Secure User Authentication Mechanism in Digital Home Network Environments *

Jongpil Jeong, Min Young Chung, and Hyunseung Choo

Intelligent HCI Convergence Research Center
Sungkyunkwan University
440-746, Suwon, Korea +82-31-290-7145
{jpjeong,mychung,choo}@ece.skku.ac.kr

Abstract. The 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 and wireless communication networks, such as mobile communication, Internet, and sensor network. However, there are many risks involved, for example user privacy violations and service interference. Therefore, security service is required to block these risk elements, and user authentication is an essential component for secure home network service. It enables non-authorized persons not to use home network. In this paper, an authentication protocol for secure communications is proposed for secure home network environments. The proposed authentication protocol is designed to accept existing home networks based on public key infrastructure (PKI) and Authentication, Authorization, and Accounting (AAA), which both use Kerberos.

1 Introduction

Not that the home network is entirely new network system, but that existing network system is applied to home. That is, the home network is that various home appliances communicate with each other and the home members use outdoor network services supplied by internet service providers at indoor. The home network supplies to us convenient and secure life. For example, turn off our home's gas valve, turn on/off the light, and control the temperature of boiler or air conditioner by remote control at indoor or outdoor. And we can use internet banking services through TV stations, use T-commerce, and use remote medical treatment. These infrastructure building is the purpose of the home network. For

* This research was supported by the Ministry of Information and Communication (MIC), Korea, under the Information Technology Research Center (ITRC) support program supervised by the Institute of Information Technology Assessment (IITA), IITA-2005-(C1090-0501-0019). Corresponding author: H. Choo.

security and privacy protection of the home network users, the home network security is necessary.

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. There are several wired-based network technologies for networking between devices in the home, such as HomePNA technology, constructing a high-speed in-home network using the existing telephone line, power-line communication (PLC) technology and networking technology with peripheral devices such as Universal Serial Bus (USB), Ethernet technology which is in use widely in local area networks, and IEEE 1394 technology to transfer multimedia data of Audio/Video digital devices, due to high-speed serial transmission. There are also several wireless network technologies such as Wireless LAN technology, Wireless PAN technology (e.g. Bluetooth), Zigbee, and ultra wideband (UWB) [1]. In addition, integrated home gateway technology exists [2][3], in order to accept heterogeneous networks. Security technologies are the first consideration for making the home network phenomenon possible. For example, a home network user's privacy can be violated if an attacker forcibly enters the home network and inspects the inside of a home with a web-camera. In addition, if attackers can control information appliances, these attackers may execute actions resulting in a loss to home users, possibly blocking home network services. There are many risk elements for different attack types, due to network extension.

For home network environments, information security technology is gathering strength as a critical issue. Security issues from information security requirements are very important, for example, mutual authentication between devices, user authentication services and access control services. In the case of wireless communication, wireless security aspects are extremely important because radio waves are continuously open.

The rest part of the paper is organized as follows. In Section 2, related works is presented. The definition of home network security requirements is presented in Section 3. In Section 4, an authentication protocol suitable for home network environments is proposed. Finally, this paper is concluded, and future directions are noted in Section 5.

2 Related Works

In home networks, several networking technologies exist, such as wired/wireless network technology, access network technology for communication between information appliances in home, and gateway technology for integration between outside networks and home networks. Network configuration equipments such as in-home information appliances, electronic appliances, home automation appliances, home gateway devices, and PDA/ Smart Phone/ Notebook/ PC are used for accessing the home network from outside.

Fig. 1 presents an example of the home network architecture, consisting of various technologies and equipments. Integrated Authentication Server (IAS)

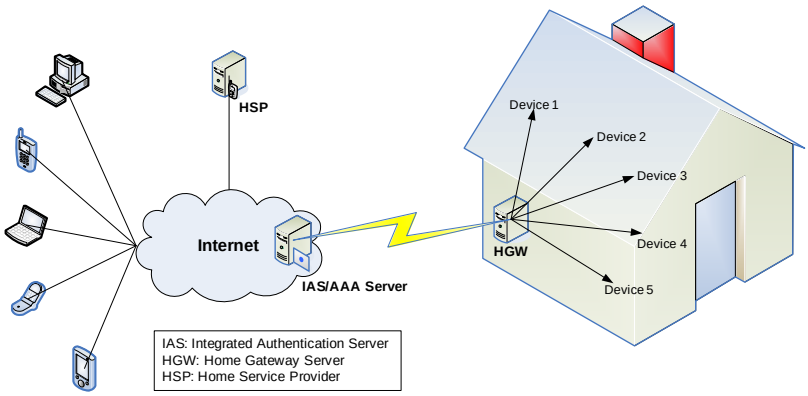

Fig. 1. Home Network architecture.

has interfaces for several devices, making it possible to use the Internet, control networking technologies, and manage the home gateway. In addition, it not only performs transmission of home network service software to the home gateway, but also performs authentication, granting the privilege, accounting for home network users, and forwarding accounting information to Home Service Provider (HSP) [4]. Home Gateway (HGW) requires an open architecture platform to communicate with heterogeneous networks. This platform should be independent of hardware and software vendors. In addition, address transition, protocol transition, and seamless data transition, for supporting interconnection and compatibility with heterogeneous networks should be guaranteed. This platform should connect with existing entire networks, and accept new networks in the future.

Open Service Gateway Initiative (OSGi) [3][7][8], one of the home gateway standardization organizations, distributes the OSGi Service Platform and maintains a framework standard for home network services, indicating the direction of several methods such as ID/PW, PKI, and Token card, for security related user authentication.

If node A desires secure communications with node B, node A receives the session key and the ticket that can only be decrypted by correspondent node B from Trusted Third Parties (TTP). Node A transmits its ticket and session key to node B. Thus, secure communication between nodes A and B is made after that the session key received by node B. There are two representative protocols for reusing tickets within the ticket's valid time; the Neuman-Stubblebine authentication protocol [5] and the Kerberos authentication protocol [6] developed by MIT. [5] takes advantage of its ability to prevent replay attacks, within a ticket's valid time, by not requiring synchronization of the time stamp with each party. Fig. 2 shows the operation flow of Kerberos authentication protocol. [6] consists of Authentication Server (AS) and Ticket Granting Server (TG). If node A user desires communication with the Service Server securely, node A receives a service issue ticket from TG after user authentication from authentication server. Node A achieves service privileges from the Service Server using this ticket. Node A keeps the privileges for the service, without communicating with

the Kerberos system within the ticket's valid time. The Kerberos authentication mechanism is based on distributed environments receiving the server's service over the network, eliminating the user's inconvenience of repeatedly entering the password, in addition to providing authentication for clients and performing mutual authentication for the authentication server and ticket granting server.

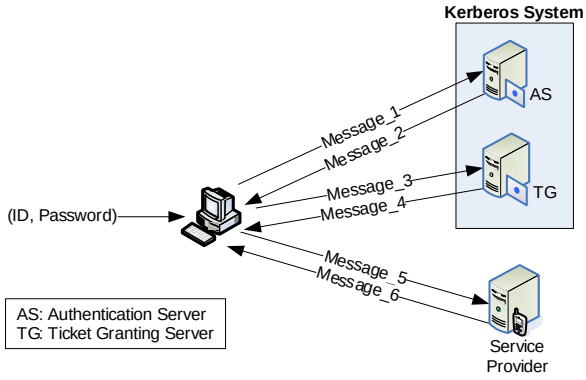

Fig. 2. Kerberos authentication protocol.

3 Home Network Security Requirements

In home networks, the security requirements can be varied as the corresponding home network configuration. If the network is connected with a PC using a cable modem, users can execute their network security services. However, the home network consists of heterogeneous networks that connect to the Internet, therefore situations at outside home are considered for secure communication.

3.1 Entity Authentication

In home networks, entity authentication is classified into two types, user authentication for verifying right users and device authentication for verifying information appliances consisting of home networks in inter-device communication. Fig. 3 presents the authentication architecture for users to access information appliances in the home through a home gateway. It is necessary for users to be authenticated a minimum of 3 times to access information appliances between User-IAS, User-HGW, and HGW-Information appliances. Mutual authentication is conducted to prevent impersonation attack from malicious users.

It is required to apply the concept of single sign on (SSO) for providing user's convenience. In other words, when a user logs on to a home gateway as a legitimate user, any additional operation should not be required to access additional resources in the home network [8].

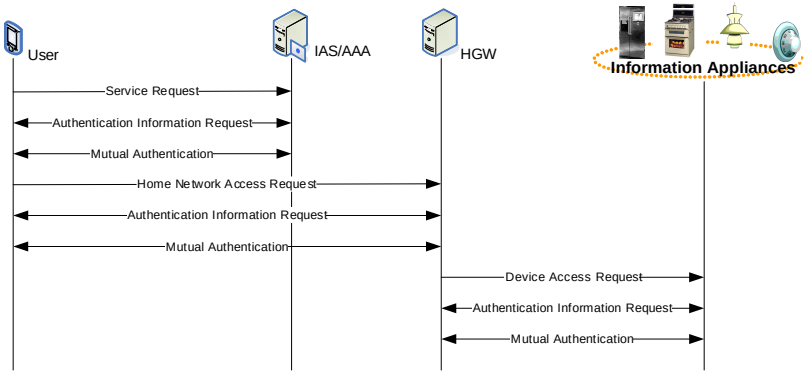

Fig. 3. Home Network authentication architecture.

3.2 Privilege Delegation

Home network users should grant specific privileges to programs. Therefore, programs should have access to the resources authenticated by users. In addition, a master user who has home network service privileges, should be granted all services accessed to users. The privilege granting function is performed by the privilege granting service command to HGW after master user access to HGW. For these methods, there are functional limitations for each entity.

If the authentication process is completed with legitimate keys, information appliances should be required to know what an authenticated entity could achieve. For this method, access control list (ACL) is considered. This is to provide limited services, after finding a user ID in the ACL and checking a user's capabilities. It is stored in HGW, and can be updated by HGW with the master user privilege granting command. Table 1 represents the ACL specification. Functional limitation method is having lists of applicable functions explicitly, making it possible to list one function or group of functions.

Table 1. ACL specification.

Subject	Identifier of entities able to be accessed
Authentication	Indicator to decide what functions to perform
Validity	Indication of entity validation, such as a timestamp

Table 2 presents ACL specification to limit functions. This demonstrates the functions that can be performed with a specified ID. After service users authenticated by the home gateway, and they can take suitable service privileges for each ID. In Subject field, *none* means that an authenticated entity can access S_1, S_2, and S_3 services in the T_1 timestamp, for home gateway access.

Table 2. Functional limitation.

Subject	*none*	B_2	B_3	B_4
Authentication	S_1, S_2, S_3	S_1, S_4, S_5	S_1, ... , S_n	S_1, S_5, S_6
Validity	T_1	T_2	T_3	T_4

3.3 Integration of Heterogeneous Network Security Solutions

A home network consists of heterogeneous networks having security solutions. Therefore, security solutions should not be replaced, but should provide mapping. These functions should be performed on HGW-*built* applications and can be integrated with middleware such as OSGi.

3.4 Confidentiality and Integrity

It is necessary to provide confidentiality and integrity services for secure data communication control of each system. For these services, it is required to share the secure private key between information appliances, service users and authentication server, authentication server and home gateway, and users and home gateway. The secure key is shared between information appliances in the home network. It is simply verified by using the message authentication code (MAC) validation function for providing integrity services for data. Also, it can be used to authenticate information appliances in the home network.

4 Security in Home Network Environments

4.1 Authentication Mechanism between HGW and IAS

HGW downloads the home network service modules from IAS and installs them, during the boot-strapping process that initializes the home gateway. At this time, HGW requires a secure mechanism for downloading home network services from IAS, in order to prevent illegal falsification from service software errors and attacks during the mutual authentication or the sharing of the secure key. This secure mechanism can be implemented through the public key infrastructure (PKI) [9] or symmetric key algorithm. In general, PKI algorithm is superior to symmetric key in managing and distributing keys. However, this PKI algorithm require the complicated operation for data encryption/decryption and the additional certificate verification. Thus, PKI algorithm cause a longer delay than symmetric key algorithms.

Table 3. Notation.

Notation	Meaning
R_1	Number calculated by IAS using U_{ID} and Password
R_2	Random Number generated by IAS
$E_{P-IAS}(-)$	Encryption using IAS's public key
S_{key}	Shared Session Key between Client and HGW
U_{ID}	User's Identifier
IAS_{ID}	IAS's Identifier
$E_{IAS-HGW}(-)$	Encryption using Symmetric key between IAS and HGW
$E_K(-)$	Encryption using K
T	Timestamp to decide Session key's validation

4.2 User Authentication Protocol

Service subscribers require mutual authentication between IAS and HGW, in order to access home network services. In addition, they must be able to operate service access control when privilege services are granted. Users, authenticated through SSO, can access other home services without additional authentication procedures. Fig. 4 illustrates the user authentication mechanism.

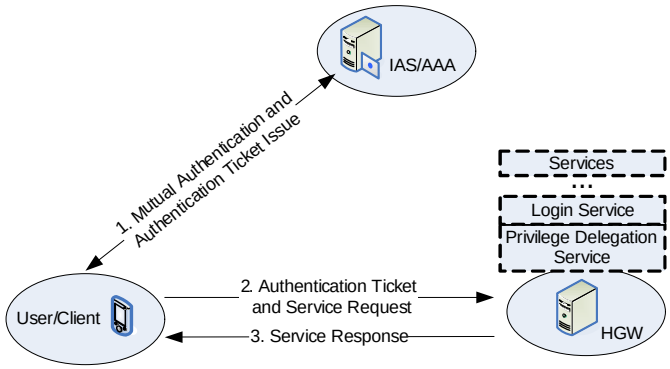

Fig. 4. User authentication mechanism.

In this section, it is assumed that IAS is located on the outside of the home network environment, manages the home gateway, and performs AAA functions. Another assumption is that clients have already taken and validated the IAS certificate. A suitable user authentication protocol is proposed for home network environments, focusing on authentication for users receiving the home service and controlling the service privilege.

The proposed authentication scenario is described in Fig. 5, the protocol is outlined in each step as follows.

1. Client transmits U_{ID} and $Password$ to IAS/AAA. Here, $Password$ is encrypted using IAS's public key. IAS verifies U_{ID} and $Password$ after decrypting the message using IAS's private key, and then authenticates client. Also, R_1 calculated as $h(U_{ID}, Password)$.
2. IAS delivers the authentication ticket $E_{IAS-HGW}(U_{ID}, IAS_{ID}, R_1, R_2, T)$ and the encrypted message by R_1. In case of having the right IAS's private key, R_1 could be decrypted by IAS and S_{key} also could be calculated by IAS, thus client implicitly authenticates IAS. In other words, client decrypt the encrypted message $E_{R_1}(IAS_{ID}, U_{ID}, R_2, h(S_{key}, U_{ID}), T)$ from IAS using R_1, and obtain R_2 and U_{ID}. After calculating of S_{key}, client verify the value of $h(S_{key}, U_{ID})$ and then validate U_{ID} and S_{key}.
   Fig. 6 demonstrates that IAS indicates the authentication to access point (AP) in wireless network, after transmission of key material to AP and AP handshakes with client, keys for encryption/decryption are established on the MAC layer [10],[16].

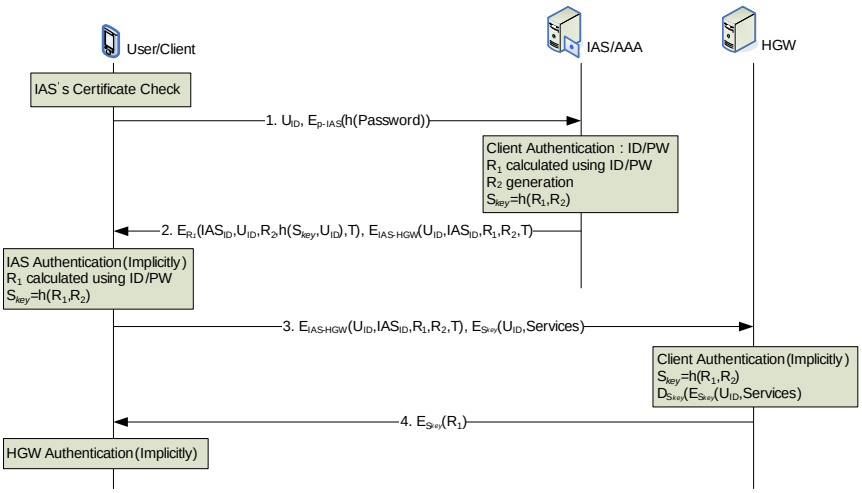

Fig. 5. Proposed authentication protocol.

3. Client transmits the authentication ticket $E_{IAS-HGW}(U_{ID}, IAS_{ID}, R_1, R_2, T)$, U_{ID} and *Services* encrypted using S_{key} to HGW. HGW compares U_{ID} of authentication ticket and U_{ID} of $E_{S_{key}}(U_{ID}, Services)$ and then implicitly authenticates client.
4. HGW transmits R_1 encrypted using S_{key} to the client, and then authenticates HGW implicitly.

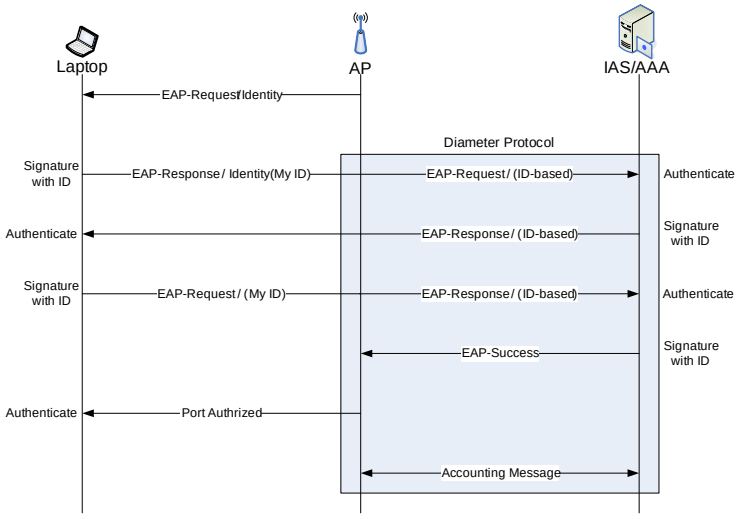

Fig. 6. Wireless LAN access authentication.

4.3 Security Analysis

The proposed protocol is designed under the assumption that public key or symmetric key infrastructure is used according to HGW's storage and computation capabilities, the symmetric key is shared between IAS and HGW. In addition, it is assumed that IAS exists outside the home network, it manages the home gateway, authenticates users, grants privileges, and controls accounting as the home gateway operator. Another assumption is that service users trust IAS. Actually, the OSGi operator exists in OSGi framework, it is outside the home network as the home gateway manager for managing the home gateway and authenticating users.

HGW knows that the authentication server is legitimate using the PKI-*based* public key algorithm or symmetric algorithm as a mechanism to authenticate IAS in the home network. In addition, the user authentication mechanism is based on U_{ID} and $Password$, and can transmit $Password$ securely, using a public key algorithm with the certificate received from the authentication server (IAS). In addition, it encrypts the challenge with the $Password$ transmitted from senders, and prevents the replay attack from attackers. Authentication between HGW and users employ the authentication ticket granted from the authentication server, and users can request and receive services with a valid authentication ticket after single authentication, there is no requirement to login each time when requesting services. Authentication ticket's validation can verify with its time-stamp, satisfied with authentication requirements as mentioned earlier. In addition, as U_{ID} is checked in authentication ticket after login, it can control whether having service privileges. ACL is stored as table format for U_{ID} privileges list in HGW's policy file, the purpose is to supply suitable services in response to user identification information.

5 Conclusion

Home network is defined as environments where users can receive home network services for anytime and anywhere access through any device, connected with a wired/wireless network to home information appliances including the PC. In this environment, there is many security threats that violate users privacy and interfere with home services. In addition, the home network consists of several networks with each network being inter-connected, so network security for each network is required. This means that there are a number of security threats to other networks when a security threat occurs in any network. Also, users in home network are needed security mechanism, for receiving home services from attackers and sharing information between home information appliances.

In this paper, the security requirements in home network environments are defined, and a user authentication mechanism between a home gateway and user is proposed, an authentication mechanism between home gateway and home gateway operator (IAS) can perform AAA functions. Authentication technologies in the wireless network are investigated and are acceptable in home network

environments. In this paper, integration of home network environments and authentication servers in wireless networks are discussed, regarding methods of authenticating wireless networks effectively.

There is still progress in the standardization of home network architecture, which is required to be researched in the future. In addition, research regarding the integration of authentication servers for 3G-WLAN and authentication servers in home networks needs to be conducted.

References

1. K. Choi *et al.*, "Trends of Home Networking Standardization in Korea," KETI Journal, 2003.
2. Y. Park *et al.*, "Home Station Architecture based on Digital Convergence toward U-Home age," ETRI Journal, 2003.
3. "OSGi Service Platform, Release 4 Specification," http://www.osgi.org, October 2005.
4. S. Lim *et al.*, "Home Network Protocol Architecture for Ubiquitous Communication," Journal of KIPS, vol.10, 2003.
5. B. Clifford Neuman, Stuart G. Stubblebie, "A Note on the Use of Timestamps as Nonces Operating Systems Review," 1993.
6. B. Clifford Neuman, Theodore Is'o, "Kerberos: An Authentication Service for computer Network." IEEE, Computer Magazine, September 1994.
7. OSGi, "RFC 18 - Security Architecture. Specification," Draft, 2001.
8. K. Jeon *et al.*, "User Authentication Mechanism in OSGi Service Framework Enviroments," Journal of KISS, vol.9, 2003.
9. CCITT Recommendation X.509. The Directory Authentication Framework, CCITT, December 1998.
10. IEEE P802.11i/D9.0 "Medium Access Control(MAC) Security", 2004.
11. J. Gu *et al.*, "Security Clustering: A Network-wide Secure Computing Mechanism in Pervasive Computing," Networking 2004, pp.1326-1331, May 2004.
12. H. Jo, H. Youn, "A Secure User Authentication Protocol Based on One-Time-Password for Home Network," ICCSA 2005, vol.3480, p.519, May 2005.
13. MIT Media Lab: Things That Think Consortium, http://ttt.media.mit.edu
14. Microsoft Research: Easy Living, http://research.microsoft.com/easyliving
15. Y. Chen, L. Yeh, "An Efficient Authentication and Access Control Scheme Using Smart Cards," Parallel and Distributed Systems, 2005. Proceedings. 11th International Conference (ICPADS'05), vol.2(20-22) , p.78-82, July 2005.
16. B. Aboba *et al.*, "Extensible Authentication Protocol (EAP)," RFC 3748, June 2004.