International Journal of Security and Its Applications
Vol.8, No.2 (2014), pp.173-182
http://dx.doi.org/10.14257/ijsia.2014.8.2.18

The Study of Privacy Security in Mobile Traffic Control Environment

Byeong-Choon, Lee* and Seung-Jung, Shin*

*Hansei University, GyeongGi-Do, Korea
e-mail: choon7@kaist.ac.kr, expersin@hansei.ac.kr

Abstract

Smart phone became the generalized device now and tends to be used much even for business with escaping from an individual's taste. Smart-phone users are enough to reach about 400 million people worldwide. This trend is continuously growing. Owing to the generalization of smart device, even a plan of increasing corporate competitiveness is being considered by many enterprises. There is the biggest merit available for increasing efficiency of business by getting access to network anytime and anywhere and for maximizing power and agility by integrating it into specific business. However, there are many matters to be considered for this. The most important problem among those things is the biggest concern about information protection. Smart phone is high in a risk of being lost as excellent as mobility is. Due to this, the possibility of information leakage exists always. The purpose of this study is to supplement the existing demerit of MDM and MAM in the above and to solve fundamental problem, and to solve this by integrating traffic and suggesting MTM through strengthening and grouping security on the integrated traffic. Especially, it suggested fundamental security by definitely dividing information of business and an individual through analyzing network traffic, and proposes even a plan of utilizing dual USIM.

Key Words*: MTM, MDM, MAM, Mobile, 3G, 4G, Dual USIM*

1. Introduction

One of the basic characteristics of mobile office is a point as saying that mobile terminal plays a role of exit in intranet. Considering reality that security on terminal is loose, this may cause intranet to have largely 2 types of fatal threat elements. Firstly, it is a case of attacking intranet or leaking information by getting access to intranet after the authorized mobile office users' terminal is exposed to malicious code or malicious APP. Secondly, it is a case that hacker, who captured intranet access account (mobile office APP and ID/password, *etc*.,), attacks and leaks information by getting access to intranet through the unauthorized terminal [1].

Considering reality that the mobile office terminal is exposed defenselessly to malicious code and malicious APP, the intranet can become the attack target of hackers, who secured access path through the infected terminal with malicious code anytime. In case of coming to use the tethering function in the Zombie-made terminal or the terminal infected with malicious code because the terminal of staff in institution or enterprise is infected with Botnet malware, the hacker comes to secure the mobile-office intranet access path. Thus, mobile office system comes to confront a fatal crisis. As the situation on March 20, 2013, it may lead to hacking servers within mobile office, deleting data, or leaking massive data. It may destroy mobile office such as utilizing it as the

ISSN: 1738-9976 IJSIA

malicious-code distribution route of allowing the whole of the mobile office terminal to be infected with malicious code by inserting malicious code into APP store of institution/enterprise, which operates it within the mobile office.

Also, one of the mobile-office characteristics is a point as saying that the access authorization is limited to the account authorization method. This is accredited to weak point as saying that there is no special method available for authorizing connector or interface terminal in light of the characteristics in Mobile IP network. It means that anyone can get access to intranet given acquiring access account, thereby coming to face serious threat as saying of being unable to block unauthorized person's intranet access when the access account is captured by hacker. If the network security measure in the level of wired office terminal isn't applied to mobile office terminal, even any of the mobile security solutions is a house built on the sand. It is difficult to be expected the safe mobile office environment. Largely 3 kinds of threats exist in mobile office environment. It can be divided into, firstly, a physical threat to terminal, secondly, a network threat to terminal, and finally thirdly, a threat of intranet via terminal. Security countermeasures against each of these things are already defined. However, it is a situation of being beyond the capacity in solving all the problems with the existing solution due to the solution limit and the institutional problem.

The mobile office terminal offers merit as saying of being able to do business anytime and anywhere by performing the function as the mobile network access device of sending and receiving data by getting access to intranet or internet through mobile communication network. However, in the meantime, it causes weak point as saying of being difficult to guarantee security point for applying security solution in the level of network in light of characteristics in mobile communication network. In addition, office terminal is being mixed to be used for business and for an individual, thereby being able to cause controversy over invasion of privacy by any possibility, resulting in leading to a problem about which institution or enterprise avoids introduction of security solution in the level of network. Considering reality that the mobile office terminal is exposed defenselessly to malicious code and malicious APP, the intranet can become the attack target of hackers, who secured access path through the infected terminal with malicious code anytime. In case of coming to use the tethering function in the Zombie-made terminal or the terminal infected with malicious code because the terminal of staff in institution or enterprise is infected with Botnet malware, the hacker comes to secure the mobile-office intranet access path. Thus, mobile office system comes to confront a fatal crisis. As the situation on March 20, 2013, it may lead to hacking servers within mobile office, deleting data, or leaking massive data. It may destroy mobile office such as utilizing it as the malicious-code distribution route of allowing the whole of the mobile office terminal to be infected with malicious code by inserting malicious code into APP store of institution/enterprise, which operates it within the mobile office.

This study aims to make it available for implementing the safer mobile office environment by having complementary function with the existing solutions through providing enterprise with fundamental security measure and solution for the sphere with which the existing mobile office security solutions fail to cope among security threat elements of mobile office like a physical threat to terminal of being caused by weak point of mobile office, a network threat to terminal, and a threat of intranet via terminal.

2. Text

The biggest characteristic merit of this study is what overcame the limit of security-based sphere that the existing mobile office solutions couldn't do, by securing the

network security management point in the wired level through gathering mobile traffic in terminal on mobile communication network and by performing monitoring and filtering in the elaborate and high performance as for the concentrated traffic. For instance, the mobile traffics toward mobile office in the terminal subscribed to the mobile traffic management service are classified and managed on mobile communication network. Thus, the traffic in false terminal infected with malicious code cannot flow in the mobile office, resulting in being protected originally the mobile office. This can be expected the effect of being separated the non-subscriber's network except subscriber to mobile traffic management service on mobile communication network.

Mobile security in the more powerful level can be realized by borrowing merit of the existing mobile security solution and by adding security element in new dimension. It minimizes a problem of personal information protection, which has been indicated as a problem in the meantime, and user's opposition caused by the control of a few terminal functions by reducing control elements in terminal and by using security method in network sphere. This will bring about the effect of increasing corporate image by making it have recognition as saying of the enterprise, which implements the better security system and minimizes invasion of an individual's privacy either socially or corporate-based internally. Also, the existing solution can be immediately substituted, and is available for being overlapped to be operated according to a corporate situation, and for being substituted gradually. Accordingly, a barrier on introduction of solution was reduced.

The traffic concentration system in the mobile traffic management solution is a system of delivering the concentrated traffic to traffic management system for implementing the network security function in the wired level by gathering mobile traffic (3G/4G/WiFi) in mobile office terminal. A method for gathering mobile traffic can be divided into 3G/4G traffic concentration method and WiFi traffic concentration method according to traffic kind of the terminal media. It is varied device and method of forming traffic concentration system depending on each method.

2.1. 3G/4G Traffic Concentration

A device of forming traffic concentration system for gathering 3G/4G traffics is composed of the devices, which form core network for 3G/4G mobile communication service, and of the traffic concentration device. The traffic concentration system offers the gathered mobile traffics to institution/enterprise traffic management system by collecting mobile (3G/4G) traffics in the terminal of traffic management service subscribers within mobile office into the management point of institution/enterprise. The mobile-communication core network devices gather it into traffic concentration device by classifying mobile traffic based on IMSI and IP in terminal. The traffic concentration device delivers the gathered traffic to the traffic management device within the traffic management system. The traffic concentration device is formed by utilizing TCORE equipment, but needs to additionally support some elements, thereby likely requiring equipment in new form. MTM traffic concentration device is the one of playing a role of gathering the management-targeted traffic into specific gateway regardless of location in terminal, and needs to form gateway for MTM separately while maximally utilizing a device of forming packet core in the existing mobile communication network.

2.2. Traffic Management System

The traffic management system in the mobile traffic management solution is the core system of network security exclusively for mobile intranet in order to implement a strong security system in the wired network security level of mobile intranet as for the mobile traffic gathered by the traffic concentration system. The traffic management system is composed of a traffic management device and a device of analyzing active malicious code. The traffic management device classifies the mobile traffic in mobile intranet into private institution/enterprise traffic in order not to violate an individual's privacy, and is a mobile fire-wall device exclusively for mobile intranet, which implements the network security function according to the classified traffic. The active malicious-code analytical device is the one of analyzing malicious code exclusively for mobile traffic in order to remove a threat of malicious code, which exists in mobile traffic. The traffic concentration system and the traffic management system operate mutually and organically while making a real-time exchange of the authorized information like IMSI, IP information in terminal.

2.3. Traffic Management Service

This paragraph aims to explain about traffic management service of being offered by the traffic concentration system and the traffic management system, which are traffic management solution. The traffic management service implies the service available for implementing reliable smart work by removing elements of threatening mobile office security after performing the mobile firewall function as for mobile intranet in the wired level through traffic management system as to the concentrated mobile traffic (3G/4G/WiFi) by the traffic concentration system. The following table is the composition table of security service, which forms traffic management service.

Security service division	Item	Remark
Service of intercepting mobile malicious code	Detecting malicious code of the attached file on email	
	Detecting malicious code of the attached file on mobile and web mail	
	Detecting malicious code of APP store in open market	
	Intercepting APP download in black list	
	Detecting and intercepting malicious code in the form based on pattern and behavior	
	Real-time update of pattern and active DB filter	
Service of intercepting information leakage	Blocking leakage of the attached file on email	
	Blocking leakage of the attached file on mobile web and web mail	
	Blocking leakage of FTP file	
	Blocking leakage of file transfer on messenger	
	Blocking upload of Dropbox	
Service of intercepting the access to malicious and harmful site	Blocking the access to the terminal threat site through Smishing	Registering harmful and malicious site
	Blocking the access to black-list site	

Mobile intranet protection service is the firewall service exclusively for mobile intranet for protecting mobile-office intranet server as for the mobile-office terminal. Mobile intranet protection service is security service available for intercepting malicious packet or unauthorized packet in advance toward mobile office because of being able to control mobile traffic toward internet or mobile office through being collected all the mobile traffics (3G/4G/WiFi), which occur in the mobile-office terminal, by the traffic concentration system and through securing management point on mobile traffic gathered by traffic management system.

The network security devices have been used so far in the wired intranet environment for protecting mobile-office intranet. However, there is limitation that cannot add policy of intercepting specifically and accurately to the terminal of getting access to mobile-office service because the existing devices have no function of identifying terminal. In the mobile intranet protection service, there is function available for identifying by terminal as for mobile traffic. Thus, false access in the unauthorized terminal is originally blocked by traffic concentration system. It can control the access to mobile office server by terminal, thereby being able to control the mobile intranet access window more specifically and accurately.

Smart phones, which are sold now domestically, are offered only one piece of USIM. However, smart phones of supporting more than 2 pieces of USIM, are being sold abroad. There are many people who have job of needing to use several units of wireless telephones according to an individual's option. Also, there is tendency of being grown much even people who use by dividing it into individual phone and business phone. These days, enterprise or institution increases business efficiency by separately supplying phone for the use of business. Also, there are many cases that enterprise or institution offers cost of phone, which was used for business. However, it will not be convenient at all to carry more than two pieces of phones in domestic environment. Electrifying phone every day will be inconvenient. Cumbersome things happen much. What solves this problem is dual USIM phone. The use of dual USIM phone can lead to the use of more than two numbers with one phone, thereby having merit available for using for an individual or for business depending on number. What will need to be paid attention the most when using this dual USIM phone is a problem of security. In the wake of using phone for individual and phone for business together, there is no boundary. Even a problem of security may happen at the same time. Accordingly, this study aims to suggest that this dual USIM environment is separated to be operated. The aim is to suggest the form that allows an individual's privacy to be secured in case of using individual USIM and that can protect corporate data by being completely separated from an individual in case of using business USIM, through dividing dual USIM by sphere. It separately installs APP of offering this function and calls this APP as intelligent APP. This APP thoroughly manages personal area in order to certainly securing an individual's privacy in case of the individual USIM, and allows this area not to be mixed with the corporate area. Also, APP, which is installed within equipment, performs by distinguishing security and information-protection function by USIM, which is installed within equipment with being connected with MTM, thereby being able to perform safe dual communication. This study names the service of using this intelligent APP as MSM (Mobile Smart Management).

The function of this MSM has the new functions as follows.

- Inactivation of USIM, which isn't registered through the USIM authorization function
- Network authorization function (Controlling the information and APP access by U2U USIM)

- Encryption of the downloaded data by using USIM for enterprise

In addition to new functions in the above, it offers interface control WiFi, bluetooth, camera, data port function limit, and remote-lock and remote-deletion function, which are major functions among the functions of being provided by the existing MDM or MAM.

3. Simulation

As the suggested system in this study is what even the internet service providers don't apply now, a great expectation effect can be obtained given introducing positively. Mobile office tends to continuously grow now. Even if being the state of having already surpassed the existing PC market, the security on mobile office or mobile environment is the primary level. Thus, many security-based threats are being harbored. The following are showing expectation effects when applying the suggested system in this study.

■ Being able to separately manage only mobile traffic by using mobile traffic concentration/management system

■ Being able to implement security environment in the wired network level even if being the wireless environment

- Removal of all the terminal attack threats
- Prevention of information leakage through mobile traffic
- Effect of enhancing business through controlling private traffic

■ Maximizing security with the effect of implementing mobile network like intranet

■ Being capable of securing productivity and competitiveness in public institution by offering mobile office environment that secured reliability

Reconstruction of this suggested system leads to having effect available for forming independent network by each enterprise. Private gateway can be offered by allotting ATC gateway in mobile communication network by enterprise. This service installs private ATC gateway of specific institution or enterprise in the mobile communication core network. It sets up so that only all of the traffics, which occur in mobile-office terminal of this institution or enterprise, can be collected into private ATC gateway. The gathered traffics are classified traffic, and then are again authorized into the corresponding traffic management device. At this time, the business traffic and the personal traffic are classified. The business traffic of institution or enterprise is connected to private line or internet after being processed through management device. Still, the demerits of this composition include what high-priced cost will be taken and also what even subscriber's service cost will not be easy by offering private ATC gateway every enterprise. Accordingly, to solve this, the composition was devised that the same service can be received by using common ATC gateway.

This composition may have merit as saying that cost is reduced compared to service of offering individual equipment, but has problem that can be created by being mixed a number of corporate data.

The introduction of this service can lead to possibly obtaining the following effects.

1) Effect of implementing safe, efficient and independent mobile communication network

- Implementing independent mobile office access network that was originally intercepted outsider's access by USIM authorization
- Tunneling on all the traffics of mobile office terminal without creation of overhead

(concentration)

2) Forming the foundation of maximizing security of mobile office
- Securing environment available for managing mobile office terminal integrally (personal area + business area)
- Offering a plan for powerful authorization of mobile office access by offering matching information of user and IP
- Restricting (WiFi access interception) the mobile office access with the guaranteed media (3G/4G) with security

3) Forming user-friendly mobile office environment
- Removing a basis of violating privacy by the rational traffic classification and by the duality in the management subject according to traffic classification
- Minimizing the control of functions and resources in terminal for mobile office security
- Offering a rational BYOD compensation plan
* Function of duality in charging (business/individual)
* Forming environment of applying a specialized security plan for individual area in terminal

4) Forming the foundation of enhancing productivity by implementing the integrated management environment on the mobile office terminal
- Forming the foundation of extracting management information such as information on diligence and laziness by user
- Forming the foundation of enhancing business concentration such as controlling excessive individual traffic

Also, as for institution suitable for this service, the government department or state-invested institution is judged to be likely appropriate for the service based on private ATC gateway. Local government, small-and medium-sized company, or hospital is judged to be likely proper for the service based on common ATC gateway.

4. Conclusion

The mobile office environment offers environment that staff of institution or enterprise can handle business conveniently anytime and anywhere by using mobile terminal. There is positive effect in the aspect of mobility, openness, diversity, and usefulness of mobile office. However, it is being much harbored a problem about security, which can occur with using internet, and a physical threat such as loss and robbery. For this, BYOD solution was developed much. It is the real situation of using much solution such as MDM or MAM. However, there are fatal demerits in the current solution. In case of not solving this, the environment in mobile office isn't safe anymore. It will be difficult to be formed with new infrastructure. The existing solution of using BYOD offers the remote lock and initialization, and location search given robbery or loss of mobile equipment, and controls the equipment media function, thereby providing the strengthening in equipment. Also, it makes it available for controlling execution on APP. However, infringement of privacy caused by the equipment security and control is very serious. The bigger problem was what fails to offer security function at all as for mobile traffic. For this, this study aimed to solve two problems through MTM and MSM. Traffic part and privacy infringement were proposed. Through several services for verifying this, it proved that the suggestion is proper.

More important element is that rational solution needs to be suggested with supplementing demerit of the existing solution. That is because of needing to be very careful in handling an individual's data according to Personal Information Protection Act when possession of a phone belongs to an individual. Accordingly, the introduction of this solution leads to being available for using traffic more safely. It focused on designing so that an individual can be further free from violation of privacy. Recently, the introduction of a phone for enterprise is being very active in large company or public institution. Also, it is a situation that even the restriction to an individual's phone is intensified very much. It is reality that cannot help applying security function even to an individual's phone for security of enterprise or institution. However, many employees are being dissatisfied because an individual fails to be free from own personal property and privacy. Side effect is taking place that this dissatisfaction is developed into a conflict between organization and an individual. Still, to realize the suggestion in this study, the positive investment in ISP is needed. Even an individual or organization will need to get over demerit as saying of needing to bear additionally.

The suggestion in this study is confirmed to likely implement the advanced mobile office by solving this conflict between organization and an individual and by offering the more enhanced security function.

Acknowledgements

This article is a revised and expanded version of a paper entitled [The Study of Privacy Security in Mobile Traffic Control Environment] presented at International Symposium on Advanced and Applied Convergence held on November 14-16, 2013 at Seoul, Korea.

References

[1] L. Byeong-Choon and S. Seung-Jung, "The Study of Privacy Security in Mobile Traffic Control Environment", ISAAC 2013/ICACT 2013, AACL 01, **(2013)**, pp. 1-4.
[2] Y. Zhou and X. Jiang, "Dissecting Android Malware: Characterization and Evolution", Proc 33rd IEEE Symp Security and Privacy, **(2012)**.
[3] Mobile security technology research society, "Demand and outlook for mobile security technology", Data collection for Mobile security technology research society seminar, **(2011)** September.
[4] Y. Hyo-seon, "Implementation of mobile office, Top priority of arranging security countermeasure", Network Times, vol. 3, **(2011)**.
[5] R. P. Mislan, "Cellphone crime solvers", Spectrum, IEEE, doi: 10.1109/MSPEC.2010.5491013, **(2010)**, pp. 34-39.
[6] Androulidakis, "Digital evidence in mobile phones", IT security professional magazine, no. 13, **(2010)**, pp. 36-39.
[7] K. Amoroso, "Selection Criteria for Intrusion Detection Systems", 14th Annual Computer Security Applications Conference, Phoenix, AZ, IEEE Computer Society Press, **(2008)** December 7-11.
[8] Base. Intrusion Detection. Macmillan Technical Publishing, ISBN: 1-57870-185-6, **(2000)**.
[9] Bobbit, "The Attacker's Arsenal", Information Security. (Online), [Referenced 25 February 2004], **(2002)** May.
[10] CERT. CERT/CC Statistics 1988-2003. (Online), [Referenced 6 January 2004], **(2003)** October 17.

Authors

Byeong-choon, Lee
Year in 2002, Master for Dongguk University Graduate School of Public Administration
2011-2013, Doctorate course for the general graduate school, Hansei University
1992-2009, Worked at Presidential Security Service Office
2010-Present, Working at KAIST (Korea Advanced Institute of Science and Technology)

Seung-Jung Shin, he received the Ph.D. degree from Kookmin University in 2000, Korea. Currently, he is a professor at Department of Information & technology, Hansei University. His current research interests include security and privacy.