Internet Research

Security technologies based on a home gateway for making smart homes secure
Geon Woo Kim Deok Gyu Lee Jong Wook Han Seung Hyun Lee Sang Wook Kim

The current issue and full text archive of this journal is available at
www.emeraldinsight.com/1066-2243.htm

Security technologies based on a home gateway for making smart homes secure

Geon Woo Kim, Deok Gyu Lee and Jong Wook Han
Information Security Research Division, Electronics and Telecommunications Research Institute, Daejeon, South Korea
Seung Hyun Lee
School of Architectural Engineering, Hongik University, Yeongi-Gun, South Korea, and
Sang Wook Kim
Computer Science and Engineering, Kyungpook National University, Daegu, South Korea

Abstract

Purpose – The purpose of this paper is to identify security technologies that are essential in making home network systems secure and to describe specialized security mechanisms for the home network and the relationships among them.

Design/methodology/approach – The research model is designed to support three functions: authentication, authorization, and security policy. Authentication is tested in several methodologies such as id/pw, certificate, or bio; authorization is tested using RBAC methodologies; and security policy is specified using newly-designed script language, such as xHDL.

Findings – The findings for "authentication" suggest that home network users can access services conveniently and securely. In addition, the findings for "security policy" suggest that security policy for home network requires specialized rather than general specification.

Practical implications – The paper identifies three security functions essential for home network: authentication that supports most existing authentication mechanisms, so as to maximize user accessibility; authorization that is middleware-independent and beyond the physical transport layer; and security policy optimized for the home network environment.

Originality/value – The paper focuses on an implementation-based security model for the home network. Though interest and research in home network security are increasing, only limited authentication applications have been adopted in real deployment up to now. This paper introduces an integrated security model and emphasizes safety and convenience so as to promote reliability in home network services.

Keywords Computer networks, Data security, Communication technologies, Local area networks

Paper type Research paper

Introduction

The home network is a new IT technology environment offering convenient, safe, and pleasant lives to users, making possible the provision of a variety of home network services by constructing home network infrastructure anywhere, anytime, and with any device. It can be implemented by connecting home devices based on heterogeneous communicating network protocols, such as mobile communication, internet, and sensor networks. With the home network, we can easily control home devices, make use of a

Internet Research
Vol. 19 No. 2, 2009
pp. 209-226

1066-2243
DOI 10.1108/10662240910952355

number of services such as a video on demand (VOD) services, remote healthcare services, t-commerce services, etc. Specifically, a home network can be defined as a total home information system providing a number of services and solutions, not just simple networking within a single home.

Unfortunately, the home network is subject to infection by all legacy security threats that exist in an open network, since it is accessible from an open network and a variety of coexisting network protocols, where each network contains its own security threats.

In particular, as a home network consists of heterogeneous network protocols and a variety of service models, it is likely to be exposed to various internet-based cyber attacks, such as hacking, malicious codes, worms, viruses, denial of service (DoS) attacks, and eavesdropping, since it is connected to the internet.

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

Related work

There have been a few security deployments in home network systems up to now. Authentication and authorization are considered to be the basic functions used to guarantee safety and privacy protection in enforcing home network services. In addition, a security policy system is generally used in security applications. However, there is no specialized security policy deployment for home network.

Authentication

Authentication is essential in every security system, and for this, the identity-related information from the authentication process is used as basic information in other security functions. And many other security functions are based on the authentication function.

Most of the deployments adopt authentication. This means that only registered users can access the home network to ensure protection from indoor/outdoor illegal access at the earliest stage. Nevertheless, these authentication applications adopt only some limited authentication mechanisms, such as ID/Password-based authentication and certificate-based authentication. In addition, biometric-based authentication can provide a strong security guarantee of the identity of users. However, the security of biometric data is particularly important as any compromise in biometric data will be permanent. In the home network system, a variety of users participate, where each user has own age, character, habits, preferences, and so on. User convenience is one of the goals of home network services. To make it possible, each user can select his/her preferable authentication mechanism. The current realized authentication applications are less than satisfactory.

Authorization

Though authorization is expected in home network systems, only a few applications enforce it. Additionally, those applications do not provide authorization in the service layer. It means that access control is enforced by each deployment of middleware or in the physical layer. Actually, some middleware used in home network, such as UPnP, supports its own access control mechanism. However, this is not considered to be

secure and efficient as a service-layer authorization mechanism. Physical layer authorization is the same. In addition, existing digital right management (DRM) systems focus on the relationship between media distributors and end consumers, not the complex interactions among all the parties involved in the process of producing content.

General model for home network

The home network comprises a number of factors of legacy networks and systems. Categorization of the above entities, of which the home network is comprised, is from ITU-T recommendation X.1111 regarding "framework of security technologies for home network".

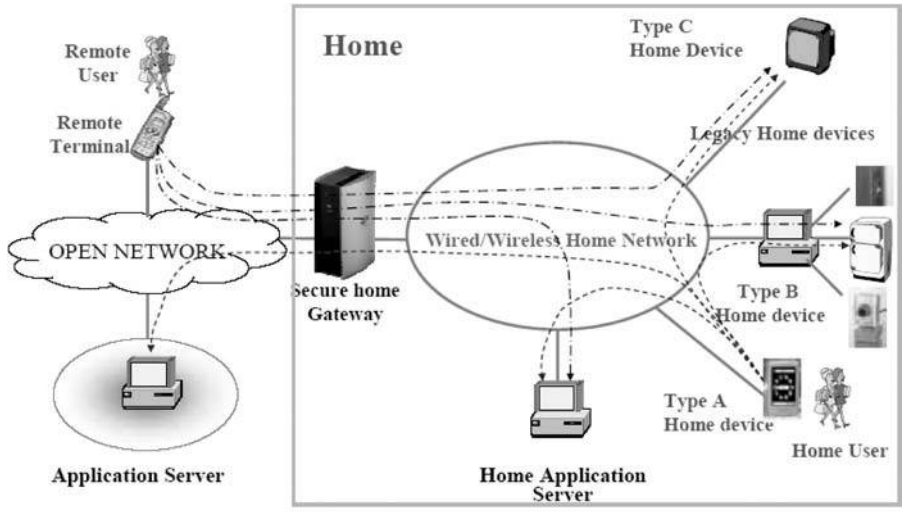
Figure 1 describes the general model for home network from X.1111. All security requirements and technologies are recommended to conform to the above model.

Necessities of security for home network

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

Target of existing attacks due to connection to the internet

Because the home network is composed of heterogeneous network protocols, it is subject to being 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.



Note: All security requirements and technologies are recommended to conform to the above model

Figure 1.
General model for home network

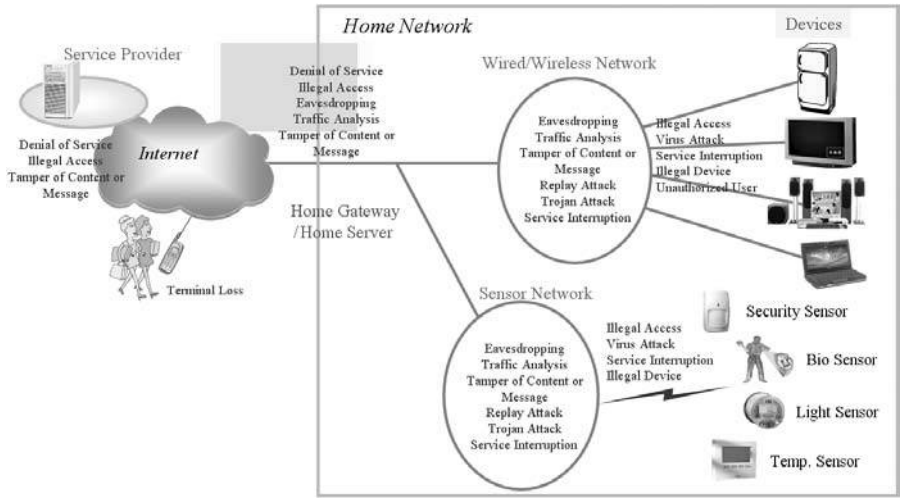


Figure 2.
Security threats in home network

Trusted relationships among entities

In order to make the home network reliable, safe, and available, the means of establishing trusted relationships among entities deployed in the home network is most important from a security standpoint; especially regarding the ubiquitous home network environment, where the majority of services are based on communication among home devices.

During communication among home devices, some exchanged information is critical and should not be revealed to others. For example, in remote health-care services, tampering with or modification of vital information is closely related to the breath of life and personal medical information known to other un-trusted entities may result in serious privacy violation. Furthermore, it is possible to launch a new attack by collecting and analyzing behavioral patterns or habits.

Others

There is an evolution in ubiquitous environments for the home network, where each device tends to be lightweight and portable. A ubiquitous environment seems to be infrastructureless, and security is gaining in importance. There are also incremental security requirements. For example, Intel and Verisign are establishing strong security infrastructure by enforcing device authentication. Therefore, security for the home network must offer convenience and require minimal intervention by the home user.

Security technologies for home network

The enormous growth of the internet in the last few years has brought about new problems and needs that have triggered the creation of new services on the edge of the network. Some examples of these services are security components introduced into the network, such as firewalls or intrusion detection systems, caching devices, translation of IP address (NAT), and the trans-coding of multimedia flows to adapt them to the network, or link requirements.

The home network is supposed to be a service environment in which all these services converge.

There are some security technologies for making the home network secure. Among them, authentication and authorization are viewed as essential.

Authentication

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

Authentication is recognized as the most important in providing security for the home network, including ubiquitous service, and other systems requiring security.

In offline communication, we can identify the others by ourselves. On the other hand, with online communication, one can conceal his/her identity and take on the identity of another.

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

The authentication mechanism supplying a variety of authentication methods uses encrypted extensible authentication protocol (EEAP). EEAP packet is similar to extensible authentication protocol (EAP) packet, and also is similar to EAP Tunneled TLS (EAP-TTLS) or protected EAP (PEAP).

The authentication server is different from the CA server in that it supports authentication using certification, as well as ID-password or biometric information, and stores authentication information registered in the various content server securely. The certificate authority (CA) server in public key infrastructure (PKI) plays the role of issuing and managing certificates and takes a neutral attitude in authentication process.

Once an entity is successfully authenticated, it can use his/her authorized service. If it wants to control home appliances remotely, it can control them. And if it wants to use content by internet service providers (ISPs), it connects to the target server in order to provide the requested service. The general authentication model for ubiquitous home network is shown in Figure 3.

In the 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 the above circumstances and relative requirements.

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

For authentication within a 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 (Figure 4). The decision to adopt a specific authentication mechanism depends on application.

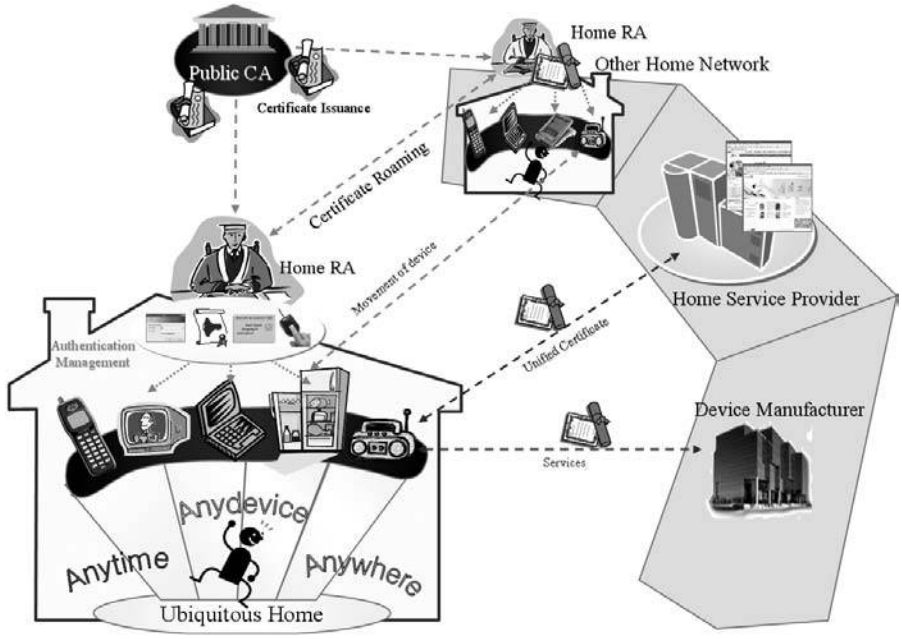


Figure 3.
General model for authentication in ubiquitous home network

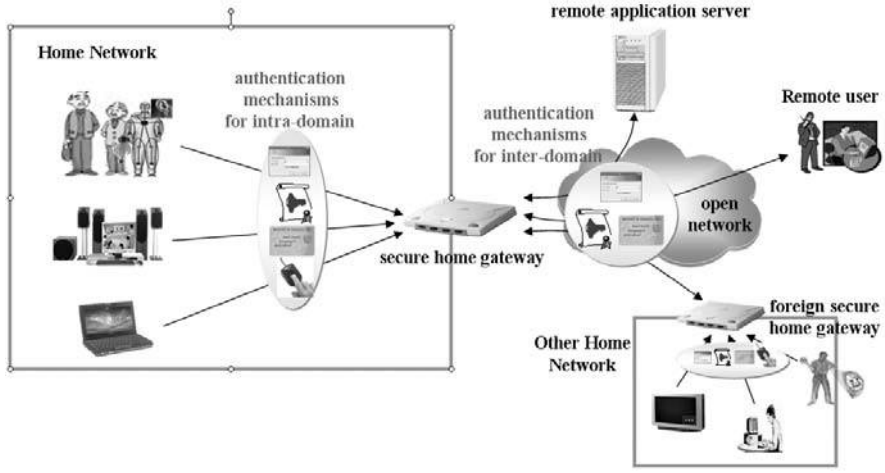


Figure 4.
Authentication mechanisms for the ubiquitous home network

On the other hand, it is desirable to exclude 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 each home network service. Specifically, each user is authenticated by a secure home gateway and does not consider the following authentication process: for example, when a user wants 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 carries out authentication with the remote application server instead of the user.

To make this possible, the secure home gateway contains an authentication mapping function, which enables mapping between both intra-domain and inter-domain authentication mechanisms.

Authorization

The purpose of authorization is to control access of any entity, even though it has been successfully authenticated, and to restrict privilege and access rights. It can also minimize losses when the home network system is penetrated and attacked by malicious accessing or unauthorized uses.

For this we can use an access control list (ACL) or a role-based access control (RBAC). The ACL directly establishes relationships between subjects and resources, where the subject refers to an entity wishing to gain access, and the resource refers to an entity that the subject is accessing. The ACL is simple, and is therefore useful for relatively small-scale networks. On the other hand, the RBAC adapts an intermediate component referred to as a role between a subject and a resource; it indirectly sets up relationships between the two. The RBAC seems to be adequate for relatively large-scale networks.

Figure 5 simply illustrates ACL and RBAC. As the home network includes a variety of network protocols and is expected to support many service models, such as a client-server model, peer-to-peer communication model, and hybrid model, it is difficult to define which mechanism is most suitable for the home network. Actually, we advise using a different authorization model according to the specific home network service; and as a result, we require an integrated authorization framework for the home network.

Figure 6 shows authorization modules for the home network. Existing authorization mechanisms can be categorized into three fields: server-based authorization mechanism, peer-to-peer authorization mechanism and certificate-based

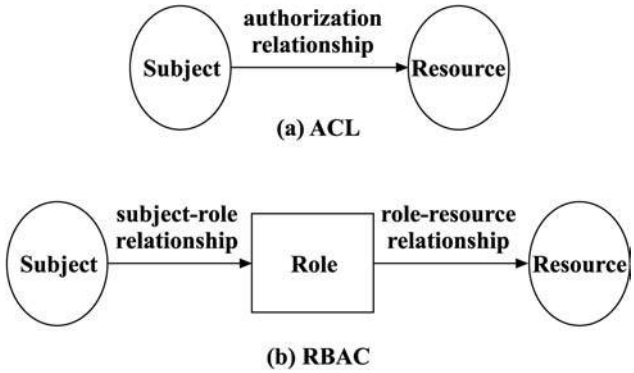


Figure 5.
ACL vs RBAC

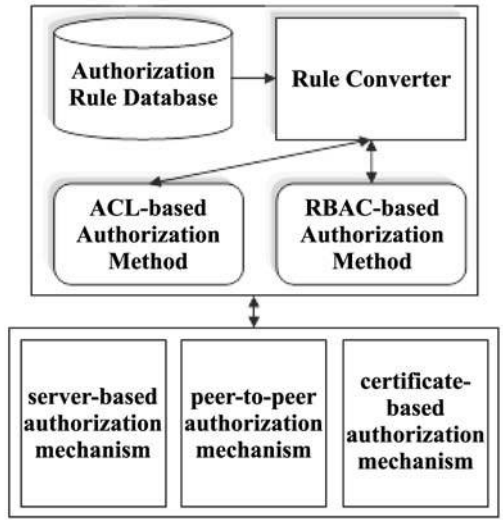


Figure 6.
Authorization modules for home network

authorization mechanism. A server-based authorization mechanism works on the client-server model where the server generates, maintains and enforces authorization rules. This method is relatively simple and easy to apply; a peer-to-peer authorization mechanism works for p2p communication service models, through which a peer can manage authorization rules by itself or request help from the 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 devices, etc.; a certificate-based authorization mechanism is generally used in open networks and conforms to the PKI.

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

An authorization rule database contains raw authorization rules, the details of which are not described in this paper. The rule converter translates the raw authorization rules into ACL- or RBAC-based authorization rules and vice-versa. It can also maintain consistent authorization rules between ACL- and RBAC-based authorization methods by reflecting changes in one type of authorization rules to the other instantly.

The authorization model for the 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.

Whenever a home network service request occurs, the authorization module decides whether or not to permit access, based on the information collected by the authentication module, configuration, and access control database. After making a decision, it enforces the authorization based on the policy and stores the result in the log database. It can also discard the request or, alternatively, require home network services.

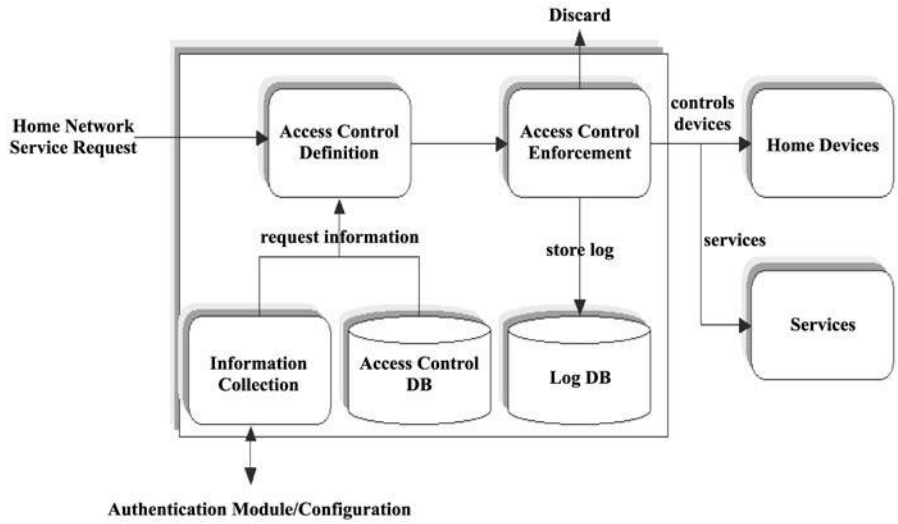


Figure 7.
Functional components for authorization

Security policy

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

- time (date, day, duration);
- event (sensor, user-triggering, state); and
- log (statistics).

We also define relationships (interaction, union) among the above elements and support recursive structure, making it possible to build complex conditions.

Time and event are the basic elements of condition and can generally be used for this purpose. On the other hand, log-based condition controls gain access through statistical information. For example, there is a pre-condition that the security policy manager sets the policy that children cannot use the game service more than 30 hours per month. Whenever the children access the game service, their usage information may be stored in the log database. If the above condition is satisfied, connection will be rejected and access denied for the remainder of the month.

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

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

Before enforcement of home network policy can commence, an administrator of home network policy should set the security policy, where each rule comprises a pair of "if" and "then" clauses. If there is a request from another module triggering the security policy enforcer, it then looks for an appropriate rule for the request and investigates the

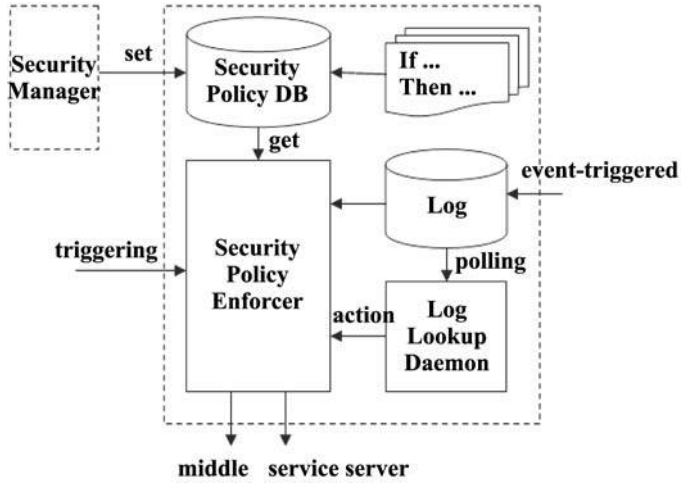


Figure 8.
Security policy system for home network

related information in the log database. The security policy enforcer can connect a middleware application or a service server so as to enforce the policy.

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

Considering the features of the home network, usability must be sufficient for users unfamiliar with IT. In our system, we use a drag-and-drop mechanism to establish the security policy, allowing easy access and control to any user who has been successfully authenticated. Figure 9 illustrates the functions provided by the security policy manager.

The home network user can monitor and manage the three components using a GUI implemented in the home pad. Also, the get module reads the old policy and the set module generates the new policy. In our system, we use a new defined language called extensible home security description language (xHDL), based on XML.

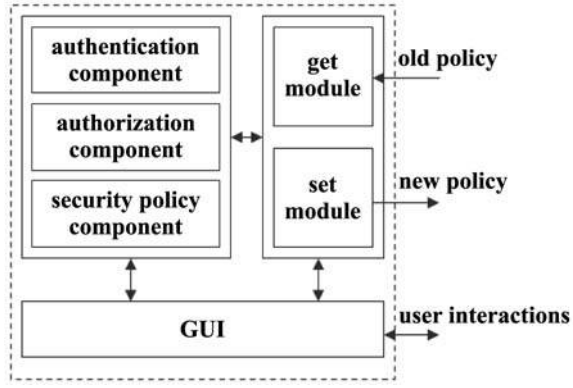


Figure 9.
Security policy manager for home network

Security policy specification

In order to efficiently enforce the security policy, we need a consistent means of describing and specifying the security policy and the components constructing it. Extensible access control markup language (XACML) standardized by OASIS and ITU-T may be an alternative solution for specifying home network policy. It is a declarative access control policy language implemented in XML, and a processing model describing how to interpret the policies. However, using XACML for describing home network policy requires redundant syntax notations, since it has been of general-purpose. Home network policy is also likely to support authentication and security policy specialized for the home network, including authorization.

Therefore, in our system, we use a newly-defined language called extensible home security description language (xHDL), based on XML. The xHDL comprises seven elements.

XML scheme for xHDL is shown in Figure 10.

(1) *Combining-rule element*. The combining-rule element makes it possible to address the conflicts among duplicate security rules. Some security rules may encourage what other security rules forbid. To solve inconsistency among security rules, we use several combining-rules, mainly from XACML. These rules are as follows:

- Permit-overrides: permit access if at least one permit-access rule exists.
- Deny-overrides: deny access if at least one deny-access rule exists.
- First-applicable: applies the first rule which is applicable.
- Only-one-applicable: if and only if just one rule satisfies the condition, applies the rule; fails in other cases.
- High-priority-applicable: apply a rule with the highest priority.

If the combining-rule is not defined, the default combining-rule shall be provided. The combining-rule is recommended to be defined explicitly.

```
<element name="xHDL">
  <complexType>
    <sequence>
      <element name="combining_rule" type="combiningRuleType" />
      <element name="objects" type="objectsType" />
       <element name="object_groups" type="objectGroupsType" minOccurs="0"
          maxOccurs="1"/>
       <element name="authentication" type="authenticationType" minOccurs="0"
          maxOccurs="1"/>
      <element name="users" type="usersType" />
      <element name="roles" type="rolesType" />
      <element name="rules" type="rulesType" minOccurs="0" maxOccurs="1"/>
    </sequence>
    <attribute name="xmlns" type="string" />
  </complexType>
</element>
```

Figure 10.
XML scheme for xHDL

(2) *User element*. The user element specifies user-related items. The items contained in the user element are as follows:

- Security level.
- User information including name, sex, ssn, e-mail, birth date, address, phone, employer, marriage, etc.
- Authentication information for ID/PW, certificate, bio information, rfid.
- User access privileges for home network services.

The security level is categorized into four levels: s0, s1, s2 and s3. S0 ensures that the user can access all home network resources while s3 guarantees no access.

(3) *Authentication element*. The authentication element specifies items related to the authentication used in the home network as follows:

- Authentication method:
  - EAP_MD5.
  - EAP_TLS.
  - PEAP.
  - EAP_TTLS.
- Whether to provide mutual authentication.
- Whether to use abbreviation during performing of authentication protocol.
- Maximum number of failed logins allowed to the user.
- Maximum time elapsed since successful login.
- Maximum period without access.
- Default encryption algorithm:
  - DES.
  - 3-DES.
  - AES.
  - SEED.
- Default hash algorithm:
  - MD5.
  - SHA-1.
- Preferred encryption algorithm:
  - DES.
  - 3-DES.
  - AES.
  - SEED.
- Preferred hash algorithm:
  - MD5.
  - SHA-1.

- Preferred compression algorithm:
  - rle.
  - zlib.

(4) *Object element*. The object element defines home network resources installed in the home network. The objects include home electronic appliances, home network services, living supplies, and so on. The items contained the object element are as follows:

- Object name.
- Object type: device, service, sensor.
- Installed location:
  - Living room.
  - Kitchen.
  - Porch.
  - Laundry room.
  - Room 1.
  - Room 2.
  - Room 3.
  - Room 4.
- Installed coordinates.
- Operations.
- Arguments for each operation defined.
- Contained group ID.
- Security level.

(5) *Objects-group element*. The objects-group element enables the grouping of objects of features. The items described in the objects-group element are as follows:

- Containing object ID list.
- Security level.

(6) *Roles element*. The roles element specifies the access rights of users. It adopts the RBAC method and establishes relationships between subjects and resources, where the subject refers to the user and the resource refers to the pre-defined object and object-group. The items described in the roles element are as follows:

- Access rights of the User ID.
- Role hierarchy:
  - Export.
  - Import.
- Security level.

- Permission:
  - Resource type: device; service; sensor; group.
  - Resource ID.
  - Direction.
  - Negation.
  - Operations.

In the role hierarchy, the roles element uses two terms: export and import. The export item enables the role element to be a super element of role elements, following the export item. The import item means that the role element is a sub element of rule elements, following import item. In other words, the two terms are used for describing the relationship of parents and children.

Regarding permission, the negation item makes it possible to deny access to the designated operations listed in the operations item.

The operations item designates several specific operations allowed or not allowed to the user list in the user ID.

(7) *Rules element*. The rules element specifies the enforcement of security policy, specialized for the home network. It comprises set of conditions and actions: the condition item specifies when the operations following the action item should be enforced; the action item specifies what is enforced, whenever the condition is satisfied. The items described in the rules element are as follows:

- Condition:
  - Intersection: event; date; day; time; union.
  - Union: event; date; day; time; intersection.
- Actions:
  - Subject: user, role, group.
  - Resource: device, service, sensor, group.
  - Event: location, duration (cycle, unit).
  - Action: operation, arguments, value.

In the condition item, multiple conditions may be connected to create a final condition. Each condition, including event, date, day, and time, may be intersected or unionized. In the action item, multiple designated actions are described. It requires the subject to perform the actions described in the action item on the resource, and sets restrictions such as location and duration.

Implementation

This section describes the implementation of security for the home network. Figure 11 shows entities and their relationships in our implementation.

With the above structure of implementation, authentication flow when using device certificate is shown in Figure 12.

For using certificate, it is issued by the public CA with the help of the home pad and the secure home gateway to the home device. When verifying the certificate, our system uses the delegated server involving SCVP and OCSP, which is known to reduce

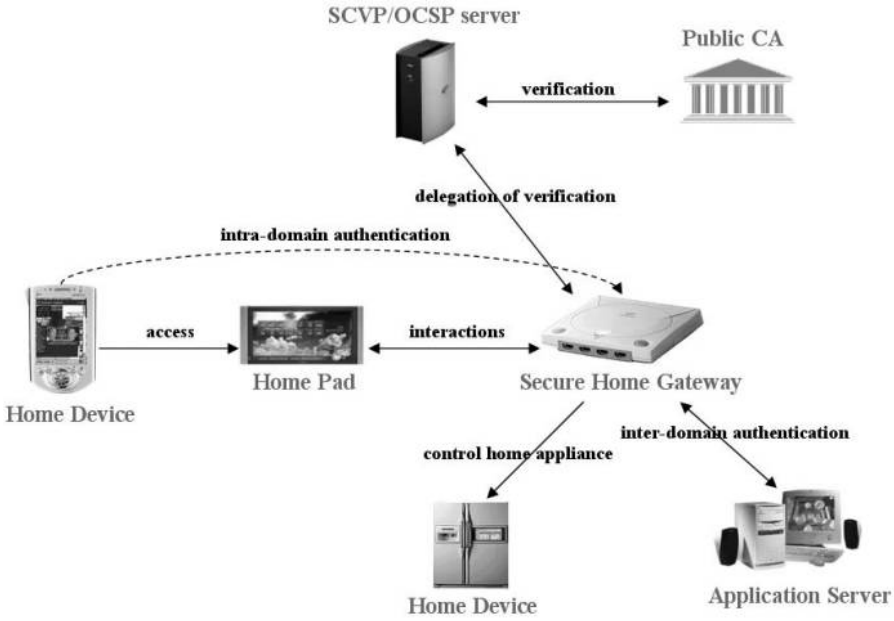


Figure 11.
Structure of our implementation

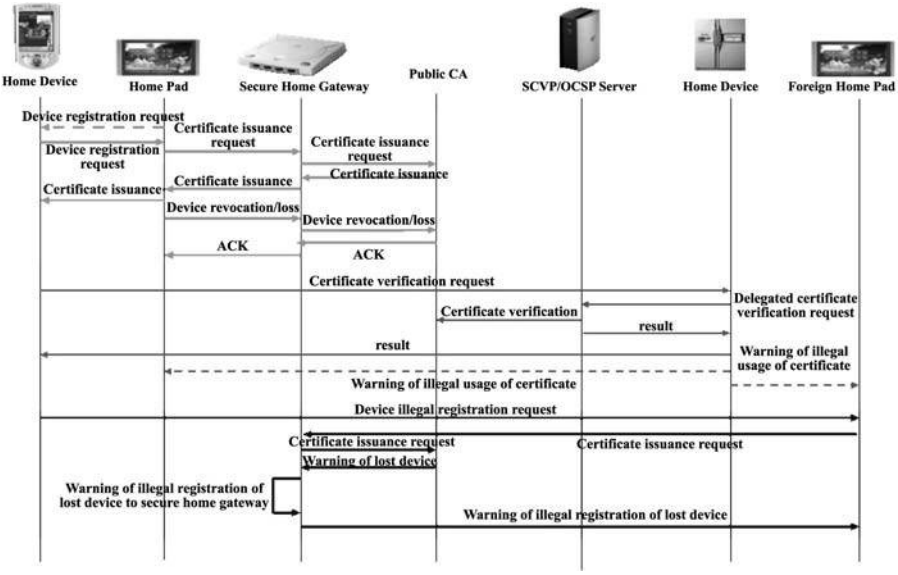


Figure 12.
Authentication flow when using device certificate

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

The first phase describes a procedure related to certificate issuance, the second phase describes the procedure of certificate validation in using indoor home network

service, and the third and final phase describes the procedure of certificate validation in using outdoor home network services.

In issuing a new certificate, the home pad provides user interface and the secure home gateway plays a role of registration authority (RA).

In using indoor the home network service, the entity that provides the service is responsible for checking the validity of the certificate upon accessing the home device. In our home network system, as every home device is not supposed to support sufficient computing power and capacity, the validating procedure is delegated to the trusted third-party, enforcing server-based certificate validation protocol (SCVP) and online certificate status protocol (OCSP).

In using the outdoor home network service, the procedure for requesting certificate validation to the secure home gateway by the foreign home pad is added. Figure 13 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 this, the home device can control other home devices without additional authentication. Also, each home device is expected to perform the authorization process since it only needs to execute symmetric key-based encryption algorithms.

In Figure 13 the first phase describes a procedure for monitoring and managing the security policy related to authorization set in the secure home gateway. The administrator can manage the authorization policy using the GUI of the home pad. The second phase describes a procedure for key management. As our implementation uses a symmetric key, an additional key management mechanism is required. The third phase describes a procedure of authoricate issuance, where an authoricate is designed to contain authorization-related information in a secure manner. The significant

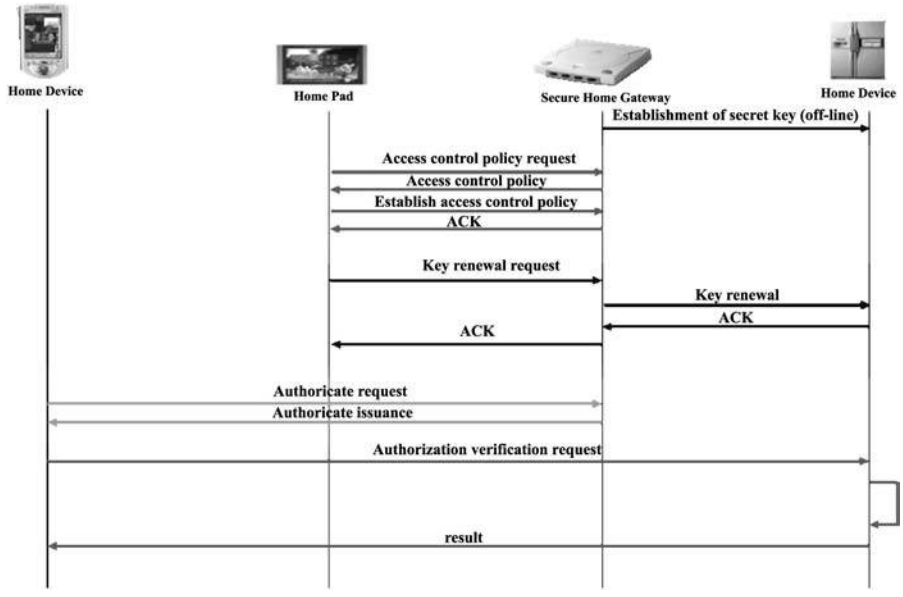


Figure 13.
Authorization flow when using authoricate

difference between authoricate and authorization certificate is that the authoricate developed in our implementation is based on a symmetric key, whereas the existing authorization certificate uses asymmetric key mechanism. The fourth and final phase describes a procedure of authoricate verification while using home network services.

In our implementation, most of the systems operate in Linux, except the home pad, for which the operating system is Windows XP. Regarding the current trend in deploying home network services, the majority adopts both the home pad and the home gateway simultaneously. This means that the home pad is responsible for user interface and other functional requirements, whereas the home gateway focuses primarily on functionality in the middleware or physical transport layer.

Conclusion

Since the home network comprises heterogeneous network protocols and is vulnerable to the existing security threats and holes in the internet, such as hacking, malicious codes, worms, viruses, DoS attacks and eavesdropping, due to connections to the open network, we require a security framework to safeguard against these dangers and efficiently guarantee reliability and availability.

Therefore, in this paper, we propose home network security technologies, including authentication, authorization, and security policy, and include descriptions of implementation.

An authentication mechanism authenticates an entity that accesses the home network. We also provide the option to 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 privileges and access rights. When an authenticated user wants to use the home network service, the authorization mechanism receives identity-related information from the corresponding authentication mechanism and looks for an adequate authorization rule in the security policy database of the security policy mechanism. Based on the found rule, the access control enforcer carries out authorization and informs the entity of the result. It may use both ACL and RBAC simultaneously. We propose an integrated authorization framework, where a variety of authorization methods can work collaboratively, such that we need not 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 extensible home security description language (xHDL).

Further reading

Abobo, B. *et al.*, (2004), "Extensible authentication protocol (EAP)", IETF RFC3748, June.

Alarcos, B., Sedano, M. and Calderon, M. (2005), "Multidomain network based on programmable networks: security architecture", *ETRI Journal*, Vol. 27 No. 6, pp. 651-65.

Fund, P. (2005), "EAP tunneled TLS authentication protocol", IETF draft-funk-eap-ttls-v1-00, February.

Han, J-W. (2004), "Revitalization policy of home network industry", *Korea Information Science Society*, Vol. 9, 22nd ed..

Han, J-W., Kim, D-W. and Joo, H-I. (2004), "Considerations for home network security framework", *Korea Information Science Security*, Vol. 9, 22nd ed.

ITU-T (2007), "Framework of security technologies for home network", *ITU-T Recommendation X.1111*.

Kim, G.-W. (2006), "eXtensible Home Security Description Language", Telecommunications and Technologies Association.

Lee, Y-K., Ju, H-I., Park, J-H. and Han, J-W. (n.d.), "User authentication mechanism using authentication server in home network", *Proceedings of the 8th International Conference on Advanced Communication and Technology*.

Lee, H-K., Lee, Y-K., Ju, H-I. and Han, J-W. (n.d.), "User authentication mechanisms for home network using home server", TTAS.KO-12.0030.

Lee, J-S., Hwang, S-O., Jeong, S-W., Yoon, K-S., Park, C-S. and Ryou, J-C. (2003), "A DRM framework for distributing digital contents through the internet", *ETRI Journal*, Vol. 25 No. 6, pp. 423-36.

Moon, D-S., Chung, Y-W., Pan, S-B., Moon, K-Y. and Chung, K. (2006), "Fingerprint images for embedded processors", *ETRI Journal*, Vol. 28 No. 4, pp. 444-52.

Palekar, A.S., Salowey, D., Zhou, J. and Zorn, H. (2004), "Protected EAP protocol ("PEAP) version 2", IETF draft-josefsson-pppext-eap-tls-eap-10.

Corresponding author
Sang Wook Kim can be contacted at: swkim@cs.knu.ac.kr