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

Mobile Devices and Platform Security: A review on Mobile Device Malware and Botnets

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

Abstract
Smartphones and mobile devices are rapidly growing in their popularity in support of the current way of living. In this regard mobile botnets are also becoming more of a threat to users and network operators. The cell phones have gone online through the technologies such as EDGE, GPRS, UMTS and others. Cellphones are therefore exposed to the high risks caused by malwares, worms and Trojans that have been designed for mobile phone environment. The security threats caused phenomena is so severe that the hackers of mobile phones using malicious software can delete any data that belongs to individual users. The functionality of mobile phones has increased the attractiveness of the platform as a prey for attackers. Botnets depict a serious security threat on the Internet. Although security appliances exist, they are typically deficient for protecting against the latest breed of botnets, because botherders constantly develop new techniques and methods to discourage investigators. Due to the use of (WiFi, GPRS and 3G) in smartphones, building practical mobile botnets has become a key trend. This paper examines the possible threat of botnets and malware based on mobile networks and mobile device platform security. It then concludes by suggesting possible defense against these emerging threats.

Keywords
Malware, Botnets, Virus, Worms, Trojans

I. Introduction

Smartphones and mobile devices are rapidly growing in their popularity in support of the current way of living. In this regard mobile botnets are also becoming more of a threat to users and network operators. The cell phones have gone online through the technologies such as EDGE, GPRS, UMTS and others. Cellphones are therefore exposed to the high risks caused by malwares, worms and Trojans that have been designed for mobile phone environment. A botnet is defined as a set of compromised devices which can be controlled and synchronized remotely.
According to [6], the security threats caused by these malwares are so severe that the hackers infect mobile phones with malicious software that can delete any personal data. Although improvements in hardware and software have enabled more complex tasks to be done on mobile devices, this functionality has also increased the attractiveness of the platform as a target for attackers. Botnets depict a serious security threat on the Internet.

[6] further argue that a distinctive formation of botnet can be defined by the following steps:-

i. The perpetrator of botnet sends out worms or viruses to infect victims' machines, whose payloads are bots.
ii. The bots on the infected hosts log into an IRC server or other communications medium, forming a botnet.
iii. Spammer makes payment to the owner of this botnet to gain the access right.
iv. Spammer sends commands to this botnet to order the bots to send out spam.
v. The infected hosts send the spam messages to various mail servers in the Internet.

Botnets can be exploited for criminally purposes or just for fun, depending on the individuals.

A. Vulnerabilities and Security Challenges

Mobile device capabilities has heightened resulting in successive consumer adoption, people now perform their tasks both at work and in their personal lives as evidenced by [4], in this regard the mobile functionality has also increased the attractiveness of the platform as a target for attackers.
Many hosts worldwide have been infected by botnet which is widely spreading. Bots can spread across thousands of computers at a very high speed as worms. Unlike worms, bots in a botnet are able to work together towards a common malicious purpose as per [6]. [13] asserts that Botnet is similarly called zombie network. Zombie network is a network of infected computers (zombies) that permits cybercriminals to control the infected machines remotely without the owner's awareness. Of late, Zombie networks have become a basis of income for entire groups of cybercriminals.

There is need for mobile devices, such as smart phones and tablets to support multiple security objectives. To achieve these objectives, mobile devices should be secured against a variety of threats. The three common security objectives according to [8] are:

i. Confidentiality—guarantee that data cannot be accessed by unauthorized parties.
ii. Integrity – Data is consistent and correct, such that changes are made only by authorized persons.
iii. Availability - makes sure that users can access resources using mobile devices whenever needed.

This has been famously named as the CIA triad which gives the minimum requirements of the security of a system.

B. Mobile Malware

Mobile platforms gradually resemble traditional operating systems; the security threats characteristic for PCs are migrating to mobile devices. [2], [17], [1], [3] argue that the real attacks usually combine multiple variants of the following mobile malware:-

II. Trojan horse

A malicious mobile application is deployed by an attacker which then controls the device. The applications will execute a useful functionality and runs malicious activities in the background. In the process the Trojan is used to harvest personal information or to install other malicious applications. Trojans can also be used

carry out phishing activities.

A. Botnet

Botnet is used to hijack the power of computing to send spam mail and hence create Denial of Service attacks.

1. Worm

Worm is a self-replicating malicious application intended to disperse unconventionally to uninfected systems.

2. Rootkit

Rootkit gain the rights to run in a privileged is a malicious application which may gain the rights to run in a privileged way. Rootkit camouflage their presents from the user and changes standard operating system functionalities.

Malicious software is abundant in a world where accountability in computer users is minimal, these poses threats from various sources like the internet, local networks and portable drives. This situation makes Malware to be of high risk and can cause systems to malfunction paving way for stealing of data and even crash. In this way Malware may behave in the form of viruses, worms, Trojans, ultimately tampering with security of the system and breaching on user privacy. Although anti-virus software may be enough for home-users, a security risk from a new virus could threaten an entire enterprise network as supported by [9]

B. Mobile Device Security Recommendations

According to [10] they propose certain security techniques that are used to leverage and mitigate the risk of threats to mobile devices are explained below: -

1. Mobile device access

Power-on authentication – The remedy here is to require a power-on password or PIN, to enable the device not to be powered by any user. The proprietor need to provide a typical process for assigning user names and pins to be used while powering on the devices.

2. Auto-lock

The auto-lock involves configuring of the devices to automatically lock up after a certain period of time. In this case an authentication for access to systems that contain Protected Health Information (PHI) which is Two-factor authentication is a recommended.

III. Storage-Data encryption

This is a requirement for the establishment of data encryption for mobile devices. Identify the sorts of hardware and electronic media that are essential when tracking data such as hard disks, memory cards and the creation of inventory control systems.

1. Auto-run applications

This will prevent memory cards from automatically running specific programs.

2. Data transmission-Encryption

Implement and mandate appropriately strong encryption solutions for transmission of PHI. Access can be implemented over Secure Socket Layer, Internet Protocol Security (IP Sec) or a similar Virtual Private Network (VPN) technology. To allow only signed applications to be loaded onto the devices.

3. Data access-Role-based

Different users may require different levels of access based on job roles. Engage role-based access as part of a user-provisioning solution. There is need develop and utilize decent clearance procedures and uphold training of workforce members prior to granting access.

4. Logging and Auditing

The implementation of logging and auditing of mobile device as they interact with the parent network should ensure that the issue of illegal access of PHI is appropriately addressed in the required permission policy.

B. Mobile Botnets Possible Attacks

An infected mobile device can send Multimedia Message (MMS) or Short Message Service (SMS) to other mobile devices or to service numbers as argued by [6], [6] and [11]. Victims can be chosen by the botherder or they can randomly be chosen from the address book on the infected mobile device

Mobile devices are small and portable hence can be lost easily. Mobile devices are used to communicate between individuals or masses through both by voice and messaging, play games exclusively or with others on the Cyberspace, make payments, check the status of accounts from financial institution, store private information like contact information, personal information such as Social security numbers, Personal Identification Number codes, bank account numbers, personal pictures or business related information and other information that criminals can exploit and misuse for financial gain. Infected mobile device will be able to act as spyware in the same way as botclient on desktop computers collecting personal information and send it to the attacker.

Some of reasons why cellular bots are attracting cyber criminals from the study of [14] are:

i. Growing features and computational power of smart devices
ii. Users are not aware about threats and risk attached to smart devices
iii. There exist the use of free applications amongst end users
iv. Smart device aids tracking activities of its user
v. Open platform such as Android which encourages cyber criminals to develop malware operate on smart devices.

C. Mobile Device Security Challenges

Some of the few protruding challenges with the mobile devices threats and vulnerabilities as seen by [12] and [14] include:

i. Poor Authorization and Authentication: Poor authorization and authentication structures relying on device identifiers values for security are the perfect way for a failure and can lead to broken authentication and privilege access issues.
ii. Insecure Data Storage: Data stored on devices or cloud is left should not be left unprotected encrypting sensitive data, hiding of information not intended for long term storage, setting global file permissions to avoid exposure of sensitive information, privacy violations and non-compliance.
iii. Security Decisions via Un-trusted Inputs: Security decision should not be made via user input, to avoid leveraging by malware or client side injection of attacks for various wicked purposes such as consuming resources which are paid for, data and exclusive escalation.
iv. Sensitive Information Disclosure: If Login credentials, shared secret keys, access token, sensitive business logic is

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

hardcoded into the application code, then this presents the possibility of sensitive information being disclosed to an attacker by reverse engineering.

v. Broken Cryptography: The use of custom instead of standard cryptographic algorithms is a risk that originates from insecure development practices like, assumption that encoding and obfuscation are equivalent to encryption and cryptographic keys being hardcoded into the application code itself.

vi. Insufficient Transport Layer Protection: Security of mobile applications is danger because there is absence of encryption for transferring data.

vii. Server Side Controls: If proper security controls are not implemented in way of patches and updates, secure configurations, changing default accounts or disabling unnecessary running services, in the backend services can result in compromise and confidentiality and data integrity risks.

viii. Client Side Injection: Mobile applications are witnessing newer attacks such as abusing phone dialer, SMS and in application payments.

ix. Improper Session Handling : Sessions should have shorter expiry time and not using device identifiers as session id because it poses security risks such as privilege escalation, unauthorized access etc.

x. x. Side Channel Data Leakage: Programmatic flaws or not disabling insecure Operating System (OS) features in applications result in data leakage thereby making sensitive data end up at places like web caches, global OS logs and screenshots temporary directories are available for malware or an attacker who manages to get the mobile device.

D. Mobile threats

Mobile threat is defined as any malware that targets smart phones and PDA. According to [13], [12] the various security threats that can affect mobile devices are as follows.

a) Application Based Threats

Applications downloaded introduces many security threats on mobile devices, including both software specifically designed to be malicious as well as software that can be exploited for malicious purposes.

i. Malware
Malware is software designed to engross in malicious actions on a device. Malware can be used to steal personal information from a mobile device that could result in theft or financial fraud.

ii. Spyware
Spyware is designed to collect or use data without a user's awareness or authorization. Data commonly targeted by spyware includes phone call history, text messages, placement, web browser history, contact list, electronic mail, and photographic pictures.

iii. Privacy threats
Caused by the applications that is not necessarily malicious, but gathers or uses more sensitive information than is necessary to perform their function or than a user is comfortable with.

iv. Vulnerable applications
Contain software vulnerabilities that can be exploited for malicious purposes. Such vulnerabilities can often allow an attacker to access sensitive information, execute undesirable actions, halt a service from functioning right, and automatically download extra applications.

b) Web-based Threats

Since mobile devices are often connected to the Internet and used to access web-based services, web-based threats pose issues. These threats include:-

i. Phishing Scams
Use web pages or other user interfaces designed to trick a user into providing information such as account login information to a malicious for the user.

ii. Party Posing as a Legitimate service Attackers often use email, text messages, Face book, and Twitter to send links to phishing sites.

iii. Drive by Downloads
Automatically begins downloading an application when a user visits a web page.

iv. Browser Exploits
Browser Exploits are designed to take advantage of vulnerabilities in a web browser or software that can be launched via a web browser such as a Flash player, PDF reader, or image viewer.

c) Network-Based Threats

Mobile devices typically support cellular networks as well as local wireless networks. There are a number of threats that can affect these networks:

i. Network Exploits
It takes advantage of software flaws in the mobile operating system or other software that operates on local (e.g., Bluetooth, WI-Fi) or cellular (e.g., SMS, MMS) networks.

ii. Wi-Fi Sniffing
This compromises data being sent to or from a device by taking advantage of the fact that many applications and web pages do not use proper security measures, sending their data in the clear (not encrypted) so that it may be easily intercepted by anyone listening across an unsecured local wireless network.

iii. Mobile Network Services
Cellular services like SMS, MMS and voice calls can be used as attack vectors for mobile devices. The cellular services provide opportunities for phishing attacks. Phishing is an attack strategy in which the attacker gains sensitive information from the user by presenting itself as a trustworthy entity. Two basic phishing attacks over mobile networks exist: Smishing and Vishing. Smishing attacks are executed using SMS messages. Vishing attacks are carried out using voice calls.

d) Physical Threats

Since mobile devices are portable, their physical security is an important consideration.

i. Lost or Stolen Devices
The mobile device is valuable not only because the hardware itself can be re-sold on the black market, but more importantly because of the sensitive personal and organization information it may contain.

ii. Computing Resources
The increase in computing resources is setting the contemporary mobile devices into focus for malicious attacks with aim to covertly exploit the raw computing power in combination with broadband network access.

iii. Internet Access
Mobile devices can access the Internet using Wi-Fi networks or 3G/4G services provided by mobile network operators. Although such high speed Internet connections ensure comfortable browsing, they also expose the mobile devices to the same threats as PCs. Since mobile devices are usually constantly switched on, they can maintain a continuous connection to the Internet. However, prolonged connection to the Internet also increases the chances of a successful malicious attack.

iv. Bluetooth
Bluetooth attacks are a method used for device-to device malware spreading. Once the two devices are in range, the compromised device pairs with its target by using default Bluetooth passwords. When the connection is established, the compromised device sends malicious content. Consolidating all the above issues the following Table 1 compares the various mobile threats.

IV. Vulnerabilities and Security Challenges

From the studies of [8], and [5] the vulnerabilities and security challenges include:

A. Device-based mobile application vulnerability exploitation

Using the information gathered during the vulnerability identification phase, attempts to exploit the identified application vulnerabilities should be performed through some of the procedures outlined below:

1. Authentication and session management

Due to usability restrictions, mobile aapplications use many new approval techniques, such as swipe patterns, to reduce the password complexity. Application authentication mechanisms should be verified in order to bypass these controls or access another user's data. Once authenticated, the application's session management should be reviewed. By observing how the application keeps track of users, a tester can assess if it is possible to replay a session or predictably jump to another user's session.

2. Authorization

Application permissions on the device should be defined with specificity. These controls prevent devices from being exploited to gain further access to the device or its features. Within the context of the application, attempts to gain access to functions that a normal user would not have permissions to execute should be performed.

3. Input validation

By mapping out areas of input into the application and observing the output, a security assessment can determine if client-side JavaScript can be inserted and executed in the browsers of other targeted application users. This could potentially allow for the harvesting of other users' session credentials and/or application usernames and passwords.

4. Data storage

Many applications collect usage data regarding their users. This data may be overly invasive and could conflict with user privacy. This data should be reviewed to determine what data is collected and stored by the application and how it is accessed. A test should be performed to determine if the data is accessible to unauthorized users or third parties.

V. Possible Defense of Mobile Device Malware and Botnets

A. Recommendation for mobile security [13] recommends the following.

i. Add mobile security to existing employee security awareness programs.
ii. Create and implement an Information Technology policy that governs usage and ensures employees' understanding.
iii. Perform threat modeling to identify the risks of moving applications to a mobile platform.
iv. Train application developers in secure coding practices for mobile device platforms.
v. Limit the sensitive data transferred to mobile devices, or consider view-only access.
vi. Utilize Mobile Device Management software to create an encrypted password-protected sandbox for sensitive data and enforce device-side technical policies.
vii. Perform technical security assessments on mobile devices and the supporting infrastructure — focus on device-side data storage.
viii. Establish a program that continually evaluates new and emerging threats in mobile platforms.
ix. Increase monitoring controls around mobile device connection points when feasible.
x. Assess classic threats against web-based applications and infrastructure

B. Platform and security architecture

Table 1 : (Adopted from [16])

Risk	Remedies
Data lost due to lost or stolen devices	• User authentication at the device level • Remote lock and wipe • Data encryption • Data control
Unauthorized user accesses data with a lost or stolen phone	• User authentication at the device level • Remote lock and wipe • Data encryption • Data control
Authorized user gains unauthorized access to, or makes inappropriate use of, proprietary information	Security policies • Mobile application provisioning and settings • Remote configuration updates • Event and activity monitoring and logging
Risks arising from combining personal and work use in one device	Security policies • Segregating business functions on the mobile device

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

	• Remote data wipe • Data fading
Gaps in device management and policy enforcement	• A single security management platform

Preventive measures that can be taken by users as a security solution required specifically for smart/ cellular devices [14]

i. Users should not rely only on operating system to protect themselves from attacks. Owners are supposed to use antivirus and anti- malware software on smart devices too.
ii. They should install applications only from trusted sources developed by trusted developers.
iii. Read and check default permission required by the application before installing.
iv. Use up-to-date software and operating system.
v. Avoid accessing sensitive information over public networks which are not having password or encryption strategy.

C. Mobile botnets defense mechanisms

The following defense techniques against mobile botnets should be used [11]

i. Antivirus Scanning
ii. Intrusion Detection System (IDS)
iii. Firewalls
iv. Packet Filtering
v. Monitoring at SMSC
vi. Infiltration
vii. Building International Co-ordinated Mechanism

VI. Discussion

Mobile device security concerns create a new business dilemma for innovative SMEs that over the last five to eight years have become early adopters of the latest technology breakthrough in mobile technologies. Technology has evolved from stand-alone PCs to dial up internet, then broadband internet with wireless networks, and finally, the recent introduction of smartphones and tablets as supported by [9].

One of the traditions that mobile devices security can be enhanced is through two-step authentication system. Which consists of a server connected to a GSM enabled service provider and a mobile phone client equipped with SMS receiving functionality. This system involves an accomplishment where corporate server web application authorize customer with username or password, then connect with a service provider who will create token and send token to customer via SMS returning transaction ID, asking customer to enter token, then match entered token against transaction id obtained from service provider according to [15].

[14] argue that Mobile Network Operators and service providers ought to maintain security policy for their customers. They can create a secure atmosphere for customers by using proper and sufficient preventive measures to protect their users. Concurrently, cellular application developers should take care while creating applications to use proper channels for communication between application and device related data.

VII. Conclusion

A lot of sensitive individual and commercial information, such as login credentials, credit card details, account details, private contact entries, invoices, purchase orders among others, are being kept or communicated through mobile applications. The advancement in the creation and maintenance of secure identities for mobile devices has created challenges for individuals, society and businesses particularly in mobile added value services (mobile banking, mobile check-in, mobile ticket, etc.) and government security services as supported by [12]. A risk management and security framework is needed to protect applications and data on mobile devices when they are lost. Since the physical security of mobile devices can change, access control should be managed in accordance with the threat plane. This paper gives a description of the measures and gives suggestion defenses for combating botnets, applying measures contributes to important results in defense against botnets in the mobile platform which is becoming an important part of our daily lives.

Reference

[1]. Alice Hutchings (2012) Computer security threats faced by small businesses in Australia. Trends & issues in crime and criminal justice No. 433 February 2012

[2]. Ammar Ahmed E. Elhadi, Mohd Aizaini Maarof and Bazara I. A. Barry (2013), Improving the Detection of Malware Behaviour Using Simplified Data Dependent API Call Graph. International Journal of Security and Its Applications Vol.7, No.5 (2013), pp.29-42

[3]. D. Roselin Selvarani & T. N. Ravi (N.D) Issues, Solutions And Recommendations For Mobile Device Security Issues, Solutions And Recommendations For Mobile Device Security" International Journal Of Innovative Research In Technology & Science. Volume 1, Number 5,

[4]. Keunwoo Rhee, Woongryul Jeon and Dongho Won (2012), Security Requirements of a Mobile Device Management System. International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012

[5]. Kyung Jin Cha and Joon Seub Cha (2014), The Common Challenges to the Successful Implementation of SmartWork Program. International Journal of Multimedia and Ubiquitous Engineering Vol.9, No.2 (2014), pp.127-132

[6]. Jing Liu, Yang Xiao, Kaveh Ghaboosi, Hongmei Deng, and Jingyuan Zhang(2009), Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures. Hindawi Publishing Corporation EURASIP Journal on Wireless Communications and Networking Volume 2009, Article ID 692654, 11 pages doi:10.1155/2009/692654

[7]. Mark A. Harris and Karen P. Patten (2014), Mobile device security considerations for small-and medium-sized enterprise business mobility. Information Management & Computer Security Vol. 22 No. 1, 2014 pp. 97-114

[8]. Murugiah Souppaya & Karen Scarfone (2012), Guidelines for Managing the Security of Mobile Devices in the Enterprise. NIST Special Publication 800-124 Revision 1

[9]. Priyank Singhal and Nataasha Raul (2012), Malware Detection Module using Machine Learning Algorithms to Assist in Centralized Security in Enterprise Networks. International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, January 2012

[10]. PrashantJawade & Suwarna S. Thakre 2013), Physical Security for Mobile Devices Using Novel Application Lockbox. International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 5, July 2013

[11]. Rizwan Ahmed & Rajiv V. Dharaskar (2012), Study of

Mobile Botnets: An Analysis from the Perspective of Efficient Generalized Forensics Framework for Mobile Devices. National Conference on Innovative Paradigms in Engineering & Technology (NCIPET-2012)Proceedings published by International Journal of Computer Applications (IJCA)

[12]. Sujithra. M & Padmavathi .G, (2012), Mobile Device Security: A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism. International Journal of Computer Applications (0975 – 8887) Volume 56– No.14, October 2012

[13]. Sagar A. Yeshwantrao,Vilas J. Jadhav(2014), Threats of Botnet to Internet Security and Respective Defense Strategies. International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 1, January 2014)

[14]. Sonali Tidke.(2014), Mobile Botnet: A Threat to User Privacy. International Journal of Advanced Research in Computer Science and Software Engineering 4(2),February - 2014, pp. 907-910

[15]. Stefan Certic (N.D), The Future Of Mobile Security. Http:// www.cs-networks.net, Retrieved July 31, 2014

[16]. Sybase, Inc. (2011). Mobility Advantage Why Secure Your Mobile Devices. www.sybase.com. Retrieved July 31, 2014

[17]. Tala Tafazzoli and Seyed Hadi Sadjadi (2008), Malware fuzzy ontology for semantic web. IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.7, July 2008