Implementation of Home Network Security System based on Remote Management Server

Young Gun Jang, Hoon Il Choi, Chan Kon Park

Dept. of Computer & Information Engineering, Chongju University, Rep. of Korea

Summary
The user authentication and access control technology of home networks has, up until recently, adopted a practice of direct security management by residents, with the placing of the security system in the home network of each house. Such a type of system has a high probability of producing weaknesses in security, because home residents must manage their security. Additionally, as the security system is placed in the network of each house, system construction costs are incurred, and many weak points may arise in the maintenance and management of the security system. In this study, a user authentication and access control system for home networks was designed and implemented based on a remote management server. This approach, which was competitive in terms of price and service flexibility, was also suitable for mass housing types, such as apartment complexes and large buildings, and was designed in such a way that no professional knowledge was required of the individuals using the network. In the test, the system showed stable functionality for authentication and access control.

Key words:
home network, security, authentication, access control, remote management server,

1. Introduction

The network environment, originally constructed in enterprises and public organizations based in offices, has recently been expanded to the electronic devices used in the home. The combination of the rapid development in IT technology and the wider distribution of internet services through high-speed networks has resulted in an elevated interest in the home network market. The government has announced a plan to construct 10 million such “digital homes” by the end of 2007. The prediction was recently made that the home network market will produce as much as 22.2 trillion won of production induction effect and will create 160 000 jobs by the end of 2007. This forecast shows the growth opportunity and the spreading effect of home networks [1].

In the home network system, security problems such as hacking, viruses, and exposure of personal information, traditional problems in network environments, still exist, and new security problems have developed because most of the devices connected with the network are quite simple. Such problems are a major technological factor interfering with market activation, and demonstrate the great necessity for information protection and security. As home network systems may manage the information of home appliances and health care devices, access by unauthenticated users should be blocked , and even the use of devices by authenticated users should by differentiated according the user’s profile to prevent damage and leakage of information through inappropriate device usage. ”Parental controls” are a perfect example of this need; for example, when VOD services are provided through DTV, a function blocking children’s access to adult channels is needed; as well, user authentication for potentially dangerous elements such as gas control is necessary.

The most popularly developed security method is to equip the home gateway with the functions of firewall and VPN (virtual private network) as the primary countermeasure against illegal invasion [6-7]. The purpose of access control and authentication of home network resources and services is to provide the user with safe home services. In Korea, ETRI and companies such as UbiwareLab and Initech have developed technology and products addressing this need, while foreign companies operating in this market are MicroSoft, CablesLabs, and NTT. However, until now the technology has related to security products for home networks that are based in each home, and in most cases the products must be operated directly by the residents of the home [7]. The first instance of a home server for a home network being installed outside of the home was in 2002. At that time, the method of solving the problem of security was that the home internet should have a dynamic IP address. To address the problems of installing a firewall and a proxy server in the home network, the virtual home server was installed outside of the home. This method was used to control LG washing machines through the internet, and was not a general-use remote control service [8].

In this study, the security problem that might result from unskilled residents managing their home security, and the cost problem resulting from security technology being located in the home network of each home was solved; a system for user authentication and access control was

Manuscript received February 5, 2007.
Manuscript revised February 25, 2007.

suggested based on a remote management server [9] appropriate for application to mass housing and working spaces such as apartment complexes and large buildings; and such a system was designed and implemented.

2. Home Network Systems and Security

2.1 Home Network Systems

The structure of a general home network system is shown in Fig. 1. Home information devices may perform a sending/receiving function in connection with an external network through a home gateway, and the sending/receiving of information within the home is done through the home network. Home information devices may be managed outside of the home, through the use of devices such as handsets, PDAs, and computers.

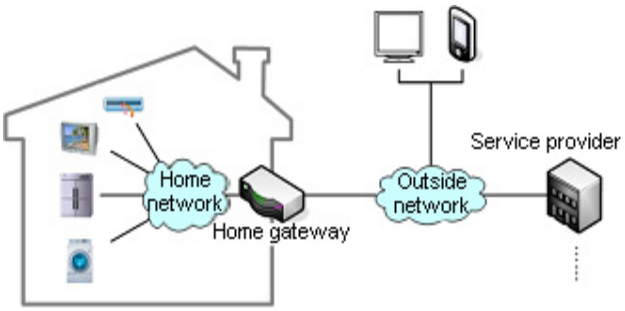


Fig. 1 The structure of a typical home network system.

2.2 Control of Authentication/Access of General Users

Information data for user authentication and access control policy data is needed to assign the authorization for access control, to authenticate the users, and control access to the general network system as shown in Fig. 2. Such data is stored in an information pool, such as an authentication and policy DB. Both an authentication server to process authentication requests from users, and a policy server to process access control are needed. These servers process the user authentication and access control requests through interworking with the DB in which such data is stored.

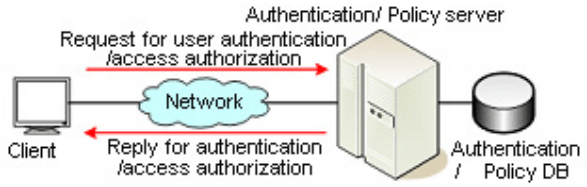


Fig. 2 The control of authentication/access of users in a general network system.

2.3 Control of Authentication/Access of Home Network Users

Methods of user authentication and access control in home network systems are largely classified as either home server-based [10], where the DB and authentication/policy service function is located in the home, or as remote management server-based [9], where the DB and authentication/policy service function is located outside of the home. Basing user authentication and access control method in the home server is advantageous in terms of protection of personal information, because the information is directly managed by the users, with no external exposure of the information taking place. However, in this type of system, it is the responsibility of residents to manage of data and the DB authentication/policy for user authentication and access control, manage and maintain the authentication/policy server, and perform system upgrades. As direct management of security by non-professional users may result in mistakes and errors, the stability of security management, reliability, and the management and maintenance of security system has the potential to become very weak. Also, since the authentication and access control system is located in the home, the user must bear the cost and time burden for installation of the system. In contrast, when user authentication and access control is based on a remote management server, the data for user authentication/policy and the function of DB and authentication/policy server is placed outside the home, resulting in possible hacking or illegal access; however, the stability and reliability for security management may be more strongly assured, because professionals are in charge of data management, management and maintenance of the DB and authentication/policy server, and system upgrades. For housing environments such as apartment complexes, a remote management server can be placed in the apartment complex office to process the user authentication and access control for each household; therefore, the cost of installing a security system in each home may be saved, and users may concentrate on using the services of the home network system to act as a positive factor in activation of the home network.

3. Design and Implementation

3.1 System Configuration

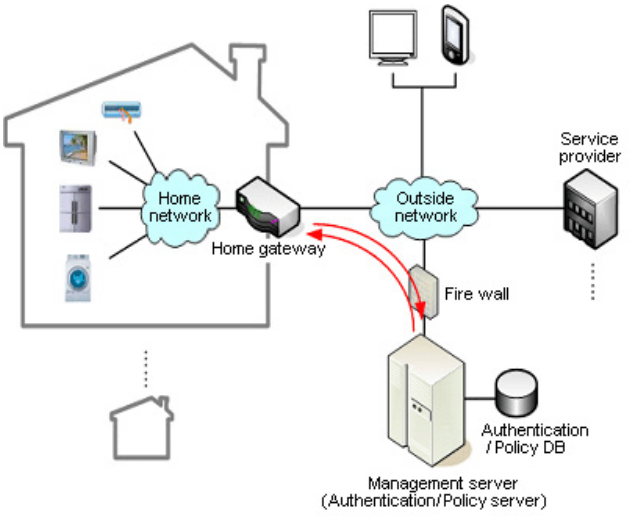


Fig. 3 User authentication/access control based on a remote management server

In this study, the user authentication and access control service of the home gateway was developed based on the OSGi framework [12] to construct the user authentication and access control system of home network based on a remote management server. A XML based communication protocol for request/reply in relation to authentication and authorization between home gateway and management server was defined, the DB to store user authentication and access control policy in communication service and management server was constructed and web-based remote management server was designed and organized for possible access from a remote location. The diagram of the system is shown in Fig 4.

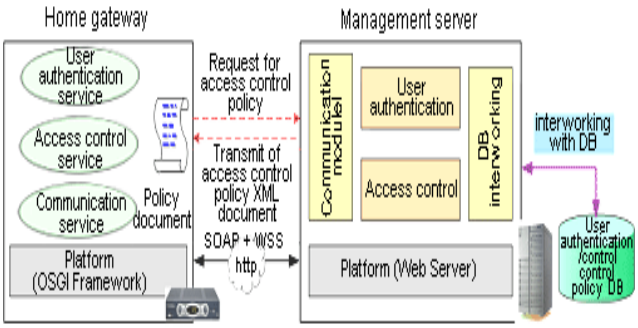


Fig. 4 Diagram of user authentication and access control system based on a remote management. server

3.2 Development Environment

The development environment of the system implemented in this study is as shown below:
- J2SDK 1.4.2;
- Eclipse 3.1 with WTP 0.7;
- Oracle 9.2.0.1.0;
- Tomcat 5.0; and
- JSP, Servlet, JavaScript, ...

3.3 Design and Implementation of User Authentication and Access Control Service

OSGi (www.osgi.org) is the abbreviation of 'Open Service Gateway Initiative', a nonprofit standardization organization established in March 1999. OSGi established an industrial standard Java-based open service platform service providers could adapt to suit the home environment. OSGi defines the UserAdmin Services for user authentication and access control; these services do not apparently express the information on Bundle and Service and do not apparently express the access control based on the roles; therefore, these services are not appropriate for the remote management server model suggested in this study. As a result, a user authentication and access control service was designed and implemented to meet the specifications of the remote management server model suggested in this study, and the services were prepared as bundles to be used in OSGi. The constitution of interface for the user authentication and access control service implemented in this study is shown in Fig. 5.

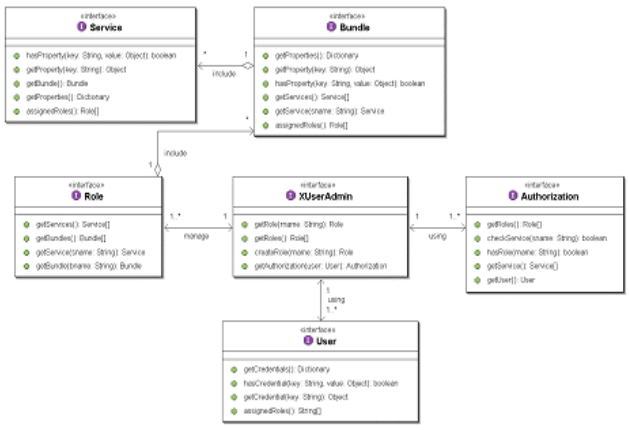


Fig. 5 User authentication and access control service interface.

3.4 Design and Construction of Database

The information for assignment of authorization for user authentication and service access was made as DB and interworking is performed between this DB and the management server. Upon the request for user authentication and the request for access control policy from the home gateway, the management server carries the needed data by making an inquiry to the DB.
Confidential information and authentication information related to users stored in authentication tables. ID/PW information is only stored when the information is related to current authentication and, in case of the addition of a new authentication method, a table having a one-to-one relationship with the user's table should be prepared at each authentication.

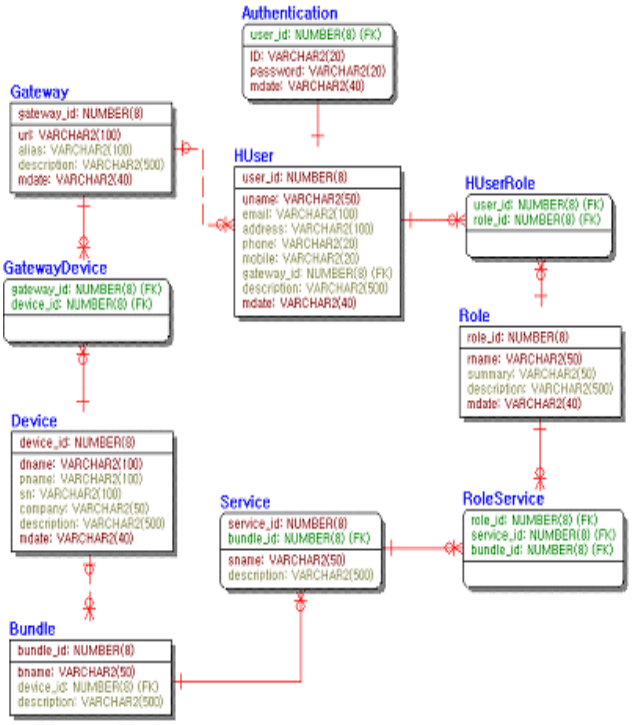


Fig. 6 DB model.

3.5 Design and Implementation of Communication Protocol Between Home Gateway and Management Server

The user authentication and access control model developed in this study performs its function by the inquiry/reply between the home gateway and the remote management server, and thus, a mutual communication protocol is needed between them. This communication protocol was configured with three kinds of XML-based message schema [13] as shown in Table 1 and a Jar type library was designed and implemented to be used with Java program.

Table 1: Communication protocol schema

Kinds of Schema	Descriptions
User authentication token	XML message structure expressing the user authentication token upon request to management server
Request/Reply message	XML message structure expressing the request/reply between home gateway and management server
Access control policy	XML message structure expressing access control policy for home gateway

3.6 Design and Implementation of Communication Service between Home Gateway and Management Server

The user authentication and access control model developed in this study performs its function by the inquiry/reply between the home gateway and the external management server; the types of user access to information devices can generally be classified as external access or at-home access, and the access sequence is as shown in Fig. 7 and Fig. 8.

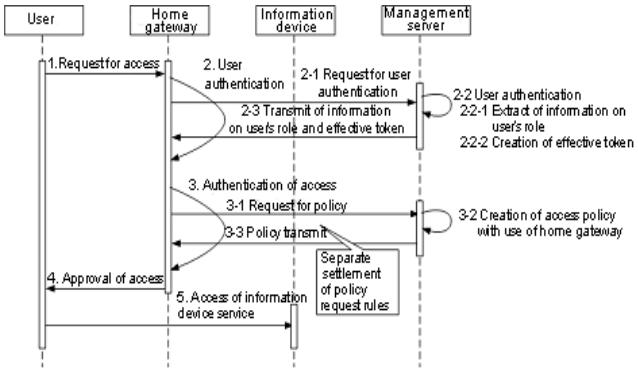


Fig. 7 The sequence of access to information device services from outside of the home

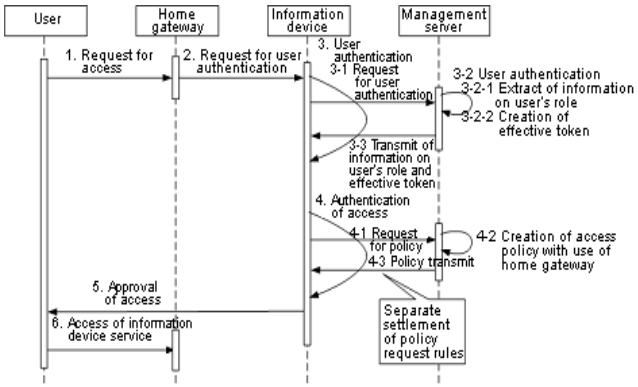


Fig. 8 The sequence of access to information device services at home

As shown in the access sequence above, the interactions between the home gateway and the management server are made through the SOAP protocol [14], and WS-Security [15] was applied for the security of this SOAP protocol.
SOAP protocol transmits the request from the home gateway and the reply from the management server in the form of an XML message designed by the above-described communication protocol. For the interactions between the home gateway and the management server, components shown in Fig. 9 were designed and implemented.

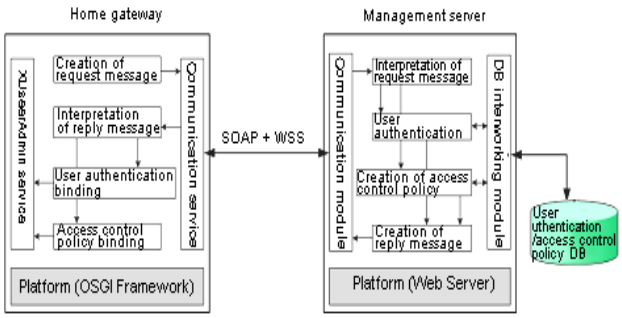


Fig. 9 The communication service structure between home gateway and management server

3.7 Design and Implementation of User Authentication and Access Control Management System

The user authentication and access control system performs user management (registration, deletion, and amendment) for user authentication and access control and performs registration, deletion, and amendment of the elements to control the access to information devices, bundles, and services. A GUI is supplied so that users can easily set up the access control policy, such as allocation or roles and allocation of services for possible access to the roles and, in this study, a web-based application was implemented for remote management of such tasks through a web browser. Only the operator may perform tasks such as registration and amendment.
The basic frame of the management system GUI consists of a menu (left), list (upper right), and setup screen (lower right) as shown in Fig. 10.

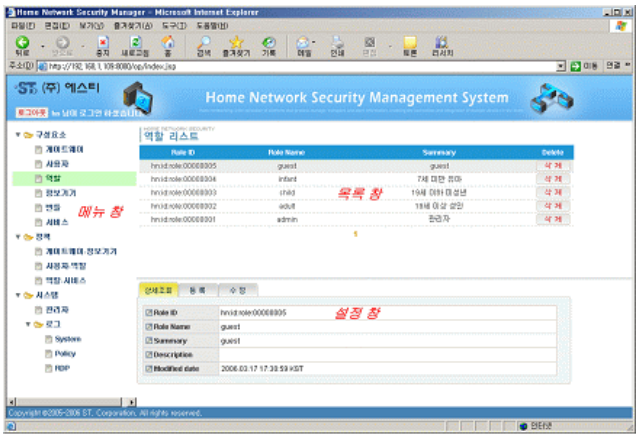


Fig. 10 Configuration of management system.

4. Test and Result

A demo system was made as shown in Fig. 11 to test the user authentication and access control system based on the remote management server system designed and implemented in this study.

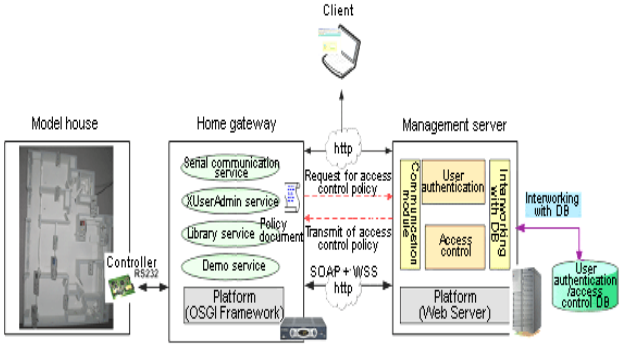


Fig. 11 Configuration of demo system

The order of actions performed in the test were as follows: The users access the home gateway through the web browser and pass the ID/PW based user authentication; The home gateway requests the management server for an access control policy for the corresponding home, and management server creates an XML document to meet the access control policy schema of the corresponding home, and transmits the document to the home gateway through the SOAP protocol; the home gateway shows the user the possible appliances information can be accessed regarding and begins the service of accessible information appliances. The information appliance service was tested by performing a test to control the On/Off LED that the controller connected to through the home gateway through RS232, representing the information appliances of the model house. The flow of this test was as shown in Fig. 12.

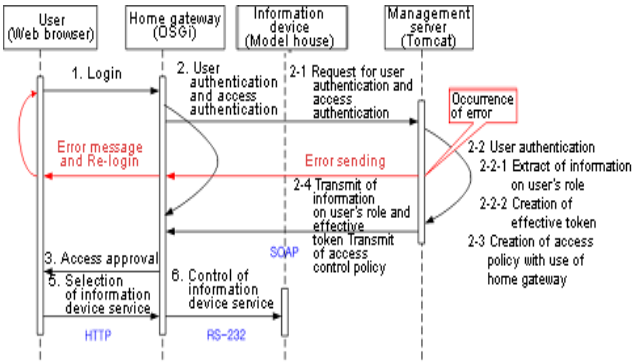


Fig. 12 Flow chart of demo system scenario

The information appliances and services of this demo system were as shown in Table 2 and the access authentication by role depending upon the roles and services allotted to the users were as shown in Table 3 and Table 4, respectively. The users, roles, and access authentication described in section 3.7 may be amended through the management system.

Table 2: List of information appliance services in demo system

Information Devices	Name of Services	Summary of Services
Lights	PowerService	Power On/Off
DTV	PowerService	Power On/Off
	AdultChannelService	Adult channel selection
	CommonChannelService	Common channel selection
Refrigerator	PowerService	Power On/Off
	TempService	Temperature control
Air conditioner	PowerService	Power On/Off
	WindService	Wind velocity control
Alarm	PowerService	Power On/Off
	OperationService	Alarm Whole/Release
Boiler	PowerService	Power On/Off
	OperationService	Boiler heating control
Door lock	OperationService	Door lock On/Off control
Gas valve	OperationService	Gas valve control

Table 3: Relationship between users and roles

User List	Role List
Father	Parents
Mother	
Son	Children
Daughter	

Table 4: Relationship of access authentication between roles and services

Information Devices	Names of Services	Roles	
		Parents	Children
Lights	PowerService	Available	Available
DTV	PowerService	Available	Available
	AdultChannelService	Available	Available
	CommonChannelService	Available	Available
Refrigerator	PowerService	Available	Available
	TempService	Available	Available
Air conditioner	PowerService	Available	Available
	WindService	Available	Available
Alarm	PowerService	Available	Available
	OperationService	Available	Unavailable
Boiler	PowerService	Available	Available
	OperationService	Available	Available
Door lock	OperationService	Available	Available
Gas valve	OperationService	Available	Unavailable

Upon logging into the home gateway of the demo system through a web browser, the available service list was properly displayed, depending upon the access authentication of the user, and the providing of each service could be checked by monitoring the flickering LED connected to the model house. Fig. 13 shows the screen displaying the available service list after user login.

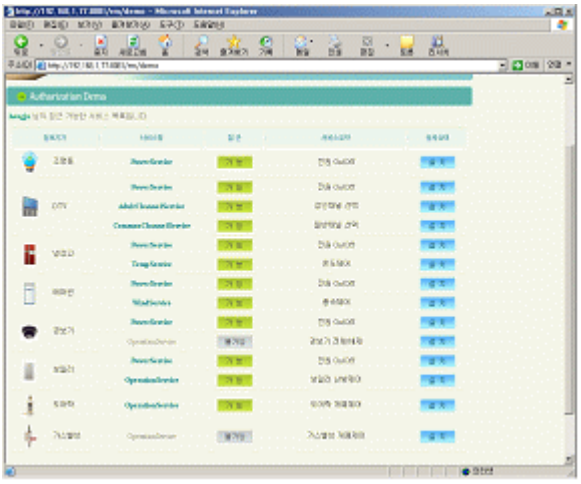


Fig. 13 Service list screen (User: “Son”)

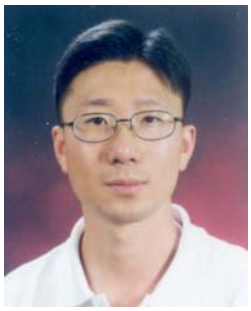
The access test was repeated 20 times for each, with operation of the list screen shown in Fig. 13 for the roles of parents and children shown in Table 3 for each service shown in Table 2, and the appropriateness of access control was determined based on the result of the information devices of model house. The test result showed the demo system performed properly in each test.

5. Conclusion and Future Direction

User authentication and access control methods in the security system of home networks may largely be classified as either home server-based, with the DB and authentication/policy server functions located in the home, or remote management server-based, with the DB and authentication/policy server functions located outside of the home. In terms of stability, reliability, and cost, it would seem that remote management server-based systems have more advantages compared to home server-based systems. In this study, a system based on a remote management server was designed and implemented for user authentication and access control of a home network system and, to test this system, a demo system was constructed. This demo system showed stability with regards to user authentication and access control functions. If user authentication and access control systems based on a remote management server were applied to residential settings such as apartment complexes, costs to individual users could be reduced and, as the knowledge required to learn to use the home network system is limited to learning how to use the services, the users' burden can be greatly reduced, making this system helpful in the activation of home networks. When this article was first reviewed, this user authentication and access control system was thought to be the first system of its kind in Korea, in the respect that a remote management server was used.
This system uses only a password method for user authentication; therefore, more studies to apply various other user authentication methods (security certificate, bio recognition, etc.) will be needed.

Reference

[1] Y. C. Lee, "Technology Trends of Homenetwork and Market Forecast", Weekly Technical Trends of Institute for Information Technology Advancement, No. 1098, 2003.6.4
[2] Y. J. Lee, "Major Difficulties and Obstructions of Promoting Korean Homenetwork Market", Issues on Information & Communication Policy, Vol. 18, No. 5, pp19-31, 2006
[3] D. Y. Rhew, "Necessity and Considerations of Information Security in Homenetwork Services", Magazine of Korean Institute of Communication Sciences, Vol. 22, No. 8, pp51-62, 2005
[4] J.W. Han et al, "Security Requirements for Construction of Safe Homenetwork", Magazine of Korean Information Processing Society, Vol. 11, No. 3, pp38-45, 2004
[5] J. H. Jung, "Analysis of Security Requirements in Homenetwork" Magazine of Korea Institute of Information Security & Cryptology, Vol. 14, No. 5, pp19-22, 2004
[6] Shintaro Mizuno et al, "A new remote configurable firewall system for home-use gateways", 2nd IEEE Consumer communications and network conference, pp599-601, 2005
[7] J.W. Han, D.K. Lee, K.I. Jung, "Trends of Home Network Security Technology", Magazine of Korean Institute of Communication Sciences, Vol. 23, No. 9, pp113-124, 2006
[8] Jonghwan Lee, Yongho Kim, Kyongsok Kim, "Development of internet home server to control information appliances remotely", LNCS 2343, pp561-588, 2002
[9] H. I. Choi, Y. G. Jang, "User Authentication and Authorization for Home Network System", Proceedings of the 26th Korean Information Processing Society Fall Conference, Vol. 13, No. 2, pp.897-900, 2006.11
[10] C.K. Park, "Technology and Market Trends of Homegateway", Weekly Technical Trends of Institute for Information Technology Advancement, No. 1114, 2003.9.24
[11] Telecommunication Technology Association, "Home-Server-Centric User Authentication Mechanism of Homenetwork"TTAS.KO-12.0030, 2005.12.21
[12] OSGi, http://www.osgi.org
[13] XML Schema, http://www.w3.org/XML/Schema
[14] Simple Object Access Protocol (SOAP) 1.1, http://www.w3.org/TR/SOAP
[15] OASIS Web Service Security TC, http://www.oasis-open.org/committees/wss



Hoon Il Choi received the B.S and M.S degrees, from Chongju Univ. in 2000 and 2002, respectively. He is currently pursuing the Ph.D. degree at the Department of Computer & Information Engineering in Chongju University. His current research interests include Home network Security, Web Services, Web 2.0, Semantic Web, ID Management.

Young Gun Jang received the B.E., M.S., and Ph.D. degrees from Inha Univ. in 1980, 1991 and 1995, respectively. He worked as a research engineer at the Agency of Defense Development(from 1979), a senior research engineer at the Daewoo Heavy Industry Inc.(from 1983), a senior engineer at the Institute of Advanced Engineering(1995-1996), visiting researcher at the University of California, Davis (2003-2004). He has been an associate professor at the Dept. of Computer & Information Engr. In Chongju Univ. from 2003. His research interest includes HCI, Assistive Technology, Security, Intelligent Robot, and Intelligent Web Information Processing. He is member of KISS, KIPS, IEEK, KOSMI, IKEEE.

Chan Kon Park received B.E., M.S. and Ph.D. degrees from Inha Univ. in 1973, 1975 and 1989, respectively. He is a professor at the Dept. of Computer & Information Engineering In Chongju Univ. after working as full time lecturer(from 1980). His main research interest includes Artificial Intelligence, Multimedia, Korean Language Processing. He is a member of KIPS, KISS and KMMS and is a director of KMMS.