홈 네트워크에서 디바이스의 유효성 검증 방법

김도우* · 김건우* · 이준호* · 한종욱*

Method to Verify the Validity of Device in a Home Network

Do-woo Kim* · Geon-woo Kim* · Jun-ho Lee* · Jong-wook Han*

이 논문은 정보통신부의 출연금으로 수행한 정보통신연구개발사업의 연구결과임

요 약

홈 네트워크 환경에서 디바이스는 동적으로 네트워크에 연결되고, IP 주소를 얻고, 자신의 기능을 알리고, 다른 디바이스의 존재 및 기능을 파악할 수 있다. 이런 과정 이후 디바이스는 서로 직접 통신을 할 수 있다.

본 논문에서는 디바이스들 사이에 대칭키를 이용하여 상호인증을 수행하는 디바이스의 안전한 검색방법을 제안하고자 한다. 이 방법은 홈서버를 사용하여 홈 네트워크 디바이스들에게 대칭키를 분배한다. 이 키를 사용하여 홈 디바이스들 사이의 상호인증이 수행되어진다. 이것은 미들웨어의 제어 하에 두 디바이스가 안전하게 통신할 수 있는 기능을 제공한다.

ABSTRACT

With a home network, a device can dynamically join a home network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices. Devices can subsequently communicate with each other directly. Device discovery protocol defines how network services can be discovered on the network.

In this paper, we propose the secure discovery method of devices that uses mutual authentication with symmetric key between devices. This method that we present distributes symmetric-key to home network devices by the home server. Using this key, mutual authentication is performed between home appliances. It enables any appliance under any middleware's control to securely communicate any other appliances.

키워드

Home Network, Security, Discovery, Home Server

Ⅰ. Introduction

Wired and wireless bandwidth in home networks is expanding, and there will become an increasing need to connect more and more devices together, first for point-to-point communication between two devices at a time, and later for any-to-any communication over a wired or wireless home network. The increasing number of devices and service together with the increasing amount of available content in the home network is challenging for some kind of universal connectivity and plug-and-play functionality in home networks.

* 한국전자통신연구원

접수일자 : 2006. 5. 26

Device discovery protocol defines methods both for client device to locate resources of interest on the home network, and for devices that provide services to announce their availability on the home network. A client device can send search request to discover devices and services that are available on the home network. Similarly, a device, upon being plugged into the home network, will send out presence announcements advertising the services it supports. Secure device discovery in home network environments is critical because there are many chances of misuse from fraudulent devices[1,3].

In this paper, we propose the secure discovery method of devices that uses mutual authentication with symmetric key and public key between devices. This method that we present distributes symmetric and public key to home network devices by the home server. Using this key, mutual authentication is performed between home appliances. It enables any appliance under any middleware's control to securely communicate any other appliances.

This paper is organized as follows. Section 2 describes discovery protocols that provide in home network middles. Section 3 describes security requirements of discovery protocol. Section 4 presents the method that securely discovery devices in home network environments. Finally, we summarize and list our future research directions in section 5.

Ⅱ. Discovery protocols in home network environments

2.1 UPnP discovery protocol

The UPnP discovery protocol allows a device to announce to the control points that it has become available on the network. On joining the network, the device multicasts SSDP NOTIFY messages to advertise its embedded devices and services to all the control points on the network. When a new control point becomes available on the network, it multicasts a SSDP M_SEARCH discovery message through an HTTPMU request to search for available devices and services. The search message can contain qualifications on the type of device or service that the control point is searching for. All devices on the network must respond to the control point if their devices or services match the search criteria in the discovery message. The response that is transmitted to the control point by one or more matching devices contains a URL to the device description. The response message is sent to the control point using the User Datagram Protocol (UDP) with Simple Service Discovery Protocol (SSDP) headers[1,3].

2.2 Jini discovery protocol

The lookup service can be viewed as a directory service, in that services are found and resolved through it. In a Jini community, services register their proxy objects with a lookup service through discovery and join process, and clients query the lookup service to find out the services they want. Jini uses three related discovery protocols, useful in different situation. Multicast Request Protocol is used when an application or service first becomes active, and needs to find lookup services in the vicinity. Multicast Announcement Protocol is used by lookup services to announce their presence to the services that may have interest in the community. Unicast Discovery Protocol is used to establish communications with a specific lookup service known to it in priori over a wide-area network[1,4].

2.3 Salutation

The Salutation architecture is composed of two major components: *Salutation Manager* and *Transport Manager*. The Salutation Manager is the core of the architecture, similar to the lookup service in Jini. It is defined as a service broker: A service provider registers its capability with a Salutation Manager. When a client asks its local Salutation Manager for a service search, the search is performed by coordination among Salutation Managers. Then, the client can use the returned service. A Salutation Manager sits on the Transport Managers that provide reliable communication channels, regardless of what the underlying network transports are[2,7].

Ⅲ. Security requirements of discovery protocol

We consider security requirements such as device authentication, confidentiality, integrity, non-repudiation, availability in discovery protocols. Although there is much research related to device or service discovery, few protocols have full security and privacy functionality built-in[5,11,12].

Authentication. Authentication in device discovery is primarily communication security. Authentication is the process of determining whether something is what it is declared to be.

Confidentiality and Integrity. Communication between service discovery components should be safe. Malicious users may listen to communication channels or even actively attack systems. We do not want service information exposed to malicious users or changed during communication. These requirements are translated to use of message encryption and message authentication code.

Availability, Privacy, and Non-repudiation. Services and directories in devices may be targets of attackers. Making services and directories available against attack is similar to other network applications. Information in devices is always a concern. We want to use services easily but keep our information private. In the mean time, service usage should be tracked. A digital signature is usually used to achieve non-repudiation of the service usage.

Ⅳ. Method that securely discovery devices

We propose a method that securely discovery devices in home network environments. It is a symmetric-key authentication scheme for verifying the identities devices in home network environments. When a device discoveries the available device to use services it provides, mutual authentication between home appliances using key that a home server gives out is performed. Also this method provides trust relationship between devices in home network and the secure communication of control message or data.

Figure 1 is the configuration to securely discovery device in home network with mutual authentication. A home server gives out a symmetric-key to devices connected over the home network. A home server or home gateway can function as a home server. A device distributed a symmetric-key can send search request to discover devices and services that are available on a home network or send out presence announcements advertising the services it supports.

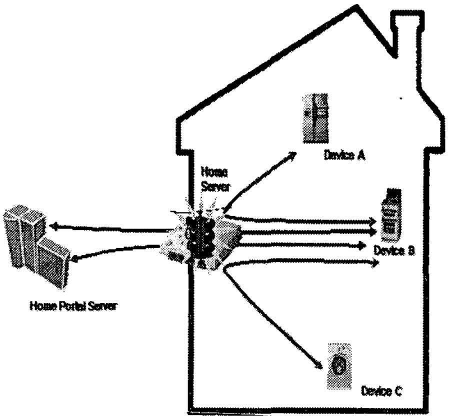

그림 1. 홈 네트워크 구성
Fig. 1 Configuration of a home network

A home server is secure server that can share key with home network devices. Figure 2 describes the process that handles secure discovery between home network devices. *E* is a symmetric encryption algorithm. N_A and N_B are nonces chosen by *A* and *B*, respectively. *K* is a session key chosen by a home server *T* for *A* and *B* to share. A and T share a symmetric key K_{TA} *B* and *T* share K_{TB}.

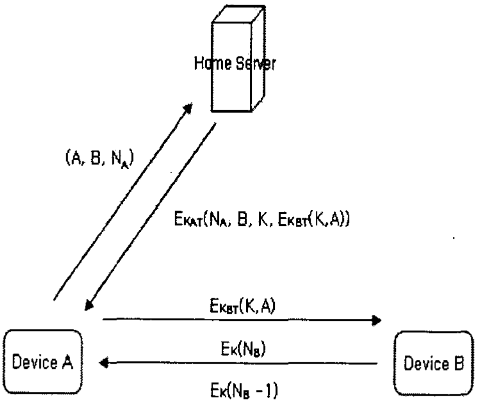

그림 2. 키 분배 과정
Fig. 2 A interacts with a home server T and B

$$A \rightarrow T : A, B, N_A \cdots\cdots\cdots\cdots \text{①}$$

$$A \rightarrow T : E_{K_{AT}}(N_A, B, K, E_{K_{BT}}(K, A)) \cdots\cdots \text{②}$$

$$A \rightarrow B : E_{K_{BT}}(K, A) \cdots\cdots\cdots\cdots \text{③}$$

$$A \rightarrow B : E_K(N_B) \cdots\cdots\cdots\cdots \text{④}$$

$$A \rightarrow B : E_K(N_B - 1) \cdots\cdots\cdots\cdots \text{⑤}$$

A home server is secure server that can share key with home network devices. Figure 2 describes the process that handles secure discovery between home network devices. *E* is a symmetric encryption algorithm. N_A and N_B are nonces chosen by *A* and *B*, respectively. *K* is a session key chosen by a home server *T* for *A* and *B* to share. A and T share a symmetric key K_{TA} *B* and *T* share $K_{TB.}$

The home device *A* sends the distribution server *T* the message. In response to the message, the home server *T* generates a shared key, *K* that is to be used to encrypt communication between *A* and *B*. Additionally, the nonce is included, to show freshness, $E_{K_{BT}}(K, A)$contains the same shared secret, as well as the name of the initiating device, encrypted with the other device B's secret. The entire message is encrypted using the device *A*'s private key to ensure that no one else can read it. After getting and decrypting the reply from *T*, *A* sends $E_{K_{BT}}(K, A)$ to *B*. After receiving $E_{K_{BT}}(K, A)$, B then generates a nonce, encrypts it using the shared key, and sends it back to *A*. By decrpyting the nonce, altering it in a predefined way, and sending it to *B*, the initiator shows that it knows the shared key needed to decrpyt the nonce. This proves its identity. The response is also sent encrpyted using the shared key. Encrpyting the response decreases the likelihood of a plain-text style correlation attack, against the prior challenge. Through above authentication process *A* and *B* share a symmetric-key. Using this key secure communication is done between A and B.

Ⅴ. Conclusion

In this paper, we proposed the secure discovery method of devices that uses mutual authentication with symmetric key between devices. This method that we present distributes symmetric-key to home network devices by the home server. Using this key, mutual authentication is performed between home appliances. It enables any appliance under any middleware's control to securely communicate any other appliances. We continue to research into secure discovery protocol using public key.

참고문헌

[1] F. Zhu, M. Mutka, and L. Ni, "Classification of Service Discovery in Pervasive Computing Environments," Institution Michigan State University, MSUCSE-02-24, 2002.

[2] Guttman, E. Perkins, C., Veizades, J., and Day, M. *"Service Location Protocol, V.2"*, Internet Engineering Task Force (IETF), RFC 2608.

[3] Microsoft. *"Universal Plug and Play Architecture, V1.0"*, Jun 8, 2000.

[4] Ken Arnold et al. *"The Jini Specification, V1.0"*, Addison-Wesley 1999. Latest version is 1.1.

[5] Dabrowski, C. and Mills, K. *"Analyzing Properties and Behavior of Service Discovery Protocols Using an Architecture-Based Approach"*, Proceedings of Working Conference on Complex and Dynamic Systems Architecture, Brisbane, Australia, Dec 2001.

[6] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 2nd ed, Prentice Hall, 1998.

[7] "Salutation Architecture Specification," Salutation Consortium, Version 2.0c, June 1, 1999.

[8] P. Dobrev, D. Famolari, C. Kurzke, and B.A. Miller, *Device and Service Discovery in Home Networks with OSGi*, IEEE Commun. Mag. August 2002, pp 86-92.

[9] "Specification of the Bluetooth System, Version 1.2, Vol.3, Part B: Service Discovery Protocol(SDP)," 2003.

[10] F. Zhu, M. Mutka, and L. Ni, "Splendor: A secure, private, and location-aware service discovery protocol supporting mobile services", in *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (Percom'03)*. IEEE Computer Society, Mar. 2003, pp. 235 - 242.

[11] Carl M. Ellison, "Home Network Security", Intel Technology Journal, 2002.

[12] Guoyou He, "Requirements for Security in Home Environments", Residential and Virtual Home Environments Seminar on Internetworking, Spring 2002.

저자소개

김 도 우(Do-woo Kim)

1997년 경남대학교 전산통계학과 이학사
1999년 경남대학교 컴퓨터공학과 공학석사
2003년 경남대학교 컴퓨터공학과 공학박사
2003년 ~ 현재 한국전자통신연구원 선임연구원
※관심분야 : 홈네트워크 보안, 자바 기술

김 건 우(Geon Woo Kim)

1998년 경북대학교 컴퓨터과학과 이학사
2000년 경북대학교 컴퓨터과학과 이학석사
2000년 ~ 현재 한국전자통신연구원 선임연구원
※ 관심분야 : 네트워크 보안, VPN, 홈네트워크 보안

이준호(Jun-ho Lee)

2002년 경북대학교 컴퓨터과학과 이학사
2004년 경북대학교 컴퓨터과학과 이학석사
2005년 ~ 현재 한국전자통신연구원 연구원
※ 관심분야 : 홈네트워크 보안, 네트워크 보안, 유비쿼터스 컴퓨팅

한 종 욱(Jong-wook Han)

1985년 광운대학교 전자공학과 공학사
1991년 광운대학교 전자공학과 공학석사
2001년 광운대학교 전자공학과 공학박사
1991년 ~ 현재 한국전자통신연구원 팀장
※ 관심분야 : 홈네트워크 보안, 네트워크 보안, Optical Security