홈네트워크 디바이스 인증을 위한 요구사항 분석

황진범*†, 한종욱*†

Home Network Device Authentication Requirement Analysis

*Electronics and Telecommunications Research Institute
†University of Science & Technology
E-mail : hjb64253@etri.re.kr

요약

홈네트워크에 사용되는 디바이스가 지능화되고 자동화되어 사람의 개입 없이 디바이스가 스스로 판단하여 서비스를 제공하거나 요청하는 상황인지 서비스가 활성화되기 위해서는 기존의 사용자 인증과 별도로, 디바이스를 인증하는 기술이 필요하다. 본 논문에서는 기존의 홈네트워크에서 사용되는 디바이스 인증 기술을 분석하고, 상황인지 서비스에 적용할 경우의 문제점을 분석한 후, 시나리오를 바탕으로 사용자의 개입을 최소화 하면서 각 디바이스들 사이에 신뢰성 있는 통신이 이루어 질 수 있도록 하기 위해서 필요한 요구사항은 무엇이 있는가를 분석한다.

1. 서론

홈네트워크는 가정의 각 가전 및 사무기기 등이 지능화되고 네트워킹 능력을 갖게 되어 서로 통신하게 되면서 사용자로 하여금 어느 곳에서도 집안의 디바이스들을 제어하거나 서비스를 사용할 수 있게 해주는 기반환경을 말한다. 현재에는 이러한 홈네트워크 환경에 값싸고 소형화된 센서가 결합되어 사용자의 개입 없이 사용자가 미리 정해둔 규칙에 따라 기기 스스로 판단하고 서비스를 제공하는 상황인지 서비스가 홈네트워크의 새로운 서비스로 떠오르고 있다[1,2]. 상황인지 서비스가 활성화되면 사용자는 최소한의 작업으로 주변의 다양한 센서와 지능화된 디바이스를 통해 보다 편리하고 안락한 생활을 제공 받게 될 것이다. 또한, 향후 홈네트워크가 USN (Ubiquitous Sensor Network) 과 결합되면 집 안에서 뿐만 아니라 사용자가 언제, 어느 곳에 있던지 집안에서와 동일한 서비스를 제공받게 될 것이다. 반면, 상황인지 서비스는 사용자의 개인정보와 밀접한 관련이 있고, 사용자의 개입 없이 기기들 간의 상호 연동에 의해서 제공되기 때문에 보안에 많은 취약성을 가지고 있다. 이러한 서비스가 활성화되기 위해서는 먼저 보안에 대한 고려가 선행되어야 한다.

상황인지 서비스에서 가장 중요한 보안 기술 중 하나가 디바이스 인증이다. 상황인지 서비스의 목적이 사용자의 개입을 최소화 하고 사용자를 대신하여 디바이스간의 협업을 통해 서비스를 제공하는 것이기 때문에 사용자가 인지하지 못하는 순간에 사용자의 중요 정보나 권리가 침해 받을 수 있다. 이를 방지하기 위해서는 서비스를 요청하는 디바이스가 적절한 디바이스인지, 다시 말해 사용자에게 권한을 허가 받은 디바이스인지를 확인하고 서비스를 제공하는 디바이스가 안전한 디바이스인지 확인하는 과정이 반드시 필요하다. 기존의 홈네트워크에서 댁내의 각 기기를 연결하는 네트워크와 미들웨어에서 일부 기기인증에 대한 기능을 제공하고 있지만, 이러한 기능들을 상황인지 홈 서비스에 적용하기에는 여러 가지 미흡한 경우가 있다.

본 논문에서는 먼저 기존의 디바이스 인증 기술에 대해 분석하고, 이러한 기술의 한계점을 분석한 후에 상황인지 홈 서비스 시나리오를 바탕으로 상황인지 서비스에 필요한 디바이스 인증 기술의 요구사항은 무엇인지를 분석한다. 본 논문의 2장은 기존의 홈네트워크에서 사용되는 네트워크 망과, 미들웨어에서 제공하는 디바이스 인증 기술의 특징을 분석하였고, 이러한 인증 방식을 상황인지 홈 서비스에 적용하였을 때의 문제점을 분석하였다. 3장은 상황인지 홈 서비스에서 제공될 수 있는 몇 가지 서비스 시나리오를 제공하고 4장에서 이러한 서비스를 바탕으로 디바이스 인증에 대한 요구사항을 제안한다. 마지막으로 5장에서 결론과 향후 연구 방향에 대해 설명한다.

2. 상황인지 홈 서비스 시나리오

상황인지 서비스의 목표는 수많은 지능화된 기기들의 협업을 통하여 사용자가 인지하지 못하는 상황에서 스스로 사용자에게 편리하고 안락한 서비스를 제공하는 것이다. 홈네트워크에서 제공하는 상황인지 서비스는 향후 USN과 결

합되어 댁내에서 뿐만 아니라 사용자가 어느곳에서 어느 서비스를 사용하느냐에 관계없이 동일한 서비스 환경을 제공하는 방향으로 확장될 수 있을 것이다. 이 장에서는 상황인지 서비스를 위해 필요한 디바이스 인증의 요구사항을 정립하기 위해 향후 발생할 수 있는 몇 가지 서비스에 대한 시나리오를 제시한다.

- 자동화 서비스

다음과 같이 디바이스 들이 스스로 상황을 인지하여 서비스를 요청하는 경우가 있을 수 있다.

ㄱ. 냉장고가 냉장고 안의 음식물의 양을 판단하여 사용자가 정한 정책에 따라, 음식물이 부족한 경우 스스로 수퍼마켓의 서버에 연결하여 음식을 주문한다.

ㄴ. 화재 탐지기, 또는 방범 기기에서 화재가 발생하거나 불법적인 가내 침입이 발생한 경우를 판단하여 소방서나, 경찰에 협조 요청을 한다.

ㄷ. 사용자가 설정한 정책에 따라 유료 서비스를 사용자에게 제공한다. 예를 들어 야구 중계가 있는 날에는 사용자가 있는 위치의 디스플레이 장치를 통해 중계를 보여준다.

이와 같은 경우에 수퍼마켓의 서버와, 냉장고 사이, 화재 탐지기/방범장치와 소방서/경찰서 서버 사이 그리고 방송국과 방송 장치 사이에 디바이스 인증이 필요하다

- 서비스 로밍

사용자가 거실의 TV를 통해 유료 VOD를 시청하던 중에 방으로 이동하면 거실의 TV와 방의 PC간의 협업을 통하여 사용자가 시청하던 VOD를 방안의 PC에서 플레이 해 준다. 이러한 경우 거실의 TV와 PC간의 디바이스 인증이 필요하다.

- 타 도메인 서비스 사용

사용자가 집에서 등록하고 사용하던 홈기기를 가지고 회사나 다른 집 또는 그 외의 스마트스페이스에 간 경우 그곳에서 제공하는 서비스를 특별한 설정 없이 기존의 홈에서 사용하던 서비스와 동일한 방식으로 사용한다. 예를 들어 댁내에서 사용하던 PDA를 가지고 회사에 간 경우 PDA에서 문서 출력을 요청하면, 가장 가까운 프린터에서 PDA를 인증하여 문서를 출력한다.

이상의 서비스 시나리오들을 바탕으로 유비쿼터스 환경하에서의 디바이스 인증의 요구사항은 무엇이 있는 가를 4장에서 제시할 것이며, 3장에서는 이에 앞서, 기존의 디바이스 인증 기술에 대한 분석과, 앞의 시나리오에 적용할 때의 문제점들에 대해 분석한다.

	인증수단	키 설정	인증 범위
802.15.1 (Bluetooth)	대칭키	사용자	지역
802.15.3	공개키	사용자	지역 /전역
802.15.4 (Zigbee)	대칭키	사용자	지역
802.11 (WLAN)	대칭키	사용자	지역
Echonet	대칭키	사용자	지역
LonWorks	대칭키	사용자	지역
UPnP	공개키	사용자	지역 /전역
Open Cable	공개키	Cablelabs CA	호환기기 /전역
DTCP	공개키	DTLA CA	호환기기

표 1 기존 디바이스 인증 특징

3. 기존 기술 분석

홈네트워크의 디바이스 인증을 제공하는, 댁내망을 구성하는 주요 기술들에는 802.15.1 (Bluetooth) [3], 802.15.3[4], 802.15.4 (Zigbee) [5], 802.11 (WLAN) [6] 등이 있으며, 미들웨어로는 Echonet [7], LonWorks [8], UPnP [9] 등이 있다. 또한 이외에 디바이스 인증을 제공하기 위한 표준으로 Open Cable 표준 [10]과, DTCP [11] 표준이 존재한다. 이 장에서는 이러한 기술들에서 제공하는 디바이스 인증방식에 대해 분석하고, 상황인지 홈 서비스에서의 디바이스 인증에 적용할 때에 문제점들에 대해 분석한다.

표 1은 홈네트워크를 구성하는 기존의 기술들의 디바이스 인증에 대한 특징을 나타낸다. 기존의 인증 기술들은 크게 인증 수단에 따라서 대칭키 방식과 공개키 방식으로 구분할 수 있다.

- 대칭키 방식

Bluetooth, Zigbee, WLAN, Echonet, LonWorks 등에서 사용하는 대칭키를 사용한 인증방식은 주로 양 디바이스에 사용자가 PIN (Personal Identification Number) 과 같은 정보를 입력함으로써 공유키를 생성하고 Challenge-response 방식으로 서로 동일한 키를 가지고 있음을 확인함으로써 서로를 인증하게 된다. 이러한 기술들의 특징은 주로 사용자가 직접 각 다비이스 간의 공유키를 설정해 주어야

하는 불편함이 따르며, 그 인증 범위가 지역적으로 제한된다는 것이다. 다시 말해 사용자가 키를 설정해 준 양 디바이스 간에만 인증이 가능하며, 사용자가 디바이스를 집 외부에서 사용하고자 할 때에는 또다른 키 설정이나 인증 방법이 필요하다. 이러한 방식의 인증을 사용할 경우에는 2장에서 제시한 서비스를 대부분 제공할 수 없다. 인증 범위가 지역적이기 때문에 외부의 서버에 접근하여 자동회된 서비스를 수행할 수 없고, 서비스 로밍도 댁내의 기기에 한정되며, 사용자가 자동차, 회사 또는 옆집등 댁외로 이동한 경우에는 제공하기 어렵다. 그리고, 타 도메인의 서비스 사용 또한 사용자가 각 디바이스들간에 새로운 공유키를 설정해 주지 않으면 서비스가 불가능하다.

- 공개키 방식

802.15.3, UPnP, Open Cable, DTCP 와 같은 기술들은 인증서를 사용하여 공개키 방식의 인증을 제공한다. 공개키 방식의 장점은 사용자가 각각의 디바이스 간의 공유키를 설정해 줄 필요가 없다는 것이고, PKI와 같은 표준 인증서 형식과 인증 방식을 사용하는 경우에 전역적인 인증 방식을 제공할 수 있다. 802.15.3과 Open Cable 같은 경우, X.509 인증서를 사용하기 때문에 CA구성에 따라서 전역적으로 사용할 수 있는 여지가 있으며, UPnP는 SPKI인증서 형식을 사용하여 기본적으로는 지역적으로 사용하지만 때에 따라서 확장하여 전역적으로 사용할 수도 있다. DTCP는 고유의 인증서 형식을 사용하여 호환 디바이스 간의 인증에만 사용할 수 있다.이러한 인증서를 기반으로한 공개키 방식은 대칭키 방식에 비해 유용한 많은 이점을 제공하지만 기존의 방식을 그대로 향후의 상황인지 홈 서비스에 적용하기에는 많은 문제점이 존재한다.

PKI 인증 기술을 따르는 경우에는 전역적인 인증 구조를 갖으며 Key와 이름을 연결해 주는 인증서를 사용한다. 그렇기 때문에 각 기기가 인증서를 발급받았다고 하더라도 각 서비스에 각 기기의 이름을 등록해 주어야만 인증과정이 수행될 수 있다. 이는 댁내의 기기가 많아 질 수록 사용자의 불편이 증가하게 되는 단점을 가지고 있다. 이것은 자동화 서비스, 서비스 로밍 그리고 타도메인 서비스를 이용하는 모든 경우에 동일한 문제로 적용될 수 있다. 자동화 서비스의 경우 각 기기들과 외부의 서비스를 제공하는 서버들 사이의 등록이 필요하며, 서비스 로밍의 경우 서비스 로밍에 참여하는 모든 기기들 사이의 등록과정이 필요하다. 타 도메인 서비스를 이용하는 경우도 마찬가지로 타도메인에 기기의 이름을 등록하는 과정이 필요하다.

UPnP에서 사용하는 SPKI 인증서 [12] 형태와 같이 지역적인 인증방식을 사용하는 경우 PKI인증 방식의 문제를 일부 해결할 수 있다. 예를 들면, 각 집에서 CA를 두고 각 기기에 대한 인증서를 발급하는 경우를 생각해 보면, 서비스 로밍 같은 경우 각 디바이스가 타 디바이스의 인증서의 발급자가 동일한 도메인의 CA라는 것만 확인함으로써 타 디바이스의 이름의 등록 여부와 관계없이 해당 디바이스를 적합한 디바이스로 인증할 수 있다. 하지만, UPnP의 보안기술에서는 타 도메인의 서비스와 연결할 경우에 대해서는 고려하고 있지 않으며, SPKI역시 기본적으로 지역적인 인증 및 권한 확인을 위해 만들어진 인증서 이므로 타 도메인과의 연동을 위해서는 여러 가지 추가적인 기술들이 필요하다.

앞서 살펴본 봐와 같이, 기존의 홈네트워크의 네트워크 기술과, 미들웨어에서 제공하는 디바이스 인증 방식은 향 후의 상황인지 홈 서비스에 적용하기에는 여러 가지 부적합한 점이 있다. 그렇기 때문에 새로운 디바이스 인증 방식의 개발이 필요하다. 다음 장에서는 새로운 디바이스 인증 방식이 고려해야할 요구사항들에 대해 분석한다.

4. 디바이스 인증 요구사항

본 장에서는 상황인지 홈 서비스에서의 디바이스 인증을 위해 다음의 3가지 요구사항을 제안한다.

Req 1. 디바이스가 사용자를 대행할 수 있어야 한다.

상황인지 서비스는 기존에 사용자가 스스로 서비스를 선택하고 요청하는 서비스 방식에서 디바이스가 사용자를 대행하여 스스로 판단하여 서비스를 제공하는 방식이다. 그렇기 때문에 디바이스 인증은 각 디바이스가 어떤 사용자의 대행자인가를 판단할 수 있는 기능이 필요하다.

Req 2. 사용자의 개입을 최소화 해야 한다.

디바이스를 설정하고 사용하는 사용자는 대부분이 보안에 대해서 알지 못하는 비전문가들이다 그렇기 때문에 디바이스 인증 설정시에 사용자의 개입이 많아지면 많아질 수록 많은 허점이 노출될 가능성이 있이 있고, 사용자에게 큰 불편을 가져 올 수 있다. 앞서 설명한 비밀키 공유 방식과 같이 각 디바이스 간 키를 공유하는 방법은 디바이스가 N개인 경우 키 설정 횟수는 $O(N^2)$ 이 된다. 사용자의 안전과 편리를 위해서 사용자의 개입을 최소화 하면서 필요한 인증을 수행할 수 있는 기술의 개발이 필요하다.

Req 3. 디바이스에게 필요한 최소한의 권한을 설정해야 한다.

디바이스는 항상 도난 및 분실의 위험을 가지고 있다. 그렇기 때문에 모든 디바이스가 사용자가 가진 모든 권한을 행사하게 된다면 하나의 디바이스의 분실 또는 도난으로 인해 사용자의 비밀과 권한이 모두 침해받아 큰 피해로 이어질 수 있다. 그렇기 때문에 각 디바이스는 사용자가 가진 권한 중 꼭 필요한 권한만을 부여 받도

록 인증하는 기술이 필요하다.

Req 4. 디바이스가 분실 또는 도난 된 경우 불법적인 사용을 방지할 수 있어야 한다.

앞에서 이야기 했듯이, 디바이스는 항상 분실과 도난의 위험을 가지고 있다. 이러한 디바이스의 불법적인 사용은 경우에 따라서 사용자에게 큰 피해를 가져 올 수 있다. 그렇기 때문에 디바이스가 분실 또는 도난 된 경우 디바이스에게 허가된 권한을 금지할 수 있는 기능이 필요하다.

Req 5. 디바이스의 소유권을 변경하기 위한 적합한 절차가 있어야 한다.

디바이스는 타 사용자에게 판매되거나 양도되는 경우가 있을 수 있다. 이러한 경우 이 디바이스가 대행하는 사용자 또한 변경되어야 한다. 또한, 디바이스를 불법적으로 취득한 사람은 소유권 변경을 할 수 없도록 제한하는 기능이 있어야 한다.

Req 6. 다양한 디바이스를 고려해야 한다.

유비쿼터스 환경에서는 다양한 종류의 디바이스를 통해 서비스를 제공 받을 수 있다. 디바이스들 중에는 컴퓨팅 파워의 제약으로 인해 공개키 방식을 사용하지 못하는 경우도 있을 수 있다. 이러한 디바이스의 다양성을 고려하여 인증 메커니즘을 설계해야 한다.

Req 7. 타 도메인의 서비스와 연동할 수 있어야 한다.

USN과 결합되어 타 토메인의 서비스를 이용하는 경우에도 사용자의 별다른 개입 없이 기존의 홈에서 사용하던 서비스와 동일한 방식으로 타 도메인의 서비스를 제공받을 수 있어야 한다.

5. 결론

USN과 결합된 홈네트워크에서의 상황인지 기반의 서비스를 위해서는 사용자의 편의와 안전을 위해 디바이스 인증이 필수적인 요소이다. 하지만 기존의 디바이스 인증 기술들은 대부분 네트워크 사용 인증, 호환 디바이스 인증, 지역적 인증 등에 국한되어 유비쿼터스 환경에서의 상황인지 서비스에 필요한 인증 기능을 제공하는 데에는 많은 제약점들이 있다. 이러한 제약점들을 해결하기 위해서는 새로운 디바이스 인증 방식이 필요하며, 이러한 디바이스 인증 방식은 그 특성에 따라서 기존의 인증 방식과 다른 다양한 요구사항들이 존재한다. 본 논문에서는 기존의 디바이스 인증방식과 그 문제점에 대해 분석하고, 새로운 디바이스 인증 방식에서 필요한 7가지 요구사항들을 제안하였다. 향 후, 이러한 요구사항을 만족할 수 있는 디바이스 인증 프로토콜에 대한 개발이 필요할 것이다.

참고 문헌

[1] Sven Meyer, Andry, A Survey of Research on Context-Aware Homes, ACSW frontiers 2003, Volume 21, pp 159 - 168, 2003

[2] MIT Media Lab, Things That ThinkConsortium, http://ttt.media.mit.edu

[3] Bluetooth Specification version 2.0, http://www.bluetooth.com

[4] Zhihua Tao, et al, Piconet Security in IEEE 802.15.3 WPAN, IEEE WCNC, 2005

[5] Zigbee Specification version 1.0, http://www.zigbee.org

[6] IEEE 802.11i/D10.0, 2004.

[7] Echonet Specification, http://www.echonet.gr.jp

[8] Introduction to the LonWorks System version 1.0, ECHELON Corporation.

[9] C. Ellison, *UPnP Security Ceremonies Version 1.0*, UPnP Forum, 2003

[10] OpenCable System Security Specification, http://www.cablelabs.com/

[11] Digital Transmission Content Protection Specification Volume 1, http://www.dtcp.com

[12] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, and T. Ylonen, SPKI Certificate Theory, RFC2693, Sep. 1999.