

Security Technologies Based on Home Gateway for Making Smart Home Secure

Geon Woo Kim¹, Deok Gyu Lee¹, Jong Wook Han¹, and Sang Wook Kim²

¹ Electronics and Telecommunications Research Institute
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea
{kingw, deokgyulee, hanjw}@etri.re.kr

² Kyungpook National University
1370, Sankyuk-dong, Buk-gu, Daegu, 702-701, Korea
swkim@cs.knu.ac.kr

Abstract. As home network is expanding into ubiquitous computing environment and lots of private information is accessible, it is required to protect home network system from illegal accesses and security threats in open network. In general deployment of home network, a secure home gateway is located at the boarder of each home and regarded to be a core entity providing services and controlling traffic. So in this paper, we propose a security system guaranteeing security, availability, and reliability based on the secure home gateway and describe our implementation on home network including authentication, authorization, and security policy.

Keywords: Home Network, Smart Home, Security, Authentication, Authorization, Access Control, Security Policy.

1 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 a variety of home network services by constructing home network infrastructure regardless of deices, time, and places. This can be done by connecting home devices based on a variety of communicating network protocols, such as mobile communication, Internet, and sensor network [1]. With the home network, we can easily control home devices, make use of a number of services such as a VOD service, a remote health care service, a T-commerce service and etc.. Namely, home network can be defined to be a total home information system providing a number of services and solutions, not just simple networking within single home.

Unfortunately, home network is subject to be infected by all legacy security threats existing in open network since it is accessible from open network and a variety of network protocols coexist, where each network contains its own security threats.

Especially, as home network consists of heterogeneous network protocols and a variety of service models, it is likely to be exposed to various cyber attacks of Internet, involves hacking, malicious codes, worms, viruses, DoS attacks, and eavesdropping since it is connected to Internet [2].

So in this paper, we propose an integrated security system to guarantee reliability, availability, and security based on secure home gateway and describe our implementation including authentication, authorization, and security policy.

2 General Model for Home Network

Home network comprises a number of factors of legacy networks and systems.

The categorization of above entities consisting home network is from ITU-T Recommendation X.1111 regarding “Framework of Security Technologies for Home Network”.

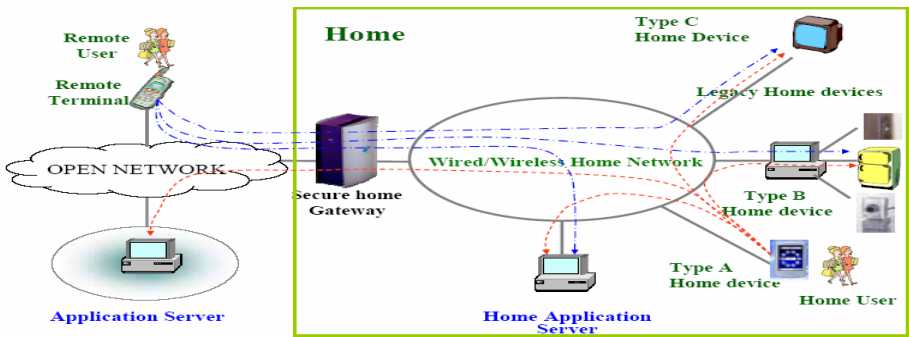


Fig. 1. General model for home network

Figure 1 describes general model for home network from X.1111 [3].

All security requirements and technologies must conform to the above model.

3 Necessities of Security for Home Network

As we mentioned in the previous section, home network is likely to contain a number of security threats that are possible in legacy applications.

3.1 Target of Existing Attacks Due to Connection to Internet

Because home network is composed of heterogeneous network protocols, it is subject to be a target of existing attacks, where every process working in the Internet can access the home network. Each network protocol has its own features and security threats as shown in Figure 2.

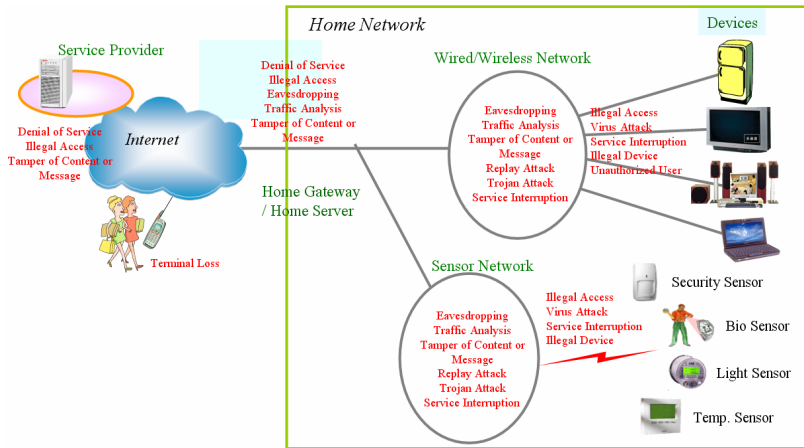


Fig. 2. Security threats in home network

3.2 Trusted Relationships Among Entities

In order to make home network reliable, safe, and available, how to establish trusted relationships among entities that are deployed in home network is most important from security point of view. Especially, in ubiquitous home network environment, majority of services are based on communications among home devices.

During communications among home devices, some exchanged information is supposed to be critical when revealed to others. For example, in remote health-care service, tamper or modification to vital information is closely related to the breath of life and personal medical information known to other untrusted entities may result in serious privacy violation.

Furthermore, it is possible to make a new attack by collecting and reasoning the behavior patterns or habits.

3.3 Others

There is an evolution to be ubiquitous environment of home network, and each device tends to be light-weight following the movement. In ubiquitous environment, it seems to be infrastructureless, where security is getting a more important requirement.

And there is an increment of requirement for security. For example, the Intel and the Verisign are establishing strong security infrastructure by enforcing device authentication.

Also, security for home network is required to be convenient and needs minimum interventions by home users.

4 Security Technologies for Home Network

There are some security technologies for making home network secure. Among them, authentication and authorization are expected to be essential.

4.1 Authentication

The purpose of authentication in home network is to identify an entity that is accessing home network, and verify that the entity is the one that it is claimed to be.

Authentication is supposed to be most important in providing security for home network, including ubiquitous service, and other systems requiring security.

On off-line communication, we can identify the other by ourselves. On the other hand, with on-line communication everyone can deceive one's identity and act as other people.

The authentication server of authentication mechanism means a computing device, which has a database storing authentication information (such as, ID-password, certificate, biometric information, etc.) and loads authentication programs. It can be a home gateway or a home portal server connected to the home gateway at home network. An entity can select a favorite authentication method. That is, the authentication server supplies authentication mechanism using ID-password, certificate and biometric information, etc [4].

The authentication mechanism supplying a variety of authentication methods uses EEAP (Encrypted Extensible Authentication Protocol) [5]. EEAP packet is similar to EAP (Extensible Authentication Protocol) [6] packet. And EEAP is similar to EAP-TTLS (EAP Tunneled TLS) [7] or PEAP (Protected EAP) [8].

The authentication server is different from CA server in that it supports authentication using certificate as well as ID-password, biometric information and stores authentication information registered in the various contents server securely. CA server in PKI (Public Key Infrastructure) does the role issuing and managing certificates and takes a neutral attitude in authentication process.

Once an entity is successfully authenticated, it can use his (or her) authorized service. If it wants to control home appliances remotely, it can control them. And if it wants to use contents by ISPs, it connects the wanted service server.

The general authentication model for ubiquitous home network is shown in Figure 3.

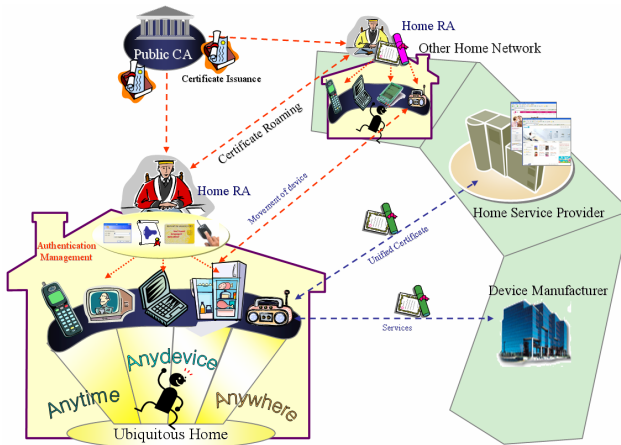


Fig. 3. General authentication model for ubiquitous home network

In ubiquitous home network environment, each entity, which is an object of authentication including a user or a device involved in home, is subject to move into other domains such as other home network domains, telematics service domain, and ubiquitous sensor domain. The authentication module must support above circumstance and relative requirements.

There are a few authentication mechanisms used for home network. They can be categorized into two layers: authentication mechanisms for intra-domain, and authentication mechanisms for inter-domain.

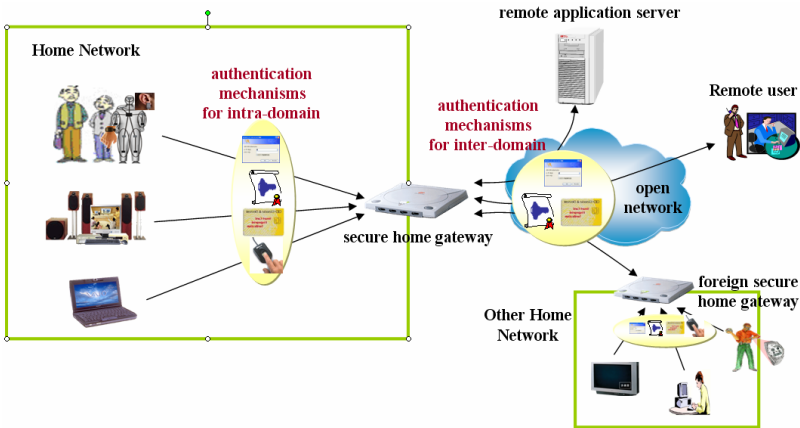


Fig. 4. Authentication mechanisms for ubiquitous home network

For authentication within single home domain, most of the existing authentication mechanisms such as ID-password-based authentication mechanism, certificate-based authentication mechanism, smart card-based authentication mechanism, and biometric-based authentication mechanism, can be used. The decision to adopt which authentication mechanism is depending on application.

On the other hand, it is desirable to exclude the biometric-based authentication from inter-domain security. In case of using other types of authentication mechanisms, even though secret information is revealed to others, we may just change it. But biometric information is not changeable. Therefore, it results in serious privacy violation when disclosed.

Each user is required to be authenticated just one time to access every home network service. Namely, each user is authenticated by a secure home gateway and doesn't consider the following authentication process. For example, when a user is to access a remote application server and the remote application server performs its own authentication, the user is identified by the secure home gateway and the secure home gateway does authentication with the remote application server instead of the user.

For making it possible, the secure home gateway contains an authentication mapping function, which enables mapping between authentication mechanisms for intra-domain and authentication mechanisms for inter-domain.

4.2 Authorization

The purpose of authorization is controlling access of entity even though it has been successfully authenticated and restricting a privilege and access right. Also, it can minimize the loss when home network system is penetrated and attacked by malicious accesses or unauthorized uses.

We can use an ACL (Access Control List) or a RBAC (Role-based Access Control). The ACL directly established relationships between subjects and resources, where a subject means an entity that is accessing, and a resource an entity that the subject is accessing. The ACL is simple so useful for relatively small-scale network. On the other hand, The RBAC adapts an intermediate component called a role between a subject and a resource, so indirectly sets up relationships between them. The RBAC seems to be adequate for relatively large-scale network.

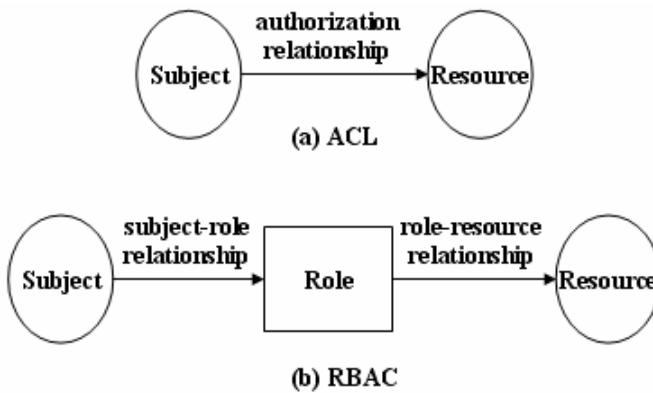


Fig. 5. ACL vs. RBAC

Figure 5 simply illustrates ACL and RBAC.

As home network includes a variety of network protocols and is expected to support many service models such as a client-server model, a peer-to-peer communication model, and hybrid model, it is difficult to definitely decide which mechanism is suitable for home network. Actually we had better use a different authorization model according to the specific home network service. As a result, we need an integrated authorization framework for home network.

Figure 6 shows an integrated authorization framework for home network.

Existing authorization mechanisms can be categorized into three fields: server-based authorization mechanism, peer-to-peer authorization mechanism and certificate-based authorization mechanism. A server based authorization mechanism works on client-server model and the server generates and maintains authorization rules, enforces it. This method is relatively simple and easy to apply. A peer-to-peer authorization mechanism is for p2p communication service model. A peer can manage authorization rules by itself or require help of designated authorization server. This model is relatively complicated to implement and there are a few constraints considering database maintenance and H/W specifications of peer device and etc., A certificate-based authorization mechanism is generally used in open network and conforms to the PKI.

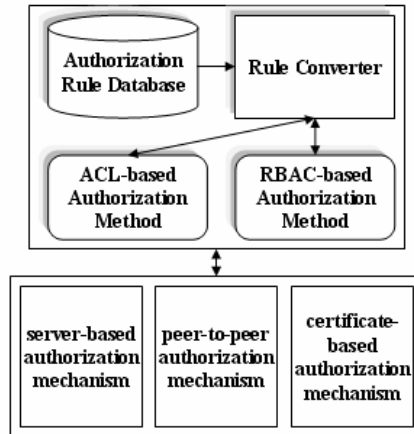


Fig. 6. Integrated authorization model for home network

These mechanisms define their own schema to specify the authorization rules, which may be of either an ACL or a RBAC.

Authorization Rule Database contains raw authorization rules and the details are not described in this paper. Rule Converter translates the raw authorization rules into ACL-based authorization rules or RBAC-based authorization rules and the reverse. Also, it can maintain consistent authorization rules between ACL-based authorization method and RBAC-based authorization method by reflecting the changes of one type of authorization rules to the other type of authorization rules immediately.

Authorization model for home network comprises an access control definition module, an access control enforcement module, an information collection module, an access control database, and a log database.

Figure 7 shows the functional components for authorization.

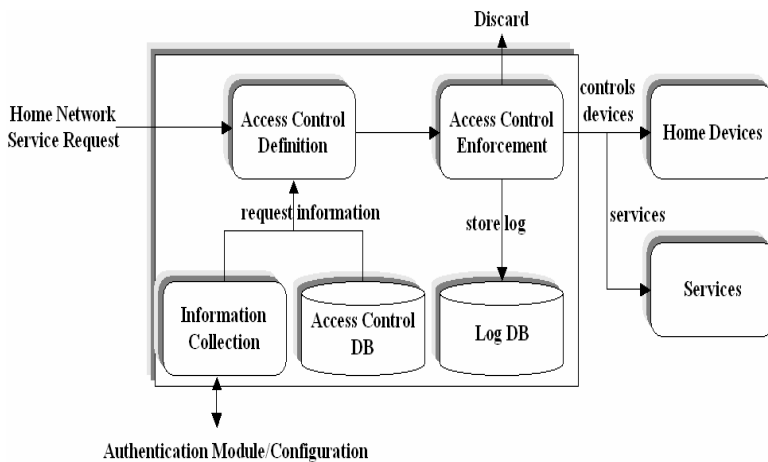


Fig. 7. Functional components for authorization

4.3 Security Policy

Security policy is a set of single rule consisting of *condition* and *action*. Whenever a condition is satisfied, action is performed, where the key issue is how to construct condition. Elements to be contained in condition are as follows

- Time(date, day, duration)
- Event(sensor, user-triggering, state)
- Log(statistics)

Also, we define relationships (interaction, union) among above elements and support recursive structure, which makes it possible to build complex conditions.

Time and event are the basic elements of condition and can be generally used. On the other hand, log-based condition controls access by statistics information. For example, there is a pre-condition that the security policy manager set the policy that children could not use the game service more than 30-hour in a month. Whenever the children access the game service, their usage information may be store at log database. If the above condition is satisfied, connection would be rejected and they can't access it during the month.

Action contains controlling device and providing home services and etc. In order to control device, it should cooperate with corresponding middleware used by controlled device such as UPnP, LnCP, zigbee, UWB, etc.

Figure 8 shows the conceptual architecture and operations on security policy enforcement for home network.

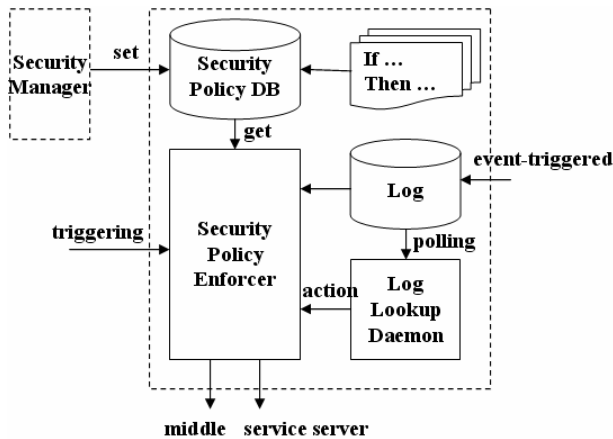


Fig. 8. Security policy system for home network

Security policy manager generates and manages the security policy specialized for home network which includes authentication policy, authorization policy and other types of security policy.

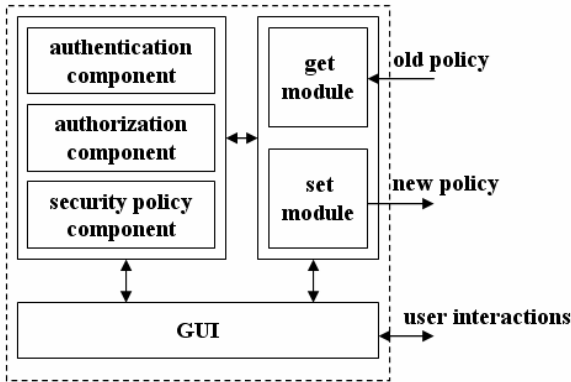


Fig. 9. Security Policy Manager for home network

Considering the features of home network, it must be enough easy for non IT-familiar user to use. In our system, we use a Drag-and-Drop mechanism to establish the security policy, so anyone can handle it if he has been authenticated successfully.

Figure 9 illustrates the functions that the security policy manager provides.

In our system, we use a new defined language called an xHDL (extensible Home security Description Language) based on XML [9].

5 Implementation

This section describes the implementation of security for home network.

Figure 10 shows entities the their relationships in our implementation.

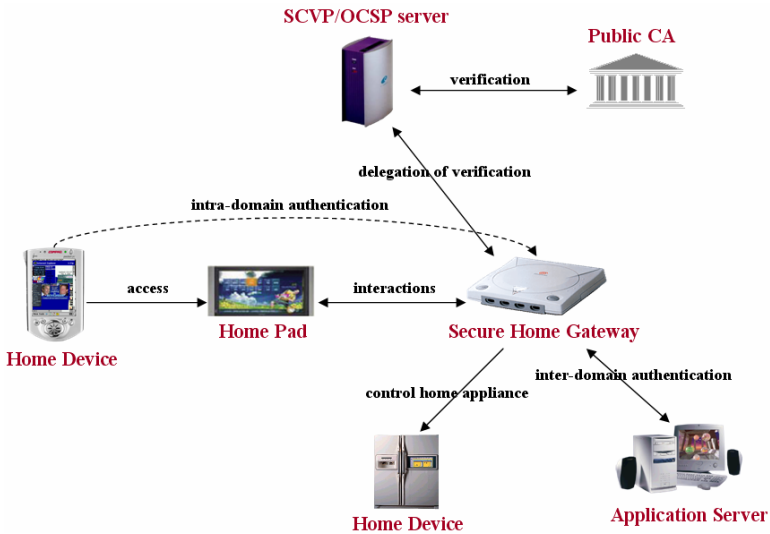


Fig. 10. Structure of our implementation

With the above structure of implementation, authentication flow when using device certificate is shown in Figure 11.

For using certificate, the home device must be issued it by the public CA with the helps of the Home Pad and the Secure Home Gateway. When verifying the certificate, our system uses the delegated server involving SCVP and OCSP, which is regarded to

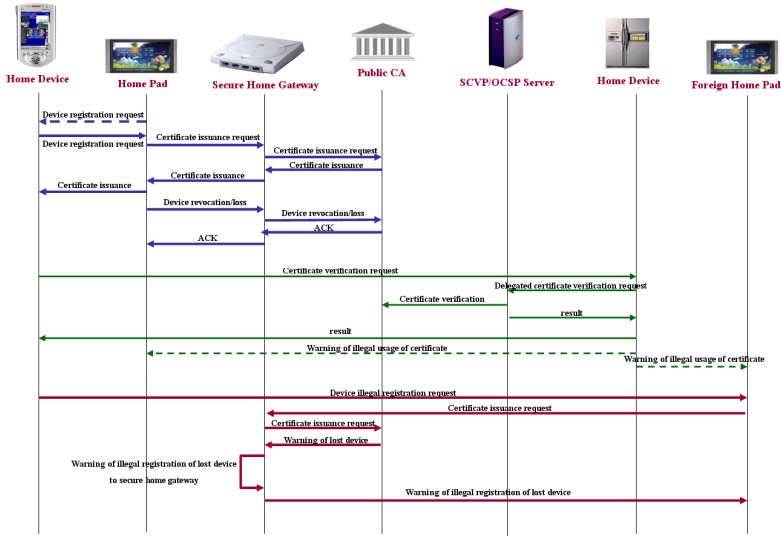


Fig. 11. Authentication flow when using device certificate

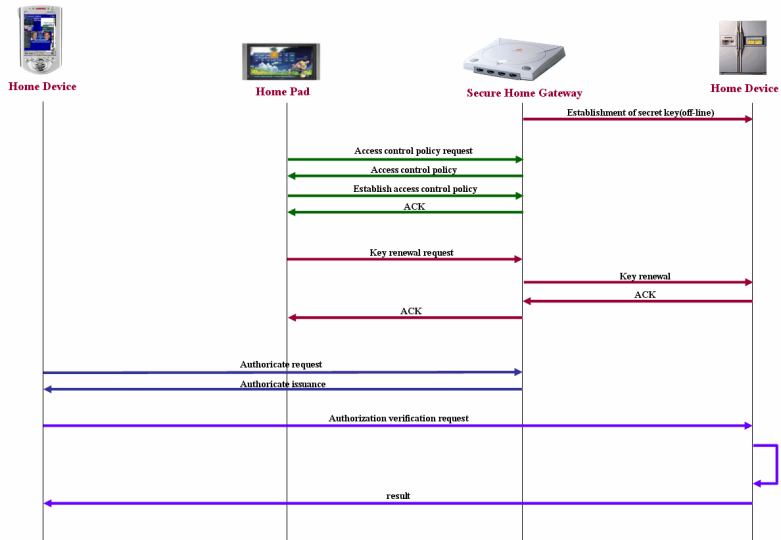


Fig. 12. Authorization flow when using authenticare

reduce the computation overhead by home devices with relative low capacities. Also, our system provides a mechanism preventing illegal usage/registration when lost.

Figure 12 shows authorization flow when using an authoricate, which is another type of certificate for authorization.

Once the home device is successfully authenticated, an authoricate is issued to it for access control. With it, the home device can control other home device without additional authentication. Also, each home device is expected to perform the authorization process since it needs to execute just symmetric key-based encryption algorithms.

6 Conclusion

Since home network consists of heterogeneous network protocols and contains existing security threats and holes of Internet such as hacking, malicious codes, worms, viruses, DoS attacks and eavesdropping, due to connections to the open network, we need a security framework to safeguard against them, efficiently guarantee reliability and availability.

So in this paper, we propose home network security technologies including authentication, authorization, and security policy and describe our implementation.

An authentication mechanism authenticates entity that is access home network. Also we can select our favorite authentication method such as ID-password-based authentication method, certificate-based authentication method, and biometric-information-based authentication method.

An authorization mechanism controls access by an entity even though it has been successfully authenticated already and restricts a privilege and access right. When some authenticated user wants to use home network service, the authorization mechanism receives identity-related information from corresponding authentication mechanism and looks for an adequate authorization rule in security policy database of security policy mechanism. Based on the found rule, the access control enforcer does authorization and informs the result to the entity. It may use both ACL and RBAC simultaneously. We propose an integrated authorization framework, where a variety of authorization methods can work collaboratively, and we do not have to care about the specific authorization method.

Security policy specifies the strategy for home network and provides basic rules for other security mechanisms such as authentication mechanism, authorization mechanism, and enforces security policy. In order to efficiently describe the security policy for home network, we define a new language called an xHDL (eXensible Home security Description Language).

References

1. Han, J.-W.: Revitalization Policy of Home Network Industry, 22nd edn., vol. 9, Korea Information Science Society (2009)
2. Han, J.-W., Kim, D.-W., Joo, H.-II.: Considerations for Home Network Security Framework. In: Korea Information Science Security, 22th edn., vol. 9 (September 2004)

3. Framework of security technologies for home network, ITU-T Recommendation X.1111 (2007)
4. Lee, Y.-k., Ju, H.-i., Park, J.-h., Han, j.-w.: User Authentication Mechanism Using Authentication Server in Home Network. In: Proceedings of the 8th International Conference on Advanced Communication and Technology
5. Lee, H.-k., Lee, Y.-k., Ju, H.-i., Han, J.-w.: User Authentication Mechanisms for Home Network using Home Server, TTAS.KO-12.0030
6. Abobo, B., et al.: Extensible Authentication Protocol (EAP)., IETF RFC3748 (June 2004)
7. Fund, P.: EAP Tunneled TLS Authentication Protocol, IETF draft-funk-eap-ttls-v1-00 (February 2005)
8. Palekar, A.S., Salowey, D., Zhou, J., Zorn, H.: Protected EAP Protocol (PEAP) version 2, IETF draft-josefsson-pppext-eap-tls-eap-10 (2004)
9. Kim, G.-W.: eXtensible Home Security Description Language. Telecommunications and Technologies Association (2006)