# Ubiquitous Computing Environment Threats and Defensive Measures

Dr. Byeong-Ho KANG

*Associate Professor*
*School of Computing and Information Systems*
*University of Tasmania*
*bhkang@utas.edu.au*

### *Abstract*

*Ubiquitous Computing is considered an information technology that fuses real space and cyber space based on the networks among existing things in the real world. Advances in ubiquitous have been topics in so much researches. In this paper, we analyze security threats of mobile computing devices with an application of ubiquitous computing and we suggest their countermeasures in technical, manageable, and physical aspects.*

***Keywords:*** *Ubiquitous Computing, Mobile, computing device, Security*

## 1. Introduction

The ubiquitous computing revolution, which is considered as an Information Technology to fuse real space and cyber space, based on the networks among existing things in the real world, has been conducted over the whole of society. Even more, the future oriented technology has changed the axis of the paradigm of Information Technology

Recent advances in hardware and software technologies have created a plethora of mobile devices with a wide range of communication, computing, and storage capabilities. As wireless communication has especially been advanced, demands of portable personal computing device has been increased and services of wireless internet like downloading of a variety of contents, mobile banking, and information searches have been commercialized rapidly . However, mobile portable computing devices which are important components in ubiquitous computing environments have been exposure in security threats such as denial service attack exploiting low information processing capability of low-powered CPU, malicious code attacks exploiting vulnerabilities of mobile platforms and application programs, and exposure of information by unauthorized users. Recently, incident cases caused by attack exploiting vulnerabilities of mobile portable computing devices have been occurred all over the world including Sweden, Finland and Japan. It has been expected that damages of such attacks is serious as Hacking Group like 29A has developed and announced worm and virus exploiting vulnerabilities of mobile portable computing devices, number of users of mobile portable computing de vices and services provided by them have been increased .Therefore, study on security threats and their countermeasures in of mobile portable computing devices is needed. From now on, previous works for above subjects have been initial step and the results are insufficient [1][2].

In this paper, we analyze security threats of mobile portable computing devices and then we suggest their countermeasures in technical, manageable, and physical aspects.

## 2. Ubiquitous Computing

### 2.1. Definition and Characteristics

‘’Ubiquitous’ is a Latin word meaning ‘anytime and anywhere’ or ‘exist simultaneously.’ The term is currently used to describe computing environment in which users can communicate information using any device on any network (portable) and information is transmitted in the optimal method as the context of users’ requirements are autonomously recognized while the users are not aware of it. In ubiquitous environment, information service is highly mobile and embedded that information users become dynamic and computer devices become diversified.

Table 1. Concept comparison of Ubiquitous computing by Scholars and Research Institutes [7]

| **Scholars and research institutes** | **Definition** |
|---|---|
| Friedemann Mattern (2001) | Tomorrow everyday |
| K. Sakamura (1987) | Ubiquitous computing is making us to be able to use<br>computers anywhere and anytime. |
| Mark Weiser (1993) | Ubiquitous computing has as its goal the enhancing computer<br>use by making many computers available throughout<br>the physical environment, but making them effectively<br>invisible to the user. |
| IBM (2004) | Pervasive computing delivers mobile access to business<br>information without limits from any device, over any<br>network, using any style of interaction. It gives people<br>control over the time and the place, on demand. |

Moreover, different from existing information service that only provides information required by users, in ubiquitous environment the computer not only serves information but also performs necessary actions as it intelligently recognizes the concerned situation. However, because computer equipment and networks composing ubiquitous computing environment have characteristics such as heterogeneity, openness, mobility and dynamicity, we need to apply distributed access control while guaranteeing the identification of each component rather than centralized one.

There are many common factors about the definition of ubiquitous computing, these vary and are slightly different according to the scholar, time and organization. Table1 arranges the definitions of ubiquitous computing [3], [4], [5], [6].

With many changes of the definition of ubiquitous computing according to technological progress, we have refined the definition of ubiquitous computing in this research. We defined that ubiquitous computing is a technology, in which invisible computers are embedded and connected with all things so that anyone can communicate, exchange and share information anywhere anytime. Based on these characteristics of ubiquitous computing, the United States of America, Europe, Japan and Korea recently have chosen their own concepts of ubiquitous computing, and have been trying to benefit from the highly focused R&D. Table 2 compares the concepts of ubiquitous computing of each country [8]. To sum up these various concepts of a BM, a BM is to identify diverse components such as the products and services, business strategies and processes, and stakeholders of a BM, to express the value created between the players by combining the components, and to set up long-term business strategy for an operating company.

Table 2. Ubiquitous Comparison

| Country | **US** | **Europe** | **Japan** | **Korea** |
|---|---|---|---|---|
| Concept | Ubiquitous computing, Pervasive computing | Disappearing computing, Ambient computing | Ubiquitous network | Ubiquitous Appliance |
| Value | Service by smart devices | Intelligent cooperation by information artifacts | Anywhere connection by small chip, smart card, context roaming | Single function appliance using short range wireless Interface |
| Research Field | Computer devices | Every objects | Network | Appliance |
| Core Technology | Short-distance radio communication, Sensor, MEMS, Small size object chip | | | |

At their core, all models of ubiquitous computing (also called pervasive computing) share a vision of small, inexpensive, robust networked processing devices, distributed at all scales throughout everyday life and generally turned to distinctly common-place ends. For example, a domestic ubiquitous computing environment might interconnect lighting and environmental controls with personal biometric monitors woven into clothing so that illumination and heating conditions in a room might be modulated, continuously and imperceptibly. Another common scenario posits refrigerators "aware" of their suitably-tagged contents, able to both plan a variety of menus from the food actually on hand, and warn users of stale or spoiled food.

Ubiquitous computing presents challenges across computer science: in systems design and engineering, in systems modelling, and in user interface design. Contemporary human-computer interaction models, whether command-line, menu-driven, or GUI-based, are inappropriate and inadequate to the ubiquitous case. This suggests that the "natural" interaction paradigm appropriate to a fully robust ubiquitous computing has yet to emerge - although there is also recognition in the field that in many ways we are already living in an ubicomp world. Contemporary devices that lend some support to this latter idea include mobile phones, digital audio players, radio-frequency identification tags, GPS, and interactive whiteboards. [16]

Mark Weiser proposed three basic forms for ubiquitous system devices, see also Smart device: tabs, pads and boards.

- Tabs: wearable centimetre sized devices
- Pads: hand-held decimetre-sized devices
- Boards: meter sized interactive display devices.

These three forms proposed by Weiser are characterised by being macro-sized, having a planar form and on incorporating visual output displays. If we relax each of these three characteristics we can expand this range into a much more diverse and potentially more useful range of Ubiquitous Computing devices. Hence, three additional forms for ubiquitous systems have been proposed: [15]

- Dust: miniaturised devices can be without visual output displays, e.g., Micro Electro-Mechanical Systems (MEMS), ranging from nanometres through micrometers to millimetres. See also Smart dust.
- Skin: fabrics based upon light emitting and conductive polymers, organic computer devices, can be formed into more flexible non-planar display surfaces and products such as clothes and curtains, see OLED display. MEMS device can also be painted onto various surfaces so that a variety of physical world structures can act as networked surfaces of MEMS.
- Clay: ensembles of MEMS can be formed into arbitrary three dimensional shapes as artefacts resembling many different kinds of physical object (see also Tangible interface).

The Rise of the Network Society, is an ongoing shift from already-decentralised, stand-alone microcomputers and mainframes towards entirely pervasive computing. In his model of a pervasive computing system, the example of the Internet as the start of a pervasive computing system is presented. The logical progression from that paradigm is a system where that networking logic becomes applicable in every realm of daily activity, in every location and every context. [16]

### 2.2 Benefits of Ubiquitous Computing

Benefits of ubiquitous computing can be summarized as enabling us to utilize information in several ways. The purpose of a software infrastructure for ubiquitous computing is to retrieve information from our real world that could not be made available before, and to control various everyday objects that could not be controlled before by embedding computers.[10] Some of the most important issues in ubiquitous computing are to provide context-awareness, to integrate physical and cyber spaces, to personalize our real world and reduce the complexities in our daily lives [8]. Many researchers are working on similar topics, such as sentient computing [12], pervasive computing [7], tangible bits [14], affective computing [22], ensemble computing [24] and proactive computing [23]. Such research shows that a software infrastructure to support ubiquitous computing is a key to realising its vision. The infrastructure makes it possible to share various devices and sensors, and to build ubiquitous computing applications easily.

## 3. Security Threats in Ubiquitous Environment

Security threats of mobile portable computing devices comprising confidentiality, integrity and availability are malicious code, vulnerabilities of mobile platform and its application, attack on communication path from wired network to wireless network, and data robbery & damages.

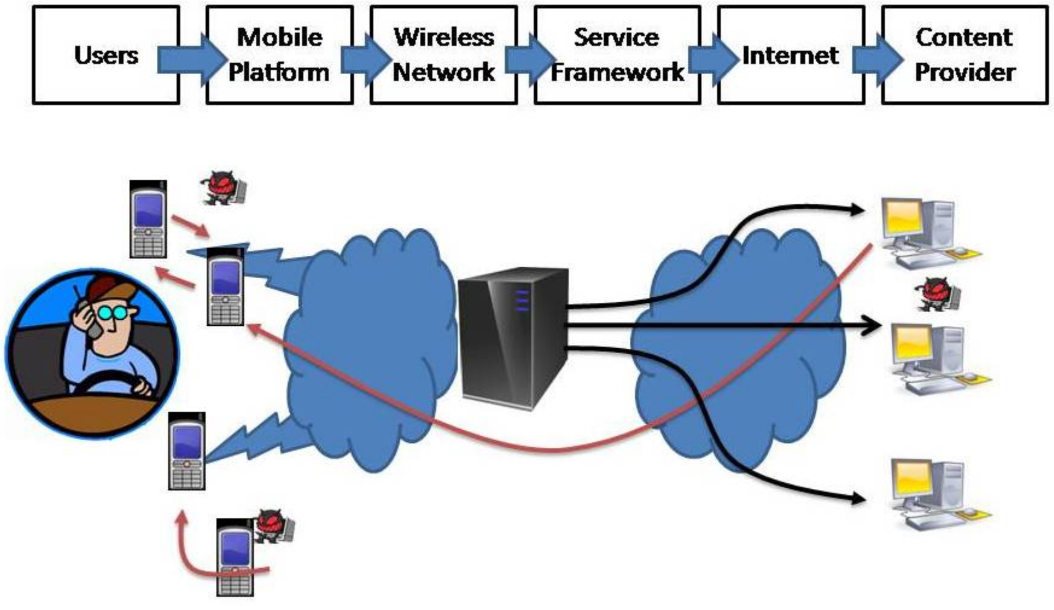


Figure 1. Infectious route of Malicious Codes

Mobile powered devices and software offer a potential benefit, including lower operating costs and greater productivity.[9] However, organization that deploy mobile solutions need to make security a priority. Illustrated in the following figure is the possible security threats to auto vaccination planner implemented in a handheld device.

**Malicious software**

Viruses, Trojan horses and worms are familiar threats to traditional workstations and laptops. While mobile devices have not yet become a significant target, there is a growing consensus among security experts that mobile devices will be a targeted. Even malicious software not designed to deliberately inflict damage may have unintended consequences such as data disclosure or corruption

### Loss of sensitive data

Some organizations consider mobile devices a security risk only if they have a business application installed. Other organizations consider the loss of calendar and contact information a security risk. Consider the potential consequences if an executive’ s e-mail inbox or calendar, full of meetings and briefings, were retrieved by a competitor. Contact information can also cause problems if it falls into the wrong hands, as recent high-profile incidents have demonstrated. Organizations need to protect the data on their employees’ mobile devices.

### Device loss or theft

Losing a device to mishap or theft can cause lost productivity, data loss, and potential liability under data-protection laws. Thousands of mobile phones and networked handheld devices are lost or stolen every year. As sales of mobile devices increase, the negative effects of device loss and theft are sure to increase accordingly.

Unauthorized device connectivity : An employee device connecting to a personal device to exchange Active Sync may bypass security settings and applications required on a corporate device

### Unsupported or unsigned applications

Older applications that are no longer supported, while they may still work, are dangerous because they may be vulnerable to attack by new viruses. If an unsigned application is installed on a device it could make changes to device that would jeopardize it security

### Intercepted or Corrupted data

With so many business transactions taking place over mobile devices, there is always concern that critical data could be intercepted along the path through the Internet cloud, via tapped phone lines or intercepted microwave transmissions

### Unauthorized Bluetooth or Wi-Fi access

Many mobile phone users employ hands-free Bluetooth headsets, potentially leaving hackers a hole for BlueSnarfing data on the device or BlueBugging to gain control of the device. Ad hoc wireless network connection can also lead to unauthorized device access.

### Unauthorized device connectivity

An employee connecting a personal device to the Exchange Active Sync may bypass security settings and applications required on a corporate device.

Table 3. Malicious Codes for Mobile Devices

| **Malicious code name** | **Date** | **Descriptions of characteristics and damages** |
|---|---|---|
| Mosquito Trojan horses | 2004. 7 | When illegal copy of Mosquito game was executed,<br>great amounts of SMS was produced and distributed<br>·It was proven that Ojom, developing company<br>of Mosquito game, implemented malicious codes in contents of its products and distributed |
| WinCE.Dust A | 2004. 7 | ·First Virus to infect files of Windows CE of Pocket PC<br>· EXE files more than 4,096 byte were infected<br>in directory execution of Virus. |
| Cabir | 2004. 6 | Made by ‘29A’, Hacker Group.<br>·It was executed in mobile phone supported by<br>Symbian Operating System and it made ‘Carbire’ messages to screen.<br>·Propagation through Bluetooth communication<br>with masquerading to security utility file, Caribe.sis |
| I-Mode Malicious code | 2004. 6 | Police telephone number in Japan, 110 was connected automatically when SMS was checked |
| Phage | 2004. 9 | A PDA virus infected by share of files.<br>·Programs of PDA was not operated when it<br>was infected |
| Timofonica | 2004. 6 | ·Transmission of great amount of SMS containing slander of specific communication<br>Company to arbitrary Phone numbers. |
| SMS Malicious code | 2004. 1 | ·Operations of Nokia cellular phone were stopped when specific SMS was received |

### Unauthorized network penetration

Because many mobile devices provide a variety of network connectivity options, they could potentially be used to attack protected corporate systems. Attackers who gain access to a mobile device may be able to impersonate a legitimate user and gain access to the corporate network.

### Infection by Contents

Malicious contents through SMS or E-mail ca infect malicious code in mobile portable computing devices. In case of I-Mode malicious code, Police telephone number in Japan, 110 was connected automatically when received SMS was checked. Propagation speed of these kinds of malicious codes is very fast. As examples, there are ‘Timofonica’, ‘SMS malicious code’, and ‘I-Mode malicious code’.

### Infection by Communication Routs Between Mobile Portable Computing Devices

Malicious codes can be infected in case of sharing files using SYN cable, USB, Infrared communication or short length communication like Bluetooth. As examples, there are ‘Phage’, ‘Cabir’, and ‘WinCE Dust.A

### Vulnerabilities of Mobile Platform and Its Applications

Like normal PC environments, mobile portable computing devices can be attacked to exploit vulnerabilities such as Buffer overflow, Format string, Parsing error. Table 3 shows known vulnerabilities of mobile platform and its applications from now on. Malicious code or Virus exploiting vulnerabilities of mobile platform and its applications is not found but it is high possibility to appear. It is expected that damages are high if worms exploiting such vulnerabilities appear, which act destructively like DoS attack and exposure of data. specially, economic loss will be high in case of vulnerabilities of Smart phone which include sensitive data used in mobile banking, and mobile electronic commerce and personal information such as social identification.

### Attacks on Communication Path from Wired Network to Wireless Network

Data can be eavesdropped and unauthorized users can access to mobile portable computing devices on wireless communication. As security mechanisms of IEEE 802.11 are not strong to prevent eavesdropping, it is easy for attackers to eavesdrop sensitive information by using SNIFFER tools. Attacker also can intrude network nodes between wireless and wired network, and eavesdrop sensitive data, exploiting vulnerabilities of wireless network which is applied to vulnerabilities and security threats of wired network as wired and wireless network have been integrated into single network. Therefore, worm and virus can be propagated widely through wired and wireless network. These cause to be denial of service, stop services themselves and bring economic damages in ubiquitous computing environments.

### Data Robbery and Damages

Attached software to mobile portable computing devices which are connected to Personnel Computer or annexed software purchased separately can cause to exposure of data to attacker. mobile portable computing devices normally provide logging functions to prevent these kinds of data robbery but these functions can't solve all of these problems**.**

Table 4. Malicious code for mobile Devices

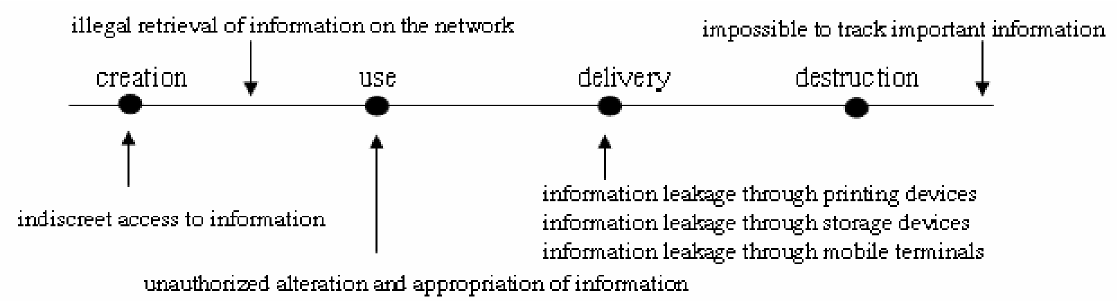
| Vulnerability name | Data | Description |
|---|---|---|
| Anonymous Bluetooth access vulnerability | 2004. 5 | Users with Bluetooth can access to mobile phone without authentication when Bluetooth of some mobile phone is executed. |
| PalmOS Memo-<br>Pad Memo Hiding Vulnerability | 2003. 7 | Bypass vulnerability exploiting edit applications is executed when security application installed in Palm OS is set to be low-level functions. |
| SIMENS mobile phone %IMG_NAME DoS Vulnerability | 2003. 5 | Denial of Service attack in Simens mobile phone is occurred when SMS message attached to modified images process |
| Nikia SGSN SNMP Vulnerability | 2003. 3 | Vulnerability able to read SNMP options which have Any community with SNMP Deamon of DX 200 based Network elements in Nokia SGSN phone exists. |
| Nikia 6210 SMS DoS Vulnerability | 2003. 2 | Attacker can send malicious vCard to mobile phone used in exchanging address lists and supported by Nokia 6210. |
| SIMENCE Mobile phone SMS DoS Vulnerability | 2002. 1 | Mobile phone received by SMS messages including specific character can not show these messages and cannot delete them. |
| PalmOS TCP Scan remote DoS Vulnerability | 2002. 1 | Vulnerability that PDA is unstable exists when TCP connect() requests PDA installed on Palm OS 3.5 |
| PalmOS Debugger Password bypass Vulnerability | 2001. 3 | Vulnerability that users able to access physically in PDA installed on Palm OS debugging mode bypass |

**Inside Information Leakage**

The trend of information resulting from the development of information technology is spreading infinitely including managing and improving resources and processes in enterprises, collecting and processing data and producing meaning information, and communicating and utilizing information and creating knowledge. The development of information technology, however, brings forth not only such functions but also fatal dysfunctions. Basic human rights are infringed as personal information and life are disclosed and communication confidentiality is not guaranteed. In organizations as well, information management is getting harder as unauthorized persons can access information in the environment of integrated system and important information is computerized. Furthermore, the development of communication technology makes easier hacking by outsiders and information leakage by insiders. Particularly in case of information leakage by insiders, because information users have to access important information inevitably for their works, control over the leakage of information accessed is mostly in user's hand because of work efficiency and technological limitations. Information leakage by insiders is more problematic when the asset value of information is higher. The leakage of technology information, customer information, national secrets, information related to rights and interests, etc. may threaten the competitiveness of enterprises and public institutions and drain national wealth. According to reports on information security accidents, 14.5% of companies surveyed experienced inside information leakage, and 82.5% of information leakage accidents were by insiders. This shows how serious inside information leakage is. In ubiquitous computing environment where information sharing and information accessibility are heightened, the problem is even more serious. Thus it is urgently necessary to develop security technology that applies more strict control to inside information leakage while enabling staffs inside the company to access inside information at any time and in any place and supporting high work efficiency.

## 3. Analysis of Information Life Cycle

Security holes along life cycle of information are analyzed in this section as depicted in the following figure.


illegal retrieval of information on the network
impossible to track important information
creation
use
delivery
destruction
indiscreet access to information
information leakage through printing devices
information leakage through storage devices
information leakage through mobile terminals
unauthorized alteration and appropriation of information

- Indiscreet access to information: If there is no appropriate management and access control system for newly created information, unspecified people (who should not see the information) may access the information indiscreetly. Then the value of information is diluted and information leakage is highly possible.

- Unauthorized alteration and appropriation of information: It is highly possible for information to be altered, misappropriated and misused.

- Indiscreet leakage of information: As devices for information storage and communication are diversified with the development of online and mobile storage devices, information leakage is getting easier and faster.

- Impossible to track important information: There is no means to monitor the use and flow of important information due to lack of devices to track those involved in information leakage and to call to account those who are responsible.

Contents of security technologies and the characteristics of information security required to solve security holes that are expected in the life cycle of information.

Table 5. Security technologies for preventing inside information leakage

| Information Life Cycle | Required Security Technology | Security | | |
|---|---|---|---|---|
| | | Confidentiality | Integrity | Availability |
| Creation | Real-time encryption of user files and folders | √ | √ | |
| | Encryption of information kept in information system | √ | √ | |
| | Control over the use of information through authorization | √ | | √ |
| Use | Just-in-time user authentication | √ | | |
| | Limiting the edition of confidential information | √ | | √ |
| | Addition of watermarking to print-outs | | √ | |
| Delivery | Control over mobile terminals taken in and out | √ | | √ |
| | Control over mobile storage devices | √ | | √ |
| | Creation of security files for outside transmission | √ | √ | √ |
| Destructiion | Automatic destruction of confidential information | √ | | |

Real-time encryption of user files and folders: Information created by users must be encrypted selectively or compulsorily according to the information security policy. If a separate security folder is designated and the access right policy is defined, all information stored or moved to the security folder must be encrypted automatically according to access right. In addition, information in the subfolders of the security folder must be encrypted according to access right in the same way. Information copied or moved to other folders must be kept in the encrypted state.

- Encryption of information kept in information system: In case a user retrieves important information stored in a system linked to the company information system, the document (including attached files) is encrypted automatically. For compatibility with other systems in the linkage of search engines and virus diagnosis, however, all documents in the information system are stored as plain texts so that they do not affect existing work flows.

- □Control over the use of information through authorization: A malicious inside user may use important company information at a level exceeding his right. Thus, rights to use information should be defined specifically by individuals and groups so that they use information within defined limits (items to define rights: reading, editing, printing, releasing, taking-out, valid term, automatic destruction, etc.).

- □Real-time user authentication: When a user uses confidential information inside or outside the company, he can use it only when he is allowed to access by realtime comparison of information on his access right with information on access right contained in the information.

- □Limiting the edition of confidential information: In a joint work, a number of people share the same information and it is hard to distinguish information editors from information users. In this case, not only the whole information but also important data contained in the information must be protected.

- □Addition of watermarking to print-outs: When confidential information is printed out, all forms of print-outs must contain watermarking so that printing actions can be monitored. When confidential information is printed out, the information and image of the output are sent to the management server and then information number, the person who prints, his staff number, his department, the time of printing, etc. are included in the print-out of the information.

- □Control over mobile storage devices: Important information in the company may be taken out not only through the network by mail and folder sharing but also through mobile storage devices (floppy disks, hard disks, CD-RW, PDA, etc.). If the information security policy of the organization requires only selective encryption of information crated by users, there is no way to prevent information creators from taking out important information, which is not encrypted, using mobile storage devices. Thus strict security must be applied to the routes of information leakage by controlling rights to use mobile storage devices in individuals' and groups' computers.

## 5. Defensive Measure

### 5.1 Physical Defensive Measure

Mobile portable computing devices which are not used should be locked, keep them in the case to be not identical to unauthorized users and keep exterior memory devices separately removing from mobile portable computing devices. Secondly, Sensitive data should be encrypted if the data are stored in exterior memory devices like memory sticks and

USB flash memory. Thirdly, ID should be removed or inactivated immediately if mobile portable computing devices are stolen or lost.

### 5.2 Periodic Data Backup

Data stored in mobile portable computing devices should be periodically backs up to data server located inside of Firewall or other mobile portable computing devices. It can minimize damages causing loss or destruction of sensitive data when incidents are occurred.

### 5.3 Implementation of Security Policy and Periodic Training

Security policy for secure mobile communication such as monitoring and filtering policy for abnormal traffics and secure operation procedure for systems should be considered in aspect of mobile service provider. Security policy like sorts of storage contents allowed, network connection policy, prevention for use of extended hardware should be implemented in aspects of users. Update management is important to reflect modification of existed system or set-up of new system environment:

- Only InforSec-approved VPN clients may be used
- User of computers that are not company-own equipment must configure the equipment to comply with the company's VPN and network policies
- By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of company's network and as such are subject to the same rules and regulations that apply to the company-owned equipment.
- It is the responsibility of employee with VPN privileges to ensure that unauthorized users are not allowed access to company's internal networks.
- When actively connected to the corporate network, VPN will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped
- VPN use is to be controlled using either a one-time password authentication such as a token device or public/private key system with a strong passphrase.
- VPN gateway will be set up and managed by company's network operational groups
- All computers connected to the company's internal network via VPN or any other technology must use the most up-to-date anti virus software that is the corporate standard; this includes personal computers
- VPN concentrator is limited to an absolute connection time of 24 hours
- Dual tunneling is not permitted; only one network connection is allowed

### 5.4 Installation and Operation of Anti-virus Products and Security Software

Antivirus products for mobile portable computing devices have been developed as worm and virus is emerged Security software to provide user authentication, access control or vulnerability scan. This is most easy and effective countermeasures for users to remove security threats. Update of antivirus products reflecting recent attack information is also important.

### 5.5 Applying Strong Encryption Algorithm and Authentication Methods

Sensitive data should be encrypted because access of mobile portable computing devices is easier than PC or Server. Capability of mobile portable computing devices and battery length are also considered in addition to its strength when encryption algorithm is used because discrepancy of processing overhead can be found for encryption algorithm. When Virtual Private Network is used, it provides confidentiality and integrity to support secure remote access. Strong Authentication of mobile portable computing devices themselves such as CHAP (Challenge-Handshake Authentication Protocol), Mobile Access Number, authentication information management integrating central directories should be needed.

### 5.5 Enhancement of Security for Mobile Platform and Contents Server

Enhancement of security like security API for mobile platform and security checks of contents server is most important to prevent security threats. Applying recent security patches to mobile platform and contents server is also curtail. Filtering abnormal traffics on communication nodes should be needed by mobile service provider.

## 6. Conclusion

In this paper, we analyze security threats of mobile portable computing devices with an application of ubiquitous computing and we suggest their countermeasures in technical, manageable, and physical aspects.

## References

[1] Didi Barnes, “ Portable Computing Device Security”, September 2003.

[2]. Symentec, “Wireless Handheld and Smart phone Security”, 2003.

[3] Friedemann Mattern: The Vision and Technical Foundations of Ubiquitous Computing. UPGRADE, vol. II, no. (2001) 3-6

[4] K. Sakamura: The TRON Project. IEEE Micro, vol. 7, no. 2 (1987) 8-14

[5] Mark Weiser: Ubiquitous Computing. IEEE Computer (1993)

[6] http://www-306.ibm.com/software/pervasive/module/index.shtml

[7] Choon Seong Leem, Nam Joo Jeon, Jong Hwa Choi, and Hyoun Gyu Shin, “A Business Model (BM) Development Methodology in Ubiquitous Computing Environments”, ICCSA 2005, LNCS 3483, pp. 86 – 95, 2005

[8] Wan Seok Kim, Jeong Kook Kim, Hyo Kee Kim, Chang Seok Kim, Heung Seo Koo, Sang Beom Lee, Tae Woong Park, Seong Kook Kim: The Technology, Infrastructure and Trend of Ubiquitous Computing. Korea Information Processing Society Review, vol. 10, no. 4 (2003)

[9] Banavar G, Beck J, Gluzberg E, Munson J, Sussman J, Zukowski D. Challenges An application model for pervasive computing. Proceedings Mobicom(2000)

[10] Buxton. W.: Less is more (more or less), In: Denning PJ (ed) Invisible Computing(2002)

[11] Charles W.L Hill & Gareth R.Jones.: Strategic management theory an integrated approach, Houghton Mifflin(2004)

[12] Harter A, Hopper A, Steggles P, Ward A, Webster P.: The anatomy of a context-aware Application, Proceedings 5th Annual ACM/IEEE International conference on Mobile Computing and Networking(1999)

[13] Ishii H, Ullmer B.: Tangible bits towards seamless interfaces between people, bits and atoms. Proceedings Conference on Human Factors in Computing Systems(1997)

[14] Picard R.: Affective Computing. MIT Press(1997)

[15] Poslad, Stefan (2009). Ubiquitous Computing Smart Devices, Smart Environments and Smart Interaction. Wiley. ISBN 978-0-470-03560-3. http://www.elec.qmul.ac.uk/people/stefan/ubicom/index.html.

[16] Wikipedia.orgs