유비쿼터스 환경하에서의 홈게이트웨어를 위한 보안 설계 분석

김정태

목원대학교

Analyses of Security Design for Home Gateway in Ubiquitous Surroundings

Jung-Tae Kim,

Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

요 약

We have developed a new remote-configurable firewall system that provides secure and easy-to-use access to home-network appliances such as network cameras, PVRs, and home file servers, through the internet. With a simple web browser operation, remote users can dynamically open and close the firewall of the home gateway. The firewall rule creation is based on an authentication of the remote client, and thus only packets from the authorized client can pass through the firewall, we analyses the security design for home gateway in ubiquitous surroundings.

Ⅰ. Introduction

In ubiquitous computing environments, users expect to access resources and services anytime and anywhere, so there is a need for more automated and secure management in ubiquitous computing formed by users accessing these resources and services. The middleware architecture should provide selective domain-specific management and be adaptive for different domain management. As home LANs are widely installed in many households, consumer electronic appliances with networking functions have increased their presence in the market, such as networked DVR, digital TV, and video camera. We believe that enabling secure access to the electronic appliances from outside creates great opportunities for many useful service offerings, such as remote viewing of recorded private contents and video surveillance of houses while away from home.

Ⅱ. Concepts of Home Network Security

As Home network, we considered the following four networks as home networks

- The information equipment network; PC connects other PC or peripheral devices through the electronic power line, and user shares files or a printer, etc.
- The AV equipment network; a DVD and television etc, are installed in one place, and these audio and visual data are delivered to other rooms through the electronic power line.
- The control system network; home electronics etc, are controlled through the electronic power line
- The community networks; electronic power lines are used as the local communication lines among the neighboring homes.

Through those networks, it is possible to be provided with, the home automation services, the home security service, and various amusement services without constructing the cable which is complex

newly.

Now, we discuss about the home network architecture. Here, we think bout the models in the followings which are introduced.

- Gate model; the gateway processes the security. of the equipment of the follows in a lump
- Hierarchical model; the used cryptographic key is different at every hierarchy.
- Individual model; each device does the security processing individually and authenticates each other mutually.

Table1. The architecture of each model of home network

	Point
Gate way model	Each mode can be reduced labor, When a GW is tom, the damage is the biggest
Hierarch model	Even if the key of some hieraaarchy is tom, it is difficult to expand damage into the other hierarchy
Individual mode	Flexible Complex ideas are requested in the key management

III. The Architecture of the system

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 1 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 1, 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.

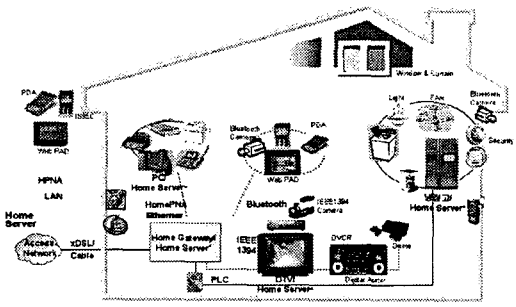

Figure 1. Configuration of Home Networks

The dynamic firewall system authenticates the remote user and receives a request for an access to an internal service/appliance via a web browser, and creates new source-address based firewall rule by reading access control list, firewall policy templates for the appliance and the IP address of the remote client PC. The source address based dynamic policy will only pass the packets from the clients PC to the particular internal service. The dynamic creation can also enable multiple internal service to share a single external port. The firewall policy template contains port numbers, protocols and internal IP address of each appliance. An access control lists contains permission for each

user to access to the appliance. The zero configuration system collects the information of the equipments connected to the home network using a build-in UPnP gateway server and automatically creates firewall policy templates.

IV. Networking with UPnP

1. The user connects a new network appliance which has the UPnP function to their home network
2. Using the UPnP protocol, the appliance finds and tries to register itself to the UPnP gateway which is built as a part of the zero-configuration system. Unlike the standard UPnP gateway system, the UPnp gateway does not open the ports for the appliance in response to the request, but it creates firewall policy templates that describe the port numbers and the IP address for the appliance. These templates will be used later by the dynamic firewall system
3. The user can configure an access polocy for the appliance by accessing a web server which is also built in the gateway system. A user who can access the appliance from outside can be selected among family members.
4. When the access control listst is set, the installation is completed and the user is ready to go outside.

V. Intrusion Detection and Prevention in Home Networks

Different networking technologies like ethernet and wireless LAN can be integrated into a home network and the system of such networks will typically be running various operating system and offering different services to the users of the home network. Furthermore, new aliasing services offered by companies like the dynamic 윤 network services company that offers a service which allows to map static host names to dynamic IP addresses, enable public offering of services even from machines located inside a home network. It is clear that such configurations represent attractive targets for potential attackers and that numerous risks arise if such home networks are insufficiently protected.

A. Reasons for and requirements of ISP operated IPS

* No special hardware or operating systems requirement;
Ideally, the intrusion prevention system will directly be located on the gateway between the home network and the ISP, the DU router, as all traffic coming in and out of the home network is going through this gateway. However, as these components are to be offered by various independent manufactures, it has to e avoided that special hardware requirements are dictated by the intrusion prevention.
* Ability to evolve over time
* Performance
* Privacy

VI. Security Mechanisms

We introduce some security mechanism secure a home network according to the threats and requirements. First we consider the establishment of trust relation of newly pursed devices and AS so administrator can set access control to the device, authorization. Secondly, the authorized entity can request access to the device, but a secondary association between the two partied must be established first, and both sides need to assures that each other is the one it claimed to be, so mutual authentication must be performed by authentication server which will authenticate both of them and share a session key between them. Then communication protection will be achieved.

We will present the security mechanism as follows.

A. Trust & Authorization

For a new device, the owner needs to ensure the newly pursed device to obey his commands, but not his neigher's. So a trust relation between the newly pursed device and the owner must be established. The management of these trust relations is always performed by authentication server.

B. Authentication & Key Management

When the device or service need low security and MAC ACL is used, the authentication of requestor is simply achieved by checking if requestor's MAC address is in the MAC ACL. If it is true, the requestor is authorized to access the device or service. This solution doesn't contain any cryptographic algorithm or protocol, so secret key is not needed.

C. Secure Routing

For general wireless home networks, we can assume that there are no malicious nodes that will launch DoS attacks to routing protocols, and then no secure routing mechanism are needed. For some applications with higher security requirements that need to protect from potential DoS attacks by malicious nodes, we assumes that every nodes in the wireless home network share a group key with which they can encrypt their outgoing routing information and check incoming neighbor's routing information. Then outside malicious nodes that have no knowledge with the shared key will not inject or modify any routing information to perform DoS attacks to the routing protocols.

D. Communication Protection

After the security association between the two communication parties is established, session key generated by AS is distributed to them securely, then we can use the shared key to protect the communication between them.

E. Other Mechanism

Since access points act as the border of the home network firewalls can be deployed in the access points to prevent unauthorized access to the home network. And we may need antivirus software installed in the access points to prevent inundant virus even more. As the all traffic between the home network and outside network pass through access points, then we can deploy network intrusion detection system in the access points to detect the intrusion from outside network dynamically. These mechanism must be modified to be more ease-of-use and robust before they can be used in the home network since the users of home network will have little knowledge about the network installation and maintaining.

References

1] Cheng-Fa, etc, "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, etc, "An end-to-end home network security framework", Elsevier, pp.412-422

[3] http://ccmc.knu.ac.kr/files/research/home.html

[4] B. Rose, "Home networks: a standard perspective, IEEE Communication Magizine 39, 2001., pp.75-85

[5] Jini Overview, http://www.sun.com /jini/faqs/index.html

[6] Peter B, etc. "Making Home Automation Communications Secure", IEE Magizine, 2001, pp.50-55

[7] Prashant K., etc, "Security in Wireless Residential Networks", IEEE Trans. on Consumer Electronics, V.48, N1, February 2002, pp.157-166

[8] S. Teger, etc, "End-user perspectives on home networking, IEEE Communication Magizine 40, 2002, pp.114-119