World Academy of Science, Engineering and Technology
International Journal of Humanities and Social Sciences
Vol:1, No:9, 2007

Home Network-Specific RBAC Model

Geon-Woo Kim, Do-Woo Kim, Jun-Ho Lee, Jin-Beon Hwang, and Jong-Wook Han

***Abstract*—**As various mobile sensing technologies, remote control and ubiquitous infrastructure are developing and expectations on quality of life are increasing, a lot of researches and developments on home network technologies and services are actively on going, Until now, we have focused on how to provide users with high-level home network services, while not many researches on home network security for guaranteeing safety are progressing. So, in this paper, we propose an access control model specific to home network that provides various kinds of users with home network services up one's characteristics and features, and protects home network systems from illegal/unnecessary accesses or intrusions.

***Keywords*—**Home network security, RBAC, access control, authentication.

I. Introduction

HOME network is a new IT technology environment for making an offer of convenient, safe, pleasant, and blessed lives to people, making it possible to be provided with various home network services by constructing home network infrastructure regardless of devices, time, and places. This can be done by connecting home devices based on wire/wireless communication network such as mobile communication, Internet, and sensing technologies [1].

However, home network is exposed to various cyber attacks of Internet, involves security homes against hacking, malicious codes, worms, viruses, DoS attacks, and eavesdropping, since it's connected to Internet [2].

So, in this paper, we present an access control model for removing security holes of home network, guaranteeing safety, and providing user-level various services, and propose correspondent technologies.

Each home gateway installed at the border of each home is a core module for home network services. As every packets pass through home gateway, it authenticates home users and controls accesses based on authentication information.

Geon Woo Kim is with the Electronics and Telecomunication Research Institute, Daejeon, Korea (corresponding author to provide phone: 82 42 860 5427; fax:82 42 840 5611; e-mail: kimgw@etri.re.kr).

Do Woo Kim is with the Electronics and Telecommunication Research Institute, Daejeon, Korea(e-mail: dwkim@etri.re.kr).

Jun Ho Lee is with the Electronics and Telecommunication Research Institute, Daejeon, Korea (e-mail: jhlee7@etri.re.kr).

Jin Beom Hwang is with the Electronics and Telecommunication Research Institute, Daejeon, Korea (e-mail: hjb64253@etri.re.kr).

Jong Woo Han is with the Electronics and Telecommunication Research Institute, Daejeon, Korea (e-mail: hanjw@etri.re.kr).

II. RBAC Model for Home Network

For providing secure and various level home network services, we need some functionalities, such as user authentication, access control and security policy management. Access Control should be strong and efficient based on user authentication information, and home network administrator can establish security policy for access control considering specific character of each home.

Home network security model proposed in this paper operates based on the home gateway.

Fig. 1 shows the home network security components:

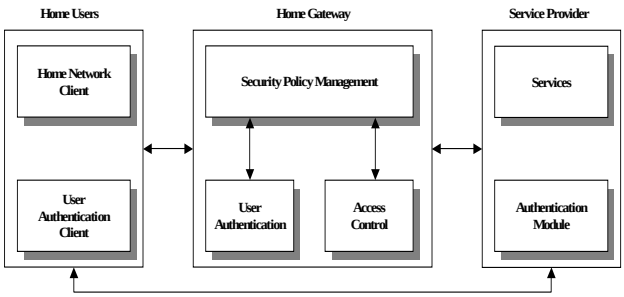

Fig. 1 Components for Home Network Security

Home network system is composed of home network client, home gateway, and service server, additionally controlled home devices and home network services.

Home network client should be useful outdoors as well as indoors, portable, and easy to use. There are a few indoor home network client devices like DTV, PC, Wall-Pad, and mobile phone, whereas it focusing on IP-based TV. Thus, home network client should provide user interface for home network services and user authentication functionality.

Home gateway is a core module for home network, and contains user authentication, access control, and security policy management functionalities, installed at the border of each home.

III. Authentication

Authentication method can be divided into two categories, device authentication and user authentication. Device authentication is used between home gateways and home devices including home clients, easy to use and manage, made much use currently.

But, it's limited to simple service model, and may be difficult to be used for various kinds of services, not guaranteeing efficient access control, what is worse, no one predict what

happen when we lost it.

So, this paper adopts user authentication method in order to address those drawbacks.

While user authentication needs user interventions compared to device authentication, it can satisfy desire for various services. Only, it's a key point how to make certain the security and easiness.

Considering the home network's own characteristics, ages and features of home users vary. Some may not used to the digital broadcasting or may have some troubles in using user authentication and home network services. Therefore we deploy various user authentication methods according to one's taste and feature, namely ID/Password authentication, certificate authentication, bio authentication, and RFID authentication.

Fig. 2 shows integrated authentication mechanism providing various authentication methods.

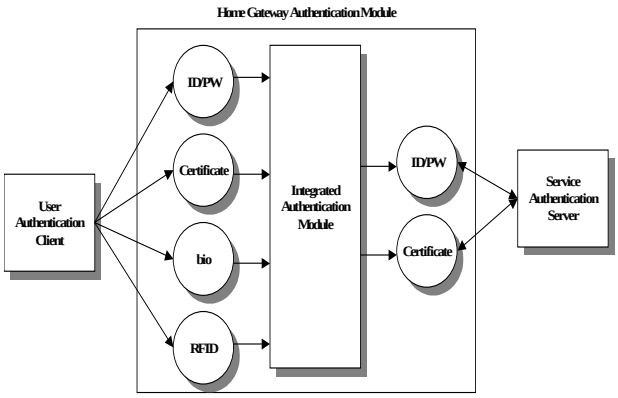

Fig. 2 Integrated Authentication Mechanism

Legacy home network service servers use only ID/Password authentication method or certificate authentication method. In other words, if users adopt bio authentication or rfid authentication, then they aren't interoperable with service server, so, integrated authentication method for automated mapping is needed. With it, we can guarantee transparency of mutual authentication method and minimized user interventions.

IV. Access Control

In order to provide more differentiated various services, user authentication must precede all others, and real-time access control can be based on it. As he access control blocks illegal and unnecessary accesses though it may be justifiable, it can maximize the system security and efficiency.

Home network access control model comprises access control definition module, access control enforcement module, information collection module, access control database, and log database.

Fig. 3 shows the access control model.

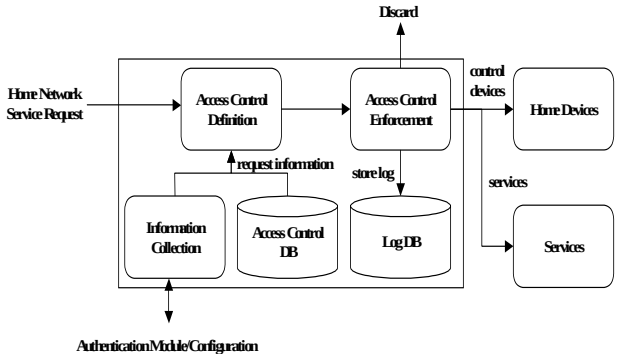

Fig. 3 Home Network Access Control Model

When access control definition module receives service request from a user, it inspects its own access control database and collects correspondent information, reporting the result to the access control enforcement module. In order to decide whether to permit the access or not, the access control definition module firstly retrieves user information from user authentication module, and inspects database using the user information and service as a key, With the result, access control enforcement module controls home devices or provides home network services, or discards the request and stores it to the log database.

Access control database conforms to xPSL(eXtensible Policy Specification Language), which is particularly defined for home network based on XML, not described in this paper. As a matter of face, access control database is within the security policy management system and uses secure communication mechanism such as TLS or IPsec protocol.

Fig. 4 shows access control database and communication structure.

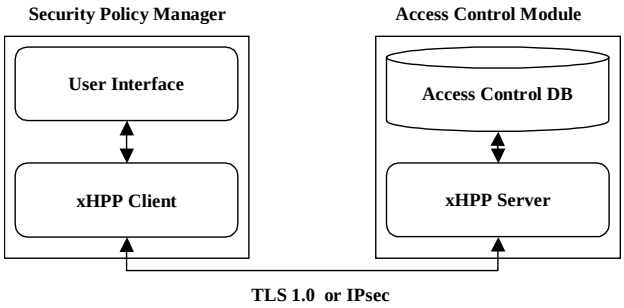

Fig. 4 Access Control Model and Communication

xHPP Protocol, which was developed for communication between a security policy manager and a access control module, must contain the following functionalities.

- Security Policy Request/Response
- Security Policy Set/Acknowledgement
- Home Device Status Request/Response
- Log/Statistics Information Collection Request/Response
- Certificate Request/Response

The capacity of access control database installed in each home gateway is determined by the number of users and the

complexity of policy. Therefore, RBAC (Role-based Access Control) is supposed to be suitable for supporting extensibility and efficiency regarding various kinds of users. Different from ACL (Access Control List), RBAC defines the relationship between users and home devices/services using a component called Role, usually used in large-scale complex model.

Access control definition module decides whether to permit access or not, when receiving service request from a user.

Fig. 5 depicts the control flows of access control definition module.

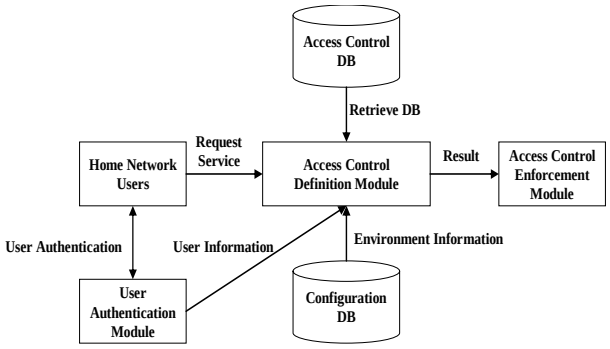

Fig. 5 Access Control Definition Module

When receiving service request, access control definition module firstly retrieves user information through user authentication process. After that, it decides the access permission, transmits the result to the access control enforcement module.

Access control enforcement module receives the result from access control definition module, and enforces it.

Fig. 6 shows access control enforcement module.

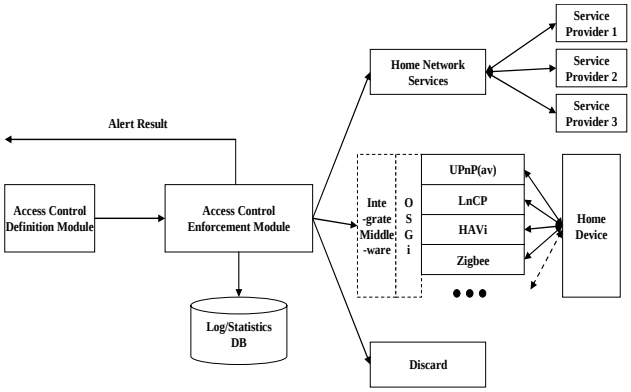

Fig. 6 Access Control Enforcement Model

Access control enforcement can be divided into three categories according to service types and result of access control. In case of controlling home devices, we uses OSGi or Integrated Middleware, ETRI (Electronics and Telecommunications Research Institute, KOREA) is developing. In case of services, we can use contents provided by home network service providers. Additionally, request may be discarded and the result and state information are stored in log/statistics database.

V. Security Policy Management

Security policy manager establishes and manages security policy of home gateways installed at the gate of each home. But, accesses to this device must be limited strictly, and only security policy manager can manage security policy on access control and context-aware policy of home gateways.

Fig. 7 shows the architecture of security policy manager.

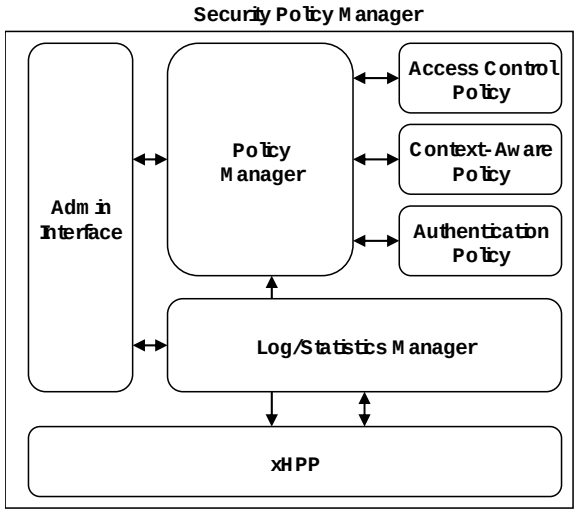

Fig. 7 Architecture of Security Policy Manager

Security Policy Manager is roughly composed of administrator interface, security manager, log/statistics manager, xHPP protocol for communication with home gateway. Managed security policy may contain access control policy, context-aware policy, and authentication policy.

VI. Conclusion

Home network is to provide various home services in easy way considering one's characteristics with home devices familiar to users. However, it can result in tremendous confusion without security.

So, in this paper, we propose an access control model based-on home gateway. It provides not only secure protection of home network system from inner/outer illegal accesses, but also blocking of unnecessary accesses to services. In other words, all users need not to have the same privilege considering each user's characteristics, and it's desirable to give a different privilege to each user fitting one's feature.

After authentication process up one's taste, we can provide real-time access service based on the information from it. Each access control policy is administrated and distributed by a security policy manager, and it uses RBAC mechanism considering extensibility and efficiency.

References

[1] Jeong-Won Kim, "Revitalization Policy of Home Network Industry", KISS, 22nd ed. vol 9, 2004.09.
[2] Jong-Wook Han, Do-Woo Kim, Hong-Il Joo, "Considerations for Home Network Security Framework", KISS, 22nd vol 9, 2004.09.