OTP Authentication Module and Authentication Certificate Based User Authenticating Technique for Direct Access to Home Network and Resource Management

Jung-Oh Park,
Dept of Computer Science, Soongsil University
Jop07@ssu.ac.kr

Sang-Geun Kim
Division of Computer Engineering, Sungkyul University
sgkim@sungkyul.edu

Abstract

Home network service industry, the driving force for future national development and new changes, may be deemed to comprehend tremendous potential of future development, however as home network services proliferate and various types of home network services emerge, home network services are growing vulnerable to cyber attacks, becoming significant source of social and economic instability in our society, and thus necessary is user authentication to prevent occurrence of infiltration upon home network service and exposure of user information.

The system proposed in this paper offers authority or control over an approach to licensed users for diverse devices used in Home Network, preventing unlicensed users from inappropriate approach. In relation to communications of security certification for each device, reduction in added resources and high security can be both met through a security token generated using OTP, which is reasonably applicable to low-efficiency instruments that compose a home network.

Keywords: *Home Network, OTP, SSL*

1. Introduction

In modern society, a natural connection of real to cyber spaces, combined with rapid advance in IT industry, has made home network service appear and develop besides our workplace setting. Among other IT technologies, home network service industry has been an on-going issue in this current as a prime mover for national development and new change, also with a great potential in its development ahead. With spread of home network service especially in diverse forms recently, however, scope in target for cyber attack has also enlarged, throwing an element of anxiety over our society socially and economically. This state of affairs necessitates user authentication that prevents occurrence of invasion incidents and exposure of user information in home network service.

In tune with the development and extension of ubiquitous home network environment, various wired and wireless network techniques are being developed and researched on, and in this accord, various researches are under active progress in security related fields like user authentication and device authentication etc. As sharing of resources among the devices in home network environment grow increasingly common, security requirements will also grow more diverse and complicated.

In home network environment, devices communicate basically wirelessly. The risks that may occur in home network environment vary widely such as device theft and loss, IP spoofing, DoS(Denial of Service) attack, Trojan horse, warm virus, signal interruption attack and battery depletion attack etc. The requirements of security for home network environment to block such attacks include authentication, confidentiality, integrity etc, and also additional requirements such as anonymity, non-repudiation, administrative right management etc are needed as well.

Authentication techniques for home network require network security techniques, verification technique and blocking technique to distinguish eligible user that may access home network service through user authentication when any user attempts to access a service that home network supports, and control or blocks any unauthorized individual that attempts manipulation of instrument, and also need safe security technique that can prevent ineligible use or access by unauthorized individual.

To enable an outside client to control home network with a mobile terminal like PDA, this thesis focused on user authentication and approach control among security elements of home network. We propose a method of home network user authentication by direct access to home server from outside home, using OTP-based authentication, not via authentication server of home network service provider that was left out of consideration from the mechanical criterion for home server-oriented home network user authentication for group (TTASKO-120030) by Telecommunications Technology Association (TTA) in Korea.

This authentication uses X509 v3- based authentication for certification, controlling devices by dividing user group on its extension area, and for devices with restricted approach, it controls approach by adding ACL (Access Control List). Such a division into user with restricted approach and its manager can present approaches for each device and protect it safely from outside attack.

2. Related Studies

2.1. Home Network

HNIT (Home Networking & IT) under CEA (Consumer Electronics Association), the U.S., defines home network as “a coupling together of home appliances and electronic systems for remote approach control possible.” That is, through home network, each product must connect each other to share mutual service, while the user must be able to remote-control scattered instruments or use the service provided by each instrument. Setting in which such home network service has been in application is called digital home. In 2003, when the Ministry of Information and Communication designated this industry as one of next-generation growth engines for Korea, the term of digital home was first used. Digital home is the concept that unites home networking technology and information electronics embodied with this technology, suggesting that ubiquitous environment has been applied to general homes.

Home network is, as shown in Figure 1, binding instruments at home into one network to make them capable of communication and connecting these to outside internet network to allow controlling consumer appliance from at/outside home, regardless of the user's position.

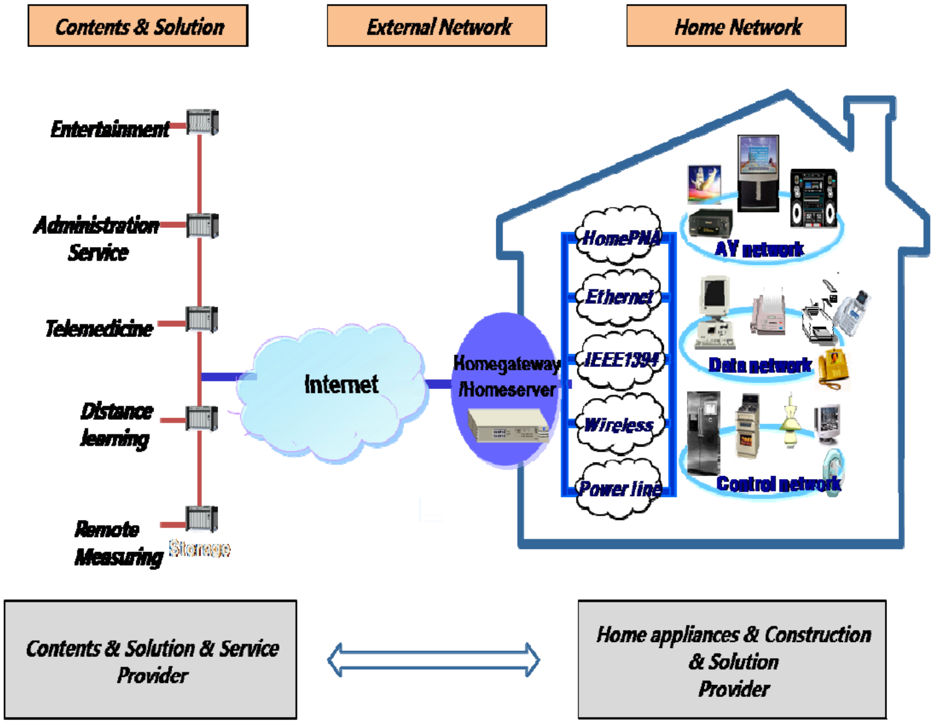


Figure 1. Home Network Composition Diagram

2.2. OTP (One-time Password)

OTP is the system of generating a password available for only one time, thus it authenticates user by using different passwords for each time. OTP, a typical method of double-element user authentication and basically devised on the basis of cryptographic idea, is the system of high security and convenience to use. Since it uses another password for each time, it is, unlike the system using the fixed password, proof against attack by reusing password, and since it uses cryptographic algorithm, it is also proof against prediction of a possible password in use for next time from the one currently used. Hence it is safe. If you enter a user password and input value for generating one-time password into the OPT program stored in OPT token or user PC, the system generates one-time password using cryptographic algorithm. Here, only by entering different values for each time for input values, does a one-time password come into being, and depending on what kind of value is entered for this input value, it is classified into diverse OPT methods.

2.3. Home Network Security Technique

Home network involves many security vulnerabilities to be considered in addition to the existing security vulnerability that occurred in internet etc due to wired and wireless network and various protocols etc. Various devices of home network, which are interlinked with internet, are subject to attack from outside, and furthermore in home network, the security requirements are growing increasingly complicated due to the diversity of devices and sharing of resources among them.

2.3.1 User Authentication

In home network, the process of user authentication is required for identification of individuals using each device. In home network, various user authentication techniques like biometrics, password, authentication certificate, Smart Card and RFID etc can be utilized, and user authentication technique can be used for remote access to home network from outside home as well as from home and use of services like internet banking from home.

2.3.2 Middleware Security

Basic security functions are provided also to middleware used for home gateway and each device, and relevant security functions also are being standardized.

2.3.3 Access Control

In the course of home services, control of access to home network resources is required. Since the types of home services differ and the ranges of control of home network elements vary, access control should be established. When home network environment is considered, the list of access controls should desirably be embedded in the terminal and access right is restricted according to consistent security policy in safety aspect or user aspect for overall management of home gateway and active counteraction against illegal infiltration by leakage of authentication information.

2.3.4 Device Authentication

To prevent illegal use of device, authentication of devices the elements of home network is required. So far, authentication of device has been provided at middleware level.

2.3.5 Authentication among Devices

Providing smooth service of home network requires the process of mutual authentication among devices for sharing of resources among home network components. Presently, authentications among devices, the basic security function for various home services, have been provided at middleware level.

3. Proposed System

3.1 Overall System

In the proposed user authentication technique, users access home network from outside via internet and are authenticated not by way of business authentication server.

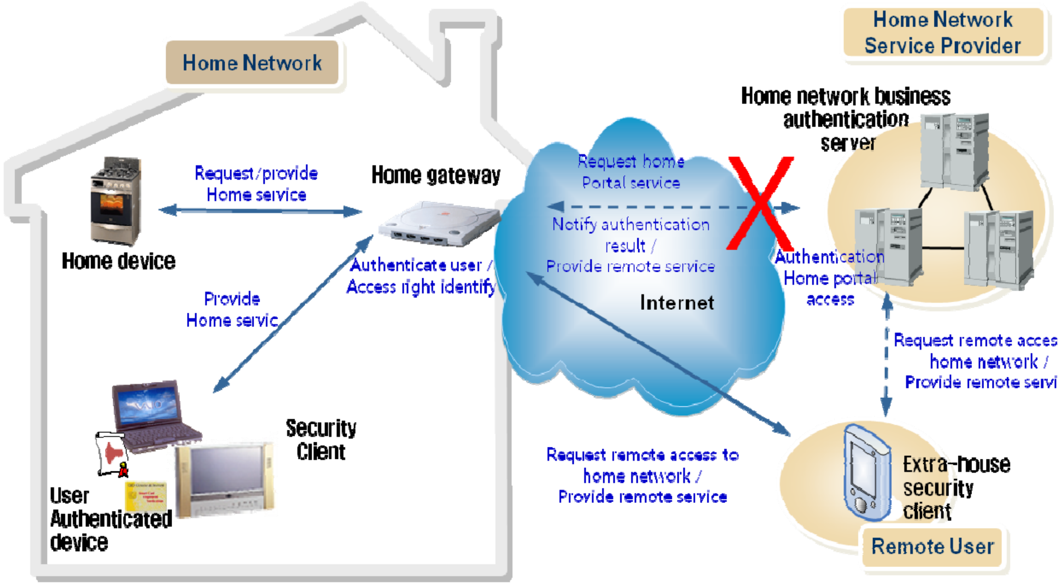


Figure 2. Direct authentication in home network

The proposed authentication method get both authentication and remote service through home server existing in home network unlike existing authentication method that receives notification of authentication result from home network business authentication server and provides remote service through home network business authentication server.

Here is the big picture of the technique. When extra-house user accesses client device, i.e., mobile device etc through mobile device, the system provides with safe user authenticate, and when the user accesses home network through SSL(Secure Sockets Layer) channel, executes multi-access control on each user's device from home gateway.

For user authentication, user should first register with home server and get certificate, and this is the only process in which user can be authenticated as the right user through authenticating organization.

User gets authentication certificate issued from home server directly through USB(Universal Serial Bus) cable, and home server issues authentication certificate after saving server and client by generating the device ID and OTP module etc. Client transfers authentication certificate request query and device ID when user accesses home network with the issued authentication certificate through internet from outside, and at this time, the transferred query and device ID generate OTP random parameter through the OTP module that client keeps and transfers authentication certificate information to server by encoding it in secret key algorithm.

The home server that received request of authentication from client also requests the authentication information of client through home gateway after decoding and checking with the use of the OTP random parameter generated through the OTP module it has.

The client generates OTP random parameter through OTP module that it has and sends authentication certificate information to server again by encoding it with secret key algorithm.

Later on, home server also decodes with the OTP random number created in OTP module and if authentication certificate is correct, controls device by assessing home network.

User authentication certificate is programmed in a way that instruments out of control in groups of instruments applicable to user right fundamentally are restricted of access by adding access rejection list. Also, about instrument which is already under user's control, user authentication certificate offers multi-access control through which other user may control access.

The overall structure of the proposed home network user authentication system is shown in Figure 3. When accessing home server, remote device requests authentication to home server by using the randomized number generated in the certificate of open key encoding algorithm and OTP module. Home server is composed of home gateway for the communication between client device of outside user and home device within home network, OTP authentication module for user authentication, and CA. The home server that received authentication request authenticates eligible user by verifying it.

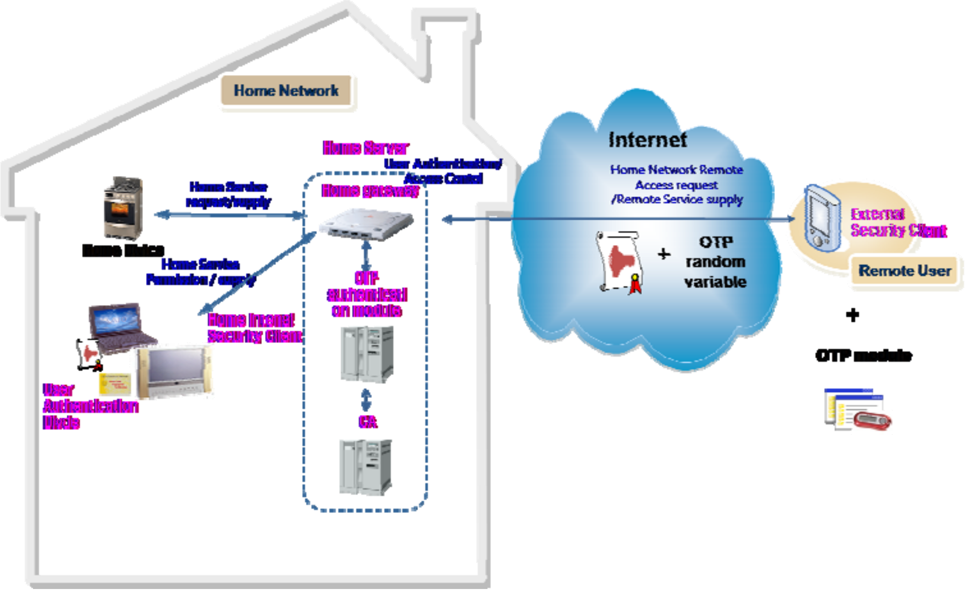


Figure 3. Structure of Proposed System

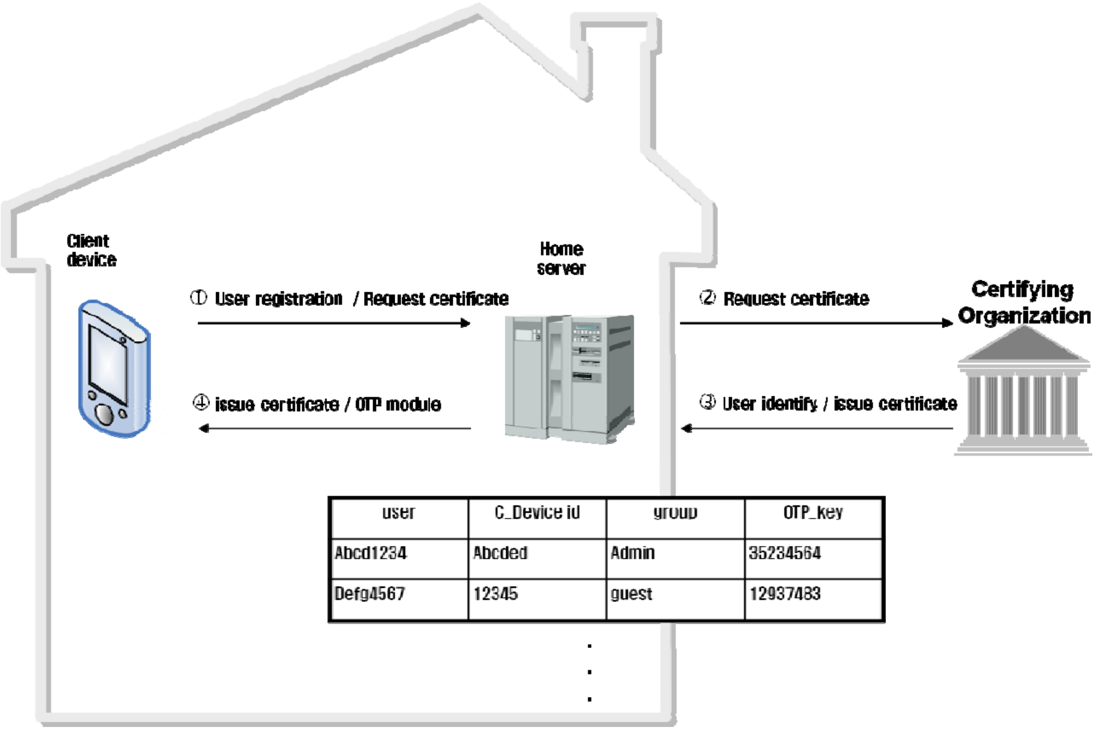
For the control of access to devices existing inside home network, the access control list composed by the users that access home network is used, and the home devices that users can access are set apart. As access control list ACL within the issued authentication certificate are organized in groups, user can access only the devices applicable to user right. Administrator can manage by dividing into devices that can be accessed depending on user class and those that may not be accessed, and client can request addition/deletion of access control list to administrator. If the requested is done, client get authentication certificate re-issued from home server.

Device that user is already using provides with multi-access control to restrict use of other user, and this is achieved with the use of OTP randomized parameter each user generates.

3.2. Authentication Certificate Issuing Procedure

Home server generates and saves the device ID and key for device of each user, and if user device is added or deleted, user registers device the device and has device ID and key re-issued with home server.

As for certificate issuing process, user connects USB cable directly from the authentication server in the home network that has client device and get user certificate issued.


Client device
Home server
① User registration / Request certificate
④ issue certificate / OTP module
② Request certificate
③ User identify / issue certificate
Certifying Organization

user	C_Device id	group	OTP_key
Abcd1234	Abcded	Admin	35234564
Defg4567	12345	guest	12937483

Figure 4. Certificate Issuing Process

For issuance, authentication server saves the device ID and key for client device in home server by generating them, and issues certificate after authenticating the status of eligible user through certifying organization. In addition, authentication server saves and synchronizes OTP module same between home server and client device after duplicating each other upon certificate issuance. User certificate is composed of client device ID and individual key, home device list and home device number as shown in Figure 4.

3.3. User Authentication Procedure

User authentication is done by using the authentication certificate that user is issued and the OTP parameter generated in the OTP module which is synchronized with the home server of home network. Then user requests authentication to the home gateway that manages the communication of home server through remote device from outside, and OTP authenticating module and CA authenticate eligible user. At this time, user requests access to home network through SSL(Secure Sockets Layer) fundamentally.

The overall procedure of user authentication is as shown in Figure 5. First off, the remote device that accesses home network from outside generates random parameter r1 through OTP module, and encodes and transfers query data and remote device DID with secret key algorithm by requesting authentication with personal key.

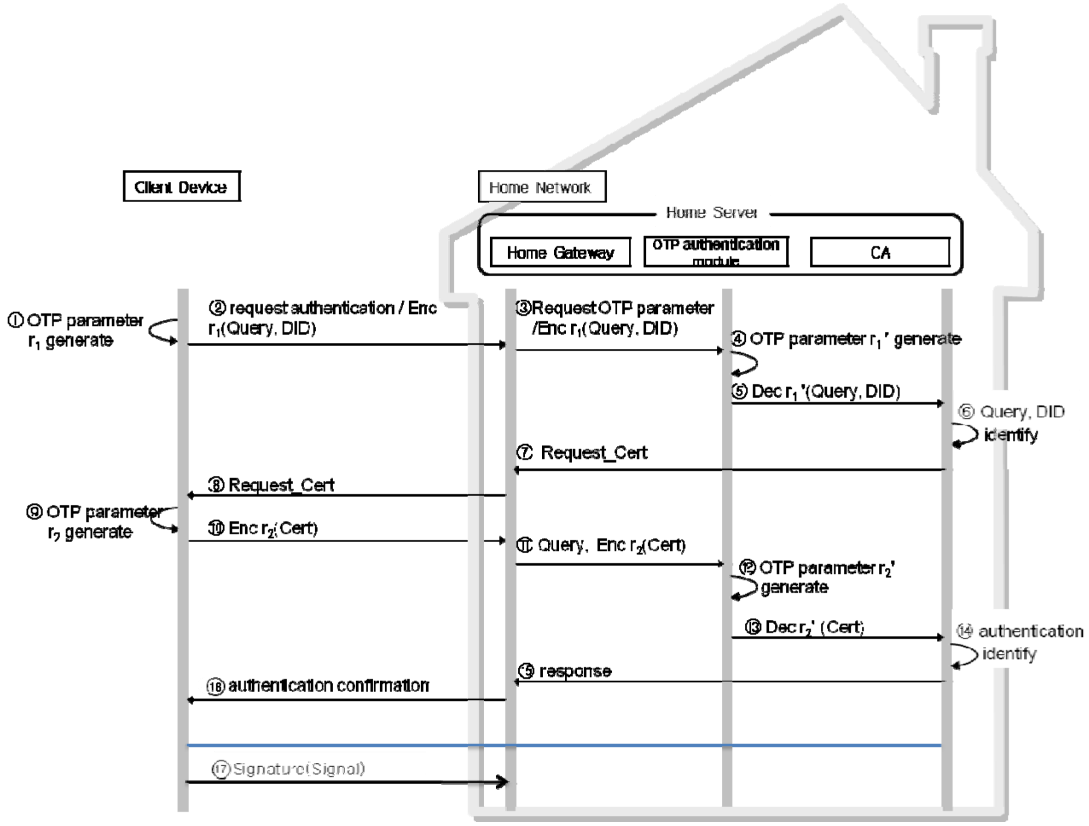

Client Device
Home Network
Home Server
Home Gateway
OTP authentication module
CA
① OTP parameter r₁ generate
② request authentication / Enc r₁(Query, DID)
③Request OTP parameter /Enc r₁(Query, DID)
④ OTP parameter r₁' generate
⑤ Dec r₁'(Query, DID)
⑥ Query, DID identify
⑦ Request_Cert
⑧ Request_Cert
⑨ OTP parameter r₂ generate
⑩ Enc r₂(Cert)
⑪ Query, Enc r₂(Cert)
⑫ OTP parameter r₂' generate
⑬ Dec r₂' (Cert)
⑭ authentication identify
⑮ response
⑯ authentication confirmation
⑰ Signature(Signal)

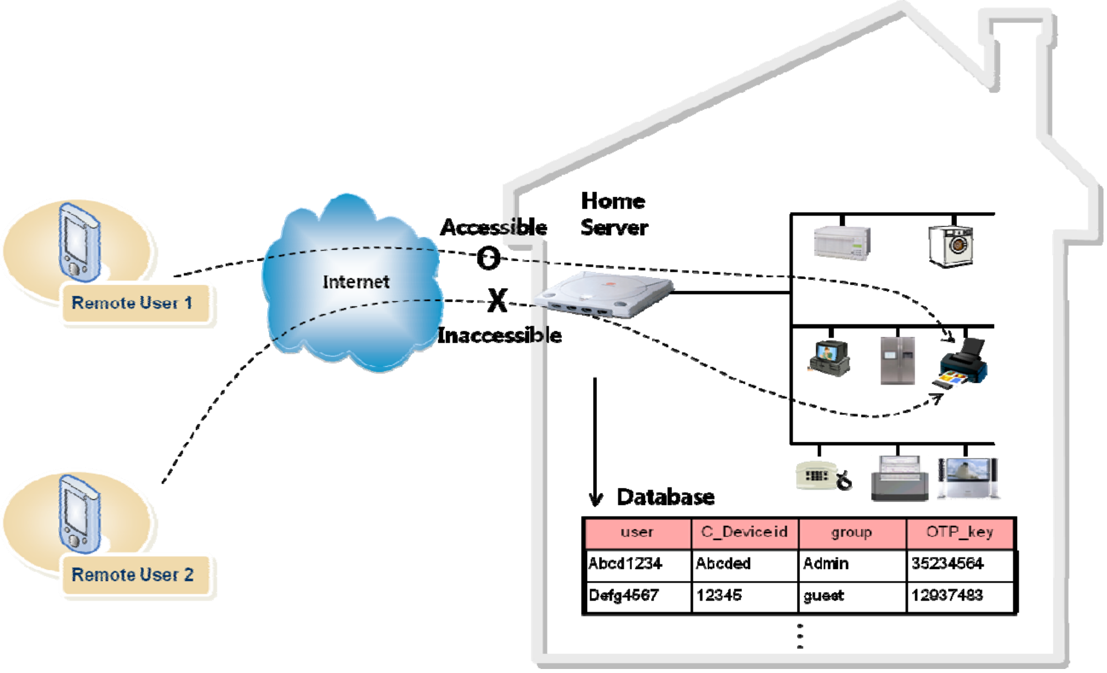
Figure 5. Procedure of User Authentication

Once the request of user authentication is transferred, home server generates random parameter r1´ by using the OTP authentication module in it, decodes the query data encoded with this random parameter and the DID of remote device, and check query data and DID value through CA. And then home server requests to user the information of the authentication certificate of the user that sent authentication request. The user that received request of authentication certificate information generates OTP random parameter r2, encodes the authentication certificate information to be sent to home server with the use of the generated random parameter r2, and transfers it to home server.

The OTP authentication module of home server also decodes the information of the authentication certificate which is encoded with personal key for the generated OTP random parameter r2´ , verifies the information of the decoded authentication certificate in CA, and if the information of the authentication certificate is verified, completes the authentication of user by transferring authentication confirmation response to user through home gateway. After that, client device can control the home device inside home network.

3.4. Home Device Access Control

Once user authentication process is done, access to each device can be done through home gateway as shown in Figure 6. When outside client accesses home device, the right to access home device is granted depending on the user, and home sever controls access to home device by judging whether access can be granted or not through the authentication certificate of outside client.



user	C_Deviceid	group	OTP_key
Abcd1234	Abcded	Admin	35234564
Defg4567	12345	guest	12937483

Figure 6. Control of Access to Device

① $Enc_{h(r\|Key)}(DIDNum, Control\ Command), DID$

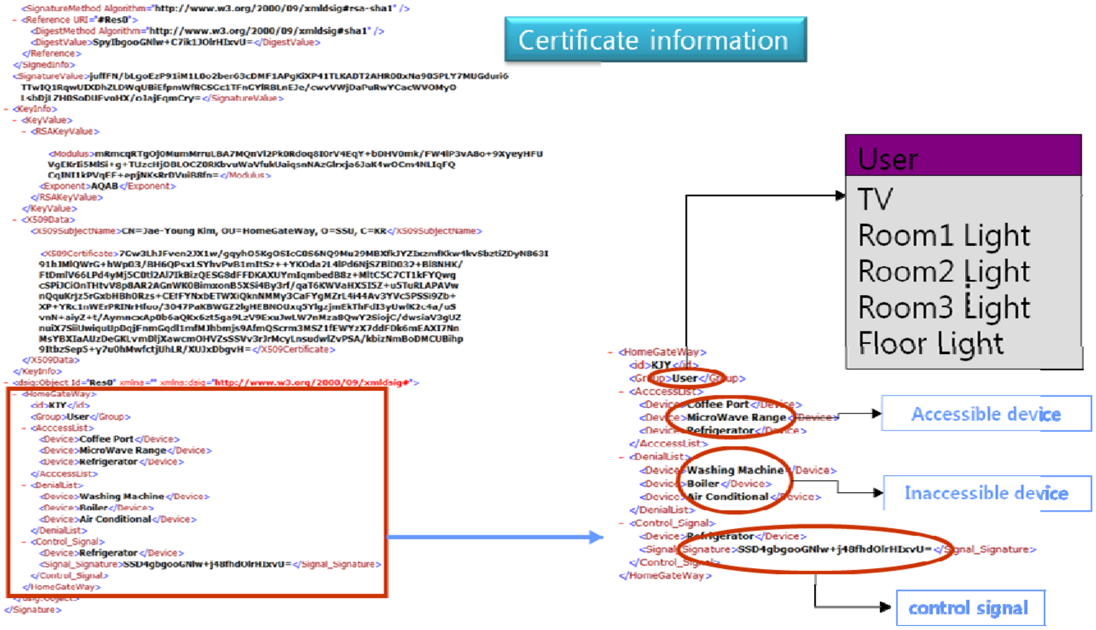
- Hashes the random parameter value generated in OTP module and its own key after linking them.

- Transfers hash value, the value that encoded DIDnum an X.509 based attribute, and control command message, and client's own DID to home server.

② Home server decodes by using client's DID value, and notifies DIDnum and control command by verifying them.

3.5. User Authentication Certificate

In the authentication certificate used in user authentication process, instruments applicable to user right are combined in groups of access control list ACL fundamentally as shown in Figure 7.



```
  <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
- <Reference URI="#Res0">
    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
    <DigestValue>SpyIbgooGNlw+C7ik1JOlrHIxvU=</DigestValue>
  </Reference>
 </SignedInfo>
 <SignatureValue>juffFN/bLgoEzP91iM1L0o2ber63cDMF1APgKiXP41TLKADT2AHR00xNa905PLY7MUGduri6
  TTwIQ1RqwUIXDhZLDWqUBiEfpmWfRCSCc1TFnCYlRBLnEJe/cwvVWjDaPuRwYCacWVOMyO
  LsbDjL7H0SoDUEvoHX/o1ajEqmCry=</SignatureValue>
- <KeyInfo>
- <KeyValue>
  - <RSAKeyValue>

      <Modulus>mRmcqRTgOj0MumMrruLBA7MQnVl2Pk0Rdoq8I0rV4EqY+bDHV0mk/FW4lP3vA8o+9XyeyHFU
     VgEKrEi5MlSi+g+TUzcHjOBLOCZ0RKbvuWaVfukUaiqsnNAzGlrxja6JaK4wOCm4NLIqFQ
     CqINI1kPVqEF+epjNKsRrDVuiB8fn=</Modulus>
    <Exponent>AQAB</Exponent>
   </RSAKeyValue>
  </KeyValue>
- <X509Data>
   <X509SubjectName>CN=Jae-Young Kim, OU=HomeGateWay, O=SSU, C=KR</X509SubjectName>

    <X509Certificate>7Cw3LhJFven2JX1w/gqyhO5KgOSIcC0S6NQ9Mu29MBXfkJYZIxzmfKkw4kvSbztiZDyN863I
   91hJMlQWrG+hWp03/BH6QPsx1SYhvPvB1mItSz++YKOda2L4lPd6NjSZBlD032+Bl8NHK/
   FtDmlV66LPd4yMj5C0tl2Al7IkBizQESG8dFFDKAXUYmIqmbedB8z+MltC5C7CT1kFYQwg
   cSPiJCiOnTHtvV8p8AR2AGnWK0BimxonB5XSi4By3rf/qaT6KWVaHX5I5Z+u5TuRLAPAVw
   nQquKrjz5rGxbHBh0Rzs+CEIFYNxbETWXiQknNMMy3CaFYgMZrL4i44Av3YVc5PSSi9Zb+
   XP+YRc1nWErPRINrHfuo/3047PaKBWGZ2lgHEBNOUxq5YlgzjmEkThFdI3yUwlK2c4a/uS
   vnN+aiyZ+t/AymncxAp0b6aQKx6zt5ga9LzV9ExuJwLW7nMza8QwY2SiojC/dwsiaV3gUZ
   nuiX7SiiUwiquUpDqjFnmGqdl1mfMJhbmjs9AfmQScrm3MSZ1fEWYzX7ddFDk6mEAXI7Nn
   MsYBXIaAUzDeGKLvmDljXawcm0HVZsSSVv3rJrMcyLnsudwlZvPSA/kbizNmBoDMCUBihp
   9ItbzSep5+y7u0hMwfctjUhLR/XUJxDbgvH=</X509Certificate>
  </X509Data>
 </KeyInfo>
- <dsig:Object Id="Res0" xmlns="" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
 - <HomeGateWay>
    <id>KTY</id>
    <Group>User</Group>
  - <AcccessList>
     <Device>Coffee Port</Device>
     <Device>MicroWave Range</Device>
     <Device>Refrigerator</Device>
    </AcccessList>
  - <DenialList>
     <Device>Washing Machine</Device>
     <Device>Boiler</Device>
     <Device>Air Conditional</Device>
    </DenialList>
  - <Control_Signal>
     <Device>Refrigerator</Device>
     <Signal_Signature>SSD4gbgooGNlw+j48fhdOlrHIxvU=</Signal_Signature>
    </Control_Signal>
   </HomeGateWay>
  </dsig:Object>
</Signature>
```

```
- <HomeGateWay>
   <id>KJY</id>
   <Group>User</Group>
 - <AcccessList>
    <Device>Coffee Port</Device>
    <Device>MicroWave Range</Device>
    <Device>Refrigerator</Device>
   </AcccessList>
 - <DenialList>
    <Device>Washing Machine</Device>
    <Device>Boiler</Device>
    <Device>Air Conditional</Device>
   </DenialList>
 - <Control_Signal>
    <Device>Refrigerator</Device>
    <Signal_Signature>SSD4gbgooGNlw+j48fhdOlrHIxvU=</Signal_Signature>
   </Control_Signal>
  </HomeGateWay>
```

Figure 7. User Authentication Certificate

4. Performance Evaluation

Performance evaluation was verified through comparison analysis with existing system and safety analysis. The symmetric key ID/password based technique which was used in existing system, and the technique of using authentication certificate etc were compared and analyzed with the authentication technique proposed in this paper, and security matters were analyzed by the issues with focus on safety.

4.1. Comparison Analysis with Existing System

The ID/password method used in existing home network system and home network method that used open key based authentication certificate were compared with the proposed protocol, and security matters were compared and analyzed with focus on safety.

[Table 1] Performance Comparison with Existing System

	P Company Protocol	S Company Protocol	M Company Protocol	Proposed Protocol
Authentication Method	ID/Password	ID/Password	Authentication certificate	Authentication certificate
Device authentication	Y	Y	N	Y
Access control	Y	N	N	Y
Mutual authentication	N	Y	N	Y
Message transferring method	Transfers after encoding with symmetric key	Transfers after encoding with symmetric key	Transfers after encoding with open key	Transfers after encoding with random r value and symmetric key
User class	N	N	N	Y

4.2. Analysis of Safety

Safety analysis was done on the safety in user authentication process, safety on sniffing attack, safety on spoofing and re-transferring attack, and safety on the reduction of authentication process, and the details are as follows:

4.2.1 Safety on User Authentication

The proposed user authentication method is done through authentication certificate. Since authentication certificate is issued directly to user through cable in off-line condition, this method does not involve any problem of on-line attack. Unlike the method in which server and client transfer the key value used in encoding and decoding in user authentication process, the proposed technique allows each entity to use key value by generating random value 'r' with the use of synchronized OTP module. In addition, the generated key values, since they use single session random value of OTP, blocks risks like leakage or loss etc fundamentally.

4.2.2 Safety on Sniffing Attack

Methods of controlling device in home network include use of cable and transferring of message to control device through existing wired network or wireless network, and whatever method is used to transfer data, data are transferred always after encoding, and thus no risk exists as to exposure of data unless illegal device holds key.

The proposed method fundamentally blocks risk of sniffing attack in network environment as server and client directly generate key value the most important of user authentication process without transferring it. In practice, in user authentication and device control process, the random value generated by the OTP module of home server and client is used as symmetric key encoding secret key, and proper key value that can be used in authentication process may not be generated or estimated without the OTP authentication module shared through synchronization at the time of initial authentication certificate.

4.2.3 Safety on Spoofing and Re-transferring Attack

For safety against spoofing and re-transferring attack, transferred data use random value that OTP module generated, and thus illegal user may not access it. After user authentication process, the control messages for home device also are electronically signed with the use of the authentication information used in authentication process and OTP random value, and even if the message is intercepted midway, the message contents may not be inferred nor be re-transferred through interception for message contents change each time.

4.2.4 Safety on the Reduction of Authentication Process

In home network, user authentication and device control methods include authentication via 3rd authenticating organization and transfer of device control message. If server of authenticating organization cannot provide service due to problem like hacking attack or server instability etc, inconvenience, safety deterioration and risk of personal user's information leakage in the use of home network are inevitable. The user authentication method proposed in this paper simplifies authenticating procedure, minimizes security risk by outside situation and obtain safety by authenticating user and transferring device control message only through home server and client devices except for initial issuance of user authentication certificate.

Compared with existing protocols, the proposed protocol somewhat differs in operation frequency, and contains some added functions like OTP etc on top of those that existing protocols have, but judging from the rapid development of hardware, such differences will not cause any significant problem, being expected to be solved through hardware development. In addition, the protocol uses only the functions that existing protocols already have regarding home network system composition, and does not require other additional function.

The ID/password based protocols of P company and S company that encode with symmetric key undergo severe infliction of security when password is exposed, and are relatively vulnerable to network based attacks like spoofing and sniffing etc. In addition they involve potential risk by re-transfer attack due to absence of Timestamp function.

M company that used authentication certificate provides higher security safety on spoofing and sniffing compared with ID/password based P company and S company by adopting the method of encoding with open key. However, they still have the vulnerability on re-transfer attack due to absence of Timestamp function.

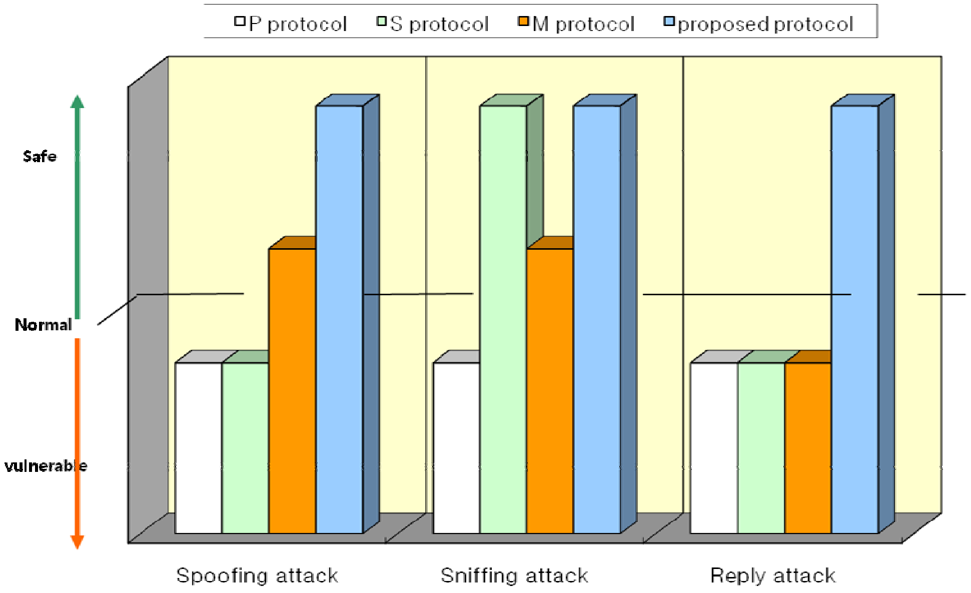


Figure 8. Graph of comparing each protocol's security

Regarding security aspect, the proposed protocol is shown to be safe against various attacks like spoofing attack, sniffing attack and re-transfer attack etc as shown in Figure 8. Even in the same hardware composition, security increases or decreases depending on how each function is used. The mutual authentication by each stage has the long point that spoofing attack and re-transfer attack can be definitely blocked in each stage.

5. Conclusion

Home network environment that receives various services to home as well as work office without restriction of time or space owing to sustainable development of information communication techniques and proliferation of internet now became generally available technique. At the same time, there still exist various security intimidations that may occur in network environment, and social economical instability elements also are increasing due to extension of cyber attack.

Information home electronic devices, which are utilized in home network environment have relatively low computing capability, leading to hardship of carrying security function, involves the problem of being vulnerable to cyber attack. Furthermore, home network can become object of cyber attack occurring in internet due to connection with internet, and thus fall victim to many problems like trespassing of private life, exposure of personal information and abuse of personal information etc due to security vulnerability to hacking, warm virus, DoS(denial of service) attack and wire-tapping of personal information etc.

To protect home network from security risks which increase with technical development, sustainable active researches should follow.

First off, to prevent infiltration accident of home network service and exposure of user information, safe technique of user authentication is required.

This paper proposed home network user authentication method that authenticates user and provides service directly through the home server of home network unlike existing authentication methods that authenticate user and provides service through the authentication server of home network business.

First off, the client device that outside user uses gets authentication certificate directly from home server through USB communication etc, encodes and safely protects the information of authentication certificate with the use of the random parameter generated in mutual time synchronization method by being embedded with the OTP module synchronized with the OTP authentication module of home server. Since user gets authentication certificate issued directly through cable on-line, no problem may occur from on-line attack. Also, since the secret key used for encoding and decoding during user authentication process uses synchronized OTP, and generates random value without transfer between server and client, this method minimizes the risk of leakage or loss. In addition, since the data in the proposed protocol are transferred always after being encoded, no data can be exposed unless illegal device knows client's personal key and random value 'r'. Moreover, as the requirement of preliminary operation to synchronize the random value 'r' generated in existing home server and transfer from the server to client is omitted, this protocol produces the effect of reducing communication overhead.

As authentication is safe against attacks like sniffing etc, inferring of personal key and authentication certificate is difficult owing to encoding of information with the use of single session random value 'r' generated in the OTP of home server and client in the process of user authentication, and messages in the control of home device are transferred with hashed value encoded again, inferring of message contents is impossible even if the message is intercepted midway.

Further studies must be done later on to develop lighter OTP generating module and maximize efficiency by simplifying authenticating procedure in consideration of various functions of remote devices. Also there need be studies on more efficient and safe method of wireless access and control of home device with the use of portable device and researches on safer security protocols applying safe security protocols used in existing wired network and the proposed method.

References

[1] Sang -hyun Kim, Chul-bum Kang, Hee-jin Jang, Sang-wook Kim,“A Secure Control of Home Network on a PDA”, Korea Information Science Society, vol.29, Oct.2002

[2] Mahfuzur Rahman, P.Bhattacharya, “Remote Access And Networked Appliance Control Using Biometrics Features”, IEEE Transactions on Consumer Electronics, Vol, 49, No.2, MAY. 2003

[3] Pan-Lung Tsai, Chin-Laung Lei, Wen-Yang Wang, “A Remote Control Scheme for Ubiquitous Personal Computing”, International Conference on Networking, Sensing & Control , March, 2004

[4] E. Callaway, L. Hester, P. Gorday, "Home networking with IEEE 802.15.4: a developing standard for low-rate wireless personal area networks", IEEE Communications Magazine, VOL. 40 NO. 08. 2002

[5] H.Schulzrinne, X. Wu, and S. Sidiroglou, "Ubiquitous Computing in Home Networks", IEEE comm. Mag. Oct. 2003

[6] 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

[7] Choi, Hoon-Il ; Jung, Chang-Hoon ; Jang, Young-Gun, “Design and Implementation of User Authentication and Authorization System based on Remote Management Server for Home Network”, Korea Information Processing Society, Vol d14, August 2007

Authors

Jung-Oh Park

He received the B.S. degree in Computer Science at Sungkyul Univ., Korea, in 2000, and the M.S. degrees in Computer engineering from Myongji Univ., Korea, in 2003. He is currently working towards a Ph.D. in computer science from Soongsil Univ., Korea. His research interests include Network Security, Cryptography and Information Hiding.

Sang-Geun Kim

He received a B.S., M.S. and Ph.D. degree in computer science from ChungAng University, Seoul, Korea in 1987, 1989 and 1996, respectively. Since 1996, he has been a professor in the Division of Computer Engineering, Sungkyul University, Korea.