Classification of Mobile P2P Malware Based on Propagation Behaviour

Muhammad Adeel, Laurissa Tokarchuk, Muhammad Awais Azam
School of Electronic Engineering & Computer Science, Queen Mary University of London,
London E1 4NS, United Kingdom
{muhammad.adeel, laurissa.tokarchuk, muhammad.azam}@elec.qmul.ac.uk

***Abstract*—With a multifold increase in the number of mobile users over past few years, mobile malware has emerged as a serious threat for resource constrained handheld devices. From experience of the Internet malware attacks like *CodeRed* and *Slammer*, it may not be difficult to predict the extent of devastation mobile malware could potentially cause. Numbering around 700 today, detection of mobile P2P malware may prove a serious challenge considering scarce memory, processing and battery resources of handheld devices. Issue may worsen if the detection takes place on mobile devices. Thus there is a strong need of identifying commonalities between various kinds of mobile malware to reduce the detection footprint. As a novel contribution, this work discusses various possibilities of classification of mobile malware and proposes a technical behaviour-based classification that could help detect a range of malware families in real time based on their behaviour during various stages of an attack.**

Keywords- Mobile P2P; Malware classification; Behaviour identification; Mobile malware families

I. INTRODUCTION

There exist over two billion mobile phones in the world today. Statistics from a survey conducted by Dong *et al* [1] reveal that Symbian is the leading operating system in terms of market density with 63% of the market share followed by Windows OS with 16% market density and Palm OS with 10% market penetration. Substantially large penetration of Symbian OS makes it a hot target for mobile worms and viruses. There are over 400 various kinds of mobile malware and around 700 of their variants discovered so far while approximately 90% of this malware targets Symbian-based handhelds [1]. It is difficult to develop an electronic system that detects all of these viruses as they use different strategies to attack the system. Mobile viruses and worms are known to have commonalities in terms of their behaviours however, no technical categorization of such malware exists to-date [2].

Besides common propagation avenues (i.e. MMS & SMS, Bluetooth and Mobile Internet), there are many other ways the malware could propagate in mobile P2P networks. Services like GPRS allow mobile devices to create IP connections with remote servers through cellular vendor's network. This may allow an adversary to take advantage of inherently weak defenses of resource constrained mobile devices. Use of WLAN on handhelds may also put smartphones at risk from various kinds of security threats [3]. Copying files to mobile devices through removable media such as SD cards has proven dangerous with regards to virus replication. Email applications and instant messaging can also act as an avenue for malware propagation while web browsing on handhelds can be dangerous in terms of download and execution of malicious code on mobile device. Damages due to malware propagation through any of the means above can range from loss of privacy and transfer of unsolicited information to the system malfunctioning and failure. Malware causing service disruptions and economic losses can be termed critical though. Figure 1 gives an overview of threat levels of prominent mobile malware by different antivirus companies.

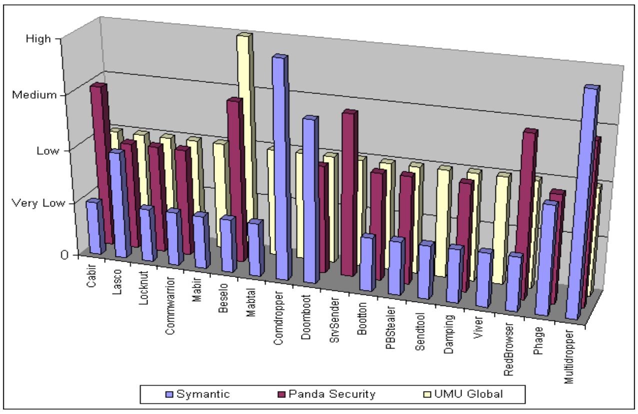

Figure 1: Malware Rating by Antivirus Companies

This work mainly intends at giving new dimensions to the classification of mobile P2P malware and discusses novel contributions in terms of technical classification of malware in Section 4 and the modifications to an existing classification mechanism proposed by Kim *et al* [4] in Section 3. Section 2 discusses another classification of malware based on propagation technologies. Although a very generic and rather theoretical classification of mobile malware could be based on operating system alone however, we keep this work focused on technical classification that could act as a baseline for detection of malware in real time.

II. CLASSIFICATION BASED ON PROPAGATION TECHNOLOGY

This section classifies mobile worm infections in terms of propagation technologies i.e. Bluetooth, MMS/SMS and Internet. It also paves the way for more elaborate technical categorizations in coming sections.

A. Infections through Bluetooth

3G/4G mobile devices are usually equipped with short-range transmission technologies like Bluetooth and Infrared. This allows them to communicate directly with other devices nearby rather than through communication via a cellular services provider's network. Bluetooth technology can be deemed as one of the contributing factors that gave rise to the concept of mobile P2P networks however, it could also be proclaimed as a major factor behind propagation of peer-related mobile malware in handheld devices. Bluetooth-based malware propagates using Bluetooth capabilities of mobile phones and exploits vulnerabilities of Bluetooth technology to cause catastrophes in mobile P2P networks. Bluetooth technology is known for its inherent security vulnerabilities, Bluetooth and others short-range technologies like Infrared open new avenues of threat dissemination from neighbours. Figure 2 gives a pictorial view of the propagation strategy adopted by the worms like Cabir [5], Metal Gear [6], PBSteal [7] and Lasco [6] mainly using Bluetooth technology. Bluetooth data transfer directly between P2P handhelds makes these resource-constrained devices and the mobile network extremely vulnerable to worm attacks.

Once infected through its mobile peer, a victim will attempt to propagate malware further through the same strategy. Victim not only suffers in terms of battery drain but also in terms of infection to SIS or system files. Infected applications or even operating system may not function properly, hence leaving a mobile functionally dead. Variants of such mobile worms may also propagate secret mobile information to other devices through Bluetooth.

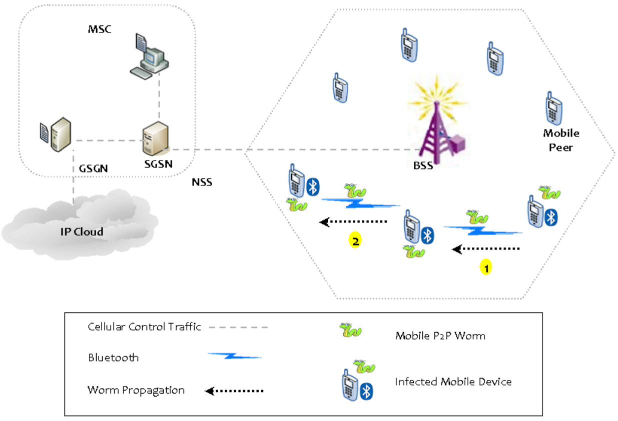

Figure 2: Bluetooth Worm Attack

B. *Infections through SMS & MMS*

MMS and SMS can be considered primary services in terms of mobile usage. Cellular service providers are offering enticing packages to attract customers use more MMS and SMS services. These services however could also be used as launching pad for different kinds of worm attacks in mobile networks. Worms like Mabir [8] and Commwarrior [5] propagate infection through MMS messages while malware like Mquito [9], Wesber [10] and RedBrowser [5] send premium rate SMS messages and incur costs on victim mobiles. An important motive of the attackers is to incur cost on customer. Mobile worms like Mabir and Commwarrior are capable of propagating through MMS thus giving worm propagation a global perspective. Figure 3 illustrates the attack scenario in which an infected mobile node can infect another mobile through a malicious MMS sent via MMS server. Variants of SMS worms besides sending premier-rate SMS messages could also disclose a mobile's private information to its neighbours.

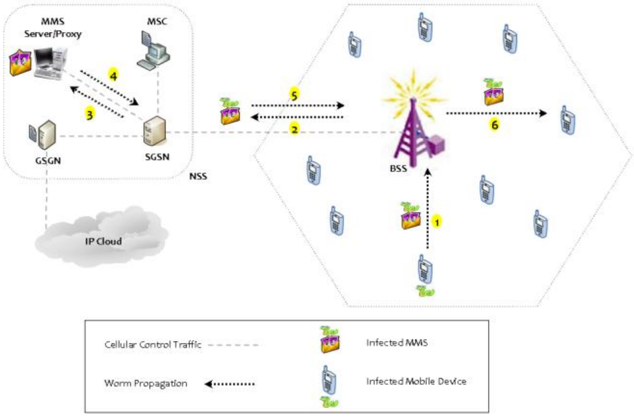

Figure 3: MMS & SMS Worm Attack

C. *Infections through Fixed P2P Networks (Mobile Internet)*

A key attraction in use of mobile P2P networks is a tempting large repository of free downloadable content over World Wide Web. Besides mobile P2P applications like MBit and PeerBox, mobile peers can also interact directly with peers on fixed P2P networks. CDMA and GSM based 3G cellular networks offer higher data rates with rather reduced costs for downloading content. This entices more mobile customers to access P2P content through mobile Internet and hence become vulnerable. Doomboot [12], BBProxy [11], CARDTRAP [14], Metal Gear, PBSteal and RedBrowser are typical examples of malware that is downloaded onto mobile peers this way. Authors in [13] propose an architecture in which mobile peers are no different than fixed peers if a few P2P-specific servers are deployed in cellular vendor's network. Their framework enables mobile users transparently download P2P content from the Internet however it might put mobile peers at a direct risk of security attacks from Internet. Figure 4 illustrates another scenario in which worms originating from fixed P2P network could infect a device after downloading malicious content. Infected device could then infect other devices using data entities of the service provider's network.

This category mainly includes the malware that can be downloaded from the Internet while browsing fixed P2P networks. It then has capability to propagate further on mobile P2P network using different propagation strategies. This category of infections also includes worms from the previous two categories, such as RedBrowser, Metal Gear and Mquito that are downloaded through web browsing or accessing P2P content over the Internet. Victim devices are thus turned into launching pads for further attacks.

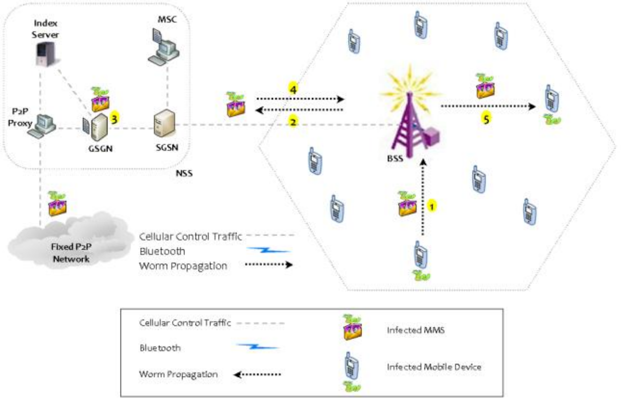

Figure 4: Worm Attack through P2P Core

It was observed that although this classification can act as a baseline for future classifications, it might not be capable of providing a practical categorization of mobile malware capable of detecting malware families in real time. A same worm can potentially use different technologies to propagate during its infection and hence making identification of malware rather infeasible through this way of classification. Thus we proceed to the next section where a rather technical classification of malware is suggested and which to some extent is capable of detecting individual worms rather distinctly during an attack.

III. CLASSIFICATION BASED ON INFECTION SEQUENCE

This section gives a categorization of malware in terms of sequence of operations performed by malware during an infection. Kim *et al* give set of operations for each of the four types of worms they brought under discussion. A set holds operations in a sequence they occur during an attack. Each line in Table 1 gives behaviour of a distinct malware in terms of sequence of operations. We extend the work of Kim *et al* by introducing more operations that enables us to cover further malware types. Rest of this section discuss various operations that could form the basis of detection of distinct malware types.

- *EXEC:* This operation involves execution of malware code on a node to infect it and initiation of the process of propagation of malware. Generic SI model of propagation of malware assumes that every node that downloads the malware should execute it and thus get infected. Every infection starts with EXEC phase however EXEC may have different consequences in different types of malware.
- *CRT_MSG:* To transmit the infection, infected payload is created and in subsequent phases forwarded to the vulnerable devices. Payload for Bluetooth based infections like Cabir differs from SMS based infections like Mosquito.
- *BT_SCAN: In* Bluetooth based infections like Cabir, Lasco & PB Stealers, infected file created through CRT_MSG is propagated to all the Bluetooth devices in coverage are (i.e. in neighbour set). Hence a Bluetooth scan must takes place through Service Discovery Protocol [15] to discover the active Bluetooth neighbours.
- *PB_SCAN:* Infection through MMS propagation like Commwarrior, Mabir and Beselo involve selection of contacts (i.e. victims) from the phonebook for onward transmission of malware. Browsing of the phonebook for this sole purpose is covered under PB_SCAN.
- *RD_PRM:* Worms like RedBrowser, Mosquito & GameSat send premier-rate SMS messages to specific phone numbers for the purpose of financial gains against victim. Attempt to read a premier number from the memory may be another significant operation in terms of detection of such kinds of malware.
- *SND_BT:* After scanning for active Bluetooth devices around, malware is transmitted to those devices. SND_BT records the device IDs and the total number of Bluetooth enabled devices to which the malware is being propagated. Section to come will reveal that the number of devices to which the malware is propagated plays an important role in identification of a family.
- *SND_MMS:* Following *EXEC*, *CRT_MSG* and *PB_SCAN*, next step in the MMS based infections is to send the infected multimedia-message to the selected contacts from the phonebook. Cellular network radio interface is used to get the messages delivered. Again, the number of contacts to which the MMS is being sent plays an important role in identification of malware families in future detections.
- *SND_SMS:* For the SMS based malware families, premier rate SMS messages are sent form the infected device using Short Messaging Service Centre (SMSC) [16] of the cellular network. Apart from the SMS infection scenario above, SND_SMS also executes in other variants of SMS based malware that repeatedly send random messages containing personal information (suppose phonebook entries) of an infected device to its neighbours.
- *CPT_BNRY:* Worm families like Doomboot besides other MMS and Bluetooth related operations also corrupt system binaries on an infected device. Consequently, the victim device could fail on reboot. This unique operation may play a vital role in aimed future detections of this kind of families.
- *LOG_SCAN:* Worm families like Lasco constantly scan the call-logs of infected mobile and reply any incoming message with copies of the malware. LOG_SCAN operation could distinguish this type of malware from others.
- *USR_IDLE:* This operation is aimed at the detection of user idle time by logging data about key-presses and interaction of user with the device. Malware may propagate without the knowledge of phone user and logging such

information may prove very effective in prevention of various malware related attacks.

Building up on the work of Kim *et al*, Table 1 gives sequence of operations for two new families i.e. Call-Loggers & Premier Chargers to be discussed in next section on lines 4 and 5.

TABLE 1. CLASSIFICATION BASED ON SET OF OPERATIONS

1. EXEC › CRT_MSG › BT_SCAN › SND_BT

2. EXEC › CRT_MSG › BT_SCAN › SND_BT › PB_SCAN › SND_MMS

3. EXEC › CRT_MSG › BT_SCAN › SND_BT › PB_SCAN › SND_MMS › CPT_BNRY

4. EXEC › CRT_MSG › BT_SCAN › SND_BT › PB_SCAN › LOG_SCAN › SND_MMS

5. EXEC › CRT_MSG › RD_PRM › SND_SMS

Although we have succeeded in extending the work of Kim *et al* in terms of adding new families and operations, the basic limitation of their work is its inherent incapability of detection of malware families as it purely follows a malware-specific classification model. For instance, their model fails in distinguishing between Commwarrior and Mutational Commwarrior (contains Beselo & Disco worms) families. A detection model based on their classification model may require definition (as in Table 1) for every single malware discovered. Maintaining such a memory-intensive up-to-date database may not be feasible on resource constrained mobile devices and hence we propose a classification model capable of acting as a baseline for detection of malware families.

IV. CLASSIFICATION BASED ON BEHAVIOUR DURING ATTACK

After attempting to classify malware based on the transmission technology and then on the sequence of operations a malware perform under an attack, this section gives a classification of malware based on their behaviour. Table 1 would suggest that although every set distinctly elaborates the behaviour of a particular malware, most of the operations in the database (Table 1) are redundant. Hence rather than selecting the whole set to describe a malware type, under this classification, we select key classification features pertaining to a group of various malware and name them as *flags*. Feature extraction and flagging mechanism is explained through Figure 5. Every malware family exhibits one or many characteristics named as flags in lower part of Figure 5. Sequence of occurrence of flags will eventually determine a malware family. Feature extraction also results in considerable reduction of the malware behaviour storage footprint.

Step 1 of the classification based on behaviours is the identification of the core threat conditions during an attack and setting an appropriate *flag* to *High* if that conditions becomes to true while Step 2 will be to see that to what family this flag or the combination of flags belong to, thus declaring an appropriate alarm. Section below explains some of the extracted behaviours (pertaining to various classes of malware) that would help distinctly identify a malware family. These extracted behaviours are called *flags*.

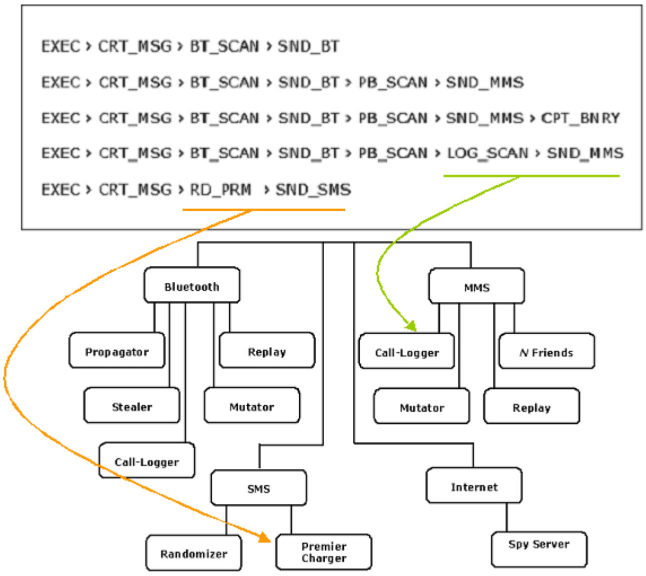
EXEC › CRT_MSG › BT_SCAN › SND_BT
EXEC › CRT_MSG › BT_SCAN › SND_BT › PB_SCAN › SND_MMS
EXEC › CRT_MSG › BT_SCAN › SND_BT › PB_SCAN › SND_MMS › CPT_BNRY
EXEC › CRT_MSG › BT_SCAN › SND_BT › PB_SCAN › LOG_SCAN › SND_MMS
EXEC › CRT_MSG › RD_PRM › SND_SMS
Bluetooth
Propagator
Replay
Stealer
Mutator
Call-Logger
SMS
Randomizer
Premier Charger
MMS
Call-Logger
N Friends
Mutator
Replay
Internet
Spy Server

Figure 5: Classification Based on Behaviours

A. BT Propagator

Worms like Cabir, Lasco, PBStealer exhibit this threat condition as do a few malware droppers like Cdropepr [17] and MGDropper [18]. BT_SCAN alongwith SND_BT triggers this flag while the conditions like malware replication to all the active neighbours and repetition of this flag confirms the existence of a malware activity relating to a Bluetooth malware family.

B. BT Mutator

BT Mutator flag corresponds to the malware that uses Bluetooth technology for its replication onto its neighbours and mutates its signature after little iteration. Variants of Cabir family use mutational strategies to remain undetected during attack. Most of the signature-based detection techniques fail in detecting such mutations however the proposed behaviour-based detection is inherently capable of detecting them.

C. BT Replay

This class encompasses the malware that uses Bluetooth technology for propagation to active neighbours of an infected device. Trojans like PBSteal repeatedly send copies of phone-critical information to first connecting neighbour in the list. Alongside stealing phone-critical information, the main motive of such malware is to flush the battery power of infected mobile device as well as the recipient of this transmission. Some dropper like SendTool [19] that eventually drop PBSteal into the target victim's inbox can also be put into this category.

D. BT Stealer

On of the main motive of the malware exhibiting this behaviour is to disclose the phone and user critical information to the neighbours around. Malware like PBStealer [20] could be put in this category that after infecting a device, makes this devices transmit confidential information to all its neighbours and repeats this behaviour with constant intervals. PBSteal and SendTool could also be put in this category of malware. Relying on various other aspects beyond the scope of this discussion, detections in future stages of this project will be capable of distinctly identifying malware from *BT Replay and BT Stealer* families.

E. MMS N Friends

MMS ***N*** Friends is one of the most important threat conditions in which an infection is propagated to a fixed number of contacts selected from the phonebook of a device. This operation is repeated with constant intervals (in most of the cases interval gap is 10 minutes). 16 Variants of the Commwarrior family and droppers like Commdropper [21] could be put in this category.

F. MMS Replay

One of the consequences of the malware exhibiting this condition is depletion of battery resources of infected and target mobiles. Infected mobiles send repeated copies of the same multimedia message to same mobiles every few minutes. As MMS is a premium service, cost incurred by the victim as a result of this replication could be way too high. Such kind of MMS replay attacks have resulted in various DoS attacks on MMS servers in the past [22].

G. MMS Mutator

Even with MMS based malware families, mutation becomes a key challenge for signature-based techniques. Worms like Beselo and Disco [23] are similar in propagation behaviour to the Commwarrior families but their strategy to mutate makes them qualify to be identified as a distinct family.

H. MMS Call-Logger

Worms like Mabir listen very intelligently to the call logs on an infected mobile phone and reply to the incoming traffic with an infected MMS. Receiving victim device assumes malicious MMS as reply of its message, executes the file attached to the MMS and gets infected.

1. MMS Binary Corruptors

Characteristic that makes this family distinct and rather deadly from the Commwarrior family is that followed by a Commwarrior like infection, it also corrupts the system binaries of the victim mobile thus making it unable to reboot at the next start-up. Worms like Doomboot belong to this family of malware.

J. SMS Premier Charger

Malware families exhibiting this characteristic aim at incurring financial losses to the victim. Making use of SMS technology, the infected devices are made to send an SMS message to premier numbers every few minutes. RedBrowser, GameSat [24] and Mosquito are the most common worms that may fall under this family of malware. Symbian OS Viver [25] is more aggressive as it sends a premier message every 15 seconds and may cause a huge financial loss if remains undetected ever for a shorter time.

K. SMS Randomizer

By constantly listening at the call logs of victim mobile, this class of malware responds to every SMS or call with a random SMS message. Motivation behind this attack is to incur financial loss on the customer. In future though, SMS randomiser can be used to launch more classified attacks like MMS Call-Logger. Symbian trojans like SrvSender [30] belong to this family of malware.

L. Spy-Server

Discovered in January 2010, Ikee worm [29] for the IPhoneOS [26] devices belongs to this category of malware. Ikee makes victim IPhones periodically transmit phone-critical information to a remote server. Cross-platform spyware like Flexispy [27], Mobispy [28] and Blackberry spyware MobiStealth [31] also belong to this category of malware.

V. DISCUSSION & CONCLUSION

Table 2 gives various flags based on which the malware families are identified.

TABLE 2. CLASSIFICATION BASED ON BEHAVIOUR

Flag	Environment	Description
BP	Bluetooth	Bluetooth Propagator
BR	Bluetooth	Bluetooth Replay
BM	Bluetooth	Bluetooth Mutation
MN	MMS	MMS *N* Friends
MR	MMS	MMS Replay
MM	MMS	MMS Mutation
BS	Bluetooth	Bluetooth Stealer
MC	MMS	MMS Call-Logger
MB	MMS	MMS Binary Corruptor
SP	SMS	SMS Premier Charger
SR	SMS	SMS Randomizer
IS	Internet	Internet Spy-Server

Every flag represents a distinct behaviour and characteristic of malware during an attack. A distinct set, sequence or pattern of flags represents the very core functionality of a malware family and thus forms the basis of its detection. Some of the families might not be detectable through one flag alone. BP flag alone if TRUE means alarms about an underway Cabir family infection while a specific pattern of repetition of BP flag confirms this infection. If both BP and MN flags are TRUE, it will prompt a Commwarrior family infection. Similarly if BP and MR flags are TRUE, it represents a Mutational Commwarrior family infection while MR flag alone if TRUE will indicate an MMS Replay family attack.

It was observed that the malware classification based on communication technology alone was not appropriate because different kinds of malware propagating even though similar technology may have varying characteristics in terms of motives, damages and infection strategy. Extensions to the operation database of Kim *et al* although resulted in detection of more malware types however, the model fails to detect the malware families due to its inherent incapabilities. As their solution requires logging definition of every malware in the detection database, its size may also prove a major concern for resource constraint mobile devices. Based on the example of Commwarrior and Mutational Commwarrior families in Section 3, it was also realized that the traditional signature based techniques may fail in identification of malware families while even some behavioural detection techniques like the one proposed by Kim *et al* may not prove effective in identification of mobile malware families. Alongside considerable reduction the in size of detection database, novel classification based on behaviours proposed in Section 4 has also proved capable of distinctly identifying 12 malware families that accommodate over 200 worms and make about 25% of the total detected mobile malware [32].

REFERENCES

[1] William Aiello & Steven M. Bellovin et al, "Efficient, DoS Resistant, Secure Key Exchange for Internet Protocols CCS'02, November, 2002, Washington, DC USA

[2] Mikko Hypponen, "Mobile Malware", Invited talk delivered at 16th Usenex Security Symposium, Boston, USA, August 2007. http://www.usenix.org/events/sec07/tech/ hypponen.pdf

[4] Hahnsang Kim, Joshua Smith, Kang G. Shin, "Detecting Energy-Greedy Anomalies and Mobile Malware Variants", MobiSys'08, June 17–20, 2008, Breckenridge, Colorado, USA

[3] Dong-Her Shih, "Security Aspects of Mobile Phone Virus: A Critical Survey"

[5] Mikko Hypponen, " Malware Goes Mobile", Proceedings of Scientific America Inc., 2006

[6] Ajay Sharma, " Bluetooth Security Issues, Threats And Consequences", Proceedings of 2nd National Conference on Challenges & Opportunities in Information Technology (COIT-2008), March 29, 2008

[7] http://www.mobile-antivirus.org/Anti-virus-Articles/PBsteal-fix.html [Last accessed 29 April 2009]

[8] http://www.f-secure.com/v-descs/mabir.shtml [Last accessed 29 April 2009]

[9] Neal Leavitt, "Mobile Phones: The Next Frontier for Hackers?"

[10] http://vil.nai.com/vil/content/v_140595.htm [Last accessed 29 April 2010]

[11] http://www.umuglobal.com/encyclopaedia.php [Last accessed 29 April 2009]

[12] http://www.f-secure.com/v-descs/doomboot_a.shtml [Last accessed 29 April 2009]

[13] Andersen F. and Kappler C. et al., "An Architecture Concept for Mobile P2P File Sharing Services", Lecture Notes on Informatics (LNI) P-51, ISBN 3-88579-380-6, Bonner Köllen Verlag, 2004

[14] http://www.f-secure.com/v-descs/cardtrap_a.shtml [Last accessed 29 April 2009]

[15] Service Discovery Protococl http://people.csail.mit.edu/ albert/bluez-intro/x290.html[Last accessed 29 April 2010]

[16] N.J Croft and M.S Olivier, "A Silent SMS Denial of Service (DoS) Attack". TechRepublic White Paper, October 2007

[17] http://www.antivirusprogram.se/virusinfo/Cdropper.A_ 8390.html [Last accessed 29 April 2010]

[18] http://www.f-secure.com/v-descs/mgdropper.shtml [Last accessed 29 April 2010]

[19] SendTool: http://vil.nai.com/vil/content/v_137772.htm [Last accessed 29 April 2010]

[20] PBSteal:http://www.symantec.com/security_response/ writeup.jsp?docid=2006-011915-4557-99 [Last accessed 29 April 2010]

[21] http://www.antivirusprogram.se/virusinfo/SymbOS.Comm dropper.A_10377.html [Last accessed 29 April 2010]

[22] Stefan Andersson, "MMS Security Considerations", 3GPP TSG SA WG3 Security, Munich, Germany. 18-21 November 2003

[23] http://threatcenter.smobilesystems.com/?p=1180[Last accessed 29 April 2010]

[24] http://www.umuglobal.com/encyclopaedia/114[Last accessed 29 April 2010]

[25] http://www.f-secure.com/v-descs/trojan_symbos_viver_as html [Last accessed 29 April 2010]

[26] www.apple.com/iphone [Last accessed 29 April 2010]

[27] http://www.f-secure.com/v-descs/flexispy_a.shtml [Last accessed 29 April 2010]

[28] vil.nai.com/vil/content/v_139178.htm [Last accessed 29 April 2010]

[29] http://www.f-secure.com/v-descs/worm_iphoneos _ikee.shtml [Last accessed 29 April 2010]

[30] http://www.f-secure.com/v-descs/trojan_symbos _srvsender.shtml [Last accessed 29 April 2010]

[31] http://threatcenter.smobilesystems.com/?p=1868[Last acces-sed 29 April 2010]

[32] Jamshed Sadiq, "Classification of Mobile Viruses", MSc Thesis Report, School of Electronic Engineering & Computer Science, Queen Mary University of London, August 2009.