Smart Computing Review

Dear authors,

Please the following information carefully.

All the edits should be checked by you to ensure that the original meaning of this paper has not been altered.

Your manuscript has been edited with Microsoft Word XP.
Please find attached an 'Edit' copy and a 'Clean' copy.
Edit copy is the one which shows "editing marks".
For your convenience, we also include the Clean copy, which has all editing marks accepted.
It is better and recommendable to use the edited copy.

In addition, to see our edits visually well in the edit copy, please read the following direction.

In the Ms word functions, use the following direction in order.

Tools-Option-Track Changes-Balloon

In the 'use of balloons' in print and web layout, see if no 'check' should be in the Check Box. Do not use the 'balloon function.

Thank you,

We will do our best to meet any of your requests.

Best Regards,

raient@ssu.ac.kr

A ~~study~~ Study on Home Network User Authentication Using Token-Based OTP

Jai-Yong Kim [1] and Moon-Seog Jun [2] (use stype: Author)

[1] Dept of Computer Science, Soongsil University / Postal Code 156-743, Seoul, Korea / raient@ssu.ac.kr

[2] Dept of Computer Science, Soongsil University / Postal Code 156-743, Seoul, Korea / mjun@ssu.ac.kr

* Corresponding Author: Jai-Yong Kim

Received; Revised; Accepted; Published

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

Keywords: Home Network, OTP

Introduction

In modern society, a natural connection ~~of~~ between real space ~~to~~ and cyber-space~~s~~, combined with rapid advances in the information technology (IT) industry, has made home network services appear and develop ~~besides~~ in addition to ~~our~~ the workplace services ~~setting~~. Among other IT technologies, the 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~~ for ~~its~~ future development ~~ahead~~. With the recent spread of home network services, especially in diverse forms ~~recently~~, ~~however, scope in target~~the potential for cyber attack has also ~~enlarged~~increased, throwing an element of anxiety over ~~our~~ society, socially and economically. This state of affairs necessitates user authentication that prevents ~~occurrence of invasion incidents~~ unauthorized access and the exposure of user information in home network services.

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

This ~~authentication~~ system uses X509 v3--based authentication for certification, controlling devices by dividing a user group ~~on its~~into extension area~~,~~ and, for devices with restricted ~~approach~~access, ~~it~~ controls ~~approach~~ access by adding an

~~ACL (~~Access Control List (ACL). Such a division into users with restricted ~~approach~~ access and ~~its~~ their manager can ~~present~~ provide ~~approaches~~ access for each device and protect ~~it~~ them ~~safely~~ from outside attack.

Related study

■ Home network

Home Networking & IT (~~HNIT~~ HNIT(~~Home Networking & IT~~), under ~~CEA (~~the Consumer Electronics Association~~),~~ in the U.S.,~~,~~ defines home network as "a coupling together of home appliances and electronic systems for remote approach control possible." That is, through the home network, each product must connect to each other product to share mutual services, while ~~the~~ users must be able to ~~remote~~ control the scattered instruments remotely or use the service provided by each instrument [1]. The ~~Setting~~ setting in which such a home network service has been ~~in application~~implemented is called a *digital home*. In 2003, when the Ministry of Information and Communication designated this industry as one of the 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 this ubiquitous environment has been applied to ~~general~~ homes in general.

Editor - Highlight - Is this the exact quote? It doesn't make sense. Please double-check. A reference would also be good.

A ~~Home~~ home network is, as shown in ~~[~~Figure 1~~]~~, ~~binding~~ connecting instruments at home into one network to make them capable of communication, and connecting ~~these~~ them to the outside internet network to allow control~~ling~~ of consumer appliances from ~~at/~~outside the home, regardless of the user's ~~position~~location [2].

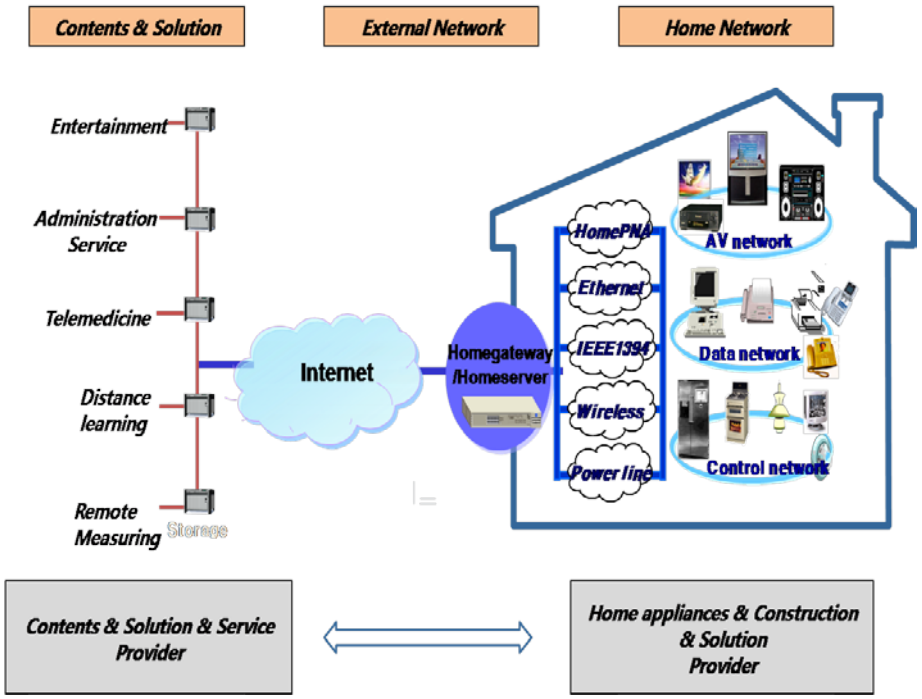


Figure 1. Home ~~Netowork N~~network system

Editor - Highlight – Change "Homegateway" to "Home gateway" and "Homeserver" to "Home server" (two words, not one word) to match Figure 3.

서식 있음: 강조
서식 있음: 글꼴: 기울임꼴
서식 있음: 강조
서식 있음: 강조
서식 있음: 강조

It is also ~~through~~ the home network that makes available from home outside service~~s from home,~~ such as remote medical care, remote instruction, etc., from providers outside ~~contents~~the home.

■ ~~OTP (~~One-time Password~~)~~

OTP is the system of generating a password made available for use only one time~~,~~; thus, it authenticates the user by using a different password~~s for~~ each time. OTP, a typical method of double-element user authentication and basically devised on the basis of ~~cryptographic~~ cryptography~~idea~~, is ~~the~~ a system of high security and is ~~convenience~~ convenient to use [3]. Since it uses ~~another~~ a new password ~~for~~ each time, it is, unlike ~~the~~ system~~s~~ using ~~the~~ a fixed password, proof against attack by reusing password~~s~~, and since it uses a cryptographic algorithm, it ~~is~~ also ~~proof~~ protects against the prediction of a possible password ~~in~~ for use ~~for~~ next time ~~from~~ based on the one currently used. Hence it is safe. If you enter a user password and an input value for generating a one-time password into the ~~OPT~~ OTP program stored in the ~~OPT~~ OTP token or a user PC, the system generates a one-time password using a cryptographic algorithm. Here, only by entering different values ~~for~~ each time for input values, ~~does~~ is a one-time password ~~come into being~~created, and depending on ~~what~~ the kind of value ~~is~~ entered for ~~this~~ the input value, it is classified into diverse ~~OPT~~ OTP methods.

■ Home Network Security Technique

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

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

서식 있음: 강조

Editor - Highlight - Spell out in full (radio frequency identification? radio frequency infrared device?).

서식 있음: 강조

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

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 the home network environment is considered, the list of access controls should ~~desirably~~ ideally be embedded in the terminal, and access rights should be restricted according to a consistent security policy in both safety ~~aspect or~~ and user aspects for overall management of the home gateway and ~~active~~ counteraction against illegal infiltration ~~by the~~ from ~~leakage~~ leak~~ing~~ed ~~of~~ authentication information.

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

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

System proposed

■ Configuration

User authentication proposed in this thesis for a home network system authenticates the user through OTP-based open-key authentication of a cryptographic algorithm, in which the home system is controlled with a personal device ~~by~~ receiving personal authentication. Rather than passing through an authentication server of a service provider, which must be included in the existing home network setting, ~~This~~ this thesis ~~also~~ presents a system~~, rather than passing through the authentication server of a service provider that must be included in existing home network setting,~~ in which the user is able to authenticate, in person from outside the home, ~~with~~ a client device and home server.

서식 있음: 강조

Editor - Highlight - Is this the intended meaning? If not, please rephrase as intended.

서식 있음: 강조

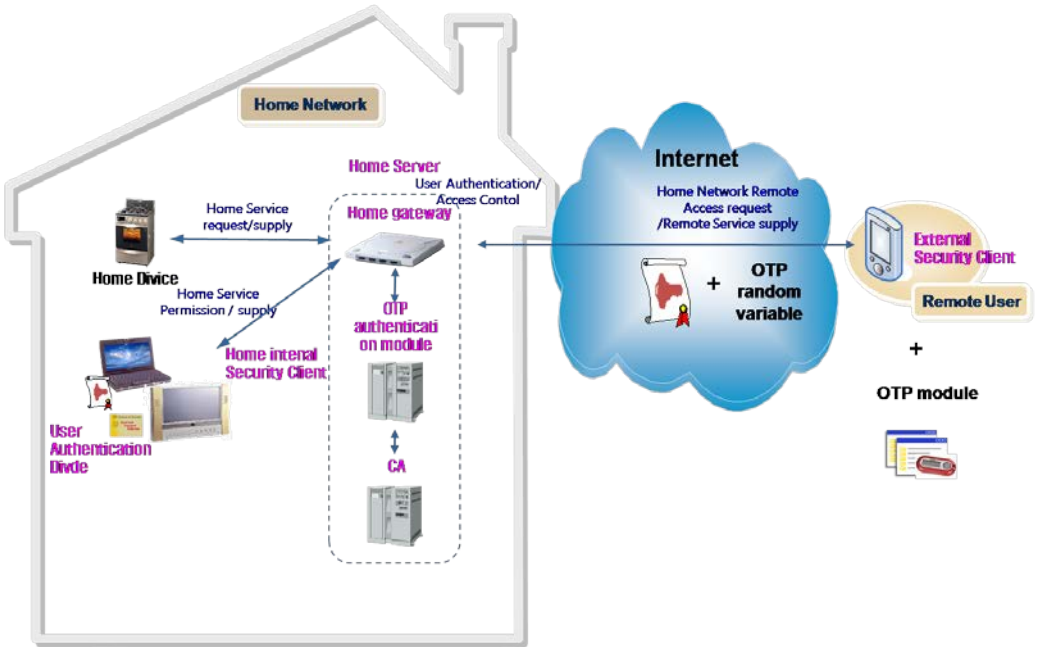


Figure 2. Total User Authentication system proposed

Editor - Highlight – Change “divice” to “device” and change “Divde” to “Device”; change “intenal” to “internal”; under “Home gateway” the word “authentication” is broken incorrectly. If hyphenation is necessary, change to: “authentica-tion” instead.

In the configuration of the system, as shown in ~~[~~Figure 2~~]~~, ~~the~~ a user from outside the home, without ~~his passage~~ passing through the internet ~~network~~ to the ~~home~~ network of a service provider, carries out ~~approach~~ access and user authentication in person. This proposal also includes, in ~~approaching~~ accessing the homer server, a method of authenticating the user using OTP-based authentication and a method of controlling ~~approach~~ access to home devices.

For user authentication, we propose a method of using OTP random variables and authentication, generated by an OTP module mounted in the client device of the user outside, which is a safer way to authenticate a user than existing ~~ones~~ways. The ~~Home~~ home server ~~is composed~~ consists of the client device for the outside user, a home gateway for communicating between home devices within the home network, and a CA, OTP authentication module for user authentication.

Editor - Highlight - Spell out in full (certificate authority? cryptoanalysis?).

Home device ~~approach~~ access control, when a client controls a home device from outside, gives a list of ~~approach~~ access controls ~~differently~~ composed differently for each user and provides multi-approach control for devices already in use by a user so that other users cannot use ~~it~~them, using OTP random variables generated by each user. A ~~Manager~~ manager can perform management, according to the grading of users, ~~in separation~~ by separating ~~into~~ devices into accessible and inaccessible~~approachable and unapproachable~~, while a client can request from the manager addition to, or ~~/~~deletion from, an ~~list of approach~~ access control list. ~~from the manager, and w~~When the request is met, the client receives a reissue of authentication from the home server.

Process of user authentication

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

서식 있음: 강조
서식 있음: 왼쪽, 들여쓰기: 첫 줄: 0 cm
서식 있음: 강조
서식 있음: 강조
서식 있음: 강조
서식 있음: 강조
서식 있음: 강조

Editor - Highlight - Is this the intended meaning? If not, please rephrase as intended.

For the process of user authentication, as shown in ~~[Diagram~~Figure 3~~]~~, the user asks for access to the home network from outside through SSL ~~(Secure Sockets Layer)~~ with OTP random variables generated by both ~~an authentication issued for a~~ the client and the OTP module ~~mutually motivated~~activated.

Editor - Highlight - Is this the intended meaning? If not, please rephrase as intended.

서식 있음: 강조
서식 있음: 강조
서식 있음: 강조

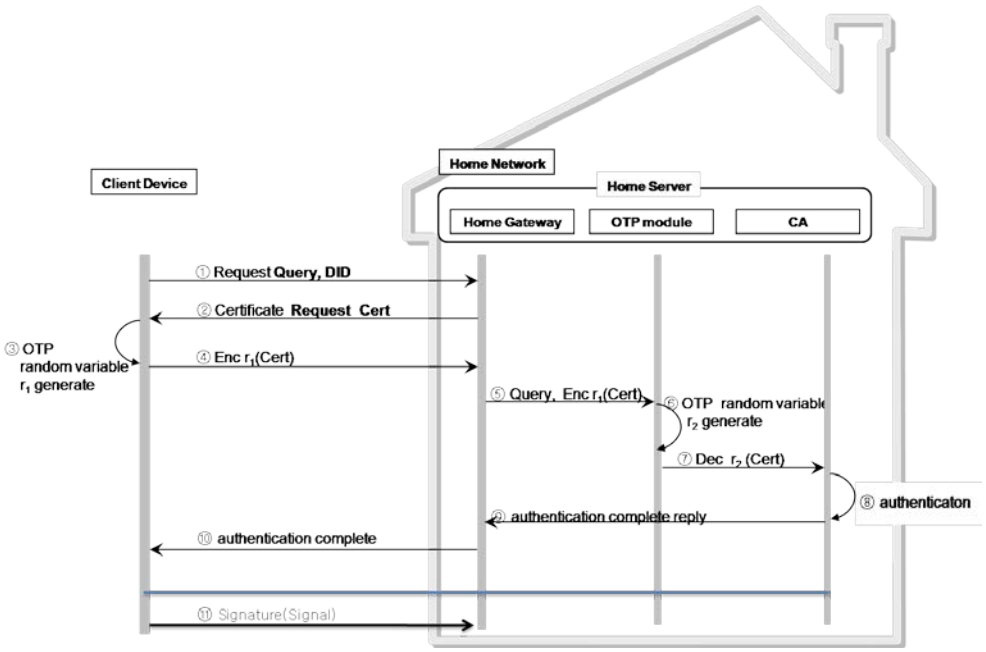


Figure 3. Process of user authentication

서식 있음: 강조

Editor - Highlight – In #3 and #6, change “generate” to “generated”; in #6, the word “variable” is partly hidden; in #8 change spelling to “authentica**tion**” instead of “authentica**ton**”.

서식 있음: 왼쪽
서식 있음: 강조
서식 있음: 글꼴: 굵게
서식 있음: 글꼴: 굵게

Once the request for user authentication has been transmitted, the home server requests ~~the~~ information on the user's authentication from the user, and the user generates the value for r, an OTP random variable generated by the home server and ~~motivated~~ the OTP module, and transmits the value for r, coding the authentication information with a personal key in a symmetric-key algorithm. The OTP authentication module ~~at~~ in the home server also decodes the ~~coded~~ authentication information with a value for r, the OTP random variable generated~~,~~ examines the decoded authentication information from the CA. If the authentication information ~~has been~~ is verified, it transmits the ~~response of~~ authentication verification to the user through the home gateway, ending the authentication process~~of the user~~. Then~~,~~ the client device can control a home device on the home network.

■ Home device approach control

When the process of user authentication is done, ~~approaches~~ access to each device ~~are~~ is made through the home gateway, as shown in ~~[Diagram~~Figure 4~~]~~. When an outside client ~~approaches~~ accesses a home device, the authority to ~~approach~~ access the home device is provided depending on the user, while the home server controls ~~approaches~~ access to the home device by analyzing whether it is ~~approachable~~ accessible or not through ~~the~~ authentication of ~~an~~ the outside client.

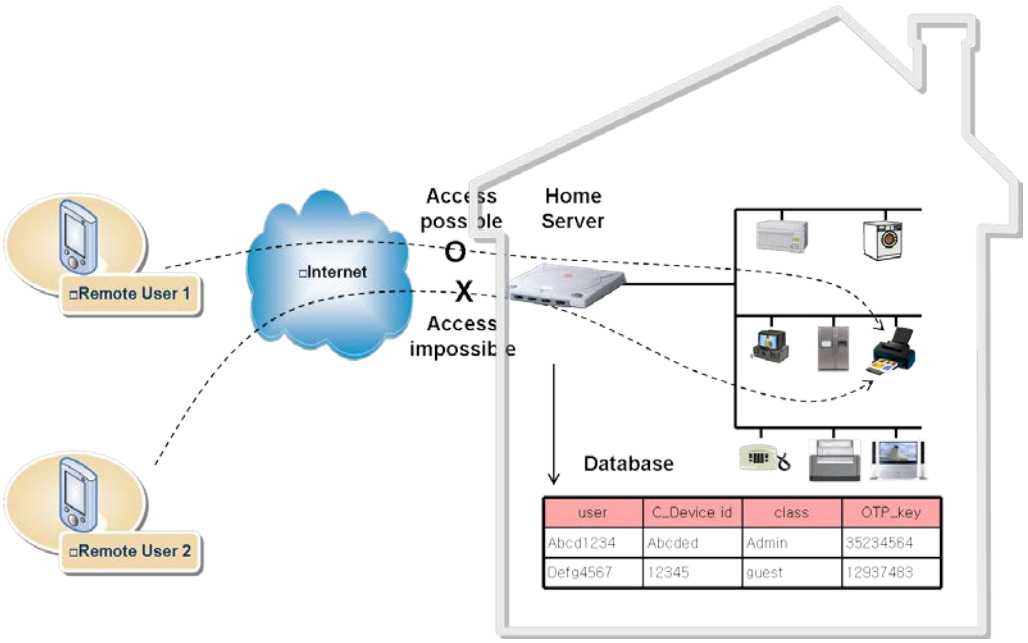


Figure 4. ~~Divice~~ Device access control

Editor - Highlight – Text “Access possible” and “Access impossible” obscured by house frame. Best to have text in front of frame.

서식 있음: 강조
서식 있음: 왼쪽
서식 있음: 강조

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

- Conjoin the value for *r*, a random variable generated from the OTP module~~,~~ and one′s key, and then hash.
- Transmit the value for hash, DIDnum, an X509-based attribute, coded value for Control Command message, and the client′s own DID to home server.

Home server decodes these using the client′s DID value to verify DIDnum and Control Command, and then notifies.

Editor - Highlight - Spell out (device ID?).

Editor - Highlight – Notifies *what*? or *who*?

서식 있음: 글꼴: 기울임꼴
서식 있음: 강조
서식 있음: 강조
서식 있음: 강조
서식 있음: 강조
서식 있음: 강조
서식 있음: 강조
서식 있음: 강조
서식 있음: 글꼴: 기울임꼴
서식 있음: 글꼴: 기울임꼴

Performance Evaluation

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

■ Comparison Analysis with Existing System

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

	P Company Protocol	S Company Protocol	M Company Protocol	Proposed Protocol
Authentication ~~Method~~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

~~[~~Table 1~~]~~. Performance Comparison with 1

Editor - Highlight – Comparison with 1 *what*?

서식 있음: 강조
서식 있음: 강조
서식 있음: 강조
서식 있음: 강조
서식 있음: 글꼴: 기울임꼴, 강조
서식 있음: 표준, 왼쪽
서식 있음: 영어(미국)

Analysis of Safety

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

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

서식 있음: 글꼴: 기울임꼴

Safety on Sniffing Attack : Methods of controlling devices in the home network include use of cable and transferring ~~of~~ messages to control devices through the existing wired network or wireless network~~, and w~~Whatever method is used to transfer data, data are always transferred ~~always~~ after encoding, and thus no risk exists ~~as to~~for exposure of data unless an illegal device holds a key.

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

서식 있음: 강조
서식 있음: 강조

Editor - Highlight - Do these changes reflect the intended meaning? If not, please rephrase as intended.

서식 있음: 강조

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

Conclusions

To prevent and reduce the security risks increasing ~~together along~~ with the advances in home network technology, continued concern and active study are needed on an on-going basis. Positive and continued responses to such problems are also needed from the actual ~~spot~~ location of the home network.

Above all, ~~it requires~~ a technique for ~~a~~ safe user authentication is needed in order to prevent the occurrence of invasion incidents in home network services and to prevent exposure of user information. This thesis proposes a safer system of authentication in which the outside user can perform ~~a~~ safe user authentication with the home server on the home network directly, without going through the authentication server of the home network service provider.

This system has ~~the~~ authentication for one's client device directly issued from the home server ~~from~~ off-line, protects the authentication information safely by coding it with a random variable generated by an OTP module ~~motivated~~ activated between the client device and the home server. Besides, it authenticates the user and controls device ~~approaches~~ access using the issued authentication and the value of the ~~OPT~~ OTP random variable. In the protocol proposed, since data is always transmitted in ~~encryption~~encrypted form, ~~when some~~ illegal equipment has no idea of a client's personal key and random number value, ~~r~~ *r*, so there is no risk of exposing data ~~information~~. It also has ~~an~~ the accompanied effect of reducing communication overhead by ~~omitting the prior movement of~~ not having to transmit from server to client by mutually ~~motivating~~ prompting the random number value ~~r~~ *r* generated from the existing home server.

서식 있음: 글꼴: 기울임꼴

서식 있음: 글꼴: 기울임꼴

In the course of user authentication, ~~it~~ the system encodes using the home server and the one-time random number value ~~r~~ *r* generated from the client's OTP to provide ~~an~~ authentication, which is safer against attacks such as ~~snipping~~sniffing. It is difficult to infer the personal key and ~~an~~ authentication, and since ~~it~~ the system transmits the message for controlling the home device by recoding the hashed value, it is impossible to infer the content of the message even if the message is interrupted halfway.

서식 있음: 글꼴: 기울임꼴

Further research ~~task~~ must include a study of controlling diverse home devices, a study on the method of ~~approaching~~ accessing and controlling wireless home devices ~~wireless~~ using mobile instruments ~~in~~ with a low capacity for arithmetic operations, and a study on an even safer security protocol by applying the safe security protocol in use for existing fixed lines and this proposed method.

References

[1] 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.

[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.

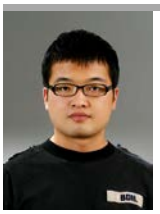
[3] Pan-Lung Tsai, Chin-Laung Lei, Wen-Yang Wang, "A Remote Control Scheme for Ubiqui-tous Personal Computing", International Conference on Networking, Sensing & Control, March, 2004.

[4] 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.

[5] Lee Young-Gu, "Design and Implementation of Security Protocol for Home-Network based on SOAP" Soongsil Universty, 2006.

[6] 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.
[7] J Jeong, MY Chung, H Choo, "Integrated OTP-based user authentication scheme using smart cards in home networks", Hawaii International Conference, 2008.
[8] B Sathish Babu, P Venkataram, “A dynamic authentication scheme for mobile transactions”, International Journal, 2008.
[9] P Venkataram, BS Babu, “An authentication scheme for ubiquitous commerce: A cognitive agents based approach”, Network Operations, 2008
[10] Kim, S.K., Chung, M.G, “More secure remote user authentication scheme”, Comput. Commun. **32**, 1018–1021, 2009.
[11] J Moon, D Lee, IY Lee, “Device Authentication/Authorization Protocol for Home Network in Next Generation Security”, Advances in Information Security and Assurance, 2009 .
[12] JS Moon, IY Lee, KB Yim , “An Authentication and Authorization Protocol Using Ticket in Pervasive Environment”, Workshops (WAINA), 2010.
[13] B Vaidya, JH Park, SS Yeo, JJPC Rodrigues, ”Robust one-time password authentication scheme using smart card for home network environment”, Computer Communications, 2011.



Jae-yong Kim received ~~the~~ his M~~.~~S degree~~s~~ in ~~Computer~~ computer engineering from the University of Soong-sil, Korea, in 2010. He is currently working towards a Ph~~.~~D~~.~~ in computer science from the University of Soong-sil, Korea. His research interests are in ~~the~~ network security, RFID, information hiding, and DRM ~~System~~systems.

Editor - Highlight – Spell out in full (radio frequency identification? radio frequency infrared device?; digital rights management?).

서식 있음: 강조
서식 있음: 강조
서식 있음: 공백 이외 밑줄
서식 있음: 공백 이외 밑줄
서식 있음: 강조