Light-weight Access Control Mechanism based on Authoricate issued for Smart Home

Geon-Woo Kim, Jong-Wook Han
Electronics and Telecommunications Research Institute, Daejeon, Korea
kimgw@etri.re.kr, hanjw@etri.re.kr

Abstract

As home network is expanding into ubiquitous computing environment and a variety of services are realized, requirements and interests on security for smart home network are increasing. In order to make home network safe and stable, some security technologies including authentication, authorization, and security policy technology are needed. So, in this paper, we propose a light-weight access control mechanism used for home network environment, where various types of users and devices coexist and heterogeneous network protocols can be deployed.

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 devices, time, and places. This can be done by connecting home devices based on various kinds of communicating networks, such as mobile communication, Internet, and sensor network [1].

Recently, the home network is expanding into ubiquitous computing environment, and boundary between network and system tend to be obscure.

However, home network is exposed to various cyber attacks of Internet, involves hacking, malicious codes, worms, viruses, DoS attacks and eavesdropping since it is connected to Internet and consists of heterogeneous network protocols [2].

Therefore, a lot of security technologies such as authentication, authorization, intrusion detection, and firewall are required to guarantee safety and availability of home network. Among them, authentication and authorization are supposed to be the core security modules.

However, it seems to have some difficulty in deploying the authorization to home network. As home network supports a variety of service models and is composed of a number of home devices with different computer powers and capacities, legacy authorization mechanisms are not considered to efficiently control home network.

So in this paper, we propose a new authorization mechanism, which is adequate for home network, and secure.

2. Legacy Authorization Models

The main 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 [3].

Legacy authorization mechanisms can be categorized into two models: centralized authorization model and distributed authorization model [4].

2.1. Centralized authorization model

The centralized authorization model adopts a centralized trusted authority, which is responsible for controlling access, and restricting privilege within the boundary of service domain.

As client-server model is generally deployed in home network, the centralized authorization model is supposed to be adequate for home network. Besides, it's reliable, manageable, and consistent.

In the application of home network, secure home gateway or application server may be an authorization server, acting as a gateway for service and establishing connection between a home subject and a home resource.

The centralized authorization model is shown in Figure 1.

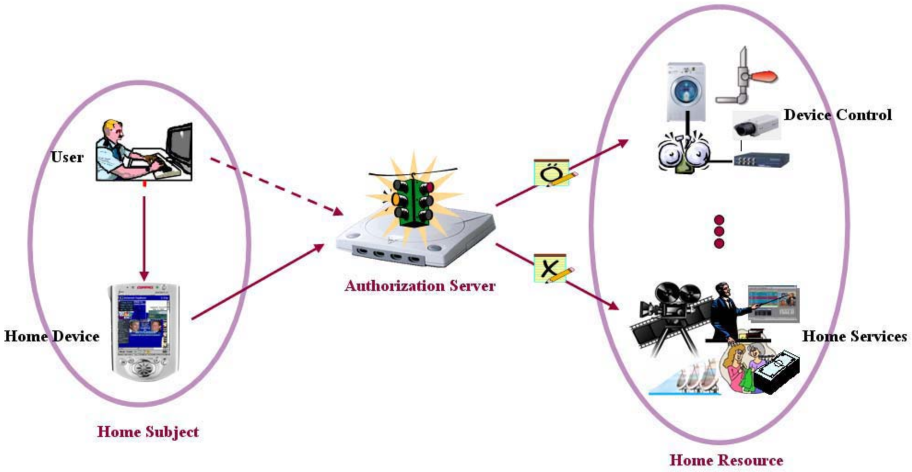

Fig.1 Centralized Authorization Model for Home Network

All accesses are controlled by the authorization server, which manages the integrated policy for access control and a variety of middlewares for heterogeneous home devices.

However, this model is not adequate in relatively large-scale network and environment where changes in their entities frequently occur. Also, this model can't support some type of middleware for peer-to-peer communication such as UPnP.

2.2. Distributed authorization model

The distributed authorization model for home network makes it possible to control access without help of a centralized trusted authorization server, which includes secure home gateway, application server, and other trusted third party.

The distributed authorization model is shown in Figure 2.

In this model, to make it possible for each home subject to immediately control all accesses to itself, it should manage its own policy for authorization and provide corresponding functions. It is applicable to either distributed environment or middlewares for peer-to-peer communication. On the other hand, this may be a burden to home device with relatively low-capacity. Also, this model is lack of manageability and has a difficult in maintaining consistency among numerous authorization policy distributed.

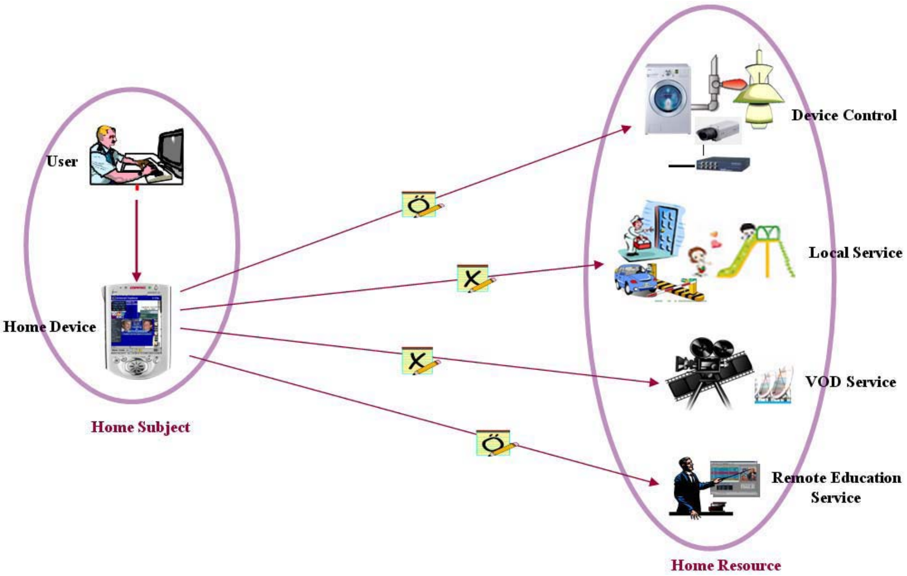

Fig.2 Distributed Authorization Model for Home Network

3. Light-weight access control mechanism

We propose a new access control mechanism to solve above problems.

First we must consider a few requirements in designing a new access control mechanism.

3.1. Requirements

We define a few requirements for efficient access control as follows:

- ❑ The authorization must apply to all possible service models in home network: It ensures that every access must be controlled by the authorization engine deployed for home network
- ❑ The authorization must work on all network protocols deployable in home network: It means that authorization must be performed regardless of network protocols and middlewares in home network.
- ❑ The authorization module must be designed considering the H/W specification of each home device enforcing authorization: It ensures that the authorization module must be performed at every device even if it provides low computing power and capacity.
- ❑ The authorization must be independent of access control mechanisms such as ACL, RBAC, and etc: It ensures that every access control mechanism must be applicable for home network.

3.2. Proposed authorization mechanism

Our proposed access control mechanism ultimately adopts a hybrid authorization model of legacy authorization models described section 2, which is shown in Figure 3.

This access control mechanism uses an authoricate, which is a certificate for authorization and contains rules for authorization.

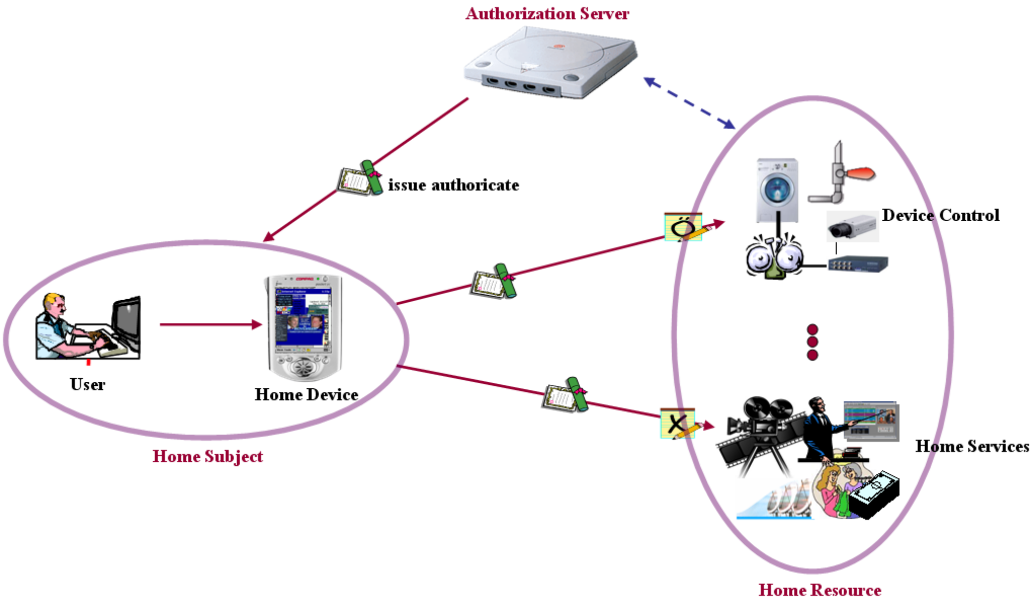

Fig.3 Proposed Authorization Model for Home Network

3.2.1. Authoricate: The authoricate is a specific type of material to make it possible for an authorization server to grant a privilege to corresponding home subject, which may be either a user or a home device.

The authoricate seems to be similar to the PMI (Privilege Management Infrastructure) in PKI. But the definite difference between the authorization and the PMI is that the authorization uses encryption algorithms based on symmetric key (e.g., AES, DES, and etc), whereas the PMI adopts a asymmetric key-based encryption algorithm such as RSA, DSA, and ECDSA.

This is very important advantage in home network. As I described in the previous section, so many types of home devices coexist and collaborate, and we must be able to control accesses to all home devices. Therefore, the authorization module must be designed and implemented considering computing power and capacity of each home device.

PMI seems to be adequate in relatively large-scale open network, but not in home network unfortunately, since each home device is not expected to perform the computations needed.

So, we define a new material for authorization applicable to a variety of home device, named authoricate.

The profile of authoricate is shown as follows;

❑ Version: defines the version of authorization, default value is 0(v1).

❑ Serial number: uniquely identifies an authoricate issued by the issuer, which may be sequentially incremented by 1 or random.

❑ Subject: uniquely identifies an entity that is going to access home network.

❑ Issuer: uniquely identifies an entity that issues the authoricate.

❑ Validity period: describes the period that the authoricate is valid, which is composed of a notBefore element and a notAfter element.

❑ Privilege: contains information for access control.

- Description: contains readable text for describing the subject, which is not closely related to the safety of using authoricate
- Signature algorithm: identifies an algorithm used in producing the signature
- Signature: contains signature data.

ASN.1 structure for authoricate is as follows;

```
Authoricate ::= SEQUENCE {
    tbsAuthoriate TBSAuthoricate,
    signatureAlgorithm AlgorithmIdentifier,
    signatureValue BIT STRING
}
TBSAuthoricate ::= SEQUENCE {
    Version[0] EXPLICIT Version DEFAULT v1,
    Serial number CertificateSerialNumber,
    Subject SubjectID,
    Issuer IssuerID,
    Validity ValidityPeriod,
    Privilege AccessRight,
    Description UTF8String
}
```

The details are not described in this paper.

3.2.2. Authorization flow: Figure 4 describes our proposed authorization flow for home network.

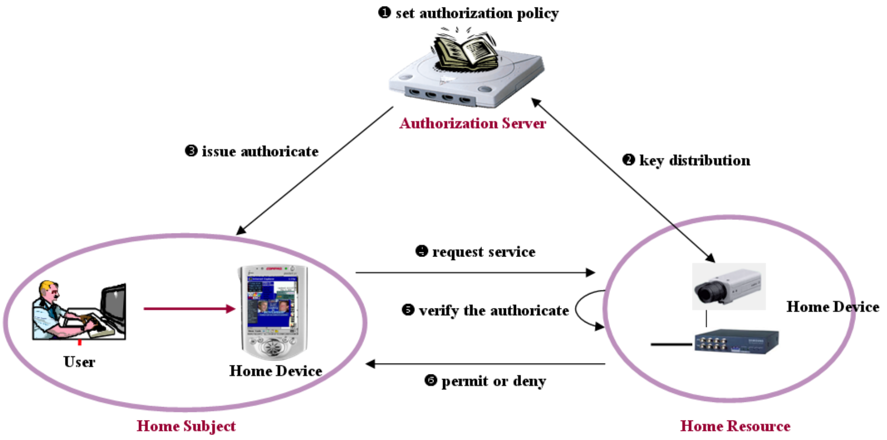

Fig.4 Proposed Authorization Flow for Home Network

The process of our proposed authorization consists of 6-step

- *The process of maintain authorization policy:* This process includes generation/modification/deletion of authorization policy, distribution of authorization policy, management of account of administrator, making the process secure, establishment of database, and others.

The process may be performed either locally or remotely with secure session, which depends on the application.

The scheme for database containing authorization policy is not described in this paper. But it is obvious that the database must support every possible authorization method, including DAC, MAC, and RBAC.

❑ *The process of key distribution*: Sharing secret key with home resource is the most important and complicated process in authorizing home network. The shared key is used for communication between authorization server and the corresponding home resource as well as for guaranteeing security in using an authoricate.
The process of key distribution is shown in Figure 5.

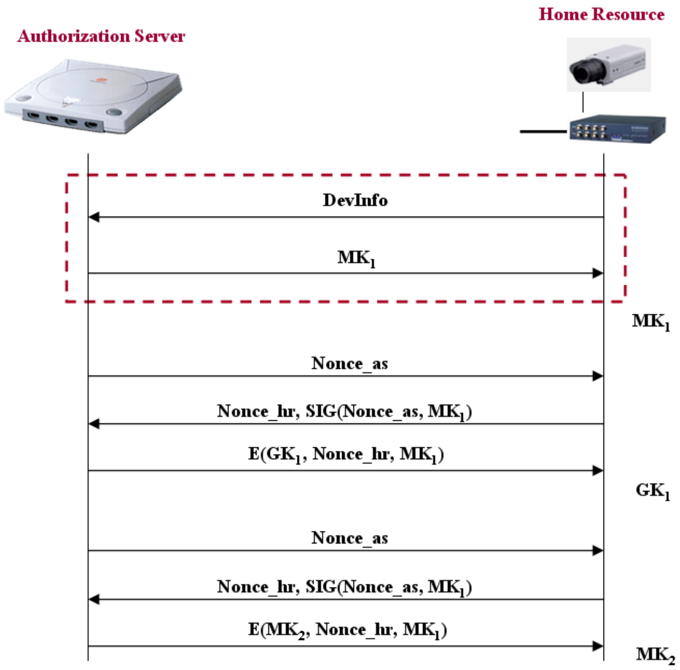
Home Resource
Authorization Server
DevInfo
MK_1
MK_1
Nonce_as
Nonce_hr, SIG(Nonce_as, MK_1)
E(GK_1, Nonce_hr, MK_1)
GK_1
Nonce_as
Nonce_hr, SIG(Nonce_as, MK_1)
E(MK_2, Nonce_hr, MK_1)
MK_2

Fig.5 The flow of key distribution

The keys shared between an authorization server and a home resource are categorized into two types: MK(Master Key) and GK(Group Key).

MK is known only to an authorization server and a home resource and used for distribution and renewal of a GK and a new MK, establishing trusted relationship between them.

The first phase of key distribution is for setting up a MK at initial stage, and must be executed in a secure manner. At initiation process, there may be no material for secure transfer of secret data. So we recommend executing the first phase with off-line, but it depends on environment and application.

The second phase of key distribution is for distributing and renewing a GK_i, which is used for signing authoricates. Home resources with the same GK_i are assumed to be single home resource from the authorization point of view. That is to say, they can be represented by single entity in applying authorization. They use nonce data for prevention of replay attack. After verifying the exchanged nonce data, they authorization server generates and distributes a GK_i encrypted with the MK for the relevant home resource.

Likewise, the third phase of key distribution is for renewing a MK. All sessions between them are protected using a MK_{i+1} instead of a MK_i.

□ *The process of issuing authoricate:* The authorization server is responsible for issuing authoricates in a secure manner.

In case of using a X.509 certificate used in global network, the private key of issuing CA is used for producing signature data, which is attached to the certificate to make sure that it is issued by the relevant CA. So an entity verifying the certificate just needs to retrieve the corresponding public key from it and verify with the attached signature data. Of course, there are additional processes in verifying it with PKI.

On the other hand, in our proposed authorization mechanism, secret key is used for signing an authoricate. The secure key may be either a MK_i or GK_i between the authorization server and the relevant home resource.

It is assumed that the authorization process follows the authentication process. During issuing an authoricate, the authorization server needs identity information of the accessing home subject. To make sure that the authoricate is issued to the appropriate home subject, the process of identifying the home subject should precede.

The process of issuing authoricate is shown in Figure 6.

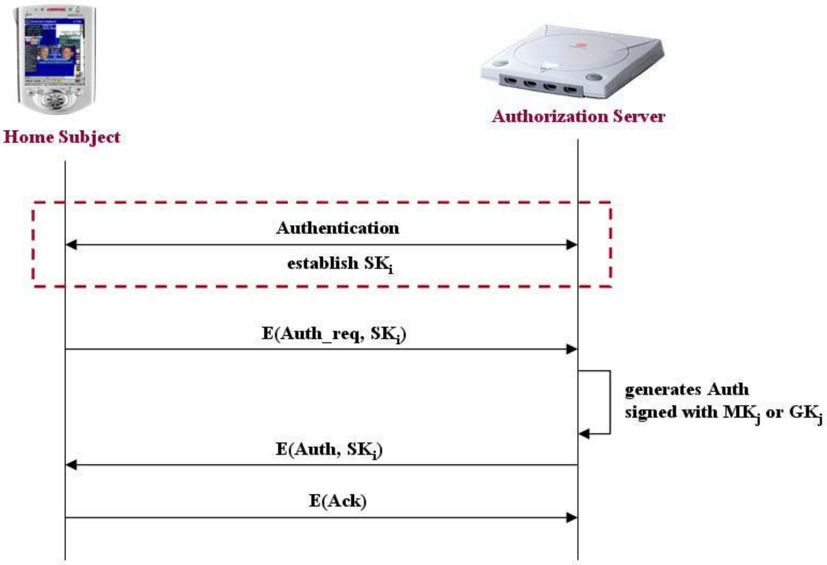

Fig.6 The flow of Authoricate issuance

Every exchange data during authoricate issuance should be protected by a session key SK_i, which has been negotiated in the preceding authentication process. The issued authoricate is signed with a secret key owned only by the authorization server and the home resource that the home subject is accessing, which may be either a MK_j or a GK_j.

The reason that doesn't use a secret key owned by the authorization server, but a MK_j or a GK_j in signing an authoricate is to make it possible for the relevant home resource to verify the authoricate by itself when receiving a service request.

□ *The process of requesting service:* This process enables for the home subject to request a service to a relevant home device or a server, which doesn't contain any specific material for security, but just following items:

- Identify information of the home subject

- Authoricate issued
- List for services that the home subject is going to use

Whether to make the session for this process secure or net depends on application.

❑ *The process of verifying authoricate:* The authoricate submitted by a home subject is likely to be verified directly by the relevant home subject, since the key used in signing the authoricate is owned by the home subject.

Single home subject may be a member of multiple groups. Namely, single home subject probably has multiple GKs.

For verifying the authoricate, the home subject must know which key has been used.

At the stage of key distribution, the home subject is expected to maintain a group key mapping table. Each record in the table contains a pair of (group id, group key), where a group id is a group identifier among groups that the home resource is participating, a group key is a secret material shared between the authorization server and all members of the group.

The group key is likely to be revoked by many reasons. So, it is desirable to refresh the group key often so far as circumstances permit.

❑ *The process of decision and enforcement of access control:* To decide where to permit access or not is complicated since many factors and circumstances may influence the result.

The following items may be factors during decision

- Rule for access control
- Circumstances
    - Emergency
    - Loss of device
    - Disclosure of private information
- Temporary prohibition
- Revocation of authoricate
- Other factors

Based-on the decision, the home resource enforces authorization as follows;

- Permit: provides relevant services
- Deny: doesn't provide relevant services
- Store it to log database
- Alert

4. Considerations

There are a few considerations in enforcing authorization for home network.

- ❑ There should be no intervention by third party during verifying authoricate by home resource: this consideration is reflected in protocols for issuance and verification of authoricate for guaranteeing safety and reliability.
- ❑ It should be easy to integrate with legacy authentication system: this consideration is related to the outer interface of authorization module. It means that authorization module is designed to use identity-related information from trustable authentication module.
- ❑ It should maintain existing service flow of home network as it is: It means that the authorization module must be available for every existing home network service and need no extra modification.
- ❑ It should guarantee extensibility and safety: It means that the deployed authorization module must be available regardless of the scale and features of home network services.

5. Conclusion

As home network have to provide a variety of services to its members with a variety of characteristics and preferences using heterogeneous network protocols regardless of places, we need security mechanisms for guaranteeing safety, availability, and etc.

To protect the home network from numerous threats scattered everywhere, authentication and authorization are supposed to be key functions.

Furthermore, it doesn't seem to be desirable to apply legacy authorization mechanisms as they are to home network. Actually, every entity in home network is not sure to perform them due to its computer power, capacity, and other factors.

So in this paper, we propose a new authorization mechanism adequate for home network, where a number of devices with low-capacity are deployed.

Our proposed authorization mechanism uses a certificate for access control, called an authoricate, which contains access control information and secret material for making the authorization process secure.

The authoricate is signed with a secret key shared between an authorization server and a relevant home resource, which may be either group key or private key. The reason that it doesn't use a private key owned by the authorization server is for making it possible for each home resource to enforce authorization by itself without help of the authorization server or other third parties.

Also, our proposed authorization mechanism can easily apply home network. Because symmetric key-based encryption algorithms are used in the authoricate, home devices with relatively low-capacity are expected to perform the authorization mechanism. Whereas, PMI developed for legacy PKI adopts asymmetric key-based encryption algorithms.

The authorization mechanism comprises five phases, and guarantees secure usages of authoricates.

6. References

[1] Jong-Wook Han, "Revitalization Policy of Home Network Industry", Korea Information Science Society, 22nd edition vol 9, September, 2004

[2] Jonw-Wook Han, Do-Woo Kim, Hong-Il Joo, "Considerations for Home network Security Framework", Korea Information Science Security, 22nd vol 9, September, 2004

[3] Geon Woo Kim, Deok Gyu Lee, Jong Wook Han, Sang Choon Kim, Sang Wook Kim, "Security Framework for Home Network: Authentication, Authorization, and Security Policy", Emerging Technologies in Knowledge Discovery and Data Mining, LNAI 4819, Springer, pp621-628, May, 2007

[4] ITU-T Recommendation X.1114, "Authorization Framework for Home Network", September, 2008

Authors

2000: MS in the Dept. of Computer Science from
Kyungpook National University
2000 ~ : Researcher of Information Security Technology Division,
ETRI
Research interests: Home network security, Network Security,
Surveillance System, Convergence Service

1991: MS in the Dept. of electronic engineering from
Kwangwoon University
2001: Ph.D in the Dept. of electronic engineering from
Kwangwoon University
1991 ~ : Researcher of Information Security Technology Division,
ETRI
Research interests: Home network security, Convergence Service
Security, Optical Security