Mobile security threats on smart phone

Tae Woon Kang[1], Yadigar Imamverdiyev[2], Ramiz Shikhaliyev[3]

[1]*National Research Foundation, Seoul, Korea*

[2,3]*Institute of Information Technology of ANAS, Baku, Azerbaijan*

[1]kungurum.kang@gmail.com, [2]yadigar@lan.ab.az, [3]ramiz@science.az

***Abstract*—With the widespread use of smart devices and ubiquitous sensors, new mobile security threats are produced. In this paper, we identified mobile security issues in ICT converging environment, and security threats due to smart phones, and research subjects for mobile security.**

***Keywords*— mobile security, smart phone security threats, mobility aspects, ICT convergence**

I. INTRODUCTION

While wired and wireless network infrastructure is steadily improved and also ubiquitous technology is gradually spread, smart phones and sensors have increased rapidly in number. Smart phones representing smart devices and ubiquitous sensors unrecognized by common people have become essential part of day-to-day life. Most smart devices and sensors are moving always, and changing their managers frequently, and also creating a variety of ad-hoc networks often.

In the past mobile security issues were mainly raised by a lack of technical capability for ICT mobility. Now it is due to improper apps for smart devices as well as imperfect and immature technologies of platforms. And besides technical issues on mobile security, an insufficient recognition of particular organizations, such as company, institute, and government agency becomes more critical issues for mobile security.

II. SECURITY DOMAINS OF ICT CONVERGING ENVIRONEMNT

The rapid ICT convergence is taking place over industrial sectors, security issues also raised extensively. From technical aspects, security issues of an ICT converging environment could be presented in 5 security domains as in Figure 1. [1], [2]

Mobility of ICT is one of the key drivers to make the convergence of industrial sectors. A smart phone, representing smart device such as ubiquitous sensors and smart TVs, is already located at the center of ICT converging industries.

A. Future Network Security

Future Network Security is for NGN (New Generation Network) and Future Internet security, which include mobility structure and procedures between NGNs and heterogeneous networks, and for Future Internet.

Mobile security issues focusing on converging communications/broadcasting/computing/sensors are especially for Future Internet.

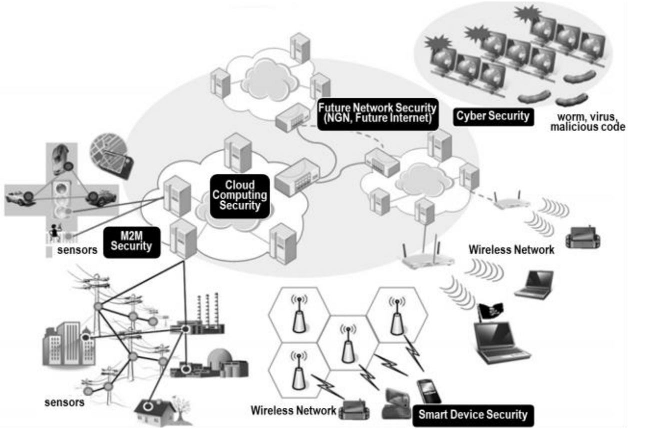

Figure 1. Security domains of ICT converging envirenment

B. Smart Device Security

Smart Device Security is for smart phone platforms, apps, and interfaces (logical and physical) to external networks and other smart devices.

For smart phone security, various security issues due to leakage of personal data and significant privacy issues in social media services are included.

C. M2M Security

M2M (Machine to Machine) security covers extremely diverse issues for industries, such as u-city, u-healthcare, u-surveillance, u-vehicle, u-logistics, smart energy (smart grid), smart education, smart home and etc.

M2M security is basically for a secure and robust communication between nodes and sensors, which includes mechanisms and procedures for each of M2M services. Furthermore M2M security covers particular requirements for specific M2M-based applications of ICT converging industries. For an example, u-healthcare security includes some particular mechanisms and procedures to keep the personal medical information quite safe.

D. Cloud Computing Security

Cloud computing security is for virtualization of IT resources, distributed computing, SLA (Service Level Agreement) and ownership of data in order to build a large-scale IT resource pool and to realize utility computing.

Cloud computing is a very different way to existing one in which we use downloaded data on our PC. But a cloud computing environment, which we place data in, raises a

Prof. Tae Woon Kang is a visiting scientist assigned to Institute of Information Technology of ANAS from National Research Foundation (NRF) of S. Korea.

unique set of security, compliance and privacy risks. Considering mobility of smart devices that might be highly computing powered mobile devices, the types of cloud computing security would be what we have never experienced.

E. Cyber Security

Cyber security is for information sharing and integrated control for cyber attack, and malicious code correspondence.

Information sharing and integrated control for cyber attack include the sharing of information between the relevant agencies to respond to DDoS (Distributed Denial of Service) attacks, and also a systematic and comprehensive integrated real-time control for wired and wireless integrated networks.

Malicious code correspondence includes the Bot-net detection and response, the collection and analysis of malicious code, automatic classification, and source/transit location detection.

It couldn’t be worse for us to understand legacy types of cyber security in existing Internet. But new cyber security attacks and intrusions by using smart phone will be persistently developed and sophisticated. And severity of cyber security threats due to smart phone will be rapidly increased in the near future.

III. SECURITY THREATS OF SMART PHONE

Because of openness, portability, and performance constraint of smart phones, they have been exposed to new security threats with the existing PC environment security threats. The smart phone security threats on this environment can be defined as follows: [2], [3]

- Openness: A variety of external interfaces and standard APIs (Application Programming Interface) for a smart phone is provided not only a convenient use to the user, but also a convenient environment to the malicious developers. Malicious code could be easily built in Apps on smart phones, and also propagated in various paths via a variety of external interfaces.
- Portability: A smart phone has high ease of using, but high risk of loss or theft too. Loss or theft is causing the direct economic damage, and leakage of confidential personal information as well as critical business information.
- Performance constraint: Compared to the PC, a smart phone is a low-power, low-performance device. It is unreasonable to install all necessary security software including vaccines for the PC to the smart phone.

These smart phone security threats can be distinguished in 5 regions of real mobile environment, as in Figure 5.

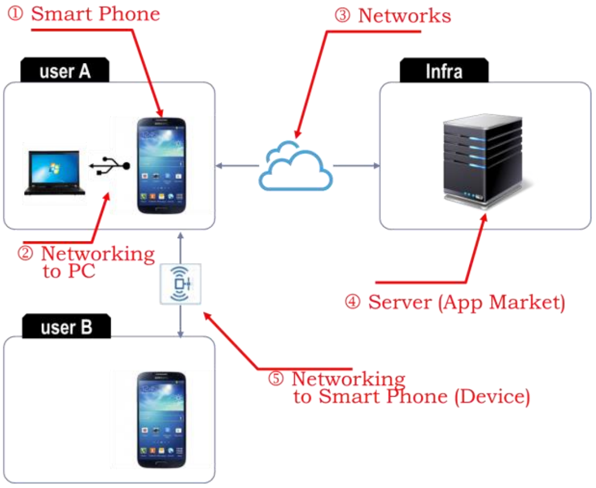

Figure 2. 5 regions of smart phone security threats

The major security research institutions and organizations, such as NIST, ITU-T, ENISA, FSA and NIPA, are continuously delivering results of the study on smart phone security threats. [4], [5], [6], [7]

TABLE 1 is for comparing their results according to 5 regions of smart phones security threats. This table is very useful to re-evaluate the types of smart phone security threats from a point of overall view of mobile security. [4], [8]

TABLE I. TYPES OF SECURITY THREATS FOR A SMART PHONE

Regions	Types of Security Threats	N	E	I	F	P
Smart Phone	Unauthorized Access	●		●	●	
	Malicious Code: Installation	●	●	●	●	●
	Soft Wiretapping	●		●		●
	Information Leaking	●	●	●	●	●
	Platform (App) Falsification /Forgery				●	●
Networking to PC	Platform (Firmware) Modification/Forgery				●	
	Malicious Code: Infection					●
	Information Leaking					●
Networks	Rouge AP		●		●	●
	Data Monitoring/Falsification		●	●	●	●
	Denial of Service		●			
Servers (App)	Malicious Code: Spread-out					●
	Remote Control					●
	Phishing, Pharming, Spam	●	●	●	●	●
Networking to Smart Phones/Devices	External (Physical) Interface		●	●		●

Note *N: NIST (National Institute of Standard and Technology, US)*
E: ENISA (European Network and Information Security Agency)
I: ITU-T (International Telecommunication Union-Telecommunication)
F: FSA (Financial Security Agency, S. Korea)
P: NIPA (National IT industry Promotion Agency, S. Korea)

A. Smart Phone

Unauthorized access, malicious code installation, soft wiretapping, information leaking and platform (App) falsification/forgery are pointed out as types of security threats that could be happened in a region of smart phone devices with users. Followings are examples of security threats for smart phone devices:

- Indiscriminate collection of user (personal) information
- Infection of smart phones by malicious code designed only for smart phones
- Infection of user information and smart phones by falsified and forged apps
- Security feature bypass via rooting or jailbreaking

In order to respond to these threats, following technologies are used:

- Application code obfuscation (or virtualization)
- Data encryption
- Anti-virus
- Prevention of personal information disclosures
- Prevention of rooting or jailbreaking
- Security keypad
- Code signing
- MDM (Mobile Device Management) for loss, theft, access control, two-factor authentication
- Auxiliary certification technology, such as OTP, for mobile payment

B. Networking to PC

In a region of smart phone networking to PC, security threats exist as types of platform (firmware) modification/forgery, malicious code infection and information leaking. Followings are examples of security threats in smart phone networking to PC:

- Influx of malicious code installed in PC
- Modification and forgery of platform firmware
- Unauthorized access to data stored in SD card
- Modification and forgery of data in SD card

Cod signing is a one of the technologies responding to these threats.

C. Networks

A region of networks between smart phones and servers has the legacy types of security threats in wired/wireless networks. However rouge AP, data monitoring/falsification and denial of service should be noted as types of smart phone security threats. Followings are for examples of these threats:

- Monitoring and modification/falsification of data by using ARP spoofing
- Monitoring and modification/falsification of data by using rouge AP
- Intrusion to networks via wireless AP

Technologies for data encryption and session randomization are necessary for these threats.

D. Servers (App)

A region of servers, which are for provision and management of smart phone apps, has various types of security threats, such as malicious code spread-out, remote control, phishing, pharming and spam. Followings are for examples of these threats:

- Self-distribution of malicious code embedded apps or contents
- Remote control of severs via improper access control management
- Denial of service via malicious code or by using protocol vulnerability

Responding to these threats, more sophisticated mechanisms of firewall, VPN (Virtual Private Network), filtering and two-factor authentication are required as a necessary way. [9]

E. Networking to Smart Phones or Smart Devices

External interfaces of a smart phone for ad-hoc networking to other smart devices are a type of security threats. Ad-hoc networks are easily comprised by using NFC (Near Field Communication), Bluetooth, infrared and WiFi. And also they are easily used as path for the flux of malicious code.

CONCLUSIONS

The emergence of smart phones, smart sensors and new wireless technologies provides a key research priority for mobile security. Analyzing security threats for ICT converging environment in mobility aspects is the beginning of well-organized research of mobile security.

In this paper, we categorized security domains of ICT converging environment in mobility aspects, and we analyzed mobile security threats caused by smart phones with comparing the research results of several security institutions.

REFERENCES

[1] ICT Standardization streategy map 2012, TTA, January 2012

[2] Security Threat Report 2012, SOPHOS, March 2012.

[3] Mobile device security, Ernst & Young, January 2012.

[4] Report on issues and trends of smart phone security for financeial service, FSA, July 2012.

[5] Guidelines on Cell Phone and PDA Security, NIST Special Publication 800-124, NIST, October 2008.

[6] Smartphones: information security risks, opportunities and recommendations for users, ENISA , December 2010.

[7] Security aspects of mobile phones, T09 SG17 110411 TD PLEN 1798, ITU-T, April 2011

[8] Guidelines for managing and securing mobile devices in the enterprise (Draft), July 2012, NIST

[9] Stefan Certic, "The future of mobile security", CS Network Solutions Limited, Feburay 2013.