A Security Framework for Ubiquitous Computing Environment

Cheol-Joo Chae, Hyo-Young Shin, Jae-Kwang Lee, *Member, KIMICS*

Abstract—Most security solutions and middleware on home network consider internet users as approaching subject. It is unrealistic where the most subjects are mobile users who want to control home network devices. Therefore minor and fast certification structures are needed to control other devices with mobile device that has lower computing capacity. To solve the above problems, this paper wants to build safe certification frame work for internet and mobile users to control household devices safely. New certification structure is proposed to get out of heavy certification structure like PKI and to minimize encrypting and decrypting operation by compounding session key and public key.

Index Terms—Ubiquitous Computing Security, Mobile Security, Authentication, PKI

I. INTRODUCTION

Ubiquitous computing environments make the society computing everywhere. Home networking takes the start point of Ubiquitous, and it is the basic environment that should be constructed. But, home network environment has security-weaknesses that are appeared in existing environment and additional security-weaknesses, which is unique in home network environment, that are due to information appliances with the lower computing performance. So, many development companies and research institutions have been working to make solutions that can safely approach and control the home network resources from remote to home. And they propose middle-wares that can certify and control approaches like UPnP, Jini, HAVi, LoneWorks, HnCP.

But, most solutions focus on the home network security server management and gateway device certification. Only a little solutions are considering public key infrastructure to approach the home network resources. And in the case of middleware, most researches are done to contain certifications between devices and home gateway device certification for approach control of home network devices. That is, current developments and researches on home network security are based on the PKI structure to secure between remote network and home network, and they are concentrated upon the certification and security in home network.

It means that even the home network has a perfect security structure, home network security can't be perfect when the former security structure has a problem. Besides, most security solutions and middle-wares consider internet users as approaching subject. It is unrealistic where the most subjects are mobile users who want to control home network devices. Therefore minor and fast certification structures are needed to control other devices with mobile device that has lower computing capacity.

II. AUTHENTICATION FRAMEWORK

2.1 Public-key based Framework

Mobile-IP uses two IP address. First, mobile host is allocated fixed IP address in home network that begin connection first time, it is allocated temporary IP address that is CoA from foreign agent that is situated to foreign network according as move by foreign network. This two IP address is combined and is used. Process that data is transmitted sends data to fixed IP address that node is offered by home network. And, if send data to the fixed IP address, the process consist of process that transmit by home network's temporary IP address. Process that mobile host registers new position information to home agent consists of 3 steps of agent

Manuscript received April 15, 2009 ; revised May 20, 2009

Cheol-Joo Chae is with the Department of Computer Engineering, Hannam University, Dae-Jeon, Korea(e-mail:cjchae@hnu.kr). Hyo-Young Shin is with the Department of Internet Information, Kyungbok College, Korea(e-mail:hyshin@kyungbok.ac.kr). Jae-Kwang Lee is with the Department of Computer Engineering, Hannam University, Dae-Jeon, Korea(e-mail:jklee@hnu.kr)

advertisement, registration request, registration response as figure 1.

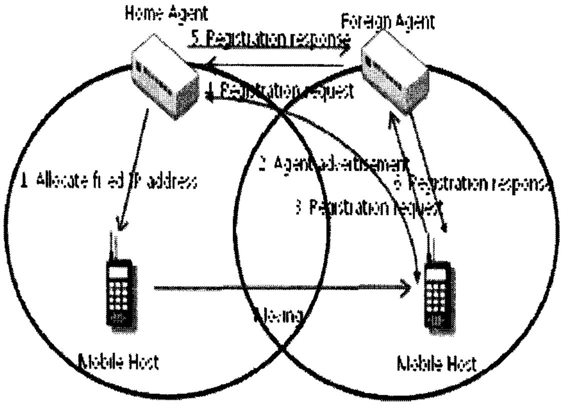


Fig. 1 Mobile-IP registration process

Method that propose in this paper as figure 2 and figure 3 and is public-key based authentication mechanism and minimal public-key based authentication mechanism's mixing mechanism. It acts equally with minimal public-key based authentication mechanism beside what mobile host adds electronic signature to registration request.

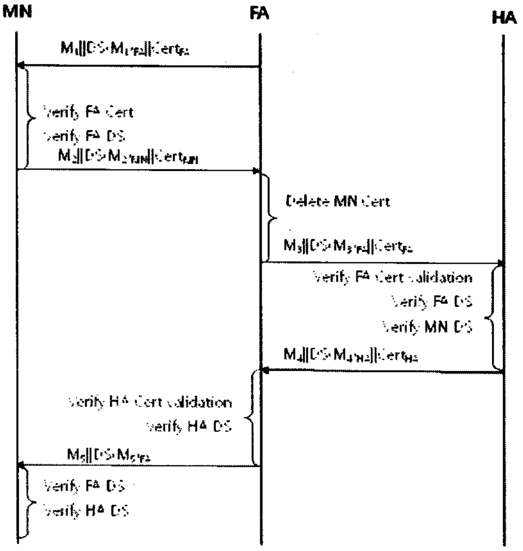

MN
FA
HA
$M_1||DS{\cdot}M_{1FA}||Cert_{FA}$
Verify FA Cert
Verify FA DS
$M_2||DS{\cdot}M_{2MN}||Cert_{MN}$
Delete MN Cert
$M_3||DS{\cdot}M_{3FA}||Cert_{FA}$
Verify FA Cert validation
Verify FA DS
Verify MN DS
$M_4||DS{\cdot}M_{4HA}||Cert_{HA}$
Verify HA Cert validation
Verify HA DS
$M_5||DS{\cdot}M_{5FA}$
Verify FA DS
Verify HA DS

Fig. 2 Authentication process

Mobile host delivers agent advertisement that foreign agent sends to home agent just as it is. Contents that home agent quotes quote indirectly through result. Mobile host sends electronic signature to home agent, and home agent proves signature after confirm public-key's truth availability approaching to certification authority. Hereupon, home agent can quote mobile host and foreign agent all.

Here, mobile host about the use of network resource administration and control can by offering important non-repudiation service about position information that register by oneself. Home agent sends electronic signature to foreign agent, receive authentication, and is authenticated directly creating mobile host MAC. Therefore, home agent can authenticate about all entities which relate to the registration process for new location.

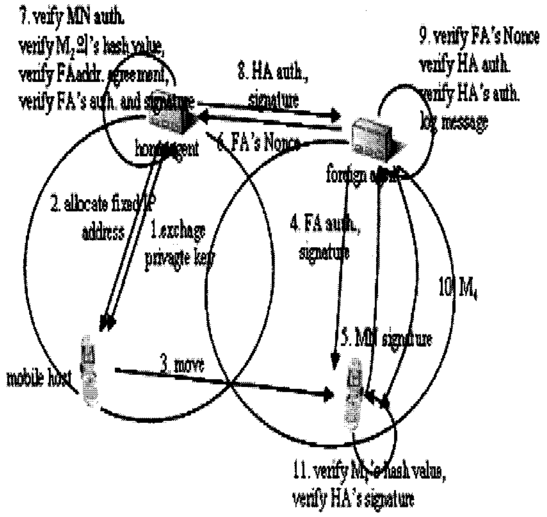


Fig. 3 Authentication framework for non-repudiation service

2.2 Session-key based Framework

IETF defines way to apply public-key based authentication mechanism for Mobile IP. This mechanism, Mobile host is not concerned, applies public-key based authentication mechanism for cross-authentication between Mobile IP entities and AAA entities. The mechanism that attach electronic signature offers non-repudiation service doing electronic signature to mobile host, and offers efficiency by using minimal public-key. Can apply public-key based authentication mechanism above described, but long delay time that is cost to public-key cryptographic operation is incongruent in fast hand off. Also, public-key infrastructure is shortcoming that construction cost enters much.

Session-key exchange mechanism that use existent regional registration that propose in this chapter is as following. First, this mechanism reuses previous allocated session-key. And it applies protocol that put calculable third-party instead of public-key operation and share key. This mechanism achieves third-party role that is worth trusting between anchor agent and foreign agent.

As describe before, it reuse previous allocated KSMN-FA and KSFA-HA. It use this session-key KSFAprev-FAnow that is session-key between previous foreign agent (FAprev) and present foreign agent (FAnow) to decrypt and encrypt the session-key. This key is shared and is distributed dynamically by anchor agent trusted.

Our mechanism offers session's confidentiality and integrity, and achieves minimal-delayed hand-off safety in area by such method. This mechanism is less far delay times and computational costs than proposed public-key based cryptographic operation before. However, this mechanism has the shortcoming that FAprev and FAnow session-key must encrypt and decrypt.

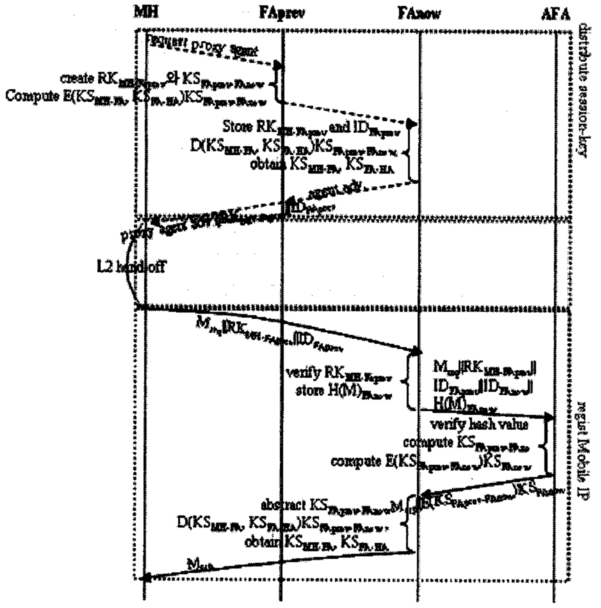


Fig. 4 The process of mobile initiative hand-off operation

2.3 Integrated Framework

Our framework is authentication and security framework between AAA server and home gateway (or home server). Also, it is composed of previous described security framework considering the smallest delay time. Its infrastructure is based on TLS. However, this framework is composed on basis of authentication and session-key cross-exchange between mobile host and home gateway substantially.

First, mobile host send mediators (foreign agent, anchor agent, and home agent) to home gateway identifier (IDHG) to do authenticate home gateway and session-key (KSMH-HG) for secure communication between mobile host and home gateway as shown Figure 6.

This time, it sends session-key (KSMH-HG) encrypted with session-key (KSMH-AAAH) that exchanged to send session-key safety to AAAH between mobile host and AAAH server. Home gateway decrypt it, then it decrypt session-key (KSMH-HG).

This session-key (KSMH-HG) created in mobile host uses secure session to control and service. Home agent's AAA server that receive message including the session-key encrypt it with home gateway's public-key (KUHG) and send it to home gateway. Home gateway encrypt the session-key, it request device to make a booting for service while send response message to home agent. Of course, suppose that home gateway and device achieved authentication mutually.

It is finished to Mobile IP registration and session-key's distribution process and device's authentication/booting process. Actually, mobile host request home gateway to presentation service in home network. The home gateway allocate authentication and authority on users. Continuously, mobile host control directly device through the presentation documents and manage to home network.

III. IMPLEMENTATION AND TESTING

Physically, Network follows IEEE 802.11 as wireless network, Its simulation composition is shown by Figure 5.

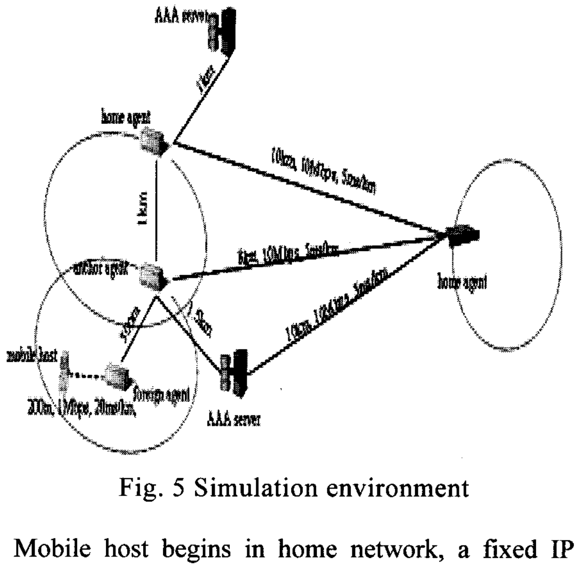


Fig. 5 Simulation environment

Mobile host begins in home network, a fixed IP from home agent, moves to foreign network and is registered from foreign agent. Because Mobile-IP is becoming to operate in domain, according as subnet does and moves to outside by radius 500m, distance between home network and foreign network differs from 1km to 40km. Come to new subnet and register new location information to home agent whenever IP changes and datagram receives tunneling.

Figure 6 shows total authentication time by authentication mechanism and authentication time in mobile host. Total registration time become 37 times and takes 1,134ms, as comparing Symmetric-key method with public-key method. If hand-off service or service in TCP/UDP, This time is fairly long time, after new registration process does on network layer. In spite that public-key heighten the strength of security, we can know the difficult of its use. Total registration time of minimal public-key based method that reduce public-key use by smallest keeping Security just as it is takes than public-key based on method 43%.

But, this method takes on thought of non-repudiation service, thus mobile host do electronic signature our suggested method in case of our suggested method. Our method decrease 60% of registration time against public-key based method, But it increase 139% against the registration time of minimal public-key method as adding on electronic signature for non-repudiation service. Our method supply non-repudiation service with not decreasing efficiency.

We decrease 60% of public-key authentication mechanism through our minimal public-key authentication mechanism with electronic signature, also we can know to decrease 40% of the delay time, as local hand-off.

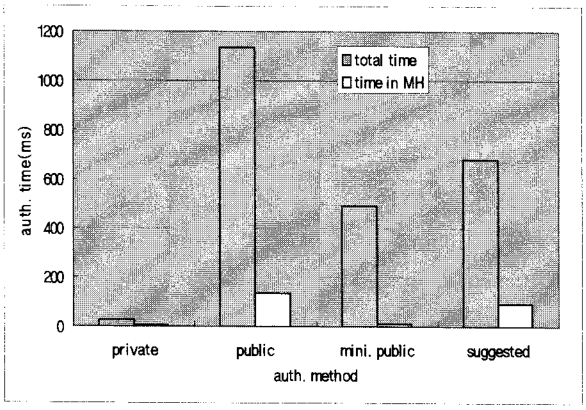


Fig. 6 Total registration and authentication

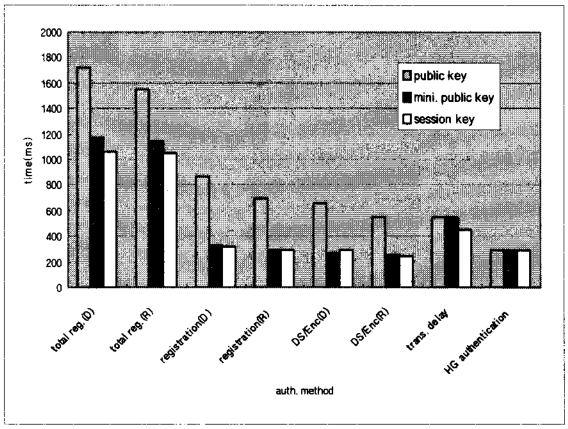


Fig. 7 Comparison of authentication and registration method

We show that the performance is improved against an existing authentication method and registration method by applying previous authentication mechanism or local hand-off method on framework including home gateway in this paper. Also, we can know that the registration time of cryptography and electronic signature time is less weight in other function' time in Figure 7.

IV. CONCLUSIONS

This paper wants to build safe certification frame work for internet and mobile users to control household devices safely. First of all, new certification structure is proposed to get out of heavy certification structure like PKI and to minimize encrypting and decrypting operation by compounding session key and public key. It also adjust certification structure to the way of registration method during hand-off time for more faster operation rate. For it, current home gateway should be changed, so new one is proposed that contains mutual authentication module mutual authentication module and user certification module. Compared with former one, the proposed synthesis certification frame work reduces the times of encrypting and decrypting operation to half and extends operation time to twice by managing the registration during hand-off. And it uses session key to make it easier for mobile device use that has lower computing capacity.

The safe certification fame work between remote network and home network, that is based on the home gateway, will give home network security more firmness, fit in with lower-computing-device-oriented home network service, and will be a foundation of synthesizing unifying certification and approaching control fame work construction. Home network services would be averted by users if they didn't insure the stability. Furthermore, according the home network services, some users can go through economical loss or even threaten their lives. So the certification service, that stands on the basis of proposed certification frame work, will activate the home network service.

ACKNOWLEDGMENT

This paper has been supported by the 2009 Hannam University Research Fund.

REFERENCES

[1] Carl M.Ellison, "Interoperable Home Infrastructure Home Network Security," Intel Technology Journal, Vol.6, 2002.

[2] F. Stajano, R. Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing, Wiley, 2002

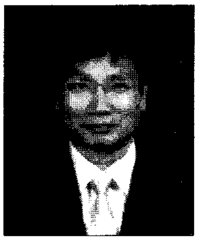
[3] F. Stajano, "Security for Ubiquitous Computing," first Security & Privacy supplement to IEEE Computer, Apr. 2002.

[4] J. P. Hubaux, L. Buttyn, and S. Apkun, "The Quest for Security in Mobile Ad Hoc Networks," ACM Symposium on Mobile Ad Hoc Networking and Computing, 2001.

[5] A. Weimerskirch, and G Thonet, " A Distributed Light-Weight Authentication Model for Ad Hoc Networks," Lecture Notes in Computer Science, Vol.2288, 2001

[6] K. Wrona, "Distributed Security: Ad-Hoc Netwroks and Beyond," Workshop on Requirements for Mobile Privacy and Security, 2002

Cheol-Joo Chae
Member KIMICS. Received B.S degree in Computer Engineering, Hannam University in 2004. Received M.S degree in Computer Engineering, Hannam University in 2006. Since 2006, he has been a Ph.D. Student in Computer Network Lab, Hannam University. The research areas of interest include Computer Security, Network Security, Ubiquitous Security.



Hyo-Young Shin
Member KIMICS. Received his B.S degree from Kwangwoon University, Seoul, Korea, in 1986 and the M.S. and Ph.D. degrees in Computer Science from the same university in 1988 and 1998, respectively. He is currently a professor in the Department of Internet Information at Kyungbok college. His research interests include network security, wireless networks, and sensor networks.

Jae-Kwang Lee
Member KIMICS. Received Ph.D. degree in Kwang Woon University, in 1993. In 1993, he joined the department of Computer Engineering, Hannam University, Korea. His research interest is in the area of Network Security that includes Wireless network, Cryptograph, PKI, WPKI and Ubiquitous security.