

Fig. 2 Home-Network Access Network Security Vulnerabilities

B. Vulnerability in Home-Network

The household network can be deployed using the technologies already available in the household or installing the new line. For that, the wired and wireless lines are used together [6]. The security threats are exposed due to the vulnerability from linking of the network technologies with house home appliances and vulnerability of the technology itself. Types of security threats are described as follows:

1) Home Appliance

The household appliances can be connected to the wired or wireless network through the home gateway. (Fig. 3) shows the vulnerability of the home gateway itself. Typically, home gateway has the Web based management program installed. Its problem is that the attacker can attain the administrator privilege using Web server or CGI vulnerability. Since the home gateway is the point that connects the household with outside, attack against it can directly lead to the attack against the whole household network. Therefore, security measures of the home gateway are more important than anything and development of technology to protect it is essential [7][8].

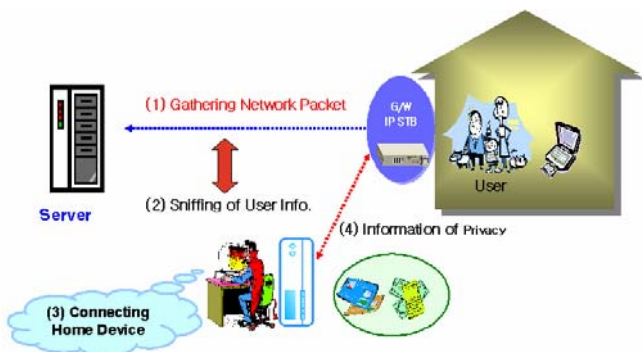


Fig. 3 Illegal Connection to Home Gateway

Furthermore, there is the possibility that the attacker can disguise itself as the internal user through the interactive DTV, IP set top box or home pad or access it illegally through other means to control the home appliances. Physical problem or malfunction of the home appliance can also leak the

information, or problems of the device can cause inconvenience to the user when needed.

2) Wired Communication Protocol

For the household network, Ethernet (IEEE802.3), PLC and IEEE1394 are the most widely used protocols. PLC monitors the electricity consumption of the household and has the privacy violation threat since it contains the pattern of the users. Particularly since the Internet access network and wired household network (mostly Ethernet) inherits the threats (hacking, virus, worm, etc.) of Internet, the currently available security measures must be quickly applied to prevent the threats to other protocols. In general, the wired Home-Network of Ethernet, PLC and IEEE1394 can be accessed by the attacker disguising as the internal user and can be controlled by the illegal user, causing the physical problem, malfunction or Home-Network communication interruption. (Fig. 4) shows the security threats of wired Home-Network.

3) Wireless Communication Protocol

The wireless protocols available for Home-Network are wireless LAN, HomeRF, Bluetooth, UWB, ZigBee, and etc. Wireless protocols are liable to bootlegging in their nature. Therefore, security arrangements between the transmitter and receiver are very important. At least, the control signals for the in-house devices in the Home-Network service require encryption. Unless this feature is enabled, unauthorized or illegal access and/or control will be possible, and physical failure or unwanted operation may occur. Furthermore, communication failure in the house may occur by attack to the service interruption using cycled wireless access request on the basis of the characteristic of wireless network. Fig. 7 illustrates security threats to a wireless network on the basis of the fire, gas, and invasion detection sensors and bootlegging of internal wireless communication.

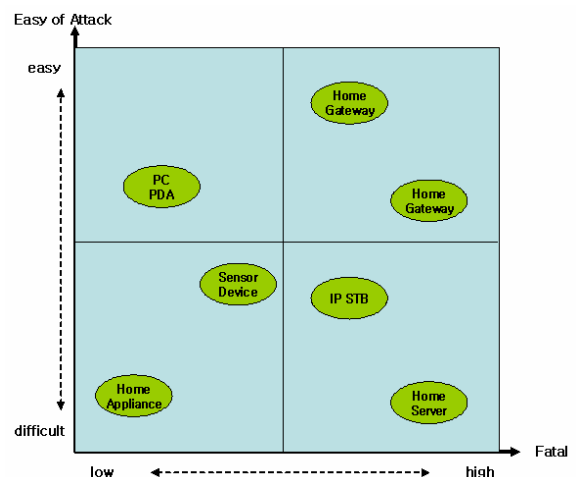


Fig. 4 Priorities of Home-Network Service Protection

For the present, Home-Networks are constructed using wired network protocols, however, wireless protocols have high possibility of replacing the wired protocols except the approach

network. Wireless protocols satisfy the requirements of ubiquitous Home-Network environment with their easiness of installation and excellent mobility [8]. Therefore, considering the possibility of linkage with such infrastructures as RFID and USN, technological development will be required for protection against security threats.

TABLE I
HOME-NETWORK PROTECTION METHODOLOGIES BY LAYER

Module 1: Base Layer, Management Activities		
Security Features	Security Goal: SNMP, HTTP, Telnet, FTP, TFTP	Countermeasures
Access Control	Application layer checks the authority of the access request.	PKI authentication technology, user authentication, access control, RBAC Invasion detection & blocking, traffic control technology, IPSEC, NAT, TLS
Authentication	Conduct user authentication for access request.	
Non-repudiation	Record the identification of the source that has sent the authentication information, time stamping, random number, etc. should be used in the authentication procedures.	
Data Security	Protected with encryption protocol. The control information such as user authentication information controlled at the network connection point should be protected.	Non-repudiation technology, IP security technology, transmission layer security technology
Communication Security	Protect by using encryption protocol.	SSH, IP security technology, transmission layer security technology, detection & interruption of invasion
Data Integrity	Protect communication information from unauthorized change, deletion, creation, and copy.	Counter-invasion technology, transmission layer security technology
Availability	Protective techniques against the active attacks such as service denial and the passive attacks such as the change/deletion of administrator's information (password, etc.) should be available.	Secure OS
Privacy	Communication information should be protected from use	

	by unauthorized person or device.	
--	-----------------------------------	--

III. SECURITY MODEL FOR HOME-NETWORK

Various information technologies and home appliances are applicable for Home-Networks. A common structure of Home-Networks controls and uses in-house services by connecting to Home-Network (hereinafter, "HN") through remote access terminal (hereinafter, "RAT"). In Fig. 5, two models are defined for general HNs; the first is the HNSC based Indirectly Service Model (HBISM); and the second is the Home-gateway-based Directly Service Model (HBDSM).

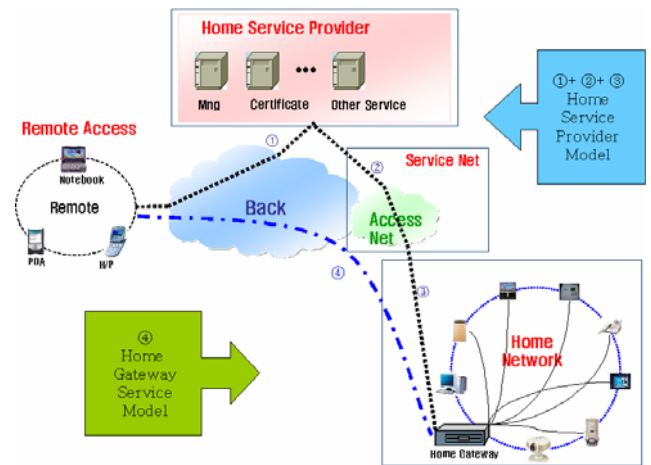


Fig. 5 Home-Network Model

The characteristics of the two models are described herein below:

A. HBISM

HBISM assigns the authority of user authentication and access control to Home-Network Service Center (HNSC) when the in-house user uses HN control service. The authorized HNSC provides the service according to the users' request. The problems of the HBISM are the concentration of the services on the service management of HN and related reliability. For the present, the model service providers in Korea are adopting the HBISM model, which has a security function in dual structure of HNSC and home gateway. However, even the simple security filtering function is not used due to the performance degradation of the home gateway. Therefore, the security level of the entire HN services depends on the security level of the HNSC, which is the case of present HN model service providers. The extra cost incurred by using HNSC which is required by the structure of the HBISM should be solved by the differentiated services.

B. HBDSM

In the HBDSM model, HN users directly control home appliances by accessing home gateway, thus, depends on the security capability of the home gateway. That is, the

performance of the home gateway and the security are closely related. This model will be able to solve the reliability and cost issues by direct control of the users, not relying on external proxy. However, cautious consideration should be taken because all the on-house information can be disclosed if the home gateway is hacked. The technologies required to solve the security issue of HN are classified by section. This sectional classification will be applicable for these two service models. As shown in Fig. 6, remote access terminals require user authentication, which is implemented with ID and password, for the present. Using ID and password may incur problems because weak points may be exposed to network packet collection. In the future, diversified user authentication techniques such as authorized certificate or biological identification should be implemented for better convenience and safety.

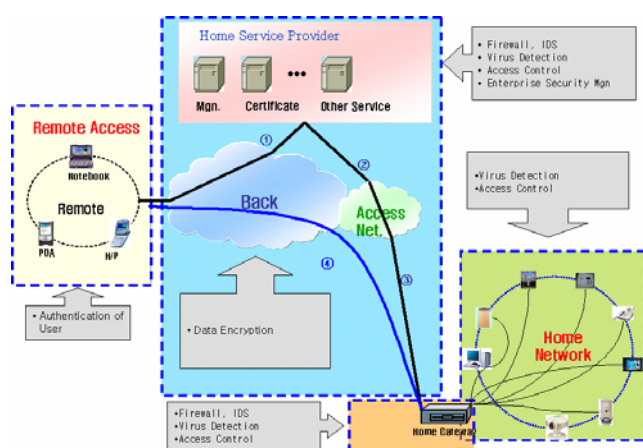


Fig. 6 Security Issue of Home-Network

The considerations on the security of the transmission network are mostly focused on the risk of data exposure. For the present, data encryption of the in-house control signals is required. In addition, there are further issues to be considered, such as invasion blocking, invasion detection, weak point diagnosis, virus detection, user and device authentication, and integrated management (personnel and equipments). Especially, HNSC requires various managerial considerations. To this end, the roles and responsibilities of the service provider and user should be clearly defined in SLA, etc., regarding the assignment of the authority of approaching the subscriber information and access into the house.

IV. CONCLUSION

In the future, when the wide-area network is connected with FTTH(Fiber To The Home) for the integration of communication and broadcasting, the hardware and software structures of home gateway need to be developed to implement BcN-based Home-Network performance in addition to the security technologies for network. Therefore, HN is expected to evolve into more complicated and diversified structure, demanding high importance of the security needs.

In conclusion, it is recommended to develop a safe HN service model taking the basic HN security issues, before entering full-scale HN services. It is said that "A disease must not be hidden, but disclosed." Similarly, security issues should be disclosed to be solved by system improvement and technology development. The service providers shall recognize the importance of the security, as their basic responsibilities, and the users should be aware of the security and observe relevant rules. In addition, differentiated security services should be developed for better service quality, and users should recognize the necessity of security and that safety can be guaranteed according to the service level.

REFERENCES

- [1] "Ministry of Information and Communication IT893 Strategy", MIC, 2005, <http://www.mic.go.kr>
- [2] Home-Network Security, ITU-T SG17 WP2 Q.9,
- [3] "Home-Networked Device Interoperability Guidelines", Members of the Digital Living Network Alliance (DLNA), June 2004.
- [4] "Present Status and Future Development Strategies of Domestic and Foreign Home-Network Industries,"Home-Network Industry Association, 2005.5
- [5] "Policies and Technological Weak Points of Home-Network,"1st Home-Network Security Workshop, Kim T. G., Institute of Information Technology Administration, 2004.7.12
- [6] "Introduction to the Standard Technology for Digital Home-Network," Han. C. M., Park G. N. Korea Telecommunication Technology Association (TTA), 2004.2
- [7] "Threats and Countermeasures against the Invasions in the Ubiquitous Home-Network Environment,"Yoo D. Y., Kim Y. T., Rho B. G. Korea Information Security Agency, 2004.10 Jorunal V31, B2, KIISE
- [8] "BcN and Home-Network,"Lee J. W., 03/05/2005.