ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Ways in Which Mobile Devices Can be Infected with Malware and Proposed Counter Measures

[12]Erick K. Rotich, [23]Shadrack K. Metto, [2]Ikoha Anselemo P
[1]Dept. of Maths and Computer Science University of Eldoret
[2]Dept. of Information Technology Kibabii University College
[3]Dept. of Information Technology Moi University

Abstract
Of late, mobile handsets are becoming more smart and multifaceted in functionality, much like Personal Computers. Likewise, mobiles are more widely held than PCs, and are being used more and more frequently to do business, access the Internet, access bank accounts, and pay for goods and services. This has resulted in an increased number of offenders who wants to feat these actions for unlawful attainments. Malware is capable of undertaking many things, such as stealing and transmitting the contact list and other data, barring the device completely, giving remote access to criminals, sending SMS and MMS messages etc. Mobile malware causes severe public concern as more so because mobile phones are more in numbers than the population of PCs. In this paper we explore on ways in which mobile devices can be infected with malware and their counter measures.

Key words
Mobile Devices, SMS, malware, Bluetooth, GSM, GPRS

I. Introduction

Of late, mobile handsets are becoming more smart and multifaceted in functionality, much like Personal Computers. Likewise, mobiles are more widely held than PCs, and are being used more and more frequently to do business, access the Internet, access bank accounts, and pay for goods and services. This has resulted in an increased number of offenders who wants to feat these actions for unlawful attainments.

Malware is capable of undertaking many things, such as stealing and transmitting the contact list and other data, barring the device completely, giving remote access to criminals, sending SMS and MMS messages etc. Mobile malware causes severe public concern as more so because mobile phones are more in numbers than the population of PCs. [6].

According to [7] Current mobile devices (smartphones) offer lots of the capabilities of traditional personal computers (PCs) and offer a large variety of connectivity options, such as IEEE 802.11, Bluetooth, GSM, GPRS, UMTS, and HSPA. This overabundance of attractive features has led to a extensive diffusion of smartphones that, as a result, are now an ideal target forattackers. Earlier smartphones came packaged with standardized Operating System (OS): less heterogeneity in OS allowed attackers to exploit just a single vulnerability to attack a large number of dissimilar kinds of devices by causing major security outbreaks

A. The mobile handset malware obstacles

i. Mobile handset users treat mobile handset malware as a problem which has not occurred yet, or believe that it's not an issue which really concerns them.
ii. It is not easy to execute a detection framework due to the device resources e.g. CPU, memory and power.
iii. Most new malicious programs for mobile handset devices are mixtures, containing functionality from two or more different types of malware.
iv. Because of the fact that mobile device have no clear prominent operating system it is possible to target the majority of mobile device users with a single attack. Hence virus writers write malware which targeted specific platforms, and more on creating programs capable of infecting several platforms.
v. Mobile handset connects to the cellular network through SMS/MMS services, as well as its Bluetooth interface that is frequently used to interact with other devices. This is on top the internet connection through the IP. These interfaces are rapidly becoming the new infection vector for viruses, which makes the mobile handset vulnerable to get infected even when it is disconnected from the internet.
vi. A mobile handset is extremely mobile and continuously on, resulting in a more degree of difficulty in quarantining the virus in a local region.
vii. To elude discovery, malware writers are progressively using polymorphic coding techniques. Polymorphism is a process through which malicious code changes [6].

B. Types of attacks against mobile devices According to [4] types of attacks against mobile devices include:

i. Theft of data: Hackers often attack mobile devices to get transient information and static information. Transient information includes the phone's location, its power usage, and other data, which the device does not normally record
ii. Phone Hijacking: Some malware might endeavor to use the prey's phone resources. Opportunities include placing long-distance calls, sending expensive SMS messages
iii. Denial-of-Service (DoS):DoS could be done by saturating the device and draining power. It is really easy to crash or overwhelm most Bluetooth applications on mobile devices just by sending recurring pieces of information, corrupted packets, and incorrect file formats [15].

C. Key aspects distinguishing mobile security from conventional computer security

i. mobility: each device comes with us anywhere we go and therefore, it can be easily stolen or physically tampered;
ii. Strong personalization: usually, the owner of device is also its unique user;
iii. Strong connectivity: a smartphone enables a user to send e-mails, to check her online banking account, to access lot of Internet services; in this way, malware can infect the device, either through SMS or MMS or by exploiting the Internet

connection;

iv. Technology convergence: a single device combines different technologies: this may enable an attacker to exploit different routes to perform her attacks;

v. Reduced capabilities: even if smartphones are like pocket PCs, there are some characteristic features that lack on smartphones, e.g. a fully keyboard.[7].

D. The following are high-level network threats: [5].

i. Information gathering
ii. Sniffing
iii. Spoofing
iv. Session hijacking
v. Denial of service

II. How mobile devices are infected with malware

A. Malware infection routes

Possible routes of mobile virus infection [2] include:

i. MMS.
Malicious software can spread via multimedia messaging service (MMS) messages by attaching a copy of itself on to a MMS message and sending it to some other device capable of receiving MMS

ii. Bluetooth.
The first mobile phone viruses spread via Bluetooth. The viruses written so far do not seem to use any actual vulnerability in Bluetooth. If the virus could make itself a part of a file often exchanged via Bluetooth it could spread quite efficiently.

iii. IP connections via UMTS.
Usually internet connections made by mobile phones are temporary and the connectivity is only used by explicit request. An IP connection is opened only when it is needed and it seldom runs in the background. However, this might change in the future if WLAN connections and 3G services with flat pricing models will become more common. Still a mobile worm spreading efficiently trough a VPN is a possibility.

iv. Copying files.
Many viruses spread themselves to other files upon infection. These files can be copied to other devices and the virus spreads.

v. Removable media.
It is also possible for a virus to spread explicitly over removable media much like in the old days with floppy diskettes. This will probably change if people start to use their phones more like digital cameras.

vi. E-mail applications.
Many mobile phones run e-mail applications on its platform. However, a virus author probably would write mobile malware that uses e-mail attachments to transmit itself to wireless devices.

vii. Instant messaging (IM).
As mobile IM's popularity grows, the same sorts of attacks seen on PCs are likely to appear, such as hijacking lists of IM names and sending links to recipients to direct them to malicious sites. Mobile viruses could also send out IM messages with the malicious code attached.

viii. Warez.
Warez is software stripped of copy protection and placed on the internet for downloading, generally it is illegally. The community that develops Warez could make infected mobile games available online to unsuspecting users.

ix. Webpage browsing.
When the infected webpage is browsed by using mobile phone's browser, the malicious code hidden in webpage may execute. This malicious code may intrude your phone and cause some damages.

B. Obfuscation techniques

According to [10], [3] some obfuscation techniques include:

1. Self-Encryption and Self-Decryption

Certain viruses can encrypt and decrypt their virus code forms, hiding them from straight inspection. Viruses that employ encryption might use many layers of encryption or random cryptographic keys, which make each instance of the virus, look to be dissimilar, even though the fundamental code is the same.

2. Polymorphism

Polymorphism is a predominantly strong form of self-encryption. A polymorphic virus usually makes several variations to the default encryption settings, as well as changing the decryption code. In a polymorphic virus, the content of the original virus code body does not change but encryption varies its appearance only.

3. Metamorphism

The impression behind metamorphism is to modify the content of the virus itself, rather than hiding the content with encryption. The virus can be altered in numerous ways. For instance, by adding unnecessary code sequences to the source code or changing the order of pieces of the source code. The changed code is then recompiled to generate a virus executable that looks essentially dissimilar from the original.

4. Stealth

Stealth is a virus that uses various methods to obscure the features of an infection. Many stealth viruses hinder with Operating Systems file listings so that the reported file sizes reflect the original values and do not comprise the size of the virus added to each infected file.

5. Armoring

The intention of armoring is to write a virus so that it tries to prevent antivirus software or human experts from examining the virus tasks through disassembly, hints, and other means.

6. Tunneling

A virus that hires tunneling supplements itself into a low level of the Operating System so that it can interrupt low-level Operating System calls. By placing itself under the antivirus software, the virus endeavors to manipulate the Operating System to prevent discovery by antivirus software.

7. Mobile malwares

Malware is a malevolent software program that are planned to damage the hand-held devices such as smart phones, tablets and Personal Digital Assistant(PDAs).There are many types of malwares existing such as mobile phone virus, worms, trojan,

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

etc.[13] ,[8].

8. Mobile Virus

If a phone is infected, it can become a source for diffusing the virus by transferring texts and emails to other susceptible devices. These texts and emails can lure other users to open or download the virus. They also come in the form of malware that spreads through downloaded applications. Viruses insert themselves into one or more files and then perform some action.

9. Worms

Worms can spread from detachable media to computers (Compact Disks(CD), Universal Serial Bus(USB sticks, etc), Can move between mobile phones through(SMS or MMS messages over the telecommunications networks, or through Bluetooth wireless networks), worms can also spread between accounts on a social networking site such as Face book or Twitter. SMS-worm distributes copies of itself to new victims.

10. Trojan Horse

Trojan horse constantly requires user interaction to be activated. This kind of virus is usually inserted into apparently attractive and non- malicious executable files or applications that are downloaded to the device and executed by the user. Once triggered, the malware can serious harm by infecting and deactivating other applications or the phone itself, making it paralyzed after a certain period of time or certain number of processes.

11. Spyware

Spyware malware poses a threat to mobile devices by gathering, checking, using and dispersing user's personal or subtle information without the user's approval and knowledge The events logged by the spyware gathers email address, credit card number, key pressed by the user.

12. Adware

Adware comprises a commercial advertisement like games, desktop toolbars. It is a web based virus and collects the web browser especially in pop ups.

13. Rootkit

Rootkits are intended to take control of infected mobile devices by attaining administrator access of another device.

III. Counter Measures to malware

A. The network is the entry point to your application. It provides the first gatekeepers that control access to the various servers in your environment.

The elementary modules of a network that act as the front-line gatekeepers are the router, the firewall and the switch. As shown in Figure 1.

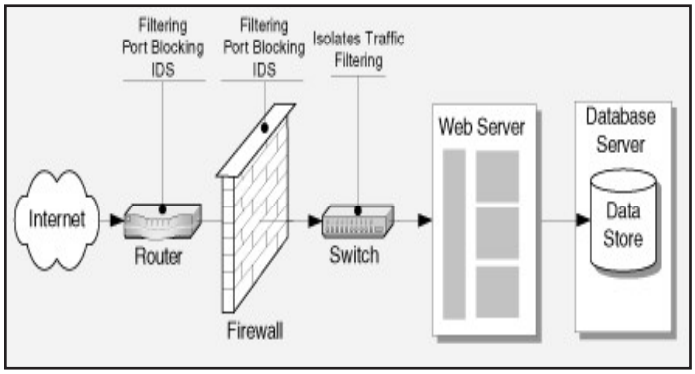

Fig. 1 : Adapted from [5].

B. Real-world countermeasures for the threats in wireless

Countermeasures and mitigation of malware [8], [11] everyone is open to threats in wireless network as no network is completely sure as secured. Therefore, network administrators and users must take extra steps in curbing security issues in wireless networks and put on countermeasures to reduce the risks of security issues. Some real-world recommendations for countermeasures to the threats in wireless networks from service providers' side include:

i. Change the default Service Set Identifier (SSID).
An attacker should not know the value for the SSID for the router and access point because that paves way for a break through to a wireless network.

ii. Turn On the Encryption
It is required that encryption must be turned on because It is much better than leaving the network as the open network. Precautions can be taken so that the attack is less probable to occur and more problematic to takeoff. Network administrators should set robust password to evade novice hackers from cracking it.

iii. Disable SSID Broadcast
If the SSID is broadcasted it can tell the existence of the network without any struggle. It is like inviting hackers to break into the network.

iv. Place the Access Point Securely
Control access to WiFi network, by putting the access point appropriately so that the signal is in the required radius.

v. Policy Enforcement
Provide a clear and plausible policy or contract of forbidden actions in wireless network. There is need for a written treaty of policy between employees and employers as from the first day of work. Employees may be given certain unique password to login into company's WiFi network and repeatedly reminded not to share the password and other sensitive credentials to others.

vi. Disable the WiFi adapter
To stop auto connection from the malicious access point in the network. Access point that will connect to the PC must always be monitored by configuring the setting in the PC.

vii. Secure Your Network
Users should use Virtual Private Network especially to stop MiTM attack. Firewall should be activated because it is a way to secure the network.

viii. Secure Your Confidentialities
Disable file sharing feature to mitigate the risk of the threats. Encrypt and set privacy to main folders as precautions when

using public WiFi.

ix. Prevent Auto Connection to Open WiFi Computers may automatically connect to the open wireless network without any warning. Wireless network should not be controlled remotely, always disable the network when not in use in a lengthy period of time.

x. Criteria for a secured network
Wireless networks development needs constant enhancements of network management to safeguard better connectivity and ease of access without putting security on the line.

xi. Flexible Connectivity
A decent network should be scalable and describe its parameter very well, for both indoor and outdoor access so it evade signal trickle to any unintended region

xii. Efficient Devices Management, Control and Monitoring
When hundreds or thousands of devices are connected to the network, it is vital to monitor and manage the applications and programs that they are using in the network.
Devices in the network need to be recorded and allocated unique IP from the network. To lessen, network access control and permit the users to register themselves to the network.

xiii. Filtering and Firewall
Users should not abuse the network by visiting malicious websites or run barred programs, filtering process must take place which in turn reduce the likelihood of users spreading virus to the core network. Every secured network should have combined firewall, intrusion prevention system and application identification and control.

xiv. Proper Network Segmentation and Segregation
To secure a network there should exist a clear and solid boundary of the core network and wireless network that can be accessed by the users, and hence elude unauthorized personnel to reach the core network intentionally or otherwise.

C. Major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment

From the studies of the authors [15], [14], [12], [9], [1] the main security areas that need to be given attention in order to uphold a reliable and secure ad-hoc network atmosphere include:

i. Confidentiality:
Information should not be exposed to unintended entitiesa thing that is difficult to achieve in ad-hoc networks because nodes (that act as routers) receive the packets for other addressees, so they can simply eavesdrop the information actuality routed.

ii. Availability:
A network without some good security procedures render its service performance and availability to be easily compromised, there is need to make ensure that network services are offered as is expected.

iii. Authentication:
The origin of a communication need to ascertain as is what it claims to be or from short of which an attacker would impersonate a node, and hence gaining illegal access to resource and sensitive information and interfering with operation of other nodes.

iv. Integrity:
Message that is transmitted is not changed.

v. Non-repudiation:
To ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message

Table 1. Layering based Attacks and Possible Security Approach

Layer	Attacks	Security Approach
Physical layer	Jamming and Tampering	Use spread spectrum techniques and medium access control (MAC) layer admission control mechanisms
Data link layer	Jamming and Collision	Use error correcting codes and spread spectrum techniques
Network layer	Sinkhole	Redundancy checking
	Sybil	Authentication, monitoring
	Wormhole	Authentication, probing
	Hello flood	Authentication, packet leashes by geographical and temporal info.
	Ack. flooding	Authentication, bidirectional link authentication, verification
Transport layer	Injects false messages and energy drain attacks	Authentication
	Flooding	Client puzzles
	De-synchronization	Authentication
Application layer	Attacks on reliability	Cryptographic approach

Adopted from [9]

IV. Discussion

Mobile handsets are becoming more smart and multifaceted in functionality, much like Personal Computers. Likewise, mobiles are more widely held than PCs, and are being used more and more frequently to do business, access the Internet, access bank accounts, and pay for goods and services. Malware is capable of undertaking many things, such as stealing and transmitting the contact list and other data, barring the device completely, giving remote access to criminals, sending SMS and MMS messages etc. Mobile malware causes severe public concern as more so because mobile phones are more in numbers than the population of PCs. [9]. Possible routes of mobile virus infection [2] include MMS, Bluetooth, IP connections via UMTS, Copying files, and Removable media, E- mail applications, Instant messaging (IM), Warez and Webpage browsing. Countermeasures and mitigation of malware [8], [11] everyone is open to threats in wireless network as no network is completely sure as secured. Therefore, network administrators and users must be extra serious in curbing security issues in wireless networks and put on countermeasures to reduce the risks of security issues. Some real-world recommendations for countermeasures to the threats in wireless networks from service providers' side include:

V. Conclusion

In this paper we have described types of attacks against mobile devices which are mainly theft of data, Phone Hijacking and Denial-of-Service (DoS). We provided the key aspects distinguishing mobile security from conventional computer security which is basically mobility, Strong personalization, Strong connectivity, technology convergence and reduced capabilities. We have listed ways in which mobile devices are infected with malware, Malware infection routes, Obfuscation techniques and finally we looked at counter Measures to malware. We found that the network is the entry point to an application. It provides the first gatekeepers that control access to the various servers in an environment. We describe real-world countermeasures for the

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

threats in wireless from the service provider's side. We finally provide major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. Many security issues in mobile malware infection and counter measures remain open we ponder to see many research activities done in this area

References

[1]. *B V Ramana Murthy, Vuppu Padmakar and A. Vasavi (2014) "Significances and Issues of Network Security" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 6,June 2014*

[2]. *Dong-Her Shih, Binshan Lin, Hsiu-Sen Chiang, Ming-Hung Shih, (2008) "Security aspects of mobile phone virus: a critical survey", Industrial Management & Data Systems, Vol. 108 Iss: 4, pp.478 – 494*

[3]. *Ilsun You & Kangbin Yim(2010) "Malware Obfuscation Techniques: A Brief Survey" 2010 International Conference on Broadband, Wireless Computing, Communication and Applications*

[4]. *Lamia Ketari and Mohammadi Akheela Khanum(2012)"A Review of Malicious Code Detection Techniques for Mobile Devices" International Journal of Computer Theory and Engineering Vol. 4, No. 2, April 2012*

[5]. *J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha*

[6]. *Marwa M. A. Elfattah, Aliaa A.A Youssif & Ebada Sarhan Ahmed (2011)"Handsets Malware Threats and Facing Techniques" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 12, 2011*

[7]. *Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra (2012) "A Survey on Security for Mobile Devices" IEEE communications surveys & tutorials, accepted for publication 1553-877X/12/$25.00 2012 IEEE*

[8]. *Mardiana Mohamad Noor and Wan Haslina Hassan (2013) "Wireless Networks: Developments, Threats and Counter measures" International Journal of Digital Information and Wireless Communications (IJDIWC) 3(1): 119-134 The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2225-658X)*

[9]. *Mahfuzulhoq Chowdhury ,Md Fazlul Kader and Asaduzzaman (2013) "Security Issues in Wireless Sensor Networks : A Survey "International Journal of Future Generation Communication and Networking Vol.6, No.5 (2013), pp.97-116*

[10]. *Peter Mell , Karen Kent and Joseph Nusbaum (2005) "Guide to Malware Incident Prevention and Handling" National Institute of Standards and Technology Special Publication 800-83 Natl. Inst. Stand. Technol. Spec. Publ. 800-83, 101 pages (November 2005)*

[11]. *Rakesh m goyal & ankur goyal (2008)"securing wi-fi network" Center for Research and Prevention of Computer Crimes*

[12]. *Radomir Prodanovi´c and Dejan Simi´c (2007) "A Survey of Wireless Security" Journal of Computing and Information Technology - CIT 15, 2007, 3, 237–255 doi:10.2498/cit.1000877*

[13]. *R.Dhaya , M.Poongodi (2014) "Mobile Virus Prevention Techniques: A Survey Perspective" International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1, March 2014*

[14]. *Rashmi pandey,Suresh Kumar (2011) "Apprehension of threats and countermeasures in semantic web services" Apprehension of threats and countermeasures in semantic web services International Journal of Internet Computing,Volume I, Issue 1,2011*

[15]. *Sreedhar. C, S. Madhusudhana Verma and N. Kasiviswanath (2010) "Potential security attacks on wireless networks and their countermeasure" International journal of computer science & information Technology (IJCSIT) Vol.2, No.5, October 2010*