A survey on smartphone security

Di Liu
China United Network Communications Group Company Limited Postdoctoral Workstation, Beijing, China

Ni Zhang
China Unicom Research Institute, Beijing, China

Kun Hu
China United Network Communications Group Company Limited Postdoctoral Workstation, Beijing, China

Abstract—**This paper proposes a survey on smartphone security from the aspect of mobile malware, specifications related to smartphone security, and smartphone security solutions. The contribution of this paper helps people to quickly know about definition of malware, attack channels and black industry chain of smartphone security, international and domestic mobile security specification, and smartphone security solutions by security vendors.**

Keywords-smartphone security; malware; mobile secutity

I. INTRODUCTION

With the development of wireless access technology and smartphone, traditional internet gradually evolves to mobile internet. The mobile internet is a hybrid among terminal, wireless, core network, and internet with a complicated network structure. Besides the emergence of mobile internet brings out a wide range of business opportunities for industry members, government, operator, vendor, CPs, and SPs, many security challenges rise. These include not only traditional security threats from internet, e.g., vulnerabilities of TCP/IP network protocol but also new threats, e.g., vulnerabilities of operation system of smartphone, malware stealing money from subscribers' account by the characteristic of user's smartphone identity binding subscription expense. These new threats all focus on smartphone. In 2010, there are approximately 8 million smartphones infected by mobile malware in China [1]. The mobile malware not only makes smartphone unavailable to ring up a call or send a short message, but also steal personal privacy information and expense from smartphone. During malware break out, it occupies a large amount of network resource, which is harmful to development of mobile internet industry and smartphone.

To protect smartphone against from malware, both technical and management aspects should be considered. For technical aspect, terminal, network, and service three layers security solution for smartphone should be figured out. For management aspect, industry ecosystem members of mobile internet should cooperate to discuss this issue, and eventually government grants some smarphone security regulations, e.g., anti-malware policies. Thus, in order to make people quickly pay attention to the mobile phone security, this survey paper demonstrates related knowledge, e.g., definition, features and classifications of mobile malware, attack channels of malware, an analysis on black chain and business model of mobile malware, specifications related to smartphone security and many anti-malware solutions by vendors.

The rest of this paper is organized as follows. The section II introduces definition, infected channel and black chain of mobile malware of malware. Then the next section will present different international and domestic specifications related to smartphone security. Section IV proposes smartphone security solutions by native vendors. A conclusion will be provided in the last section.

II. MOBILE MALWARE

A. *Mobile malware*

Mobile malware is a kind of software downloaded to the smartphone, running, and doing illegal actions, e.g., stealing subscriber's privacy information or expense from their account without any subscriber agreement or prompt. Malware has characteristics including:

1) Mandatory installation;
2) Difficult to uninstall;
3) Browser infection;
4) Gathering user privacy information.

At present, there are five common malware, namely virus, worm, Trojan, botnet, and spyware.

1) **Virus** is a self-replicating program which enables to infect operation system of smartphones, spreading among smartphones. Its aim is to delete or alter subscriber's data on handset.

2) **Worm** is a self-replicating, widely spread malicious program that may not infect system files of smartphone. The main purpose of worm is to occupy system and network resources.

3) **Trojan** is a malicious program which disguised as legitimate software, installing on users' computer performs some malicious operations without any user's awareness, e.g., backdoor Trojan which usually contains a keyboard logger, spy Trojan stealing account Trojans, etc.

4) **Botnet** is a program that attacker can control many smartphones infected with zombie programs to perform malicious acts at the same time, such as DDOS attack on a targeted web site, or sending lots of spam text messages to a specific destination, etc.

5) **Spyware** is a program that has the ability to collect mobile phone user's data and send them to the third party without any user awareness or permission. For example, this program monitors keystrokes of mobile phone, collects confidential user information, such as IMSI, IMEI, password, credit card number, and personal identification password. It also steals e-mail addresses or tracks a user's browsing behaviors.

Published by Atlantis Press, Paris, France.

B. *Infection channels of malware*

According to the 2011 NetQin mobile security report [2], approximately 79% infected smartphone users download malicious software by the network, 13.6% of them were infected by sending SMS/MMS, 4.2% of them through Bluetooth, 3.2% of them via a memory card or other transmission ways. It is conclude that mobile internet and WAP is essential infection channel and SMS\MMS is another important channel. Therefore, it needs to focus on addressing malware problem from network and SMS\MMS, in order to reduce largely infection ratio.

C. *Black industry chain of malware*

Behind the mobile malware outbreaks, a black industry chain is hidden which consists of the following roles.

- **Employers**: A criminal group, bad SP or CP wants to spread their business information to the user forcedly.
- **Channel agent**: It is responsible for business promotion, information propagation, and proposed scheme in anyway.
- **Hackers**: It takes the responsibility of malware technical support, e.g., writing malicious code, controlling botnet, sending spam text messages, or attacking specific users as employers' need.

Black industry chain has two work modes:

Mode 1: Added value SP and smartphone manufacturers cooperate to install built-in malicious programs before handset selling. Users buy and use these infected mobile phones without any awareness.

Mode 2: Criminal group and SP distribute the malicious software on internet, and hacker controls the infected smartphone, stealing user private information, sending spam messages or doing any illegal actions.

III. The Specifications Related to Smartphone Security

Nowadays multiple international and domestic specification organizations, e.g., GSMA, ITU, OMA, and CCSA have paid attention to smartphone security against mobile malware. Their work are shown respectively as follows.

A. *GSMA*

GSMA security group (SG) had a research on smartphone security requirements from an operator's perspective.

A guide to mobile malware [3]

This project started in 2009, the goal was for operators to provide security guidelines for operators to determine how to effectively face to the challenges of mobile malware, providing the best practice and control measures, as to ensure operators safely access to information and resources. The project included two main parts:

1) Control strategy for mobile malicious software technologies, including Terminal control, network control, equipment control, server management, application authentication, and management strategies including real time management and emergency management.

2)Definition, characteristics, and trends of the mobile malware, and analysis of the industry chain.

Remote Mobile Malware Removal Study [4]

This work defined malware, provided application security testing process, and studied how to remotely remove malicious software in the application shop.

The Mobile device security patching [5]

This work was responsible for collecting and discovering weaknesses on operating systems of smartphones, shared with industry bug-fixing techniques, in order to accelerate mobile security problem solving processes on the prospective of technology and industry.

B. *OMA*

OMA ARC-SEC group had a research on mobile phone security, i.e., project of autho4API [7] and Spam report [16].

Auth4API

The Auth4API originated from IETF Oauth 2.0 [8], aiming at building a security mechanism of network programming interface in order to prevent the third party malicious application installed on mobile phone obtaining the user's user name and password, accessing to the user's protected resource.

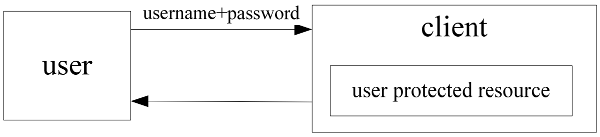

Figure 1. Traditional CS module

Traditionally, users who want to access their privacy data in the Client/Server (CS) mode must input their username and password to log in, as shown in the Fig.1. It is inevitable that applications enable to get their username and password. If the application is infected with malicious code, attackers will remotely access the users' protected resource. As emergence of open platform, the user's protected resources are often stored in open platforms. Under this scenario, the possibility of third party application carrying malicious code is bigger than CS mode. If users' username and password are sent to third party application through network programming interface, and user has no awareness on changing their password, some malicious application will access user's protected resources. To resolve this problem, Auth4API established security framework of network programming interface, as shown in Fig.2.

From the Fig.2, firstly, the third party application sends a request to the user mobile terminal. Secondly, if user agrees, an access grant approved by user will be sent to the third party application. Note that user does not need to share password with the third party application. Then the third party application sends user access grant and client information to authorization server on the open platform through API. After that, if authorization process is approved, the authorization server sends an access token back to the third party application through API. Fifthly. the third party application sends the access token to the resource server on the open platform. Finally, the resource server sends the

Published by Atlantis Press, Paris, France.

protected resource it required back to the third party application.

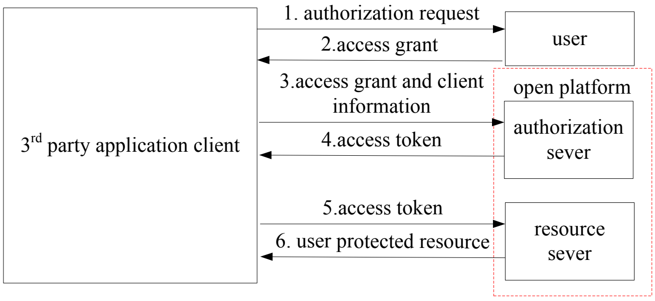

Figure 2. Autho4API framework

Mobile spam reporting (SpamRep)

The project was to implement a reporting mechanism that sent a report to the short message server when the user received a spam message. The spam report was demonstrated as follows.

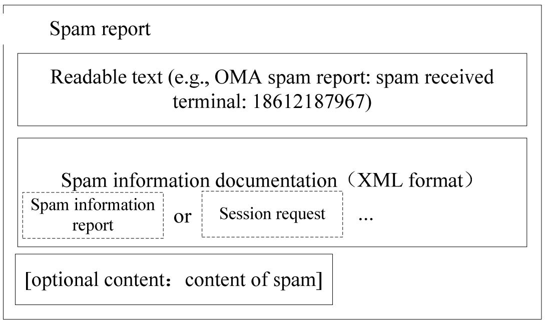
Spam report
Readable text (e.g., OMA spam report: spam received terminal: 18612187967)
Spam information documentation（XML format）
Spam information report
or
Session request
...
[optional content：content of spam]

Figure 3. Structure of spam report

A spam report contained human-readable text, spam information documentation, and optional content of the spam report. The human-readable text described the terminal address of received spam, the spam information document is a form of machine-readable XML, containing spam reporting or a Terminal-Server session requests. The optional content included the contents of the spam. SpamRep helped the short message server add spam source to the blacklist, preventing further sending spam to other users.

C. ITU

ITU SG17 group [10] launched a recommendation on security aspects of mobile phones in September 2009. The project led by the Research Institute of RITT, sought to establish a universal terminal security framework, made an analysis on main terminal security threats, security requirements, and security mechanisms in detail as follows.

1) The project listed security threats of privacy of mobile terminal, internet security threats, non-authorized access, threats on peripheral interface, mobile malware, spam text messages, threat on location based service, malicious calls attack, etc.

2) The project discussed security requirements of the hardware, the operating system, application, users' data on the mobile phone, and communication.

3) According to the requirements, the project showed security mechanism, e.g., validation mechanisms, operating systems security mechanism, conformance testing, privacy, encryption, remote control, data cleaning, junk SMS filtering, anti-malware solutions, digital signatures and trusted applications, backup software, security booting, etc.

D. CCSA

CCSA TC5, TC8, and TC11 groups involved mobile security-related technical standards.

Study of the mobile security threats and solutions [11]

This TC8 and TC5 group joint project was established by Research Institute of RITT, discussed security threats of mobile terminals, addressed security solutions related to information storage, lost, stolen, malicious software, peripheral interface of mobile terminals, and provided a mobile device security framework, as shown in the Fig.4.

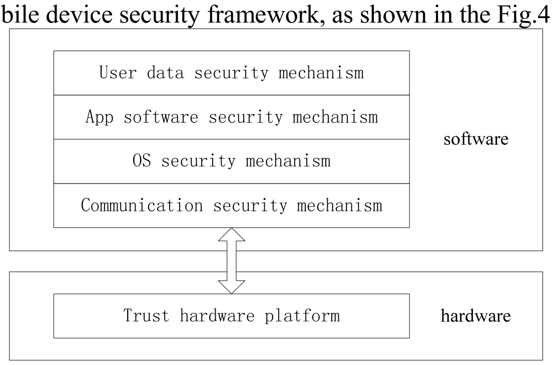
User data security mechanism
App software security mechanism
OS security mechanism
Communication security mechanism
software
Trust hardware platform
hardware

Figure 4. Mobile terminal security framework

The mobile malicious software defense scheme [12]

This TC11 project was led by China Unicom, undertaking a comprehensive analysis of mobile malware issues, discussed the source of attacks, attacking channels, as well as the final attack goal, and provided suggestions for controlling mobile malware from the industrial, technical and other aspects.

The information security technical requirements of mobile terminals [13]

This TC11 project was led by Research Institute of RITT, discussed security requirements for mobile terminals specifying the security capabilities requirements for mobile terminal, including hardware, operating system, peripheral interface, application, and data protection security requirement.

IV. SMARTPHONE SECURITY SOLUTION

To protect against malware, many solutions i.e., smartphone security products have been developed in the mobile phone security industry. As shown in the table 1, 360 [6], NetQin [8], Kingsoft [9], and Rising [15] mainstream security vendors have launched their security products on domestic market, respectively. The table 1 makes a comparison

TABLE I. SMARTPHONE SECURITY SOLUTION

vendor	Products	Supported OS	Size	Interception	Anti-malware	Cloud-based anti-malware	Traffic monitor	Privacy protection	Remote control
Kingsoft	Kingsoft handset bodyguard	Android\Symbian	2.2M	√	√	√	√	√	√
Netqin	NetQin security safeguard	Symbian\Android\ Blackberry OS\Windows mobile\iOS	2M	√	√	√	√	√	√
	Communication administrator	Symbian\Android\ Blackberry OS\ Windows mobile\iphone	3.3M	√				√	
	NetQin safeguard	Symbian\Android	970k				√		
360	360 handset safeguard	Symbian\Android \iOS	2.7M	√	√	√	√		√
	360 Payment bodyguard	Android	658k		√			√	
	360 Anti-Trojan	Android\Symbian	34.7k\127k		√				
	Xinanyi Mobile firewall	Symbian\linux\ Windows mobile\ Smartphone\iOS	300-700k	√	√			√	
Rising	Rising handset anti-virus	Symbian\Android	1.38M\439K	√	√	√			√

on different security features, e.g., supported OS, file size, interception function, anti-malware (anti-Trajon, virus, botnet), cloud-based anti-malware, traffic monitor, etc, among different security products. It can be summarized from the table as follows.

For Android, and Symbian platforms, NetQin, 360 and Kingsoft have been developed related security products. For the Windows Mobile platform, NetQin and 360 have developed corresponding security products. For the iOS and Blackberry OS platform, currently its corresponding market is still relatively small in China. iOS has high security and close characteristics itself except jailbreaking. And the number of the Blackberry handset users is so small that security need is not remarkable.

As to the security product features, basically each vendor has at least a full-featured security products, like Kingsoft handset bodyguard, NetQin security safeguard, etc. And phone security features can be divided into basic feature and extended feature. The basic features as blocking spam SMS, anti-virus, traffic monitoring, data privacy protection, etc. And extended features are like data backup and some customized functionalities, e.g., volIP or location hidden.

V. CONCLUSION

At present, the mainstream mobile phones security vendors have sophisticated basic anti-malware ability, but still have big room to develop the extended functionalities, especially for enterprise BYOD or specific field customers. In the BYOD scenario, some sensitive data, e. g., employees' ID number, password, credit card number, and enterprise data, are shown on their own smartphones. Thus, how to protect these sensitive data against mobile malware is a new issue. Security vendors should pay more attention on need of BYOD, which can produce a new business opportunity in future.

REFERENCES

[1] J. Chen, M. Fan, "Signatures extraction method based on classification of malicious software", Journal of Computer Applications vol. 31 Suppl. 1, p.83-85, 2011.

[2] "NetQin mobile phone security report on May 2011", NetQin Inc., 2011.

[3] "Operator guide to mobile malware", GSM Assoiction Offical Document SG19, Dec, 2008.

[4] "Remote Mobile Malware Removal Study" GSM Assoiction Offical Document GSON6, May, 2011.

[5] "The Mobile device security patching", GSM Assoiction Offical Document SG26, Apr, 2012.

[6] "360 security center",URL: http://www.360.cn/.

[7] "Authorization Framework for Network APIs", Version 1.0, Open Mobile Allianc, OMA-ER-Autho4API-V1_0, URL:http://www.openmo

bilealliance.org/

[8] "NetQin security", URL:http://cn.nq.com/.

[9] "Kingsoft handset bodyguard", URL:http://m.ijinshan.com/.

[10] ITU-T SG17: Security Group. URL:http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx

[11] "Study of the mobile security threats and solutions", CCSA TC8 WG2 Offical Document, 2011.

[12] "The mobile malicious software defense scheme", CCSA TC11 WG2 Offical Document, 2011.

[13] "The information security technical requirements of mobile terminals", CCSA TC11 WG2 Offical Document, 2012.

[14] "The OAuth 2.0 Authorization Protocol", URL:https: //datatracker.ietf

.org/doc/draft-ietf-oauth-v2/

[15] "Rising security ", URL: http://www.rising.com.cn/.

[16] "Mobile spam report", Version 1.0, Open Mobile Allianc, OMA-ER-SpamReport-V1_0, URL:http://www.openmobilealliance.org/