# Study on Information Security Strategy for Ubiquitous Society

LEE EUNG YONG, LIM HEE JUN, MIN KOUNG SIK,
Policy Development Division,
Korea Information Security Agency,
KISA, IT venture tower, Garakdong, Songpagu, Seoul
Korea

It is necessary for the government to anticipate threats and challenges that come with the promises of a ubiquitous information environment. Four different policy areas are distinguished for information security efforts including infrastructure, services, users and the environment, to comprehensively and effectively meet challenges to the security of the ubiquitous society. According to policy areas, four information security strategies are suggested which are securing information infrastructure, implementing trusted IT service, guaranteeing user privacy, and forming clean information use environment.

*Key-Words:* Security, Privacy, Ubiquitous

## 1 Background

Thanks to a remarkable progress of informatization and the increasing convergence between IT and the rest of the industry, Korean society is fast moving towards a ubiquitous information society; a transition expected to bring about dramatic changes touching all aspects of the lives of Korean people. Next-generation network infrastructure like BcN and USN paves the way toward a ubiquitously-networked society in which the physical world and virtual spaces are seamlessly integrated, triggering profound social and lifestyle changes. The accelerating convergence between IT and the rest of the industry offers multiple new economic opportunities, by spawning new generations of services like u-Health, and is opening up a new avenue of possibilities to strengthen national competitiveness.

Meanwhile, a u-society must contend with technological and cultural disparities in society, that sudden social changes, triggered by this process, are likely to widen, and the negative side effects of informatization, such as increasing threats to the privacy of information users. New cyber attacks of the types of bot-nets and Pharming can produce especially disastrous consequences in an information environment integrating wireless and fixed-line networks. RFID, LBS, smartcards and other ubiquitous technologies make it dramatically easier to collect, transmit and assemble personal information of users. Illegal spamming, online suicide communities or websites devoted to bomb-making and other reprehensible activities proliferate, inciting behaviors harmful to personal welfare of users and social order.

It is, therefore, necessary for the government to anticipate threats and challenges that come with the promises of a ubiquitous information environment, through appropriate response strategies, so that the benefits of u-IT may be safely enjoyed by all. In this paper, information security strategies for ubiquitous society are suggested to ensure the safety of IT-enabled services provided in a ubiquitous network environment, such as online financial transactions and medical and educational services, protect the privacy of information users and formulate clean information use environment.

## 2 Information Security Environment Forecast

### 2.1 From Information Society to Ubiquitous Society

The integration of IT in our lives and society, thus far consisting of use of communication tools linking people(P to P), is now evolving into a new, ubiquitous mode whereby people communicate with machines(P to M), and communication occurs also between things(T to T).

In this next stage of informatization in which people and things become integrated elements of an environment where information is ubiquitously present, IT has a much more direct and far-reaching impact on all aspects of life in our society.

The government has been assisting the transition of the Korean information landscape into a ubiquitous environment through its u-IT839 Strategy, providing support toward the growth of DMB, tele-matics and home networking technologies and the convergence between different IT services.

To be in keeping with the latest technological developments in IT fields, the U.S. and Japan and also the EU region have been massively investing in R&D in next-generation technologies and u-network infrastructure. In the U.S. efforts to take IT to the next level are coupled with initiatives for innovative applications by integrating IT with cutting-edge technological fields like NT and BT. Through the use of network, Japan successfully upgraded not just IT itself, but communications devices, consumer electronics, industrial equipment and peripheral technologies; in other words, its traditional areas of strength. The EU, interested in a human-centered computing approach, is looking to develop a variety of intelligent services.

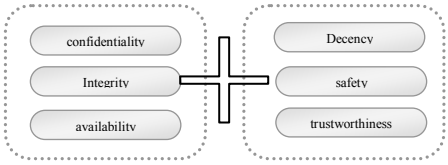
## 2.2 Characteristics of a Ubiquitous Society

Convergence between technologies, industries and services increases. New hybrid services, created from the convergence between telecommunications (internet) and broadcasting or other industries, are being introduced. DMB, a technology delivering broadcast content over mobile communications network, enables real-time TV viewing in a mobile environment. Next-generation consumer electronics and home appliances like D-TV sets, DVD players, internet refrigerators and intelligent service robots are expected soon to become industry-leading products. Integration of IT in the automotive industry (for example, cars shipped with built-in DMB devices), providing new ways to upgrade car models and differentiate product lineups, is helping to boost the sector's competitiveness.

New types of social interaction in cyberspace and lifestyle revolution are triggering personalization. A ubiquitous society offers personalized services, adapted to individual taste and interests. This will have a major consequence on the way the internet is used and how users interact with others online, giving rise to, among others, new types of virtual communities. Open communities like 'blog' are expected to sharply grow in numbers, becoming something that deserves to be called a one-person media market. With the progress of ubiquitous networking, one-person media is likely to evolve into new types of communities like 'locative media'.

Homes will no longer be simple places of residence and resting, but will be transformed into multi-function digitalized living spaces where knowledge is created, and information shared.

## 2.3 Characteristics of Information Security in a Ubiquitous Society




<Information Security Properties in the Ubiquitous age>

In a ubiquitous society, information security efforts, formerly concerned with the safety of systems and networks, now extend to that of devices. The current list of priorities in information security, consisting of confidentiality, integrity and availability, will be expanded with new goals such as trustworthiness, decency and privacy.

Information security, in a u-society, is no longer a static process, but becomes a 'conformable' process, whereby services are appropriately modified, based on contextual information captured through sensor technologies.

Information security for ubiquitous society enhances the public acceptance and adoption of new IT service by raising the level of users' trust in u-services and confidentiality of transaction information.

Information security anticipates and prevents new types of cyber attacks including hacking and viruses and cybercrime targeting the ubiquitous information environment. It prevents service disruptions for new converged-type, internet-based IT services such as

IPTV and VoIP(Voice on IP) by thwarting cyber attacks launched via wireless and fixed-line networks. It fights cybercrime making use of the latest technologies and blocking indecent or harmful information. And it provides social and legal infrastructure necessary for controlling side effects of ubiquitous networking, including information security-related laws to regulate the handling and use of location information and medical information.

Four different policy areas are distinguished for information security efforts, including infrastructure, services, users and the environment, to comprehensively and effectively meet challenges to the security of the ubiquitous society.

# 3 Information Security Strategy

| Hierarchy of u-Society | Core Strategic Objectives |
|---|---|
| environment | guaranteed privacy |
| services | trusted IT services |
| users | guaranteed privacy |
| infrastructure | secure info. infrastructure |

< Core Strategic Objectives for u-Society>

Four different policy areas are distinguished for information security efforts including infrastructure, services, users and the environment, to comprehensively and effectively meet challenges to the security of the ubiquitous society. According to policy areas, four information security strategies are suggested which are securing information infrastructure, implementing trusted IT service, guaranteeing user privacy, and forming clean information use environment.

## 3.1 Securing Information Infrastructure

| Policy Areas | Detailed Objectives |
|---|---|
| network | Establishing management system to safeguard network infrastructure |
| software | Strengthening security and reliability of software applications |
| security capacity | Enhancing capacity to prevent cyber intrusion incidents |

<Detailed Objectives for Securing Information Infrastructure >

A comprehensive security management system for BcN should be built. A strategy should be developed to effectively counter threats to personal data, posed by next-generation worms and viruses targeting mobile handsets and PDAs, and other intelligent, portable devices, magnified by the increased use of devices of this type. Cyber attack prevention and response technologies should be developed to strengthen the national response system. Security guidelines and security check methodologies to enhance security at the level of individual subscriber networks should be developed. Solutions to ensure the security of networks with different security levels and owned by different operators, interconnected within BcN should be devised.

A comprehensive security management system for USN and IPv6 should be developed. A network management system to guarantee secure transport of sensor-captured data should be created. Light-weight security chips for use with sensor nodes to effectively block attempts of illegal interception, forging or altering of information stored within sensor nodes are needed. Security standards for USN devices and develop a security test system should be established so that the reliable performance of security modules inside USN devices can be ensured from the design stage on. Security of the IPv6 environment and process of migration toward it is required. A security system for mixed IPv4/IPv6 networks to facilitate secure transition and to promote the secure operation of IPv6 networks is important.

Security and reliability of u-Society software Applications should be enhanced. An information security framework to block and respond to intrusion attempts targeting national software infrastructure to minimize disruptions of critical public services, making embedded security features mandatory and providing other security standards is required. A certification system for the security of open and embedded software products should be upgraded.

Capacity to thwart cyber intrusion attempts should be enhanced. An information tracking system allowing to trace the path of information, in reverse, back to the initiator of an intrusion attempt, should be reinforced. The focus of security efforts for networks and systems from monitoring-based protection to prevention should be shifted by investing more in

detection tools for identifying and eliminating vulnerabilities before they may be exploited by intruders. Infrastructure for digital forensic investigations should be implemented, including standard procedures for collection, analysis and use of digital evidence and authenticating digital evidence.

The framework for information security governance should be built. An information security governance framework and guidelines for developing a governance structure to help companies protect their IT investments through systemic, organization-wide efforts is required. Information security architecture linked to EA/ITA and develop a reference model should be designed.

## 3.2 Implementing Trusted IT Services

| Policy Areas | Detailed Objectives |
|---|---|
| users | Creation of a new authentication system adapted to next-generation u-services |
| contents | Integrated wireless-fixed-line content security system |
| platforms | Reliability of u-devices |
| services | Reliability of u-service use environment |

<Detailed Objectives for Implementing Trusted IT Services >

Electronic authentication frameworks targeting different levels of threats should be developed. A framework for user authentication processes geared toward providers of critical, applied ubiquitous services that include a classification of authentication services according to the type of IT services for which they are used, recommended procedures and methods.

A Digital ID management system giving greater control to users over the level of privacy and security concerning their personal data should be implemented. ID management techniques should be developed which allow users to specify, in accordance with the privacy policy of service providers, whether personal information they provided to them, may be shared with third-party organizations and, if yes, under what conditions.

Protection of copyrighted digital content should be reinforced. A system to protect content distributed through converged telecom-broadcasting media and mobile networks, from unauthorized access and use (creation of a system integrating mobile DRM, CAS and CP technologies) should be developed. A content protection environment should be created in which DRM, CAS and CP technologies, independently developed for specific domains distributing content, such as wireless and fixed-line internet domains and servers transmitting digital broadcasting content or serving digital home can be used, without interruption, across diverse networks constituting the nexus of ubiquitous information services.

The reliability and interoperability of u-Devices should be improved. Device authentication models adapted to different ubiquitous service environments by analyzing authentication scenarios, varying according to service characteristics should be developed. Certificate lifecycle-based device authentication management models for different authentication environments and related guidelines should be designed. Mobile TPM and middleware technologies for security and reliability services should be developed, to enhance the dependability of converged/hybrid service devices that are becoming increasingly open, smart and multimedia-centered.

An information security management system for protection of personal privacy to minimize theft and misuse of personal data and other social losses caused by their unauthorized access and use should be created. International cooperation efforts to build public trust for information security services through international standardization of ISMS and mutual recognition agreements should be engaged. A methodology for assessment of impact on information security for use during the development of new converged and hybrid IT services like VoIP and WiBro should be developed to minimize social losses caused by intrusion incidents targeting these services.

## 3.3 Guaranteeing User Privacy

| Policy Areas | Detailed Objectives |
|---|---|
| infrastructure | Building u-service privacy architecture |
| environment | Creation of social context and legal framework supportive of u-privacy |
| extended personal information(1) | Protection of video images |

| | |
|---|---|
| extended personal information(2) | Protection of biometrics, location and RFID data |

<Detailed Objectives for Guaranteeing User Privacy >

Privacy protection architecture should be developed. Systemic and concrete approach to the development of privacy protection technologies should be developed, to design solutions that are optimally adapted to the ubiquitous computing environment.

Social and cultural context supportive of privacy should be established. Training requirements for privacy officers of businesses with online presence and develop privacy rules adapted to individual business sectors should be reinforced. Certification marks to companies having privacy management systems meeting required standards and having completed privacy enhancement education can be issued. Special efforts to educate less information-savvy segments of the community about privacy risks and teach them how to minimize their vulnerability to identity theft should be given. International cooperation in privacy enhancement should be enlarged. A legal and regulatory framework for privacy protection should be established.

Protection of Location Privacy should be reinforced. Technical standards for personal location information security and enforcement of privacy rules should be developed. The technical standards can allow location-based services to automatically reflect user-defined settings so as to give users greater control over the information shared, and make the services more convenient for them. Legislation for protecting location privacy should be made. This legislation should make mandatory the location information security obtained by government organizations, through the bus information system or highway cameras, and employee location information from companies' internal network, and establishment of location privacy procedures.

Biometrics information privacy standards should be developed and public awareness about related privacy risks should be raised. A certification program to guarantee the integrity of biometrics information and technologies for secure transmission and storage can be effective. A central information system achieving optimal integration of individual medical information systems and enabling the efficient management of them, and common standards for medical information security should be developed.

A security system for CCTV-captured video data should be created. Rules to regulate the installation and operation of CCTVs to curb the privacy risks associated with the use of these surveillance units are required. Public awareness about potential privacy risks caused by the installation and operation of CCTV should be raised.

A privacy protection system for RFID services should be in place. Users' right to refuse tracking and tracing so that they can escape RFID-based monitoring whenever they choose should be ensured.

## 3.4 Forming Clean Information Use Environment

| Policy Areas | Detailed Objectives |
|---|---|
| digital contents | Designing response system eradicating indecent or illegal contents |
| Information users | Educating users for safe and healthy use of information |
| Information use environment | Nurturing u-clean culture |

<Detailed Objectives for Forming Clean Information Use Environment >

A response system to eradicate indecent or illegal contents in ubiquitous networks should be designed. Regulatory mechanism to control the circulation of objectionable information content threatening the decency of the ubiquitous information environment should be established. Cybercrime, cyber violence, cyber stalking and harmful content should be clearly re-defined to develop a precise classification system for internet and network-related offenses adapted to the new, ubiquitous information environment. The regulation and oversight of internet content to defend the decency of the internet should be strengthened when the introduction of converged telecom-broadcasting services and other hybrid services are triggering rapid changes in the nature of content distributed across cyberspace. International cooperation in blocking offensive and harmful content such as obscene materials or gambling-related information which can have disruptive consequences for society should be upgraded. Spam through a joint international response system should

be lessened by strengthening cooperation and exchange with anti-spam organizations of the U.S. and E.U. countries and international organizations involved in anti-spam efforts.

Educating users for safe and healthy use of information should be reinforced. Measures to fight new types of media addiction in the ubiquitously networked environment should be prepared. Prevention programs and internet hotlines for those suffering from media addiction should be operated, factors influencing excessive media dependence and identified, and related programs to ensure their effectiveness clearly monitored. The image of a model u-society citizen should be created and information ethics promoted. Internet ethics required for the well-functioning of the u-society in the public by educating general users and opinion leaders through various media should instilled.

The u-clean culture should be nurtured. Information security awareness to prevent information theft-related privacy infringement and losses should be raised. Education strategies to introduce youth, parents, teachers and online service providers should be devised. Inciting businesses to invest more in information security and take an active part in the fight against cyber attacks, and increase the supply of privacy manpower through a human resource development program in the area of personal information security, is needed. Education and prevention efforts against personal rights violations in the u-society should be launched and institutional and legal frameworks for defending basic human rights within cyberspace should be built. Programs to fill the digital divide should be launched, to ensure equal access to the benefits of the u-society by extending opportunities for informatization to all segments of the population.

# 5 Conclusion and Future Work

In this paper, strategy framework to manage information security in the ubiquitous age was suggested. Four core strategic objectives were identified to protect infrastructures, services, users, and environment in the future. Activities to perform the objectives were introduced.

This study would help information security policy makers and manager define strategic directions for information security in preparation for the ubiquitous age, and design countermeasures to emerging cyber threats.

As future work, development of metrics to measure the level of nation's security countermeasure against threats in the ubiquitous age will be considered. The metrics will be developed by considering core strategic objectives suggested in this paper and diverse security options including political, technical, and legal ones.

*References:*

[1] Ministry of Information and Communication, *information security strategy for the ubiquitous age*, 2006. 12.