. The normality model was developed by the system using the normal activities that empowers to detect the malicious activity in the system. The unknown new threats and attacks can be detected effectively by the Anomaly-based detection systems. The limitation of this system is that provide high false positive rates and they result in the poor accuracy.

B. *Host-based Intrusion Detection Systems*

The single systems characteristics are monitored and detected by the host-based intrusion detection system. To differentiate between the normal and malicious behaviors of the monitored system, the features and characteristics of the network, application and system data are stored. The functions for this process cannot scope on a single or group of capacities. Basic function of the detection system is the kernel monitoring. Moreover, for detection of malicious behavior the library calls and API are monitored.

C. *Behavioral detection*

Detection of mobile malwares existing in the mobile devices that are building with the nature of cellular

networks is becoming difficult. The malware propagation through SMS/MMS messages and Bluetooth are non-traditional and detecting these forms of behaviors is difficult to track through the signature-based detection based methods. This leads to the requirement of novel detection method named behavioral detection.

The run time behaviors of the system are monitored effectively by the behavioral detection methods. For example, API calls, file access and so on are the applications analyzed during their execution and they are compared with the normal and malicious behaviors in the dataset. These are defined as the global procedures that can be applied for all the applications to identify the abnormal behaviors. The behavioral detection method identifies and detects the unknown malware and zero-day worms effectively, though they are built with new behaviors or with the bright fresh components.

VII. CONCLUSION

In the field of recent research, security for smartphones and the detection of malwares is the spread for publication. From the launch of Symbian OS malware till the recent infecting new malwares in the smartphones, there are various malwares existing. The various threats and the different attacks are existing in the smartphones and are discussed. The various techniques such as code obfuscation, malicious payload identification, and encryption and so on are proposed by different researchers for the malware detection. Among the various existing approaches Machine Learning methods have shown the results with high Accuracy in the detection of malicious activities.

REFERENCES

[1]. Teufl P, Ferk M, Fitzek A, Hein D, Kraxberger S, Orthacker C, "Malware detection by applying knowledge discovery processes to application metadata on the Android Market (Google Play)." *In: Security and communication networks.*, 2013. doi:10.1002/sec.675

[2]. SlideME 2013, "SlideME | android apps market: download free & paid android application." *http://slideme.org/.*

[3]. García-Teodoro P, Díaz-Verdejo J, Maciá-Fernández G, Vázquez E, "Anomaly-based network intrusion detection: techniques, systems and challenges." *Computer Security*, Vol. 28, pp.18–28, 2009.

[4]. Symantec 2013, "Android ransomware predictions hold true." *http://www.symantec.com/connect/blogs/android-ransomware-predictions-hold-true.*

[5]. Burguera I, Zurutuza U, Nadjm-Tehrani S, "Crowdroid: behavior based malware detection system for android." *In: Proceedings of the 1st ACM workshop on security and privacy in smartphones and mobile devices*, Chicago, USA, pp 15–26, 2011.

[6]. Arstechnica 2013, "More BadNews for android: new malicious apps found in google play." *http://arstechnica.com/security/2013/04/more-badnews-for-android-new-malicious-apps-found-in-google-play/.*

[7]. F-Secure 2013, "Android accounted for 79% of all mobile malware in 2012, 96% in Q4 alone." *http://techcrunch.com/2013/03/07/f-secure-android-accounted-for-79-of-all-mobile-malware-in-2012-96-in-q4-alone/.*

[8]. Hardwarezone (2013) Trend micro predicts android malware increase by 185%. http://www.hardwarezone.com.ph/tech-news-trend-micro-predicts-android-malware-increase-185.

[9]. Yajin Z, Xuxian J, "Dissecting android malware: characterization and evolution." *In: Proceedings of the IEEE symposium on security and privacy (SP)*, San Fransico, USA, pp 95–109, 2012.

[10]. "NetQin Tech. Co. Ltd. Wince.cxover.a." *http://www.netqin.com/en/virus/virusinfo_1366_2.html, 2009.*

[11]. Oxygen Software Company. Oxygen forensic suite 2010. *http://www.oxygen-forensic.com/, 2010.*

[12]. M. Piercy, "Embedded devices next on the virus target list" *IEEE Electronics Systems and Software*, Vol.2, pp.42-43, December-January, 2004.

[13]. Sampath Deegalla and Henrik Bostrom, "Reducing high-dimensional data by principal component analysis vs. random projection for nearest neighbor classification" *In ICMLA '06: Proceedings of the 5th International Conference on Machine Learning and Applications, IEEE Computer Society*, pages 245-250, Washington, DC, USA, 2006.

[14]. Inc. Conexant Systems. Commands for host-processed and host-controlled modems reference manual. *http://www.zoom.com/documentation/dial_up/100498D.pdf*, April 2001.

[15]. Microsoft Corporation. Windows mobile. *http://www.microsoft.com/germany/windowsmobile/default.mspx, 2007.*

[16]. Ross Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems" chapter 10, *Monitoring Systems*, pages 207-230. Wiley & Sons, 2001.

[17]. Leonid Batyuk, Aubrey-Derrick Schmidt, Hans-Gunther Schmidt, Ahmet Camtepe, and Sahin Albayrak, "Developing and benchmarking native Linux applications on Android." *In Mobile Wireless Middleware,Operating Systems, and Applications*, 2009.

[18]. Stephen Hofmeyr and Stephanie Forrest, "Architecture for an Artificial Immune System" *Evolutionary Computation Journal*, Vol. 8, Issue. 4, pp:443-473, 2000.

[19]. Stefan Axelsson, "Intrusion detection systems: A survey and taxonomy" *Technical Report 99*, Department of Computer Engineering Chalmers University of Technology Goteborg, Sweden, March 2000.

[20]. Daniel Lowry Lough, "A taxonomy of computer attacks with applications to wireless networks" PhD thesis, Virginia Polytechnic Institute and State University, 2001. Chairman-Davis,IV, Nathaniel J.

[21]. A.A.E. Ahmed and I. Traore, "A new biometric technology based on mouse dynamics" *IEEE Transactions on Dependable and Secure Computing (TDSC)*, Vol. 4 No. 3, pp:165, 2007.

[22]. Gregory D. Abowd, Liviu Iftode, and Helena Mitchel, "The smart phone: A first platform for pervasive computing" *IEEE Pervasive Computing*, Vol.4, No. 2, pp:18-19, April-June 2005.

[23]. Karen Scarfone and Peter Mell, "Guide to intrusion detection and prevention systems (idps)." *http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf*, February 2007. National Institute of Standards and Technology (NIST) Special Publication 800-94.

[24]. Christopher Kruegel, Fredrik Valeur, and Giovanni Vigna, "Intrusion Detection and Correlation: Challenges and Solutions" *Springer-Verlag TELOS*, Santa Clara, CA, USA, 2004.

[25]. Vern Paxson, "Bro: a system for detecting network intruders in realtime" *In SSYM'98: Proceedings of the 7th conference on USENIX Security Symposium*, 1998, pages 33, Berkeley, CA, USA, 1998. USENIX Association.

[26]. Gregory White and Vdo Pooch, "Cooperating security managers: Distributed intrusion detection systems" *Elsevier Computers & Security*, Vol.15, No.5, pp:441- 450, 1996.

[27]. Teresa F. Lunt, R. Jagannathan, Rosanna Lee, Sherry Listgarten, David L. Edwards, Peter G. Neumann, Harold S. Javitz, and A. Valdes, "Ides: The enhanced prototype, a real-time intrusion detection system" *Technical Report Technical Report SRI Project 4185-010, SRI-CSL-88-12, CSL SRI International, Computer Science Laboratory*, 1988.

[28]. Albert J. H□oglund, Kimmo H□at□onen, and Antti S. Sorvari, "A computer host-based user anomaly detection system using the self-organizing map" *In IJCNN '00: Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks (IJCNN'00)*-Volume 5, page 5411, Washington, DC, USA, 2000. *IEEE Computer Society.*

[29]. Anderson, Lunt, Javits, Tamaru, and Valdes, "Detecting unusual program behavior using the statistical components of NIDES" *Technical report, Computer Science Laboratory, May 1995.*