A Static or Dynamic Reconfiguration Method of Security Functions for Mobile Devices by Using the Security Profiles

WONJOO PARK, DONGHO KANG, KIYOUNG KIM
Information Security Development Division
Electronics and Telecommunications Research Institute,
161, Kajung-dong, Yusung-Gu, Daejeon,
Republic of Korea

Abstract - This paper proposes the method for reconstructing the security function of the mobile devices based on the security profiles statically or dynamically.
The security functional profiles are defined according to the basic circumstance element including the kind of the mobile equipment, the connected network, the offered services, the level of user, and etc. in advance.
When the security function of the mobile devices is reconfigured statically or dynamically according to situation, security services are offered more actively and flexibly.

Key-Words: -Security Reconfiguration, mobile devices security

1 Introduction

Realization of ubiquitous computing is urged by desires to access various services using different kinds of devices without regarding to time and place. To users, ubiquitous signifies computing and networking functions to be omnipresent in physical environment so that services could be flawlessly coordinated.

To provide various services offered ubiquitous computing environment, current mobile device is expected to be advanced to compound mobile device that possess calculation ability of high level and various function. But, in the mobile environment, as infrastructure and service can be changed dynamically that was always not fixed, it is important that security level is defined according to any change and security services are provided suitably.

Security services of existent mobile device executed security functions that terminal manufacturing company had loaded without user's knowledge when device was announced. Or, end user bought a specification security program from the mobile communication service provider or the security program development company. These are processed without considering variety of network infrastructure and mobility of mobile devices. Also, it is hard to reconstruct flexibly according to end user's level. [1][2]

This work was supported by the IT R&D program of MIC/IITA [2007-S-023-01, Development of the threat containment for all -in-one mobile devices on convergence networks]"

Therefore, we suggest a method for reconfiguring the security function of mobile devices based on the security profiles statically or dynamically.

2 Backgrounds

Current researches on ubiquitous computing are directed to build infrastructure, connect new devices and develop valuable applications. Then again, security concerns of these environments or privacy issues are not being researched. Additional characteristics and expanded functions provided by ubiquitous computing environment makes it vulnerable to new kinds of threats. Existing security mechanisms and policies are not suitable for protection against new risks. Figure 1 shows details to guarantee security and privacy in ubiquitous computing environment.[3][4][5]

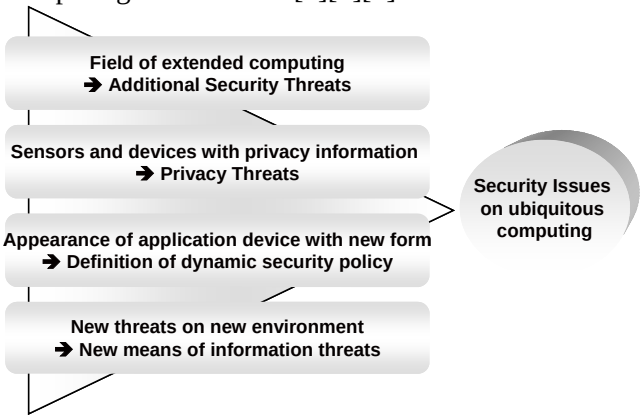

Fig. 1. Security issues on ubiquitous computing

Also, mobile terminal is evolving into compound mobile device by supporting portable internet as well as mobile communication function. And, handy electronic devices and individual computing devices support not only basic multimedia services and personal business functions but also mobile communications. So, compound mobile terminal will become device that can support high efficiency, broad bandwidth, and various interfaces as terminal that can accommodate characteristic of terminals more than two in the near future.

We define all-in-one mobile device as high efficiency and various functions mobile device for individual that would use fusion and complex services.

All-in-one mobile device is multi-function terminal that supports wireless internet service and mass multimedia service though multi-channel radio network infrastructure.

Fig. 2. All-in-one Mobile Device

By the way, all-in-one mobile device has some problems with CPU performance and throughput lower than fixing terminals, and there is limitation of power while it is advantage of portability, mobility by mobile terminal equipment. Also, telephone call, message transmission and internet use of mobile terminal are important item in economical side because is connected directly with expense. And, because various network interfaces supplement increases probability to be attacked, vulnerability of security is high.

Therefore, it needs to reconstruct security service for all-in-one mobile device and to apply a new profile according to any change or any need.

3 Suggesting reconfiguration of security services

Existing security technology for mobile terminal is anti-virus, firewall, anti-spyware, USB security mainly. But, these are limit to security for all-in-one mobile devices that have portability, mobility and multi network interface. Subsequently, in order to deal with new weakness of all-in-one mobile devices, this paper suggests a method of reconfigurable security services for all-in-one mobile devices statically or dynamically. This method reconstructs security function of terminal about the circumstance after defines profile about security service according to kind of terminal, network that terminal is connected, main service, kind of main data and knowledge level of user .

Figure 3 shows a block diagram for security function reconfiguration system.

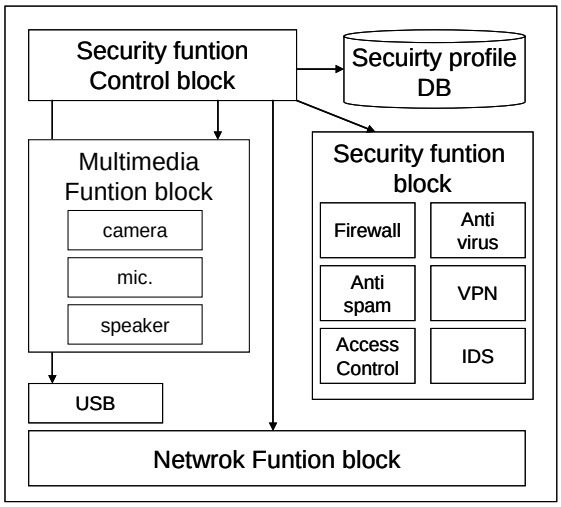

Fig. 3. Block Diagram for security function reconfiguration system

It includes security function control block, security profile DB except that have existent characteristic function of mobile terminal for security function reconfiguration. Also, security function block includes firewall, anti-virus, anti-spam, VPN, IDS, access control and so on. And then, security function control block can select some security function according to security profile.

Security function control block defines security profile and configures security function by controlling multimedia function block, security function block, USB and network function block. User creates security service profile that he is suitable in wanted

security level. And he saves it to security profile DB. If user wants to change security level of all-in-one mobile device, he loads existent high security level profile or creates a new security profile. And then, security function control block controls other blocks according to the security profile. Also, specified security profile made by the user is taken to other terminal for similar environment.

Security profile DB has several security profiles for various levels and diverse requirements. Profiles in DB can be created, saved and modified by product maker and user.

Security function block takes charge of role that provides several security services that can be offered to differ as device. In case knowledge level about user's security function is high, user can control security service function through security function control block and security profile manually because he understands security service function that own terminal offers. Otherwise, if a user has knowledge about security function little, he may use a security profile that offered by product maker.

Concretely, we suggest following procedure for all-in-one mobile devices to be provided security

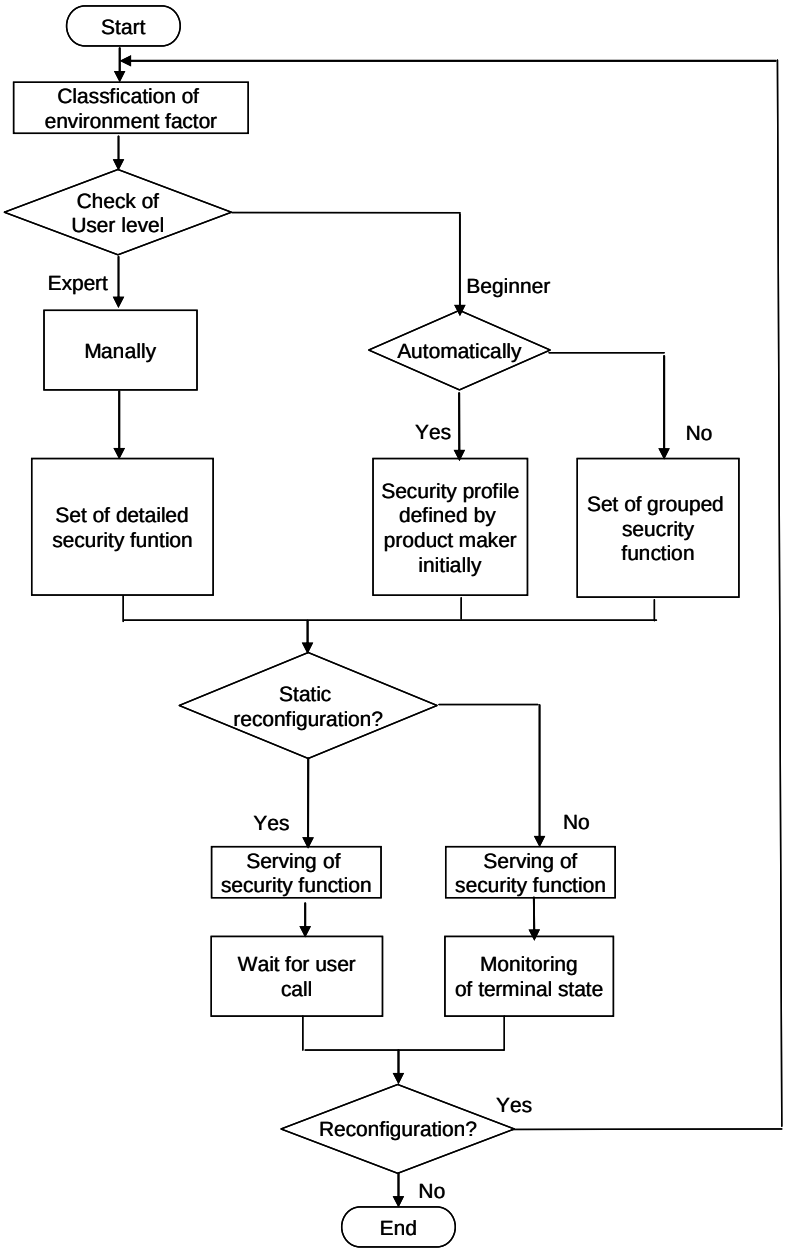

Fig. 4. Flow chart of security reconfiguration service for all-in-one mobile device

function reconfiguration service. This procedure is consisted of environment factor classification phase, selection phase for manual or automatic according to user level, setting phase for security service as wanted security level, selection phase of security service reconfiguration for statically or dynamically, and saving and serving phase of security profile.

Figure 4 shows a flow chart for security function reconfiguration service.

First, environment factor classification phase is step that fractionate infrastructure of terminal, user, main service, main medium and analysis element according to security circumstance. This phase defines circumstance analysis element, required resource and service that can influence to security of all-in-one mobile devices. Here, resources and services have to be defined abstractly so that can apply to communication environment to appear newly late. That is, when they are described abstractly and a new application is executed, security function can be expanded for new them.

If environment factor classification work is completed, terminal checks user's level. At this phase, mode is set by automatic or by manual according to end user's security knowledge level and security function of device.

When a end user is expert about security, security function set mode is manual, because he can use various security service which is provided to the devices. While a end user is beginner and has knowledge about security little, set mode is automatic. Then, he loads security profile that defined by product maker initially. Only, in case he is beginner, but wants to set a few security services, he can set grouping security function. That is, it groups to network, device, service security, and user security. And, it sorts security level that is high, middle, low and danger. Then, user can establish different security level about each group.

As explain over, if security function and level are established by manual or automatic mode in drive begging of device, it decides whether reconfigurable security service is embodied by static or dynamic. In case of static reconfiguration, user requests reconfiguration security service. User can request this function directly, when it is changed environment analysis element or security level user wants. On the other hand, when reconstruct dynamically, state monitoring module keeps track of element of analysis.

In this point, element of analysis can be information about access of resource, detection of worm or virus, program malfunction, encryption/decryption state of sensitive data, overload of CPU, power of device. If state monitoring module decides to need reconfiguring security function, reconfiguration is started. For example, if monitoring module detects low power of device and wants to increase system using time, it requests to apply other security profile and can change security function into inactivation mode. Also, when security function module detects intrusion of worm and the device may be emergent, every network interfaces can be inactive not to connect outside. If it reconstructs security function dynamically according to report of monitoring module, usability and safety of device can be improved. But, internal monitoring module can influence in performance and power of terminal, because it should be run by ordinary time.

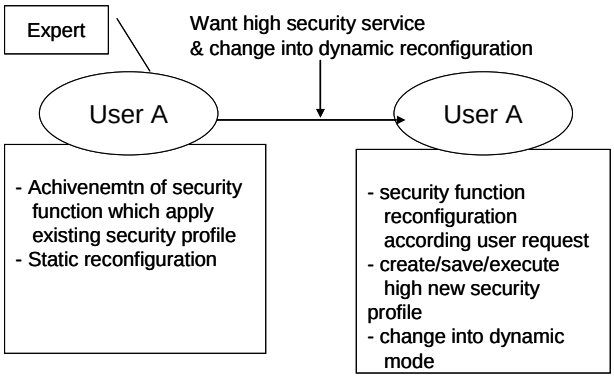

Fig. 5. An example of proposed method

Figure 5 shows an example of this method. When a user has high security knowledge, he wants new security function reconfiguration for higher security service. If he is no wanted security profile in the existing security profile DB, he creates, stores and executes the high new security profile. Also, he may change reconfirmation method into dynamic mode and activate monitoring module.

By using this method, it can establish security function and apply security level according to environment component that the device is placed. Also, as it loads and applies security profile, fast treatment is available. And user who security knowledge is low and understanding about function of terminal can use security profile and reconstruct.

4 Conclusion and future works

Convergence and ubiquitous network for all-in-one mobile device will be integrated diverse medium, devices, services and datum. Therefore when it is considered performance, limit of power and expensive

expense of all-in-one mobile devices, it is very important to strength flexibility about security function of platform.

Therefore, we suggested a method for reconfiguring the security function of all-in-one mobile devices based on the security profiles statically or dynamically.

In the future, we plan to describe this method more in detail, and implement it on common OS environment.

References:

[1] M. Weiser , "Some Computer Science Problems in Ubiquitous Computing," Communications of the ACM, July 1993

[2] M. Weiser , "Ubiquitous Computing," Nikkei Electronics, December 1993, pp.137-143 ,

[3] S.M. Hwang , S.J. Kim, "Security of Ubiquitous Computing,", KISC, Vol.21, No.5, May 2004

[4] W.J. Park, D.I Seo, J.S. Jang, D.Y. KIM, "The Study on Security Middleware Framework for the Ubiquitous Platform", VTC2006FALL, September, 2006

[5] Technology and economics research division, "The Trend of Ubiquitous computing," ETRI, 2002