

# Analyses of requirements for Network Security Technology

Jung-Tae Kim, Member, KIMICS

**Abstract**—IT industry strategy trend and home network security technology is presented. First, we consider the development strategy to improve next generation IT industry. Second, we have analyzed the technique for implementing home network. Last, we have analyzed the technique to security home network field.

**Index Terms**— Home network, Security requirement

## I. INTRODUCTION

A variety of demand is required in the field of information technology today. IT technology is related with social and cultural activity. Advanced nations try to find advanced technology to achieve a new power industry. Most of nation invests in new technology to merge audio, text and image into digital. IT industry enables this technology to realize a multimedia and ubiquitous environment. As IT technologies have developed with new idea, we have an information society. Every industry move into digitalized industry and the scope of application is extended.

## II. EVOLUTION OF IT TECHNOLOGY

To achieve a demand of a variety of economic owner according to social, development of economics and trend of IT technology is moving into intelligent and fusing. Therefore, this IT technology uses information with fast and is widespread to extend an application [1]. The main key element is how we can use the technology without time and place. The speed of network is major point to connect a variety of information and protocols. The trend of development of IT industry is as follows.

### A. Construction of broadband communication network

New IT industry basis is built with construction of broadband merging with information communication and broadcasting. The breakthrough appears today. Communication, Internet and broadcasting are emerged.

Therefore, every appliance and services can supply without considering method of transmitted information with rapidly. To cope with the trend of IT technology, the speed of high-speed Internet network is essential. From this technology, we can use existing communication, broadcasting, Internet service without limitation of time, place, equipment and contents. In future, we plan to supply information benefit with practical activity to house, government and enterprise through broadband network. The representative benefit is that we can obtain favorable e-life such as cooperative HDTV, remote education and medical service. Government can supply electric government employing on-line Internet service.

### B. Cultivation of new developed power industry

It is essential to enforce communication service quality and competitive power of H/W and S/W. The digital convergence network merging with information communication and broadcasting is essential and we have to concentrate on cultivation of IT power industry.

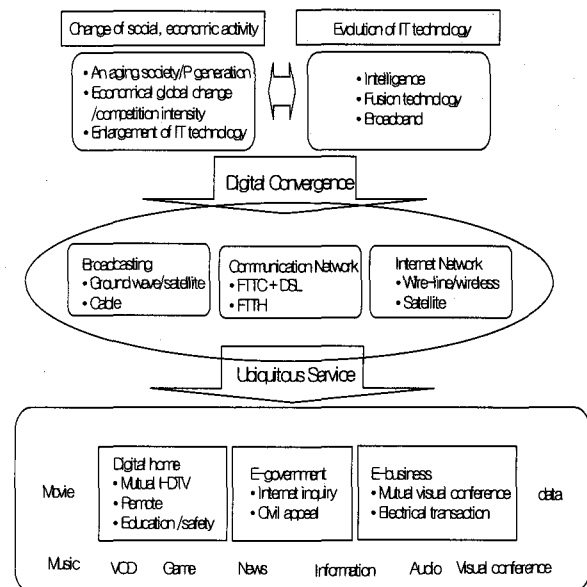


Fig. 1 Configuration of digital convergence network

## III. NEW GROWTH POWER DEVELOPMENT PLAN

### A. R&D intensive assistance and leading of standard

1. Consideration of efficiency for technology development

Manuscript received December 6, 2006.

Jung-Tae Kim is with the Mokwon University, Department of Information Electronics & Imaging Engineering (phone: 82-42-829-7657, fax: 82-42-829-7653, e-mail: jtkim3050@mokwon.ac.kr)

2. Induced of R&D responsibility administration system
3. Suggest a new idea to international standard committee
4. Cultivation of man power and IT venture complex  
Cultivation of skilled man and planned expert
5. Cultivation of IT venture industry and small enterprise with intentional technology
6. Extension of market place and prior occupation through foreign relationship

The new technology is developed according to demand of consumer. And most of digital technology combined with new idea and protocol [5, 6].

1. Intelligent service robot
2. Home network
3. New generation PC
4. New generation wireless communication
5. Digital contents and S/W
6. IT SoC
7. Telematics
8. Embedded Software
9. Digital TV

#### IV. OVERVIEW OF HOME NETWORK TECHNOLOGY

We open the digital home network to the outside world. we open the home to intruders, vandals and thieves. Business that implement enterprise networks are all too aware of the dangers posed to the integrity of their networks, and to their private information, by hackers, snoops, spies and criminals who enter through unexpected chinks in their security system. When the digital home network is connected to the Internet, the home will face even greater threats, not only from the same intruders, and the homes themselves, using Internet access to facilitate them [3,4]. To satisfy security requirements, we designed and implemented security service framework for home network. This framework is based on Open Service Gateway initiative(OSGi) home network middleware. It provides APIs to which home network applications can be attached. OSGi defines an open common architecture for home network and specifies service gateway standard. OSGi has an infrastructure to connect with various middleware and support interfaces. OSGi has its own security services. But these are limited and insufficiency. Figure 2 shows that secure control service for home appliances with mobile devices located out of home network. Second is traffic state-based firewall service to control and inspect the traffic at real time for preventing from denial of service attacks. Third is wireless LAN security service which consists of wireless intrusion detection and access control the mobile which use wireless LAN at home. Forth is user management service who access home appliances. As show in figure 2, the proposed system is designed to be installed at the boundary between the home network and the outside network where home routers or gateways are typically installed.

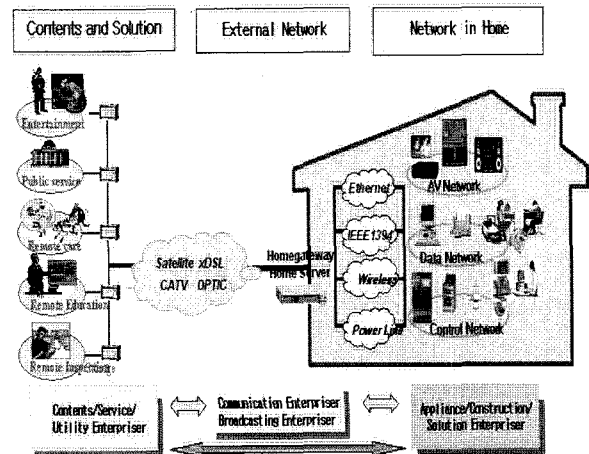


Fig. 2 Configuration of Home Network

##### A. What is home network?

Major factors driving the emergence of home networks is described [8].

- 1) *Integration of computer chips into next generation of every system devices.*  
: Cars, toys, kitchen appliances, living room entertainment system  
: Wireless network technology

##### B. What is key point of home network?

For years, the electronics industry has awaited the arrival of home automation. As we start 21<sup>st</sup> century, the old idea of home automation is rapidly dismantled and replaced with more practical concepts. Embraces home theatre, home office, intelligent appliances, smart objects, security, heating, lighting, energy management [9].

##### 1) Concept

- Home network is core element in future digital home circumstances. It enable information appliance in home to connect other equipment without any restriction such as appliance, time and place.
- Home gateway, home server, home networking, and intelligence information household electric appliance is the main item in home network.

##### 2) Characteristics

- Home network makes a home comfortable and change a space of environment. It gives an abundant digital life style. We can control remote education, entertainment, healthcare and control of information household electric appliance by using a variety of IT technology based on high-speed infrastructure.
- New industry field is developed with a variety of service
- The network is connected with internal home and external network. It is important to acquire lots of contents and develop a service for demand
- It can create a new demand and added value afterconnecting digital TV, intelligence robot, next generation wireless communication and digital contents SW solution.

- The success of home networking depends on not only a variety of line and wireless home network technology standard but also relation of interoperability.

## V. ANALYSES OF TECHNOLOG TREND OF RELATED WORK

### A. What is home network middleware?

1. Software system which is central to the fabric of all home networks
2. Allows connected devices to exchange both control information and streaming multimedia contents
3. Used to isolate application programs from the details of the underlying hardware and network components
4. Provides a set of system interface to their functions
5. Provides interoperability between diverse systems from which a number of home networking middleware applications have evolved.

### B. Representative protocols

#### 1) UPnP(Universal Plug and Play)

- Defines and publishes UPnP device control protocols built upon open, Internet based communication standards
- Enables the emergence of easily connected devices and simplified the implementation of networks in the home and corporate environments
- Enables devices to automatically configures when they connect to a network or communicate their capabilities

#### 2) JINI(Java Intelligent Network Infra-structure)

- Federate groups of devices and software components into a single, dynamic distributed system
- Network plug and play
- Enables a service-based architecture and software [7].

#### 3) HAVI(Home Audio Video Interoperability)

- HAVi has security mechanisms built in to protect against malicious applications.
- HAVi uses software elements such as registry, event manager, stream manager. Device control modules may be downloaded which exists for each HAVi appliance. The authenticity of such downloaded device control modules's is determined by a digital signature that is associated with it.

The element technology for making home networking is as follows.

1. Home PNA
2. Powerline Network
3. Bluetooth
4. HomeRF
5. 802.11B/Wi-Fi
6. IEEE1394 / HAVi(Home Audio Video Interoperability)

## VI. ELEMENT OF HOME NETWORK

It is a popular misconception that security is synonymous with encryption. In many cases, confidentiality via encryption is that the least important element of a security solution. Network security involves a number of different elements:

1. Data origin authentication
2. Command authorization
3. Message integrity protection
4. Message replay prevention
5. Data confidentiality
6. Key distribution
7. Trust versus trustworthiness

Any home computer connected to the Internet is in danger of being attacked. A broadband connection leads to preparatory to attacks every few minutes. A serial-up connection, behind the firewall of an Internet Service Provider, leads to attacks from machines that are behind with one ISP, probes came once or twice week. There exist many papers, both academic and practical, on how to use existing products to secure current home computers from attacks via the Internet. It is not the purpose of this paper to decrease that advice, but to summarize it.

1. Computers owners should have a firewall and allow no responses to any attempts to connect into the home from outside. A Firewall must have external administration disabled, and any passwords with which it was shipped need to be changed to very secure, hard to guess, passwords. These passwords can be written down, because they are defending against network attack than in-home attackers.
2. A computer should have a modern virus scanner, which is enabled to scan all inputs to the computer, as well as automatic updating of virus signature files, at least daily.
3. Computer owners should update operating systems and applications with the least security patches and scan for new patches daily.
4. Security setting should be sent to maximum on the both browsers and e-mail agents
5. If one uses wireless networking at home, the wireless access point must be placed outside the home firewall, rather than inside
6. For each operating system, there are numerous setting that must be properly to maximize security

## VII. CONCLUSIONS

IT industry strategy trend and home network security technology is presented. First we consider the development strategy to improve next generation IT industry. Second we have analyzed the technique to security home network field.

## REFERENCES

- [1] Cheng-Fa, "A Multi-agent architecture for intelligent home network service", IEEE Trans. on Consumer Electronics, V.48, N.3, August 2002, pp.505-514.
- [2] Sungwoo Tak, "An end-to-end home network security framework", Elsevier, pp.412-422.
- [3] <http://ccmc.knu.ac.kr/files/research/home.html>.
- [4] First Home security workshop, 2004.7.12, Korea.
- [5] Intel technology journal, "Home network security "Vol,6, n.4, 2002, 2002.
- [6] B. Rose, "Home networks: a standard perspective, IEEE Communication Magazine 39,2001., pp.75-85.
- [7] Jini Overview, <http://www.sun.com>.
- [8] S. Teger, "End-user perspectives on home networking, IEEE Communication Magazine 40, 2002, pp.114-119.
- [9] Peter B, "Making Home Automation Communications Secure", IEE Magazine, 2001, pp.50-55.



### Jung-Tae Kim

He received his B.S. degree in Electronic Engineering from Yeungnam University in 1989 and M.S. and Ph.D. degrees in Electrical and Electronic Engineering from the Yonsei University in 1991 and 1996, respectively. From 1991 to 1996, he joined at ETRI, where he worked as

Senior Member of Technical Staff. In 2002, he joined the department of Electronic and Information security Engineering, Mokwon University, Korea, where he is presently professor. His research interest is in the area of Information security system technology that includes Network security system design, Chaos Cryptosystem and Wireless Communication.