Sturdy of Security Reference Model of u-City Integrated Operating Center

Chansuk Jung*, Yongtae Shin*, DongHoon Shin**, Yunmook Nah**
*Soongsil University, **Dankook University
izmit70@gmail.com

Abstract: With the diffusion of ubiquitous technologies, many city facilities that are closely related with our daily life are being combined with IT technologies. As a result, various IT services running on the separate network are also being integrated into a city-based service. However, serious problems can occur in terms of the stability and reliability of the u-City(Ubiquitous City)service, if the security factor is not fully considered and applied while developing new IT services that will be integrated into u-City projects. In particular, if any security incident occurs at the u-City Integrated Operation Center (uCIOC), which is designed to collect, analyze and combine the city-related information, and manage and operate the city functions, serious chaos could occur due to a paralysis of the city functions. This paper proposes the security reference model of u-City Integrated Operating Center

Keywords: security reference model, u-City

1. Introduction

With the rapid development of wire/wireless communication technologies and the advent of the ubiquitous environment, city infrastructure facilities closely related with daily life are being mixed with IT technology. Consequently, various services running on the independent network are also being integrated into the u-City service. With the introduction of the u-City concept, duties such as civil complaint processing and security management are combined into a single duty, so that it can be managed systematically and the information can be shared. However, on the reverse side of the coin, with the appearance of the ubiquitous society and the development and expansion of u-City, the volume of information security threats - such as the inundation of unethical and anti-social content through various information media, and cyber crime that threatens the individual's property and life - has been increasing on a daily basis. In this context, the importance of the uCIOC, which is designed to manage new IT services to be newly integrated into u-City, and monitor and manage the city infrastructure facilities, has increased rapidly. Any security incident involving the uCIOC could cause chaos throughout the city. Hence, this paper analyzes the characteristics of the uCIOC in order to draw out the security threats and to propose protection measures against them.

2. Overview of u-City

2.1. Concept of u-City

u-City may be defined as the advanced city that is able to play the role of providing increased convenience of life and greater quality of life, systematic city management, the innovation of various city functions through systematic management, and the generation of various markets, by offering a ubiquitous service to the city space using the advanced information and communication infrastructure. u-City aims for the construction of a convenient, safe, pleasant, and healthy city through the convergence, integration, and intelligence of the entire city, based on ubiquitous computing and IT technology. The convenient city can be implemented by providing greater convenience to the u-City residents, and by utilizing wire/wireless high-speed Internet and home networking technology, telematics technology and online shopping, online administration, and e-Business. The safe city can be implemented through crime prevention, safety monitoring, public security and security management, and facility safety and disaster prevention functions. The pleasant city can be realized by managing water quality, soil, and atmospheric pollution, and by taking the appropriate countermeasures. The healthy city can be realized by introducing a remote medical care system, an emergency rescue method, and integrated health management techniques. All these functions are part of a new service that exploits advanced IT technologies, and which is capable of creating diverse markets and making the life of the general public more prosperous.
2.2. Characteristics of u-City

The characteristics of u-City can be analyzed from the perspectives of intelligence, network, platform, and service, as shown in Table. That is, u-City has the characteristics of the intelligence of the city functions that manages and optimizes various contexts related with the city functions, and the wire/wireless communication network connection that is the foundation for the realization of the electronic space, and the common platform and integrated management that pursue the utilization of a universal server at any time and place, and the diversification and commercialization of the application that aims for the integration of a practical service with ubiquitous network technology.

<table>
<thead>
<tr>
<th>Item</th>
<th>Major contents</th>
</tr>
</thead>
</table>
| Intelligence | - Real-time management of the city infrastructure, such as roads, and city infrastructure facilities, such as an airport, in the ubiquitous network environment.  
- Utilizes the related project in a mixed way, such as IT, BT, and NT for the intelligent city function.                                    |
| Network      | - Foundation that realizes physical space (city) as an electronic space.  
- Seamlessly connects all people, objects, and computers in a city.                                                                                           |
| Platform     | - A common platform that makes the service available regardless of the user, place, and time is required.  
- The need for a u-City UCIOC that can adjust various services, so that safe and convenience service utilization can be guaranteed, has emerged. |
| Application  | - Implements a service that provides real city functions in the electronic space.  
- Realizes the ubiquitous environment from the perspectives of space (home, school, office, and others) and functions (transportation, administration, health care, and others). |

2.3. Types of u-City service.

The u-City service can be grouped into infrastructure services and specialized services, depending on the objectives of service application, namely publicity, efficiency, convenience, profitability, and self-sufficiency. Infrastructure services are applied indispensability to the main city functions, whereas specialized services are designed for city competitiveness.

In addition, the u-City server type can be grouped into u-Home, u-Work, u-Traffic, u-Health, u-Environment, u-Public service, and u-Education, depending on the scope of service application. These u-City services are implemented by combining several elements: ① wire/wireless communication infrastructure (e.g. xDSL, FTTH, RFID, WiBro, mobile communication, HSDPA, and others); ② city infrastructure such as advanced intelligent buildings and intelligent roads; ③ solutions such as home networking, and building management systems; ④ contents like e-Learning and IP-media.

<table>
<thead>
<tr>
<th>Item</th>
<th>Major contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>u-Home</td>
<td>Remote metering, remote control, remote repair, access door control, home networking, IP-media</td>
</tr>
<tr>
<td>u-Work</td>
<td>Home working, teleconference, wireless e-Commerce</td>
</tr>
<tr>
<td>u-Traffic</td>
<td>Traffic, car accident processing, integrated road management, telematics</td>
</tr>
<tr>
<td>u-Health</td>
<td>Healthcare service, remote medical examination, remote medical treatment, first-aid</td>
</tr>
<tr>
<td>u-Environment</td>
<td>Environment management, hygiene management</td>
</tr>
<tr>
<td>u-Public</td>
<td>e-Government, crime prevention, disaster management</td>
</tr>
<tr>
<td>u-Education</td>
<td>e-Learning, school management system, school attendance management system</td>
</tr>
</tbody>
</table>

3. u-City promotion trend in Korea

As shown in Table 3, about 20 local autonomous bodies in Korea claim to stand for u-City implementation, and are either setting up the USP (Ubiquitous Strategy Plan) or are at the initial development stage [3].

<table>
<thead>
<tr>
<th>Type</th>
<th>City name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exisiting city</td>
<td>Seoul, Busan, Daejeon, Gwangju, Ulsan, Incheon, Jeonbuk, Chungnam Hongseong, Chungbuk Osong, Jeonju, Yangsan, Pohang, Gangneung, Jeju</td>
</tr>
</tbody>
</table>
In 2007, the government carried out "6 u-City test bed projects" which together served as a model project for the promotion of u-City business initiated by the former Ministry of Information and Communication. Also, the government established a "u-City Strategy Plan (USP)" for each local autonomous body through the "local informatization implementation plan" driven by the Ministry of Public Administration and Security, in order to build u-City. In addition, the Ministry of Construction & Transportation has substantially led the construction work related with u-City, conducting active promotional efforts such as the enactment of the "Act on Ubiquitous City Construction." Since the restructuring of governmental agencies in 2008, the Ministry of Land Transport and Maritime Affairs has been managing the construction of the ubiquitous city actively. According to the research performed by local autonomous bodies in 2008, 48 organizations are planning u-City construction.

### 4. u-City Integrated Operation Center

#### 4.1 Definition of uCIOC

u-City Integrated Operation Center (uCIOC) is an information system that collects city information from sensors in the u-City communication network, traffic network, facilities, and integrated terminal, and then monitors and analyzes the collected information in order to effectively operate and manage the city and to provide that information to the citizen or to related organizations.

#### 4.2 Functions and roles of uCIOC

The uCIOC performs the convergence, integration, and intelligence of the city information, and serves as an innovation hub. It also collects, processes, and provides useful information as the information media of various ubiquitous services that will be operated in the u-City. The roles to be played by the uCIOC are listed in the following table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Roles</th>
</tr>
</thead>
</table>
| City information collection | - Collects information from external organizations such as police and fire-fighting stations.  
- Collects various types of information including traffic and environmental information from the integrated terminal and CCTV. |
| Operation and management | - Integrates and monitors the collected information, and analyzes its quality in real-time.  
- Operates the device and the network infrastructure.  
- Operates the integrated control room, and processes customer complaints. |

#### 4.3 Composition of uCIOC

The following section describes the necessary technology and characteristics of each component from the perspectives of the city information flow, including collection, integration, processing, and provision.

The first component of the uCIOC is the information provisioning layer. The information provisioning layer is a collection of service modules that provides the best information usage environment to u-Service users and center operators, such as home terminals, portable terminals, PCs, and laptops. This component includes screen layout technology that is optimized for various information use terminals, contents processing system development technology, real-time communication between sensors and terminals, and context-sensitive contents provisioning technology.

The second component is the information development layer. The information development layer is a collection of service modules that develops, processes, and provides value-added information to the user, based on the collected and integrated information. It implies the common service module, such as GIS-based information presentation technology and image information interface technology.

The third component is the information integration layer. It is a collection of service modules that smoothly integrates the information collected from each sensor as well as the information received from the organization to link, and saves and stores the collected and linked information in a stable manner. This component encompasses ESB-based platform technology, interface technology such as EAI, sockets, the API to link with
various external organizations, integrated database development technology to handle large-capacity city information such as the large amount of sensor data and image data, and service design technology that considers process integration such as BPM technology.

The fourth component is the information collection layer. This layer is a collection of service modules that collects the information stably from the facilities and sensors installed in the u-City, such as networked CCTV, advanced street lamps, and USD sensors. It includes USD middleware technology that processes the information collected from the multiple heterogeneous sensors.

The last component is the information management layer. This layer is a collection of service modules that manages the u-Service operated by the uCIOC and the system that implements these services. It includes server system monitoring technology that introduces SMS, city network and sensor network monitoring technology through the introduction of NNMS, and system security technology.

5. Security Reference Model of u-City Integrated Operating Center

5.1 Overview

This paper proposes the security reference model of u-City Integrated Operating Center as shown in the diagram below.

The security reference model is designed to provide the information integration, information presentation and interface services for u-City service support and management through the managerial, physical and technical countermeasures against the security threats; and definition of entity security elements concerning the responsibility tracking and auditing, authentication, privilege, confidentiality, integrity, denial blockade, availability and information security. The internal and external security threats include the application security threats, basic technology security threats and application technology security threats against the integrated operating center platform infrastructure such as the u-service processor, information/situation processor, connection/infrastructure management processor, operation processor as well as the integrated operating center interfaces such as the information output interface, interface infrastructure interface, external agency interface, legacy/Web interface and information collection/IT based interface.

5.2 Security Threats and Countermeasures in Managerial, Physical and Technical Aspect

5.2.1 Security Threats and Countermeasures in Managerial Aspect

The electronic control/management system related to national security, administration, defense, justice, finance, telecommunication, transportation and energy; and the information and communication network according to the Article 2, Paragraph 1, Item 1 of Information and Communication Usage Encouragement and Information Security Act are designated as the information and communication basic systems. According to the "Information and Communication Basic System Act," the information security management system needs to be developed when building the u-City integrated operating center.

<table>
<thead>
<tr>
<th>Threat/Vulnerability</th>
<th>Threat Scenario</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Policy</td>
<td>Lack of operating consistency due to the lack of an information security policy and guide, confusion in operating measures and inadequate responsibility assignment within the organization</td>
<td>Preparation of information security policy document</td>
</tr>
<tr>
<td>Management System Domain Configuration</td>
<td>Increasing difficulty of asset management due to inadequate establishment of an information security management domain needed for center operation</td>
<td>Specification of information security management domain and analysis of asset status</td>
</tr>
</tbody>
</table>
Threat Management Measures

- Increasing difficulty of preparing the countermeasures against the threat due to the lack of threat management measures
- Establishment of threat analysis/evaluation, information security plan and measures

Training Measures

- Increasing difficulty of coping with the problems and intrusion accidents due to the lack of information security training
- Preparation of information security training plan

Internal Audit Measures

- Increasing difficulty of understanding the current operation level and identifying the improvement opportunities as there is no audit of center operation
- Preparation of audit plan and monitoring plan

Security Threats and Countermeasures in Physical Aspect

<table>
<thead>
<tr>
<th>Target</th>
<th>Threat</th>
<th>Threat Scenario</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Entrance and exit of unauthorized person and burglary</td>
<td>Burglary of equipment as the access control and protection zone against the unauthorized person is not set up</td>
<td>Checking of server and change of configuration using the OS specific server security guide, installation of SecureOS, etc.</td>
</tr>
<tr>
<td>CCTV</td>
<td>Personal Information Security Act violation</td>
<td>Legal conflict due to the lack of guidance for CCTV installation</td>
<td>Compliance of CCTV installation standard</td>
</tr>
<tr>
<td>IT Equipment</td>
<td>Natural disaster, fire, burglary, and lack of periodic backup</td>
<td>Loss of operating center equipment due to fire</td>
<td>Development of disaster recovery system and backup policy</td>
</tr>
</tbody>
</table>

Security Threats and Countermeasures in Technical Aspect

As the hacking and information threat environment changes from the simple hacking of showing-off to more complex environments such as inducing the confusion with the purpose of acquiring monetary value or information, the importance of information system security is becoming more and more important. The security threats of information system include the inadequate configuration of the server, network, Web application, database, PC and security systems, and management negligence by the personnel in charge. Since the integrated operating center consists of a set of such information systems and as the threat of individual target can affect the whole system, the technical security measures must be established and applied.

<table>
<thead>
<tr>
<th>Target</th>
<th>Threat</th>
<th>Threat Scenario</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Account management, privilege control, logging and virus vaccine</td>
<td>Access by the user without the privilege using the server vulnerability and unauthorized alteration of the data</td>
<td>Checking of server and change of configuration using the OS specific server security guide, installation of SecureOS, etc.</td>
</tr>
<tr>
<td>Network</td>
<td>Account management, access control, remote connection and encryption</td>
<td>Exposure of privilege to the unauthorized users through the login using the default account</td>
<td>Checking of threat and change of configuration using the security configuration guide, encryption using SSL/TLS, and communication over VPN</td>
</tr>
<tr>
<td>Web Application</td>
<td>Lack of input value verification, weak authentication and lack of session management</td>
<td>Leak of internal data due to the lack of input value verification</td>
<td>Checking of applications using the application security guide, compliance of development procedure using the Web development guide, and development of WAF (Web Application Firewall)</td>
</tr>
<tr>
<td>Database</td>
<td>Data encryption and access control</td>
<td>Leak of unencrypted personal data through the access to the DB without the access control</td>
<td>Encryption of key data (ref. NIS Encryption Standard) and installation of DB security products</td>
</tr>
<tr>
<td>PC</td>
<td>Virus vaccine and account</td>
<td>Leak of internal data due to the lack of Vaccine installation,</td>
<td></td>
</tr>
</tbody>
</table>

□ Security Threats and Countermeasures in Physical Aspect

□ Security Threats and Countermeasures in Technical Aspect
6. Conclusion

u-City can be deployed through the various services and technologies using the concept of ubiquitous. Various u-city reference models are developed and the service is deployed and operated in consideration of different areas such as the architecture, environment, transportation, health, sanitation, and public order. There are various basic technologies, application technologies and application models of different types to support u-city. The importance of integrated operating center is increasing as the need for integrating the various technologies and services is increasing. As the importance and necessity of the integrated operating center is increasing, various types of integrated operation center models are being presented and prepared. u-city forums and individual enterprises are analyzing or developing the reference models in preparation for applying them. As the various activities to build the integrated operating center are carried out and the need for the integrated operating center increases, building the integrated operating center will be considered as mandatory when developing u-city. However, the diverse nature of the ubiquitous environment, in which various environments, technologies and knowledge are applied, demands the model appropriate to all of the various environments. Nonetheless, deployment of integrated operating center through information security during the model deployment step with consideration to various environments and technologies has been inadequate up to this point. As such, this paper presents the security threats of Integrated operating center for u-city and proposes the u-city integrated operating center security reference model as a countermeasure. It is hoped that the security reference model proposed in this paper will help building a safer and more efficient integrated operating center.

References:

[8] www.ubicity.org, u-City Forum
[10] "u-City operation center and platform as a u-City infrastructure", Lim, Gyoo-gwan, Kim, Ji-seon