情 報 保 護 學 會 誌
第18卷 第5號, 2008. 10

디바이스 인증 및 인가에 기반한 유비쿼터스 홈네트워크 프라이버시 대책

이 선 영*, 임 강 빈**, 배 광 진***, 정 태 영****, 한 종 욱*****

요 약

유비쿼터스 홈네트워크에서는 다양한 디바이스를 이용하여 복수의 도메인을 오가며 서비스를 제공하거나 제공받을 수 있을 것으로 기대되는데 이때 디바이스는 반드시 정당한 디바이스여야 하며 이를 실현하기 위하여 인증서를 사용하는 디바이스 인증 기술이 제안되었다. 그리고, 계산 능력이 작은 디바이스를 인증하기 위한 방법으로서 대칭키 암호 기술에 기반을 둔 디바이스 인가 방법을 함께 사용함으로써 계산 능력이 다른 다양한 디바이스들을 인증하는 방법이 제안되었다. 이들 방법의 공통성은 사용자의 개인 정보 유출을 피하기 위하여 사용자 정보를 사용하지 않고 디바이스 고유의 정보만을 사용하여 인증한다는데 있다. 이러한 디바이스 인증/인가 방법을 홈네트워크에 사용하였을 경우 사용자의 개인 정보는 보호되는지 확인할 필요가 있다. 본 논문에서는 기존에 제안된 유비쿼터스 홈네트워크를 위한 디바이스 인증/인가 기술을 분석하여 개인 정보의 유출에 관한 문제점을 도출하고 그에 대한 대응 방법을 제안하였다.

Ⅰ. 서 론

홈네트워크는 현재 가장 주목받고 있는 차세대 IT 기술로써 댁내의 정보가전기기에 대한 제어, 관리, 통합 및 연동을 바탕으로 인터넷과 결합하여 생활의 편리함을 극대화하기 위한 기술의 집합체로서 현재는 광대역 통신, 무선 인터넷, 센서 기술 등과 결합하여 유비쿼터스 컴퓨팅 환경으로 확장되어 가고 있다.[1][2]

홈네트워크는 가정 내의 정보가전기기가 네트워크로 연결되어 기기, 시간, 장소에 구애받지 않고 서비스가 제공되는 미래 환경인 디지털홈을 구성하는 핵심요소로서, 홈 내부에 위치한 어떤 기기 간에도 네트워크가 가능하고 원격지로부터도 네트워크를 통하여 기기의 제어 및 관리가 가능한 통신 서비스 환경을 구축하기 위한 것이다. 홈네트워크 산업을 활성화시키기 위해서는 이기종, 유무선 네트워크 망간의 상호 연동 기술뿐 아니라 관리적 측면에서의 기술과 통합 측면에서의 기술 등이 필요하고, 또한 정보의 처리, 전달 및 저장을 안전하게 하기 위해서는 특히 보안 기술이 절실하게 요구된다. 언제 어디서나 컴퓨팅이 가능한 유비쿼터스 컴퓨팅 환경에서는 사이버 공격뿐 아니라 홈네트워크 및 홈디바이스의 취약성을 이용하여 댁내 홈네트워크에 불법적으로 접근할 수 있으므로 홈디바이스에 대한 안전성을 확인하여 유효한 홈디바이스만 홈네트워크에 접근할 수 있어야 한다. 불법적인 서비스의 접근을 차단하기 위해 사용자 인증기술과 유효한 디바이스에게만 서비스를 제공하는 디바이스 인증기술이 사용되고 있다[3][4][5]. 유비쿼터스 홈네트워크 환경에서는 댁내의 홈디바이스들이 유/무선 네트워크로 연결되어 하나의 서비스 도메인 내에서 서비스를 제공할 뿐 아니라, 홈디바이스가 다양한 서비스 도메인으로 이동하며 서비스를 제공하게 될 것이다. 이와 같은 홈네트워크 기술의 진화에 따라 유비쿼터

본 연구는 한국전자통신연구원 정보통신연구개발사업의 위탁연구과제(7010-2007-0038)로 수행한 연구 결과임.

* 순천향대학교 정보보호학과 (sunlee@sch.ac.kr)
** 순천향대학교 정보보호학과 (yim@sch.ac.kr)
*** 순천향대학교 정보보호학과 (kao1009@nate.com)
**** 순천향대학교 정보보호학과 (jtyworld@nate.com)
***** 한국전자통신연구원

스 환경에서 안전한 이동과 서비스를 제공할 수 있도록 경량화된 홈디바이스 인증/인가 기술이 필요하다. 홈디바이스 인증과 인가 기술은 멀티 홈 도메인에서 디바이스의 인증을 가능하게 하고 디바이스 인증 시 사용자의 개입을 최소화 할 수 있다[6][7]. 이 방법의 목적은 사용자의 개입을 최소화하여 프라이버시를 보호하고자 하는 것이다. 본 논문에서는 이미 제안되어 있는 홈 디바이스 인증 및 인가 기술을 분석하여 디바이스 인증/인가만으로 개인 정보가 유출되지 않는지 확인하고, 개인 정보가 유출될 수 있는 상황 및 시나리오를 도출하여 그에 대한 프라이버시 대책 방안을 제안한다.

본 논문은 제2장 유비쿼터스 홈네트워크, 제3장 홈디바이스 인증/인가 기술, 제4장 홈디바이스 인증/인가 기술에 대한 프라이버시 대책, 제5장 결론으로 구성된다.

Ⅱ. 유비쿼터스 홈네트워크

유비쿼터스 홈네트워크 기술은 댁내외에서 언제 어디서나 사람과 홈디바이스가 연결되어 네트워크, 단말 및 콘텐츠를 사용자가 의식하지 않고 사용할 수 있는 차세대 홈 서비스이다. 홈네트워크는 인터넷 망을 통한 외부 접근망과 다양한 장치들과 연결된 홈서버, 홈게이트웨이 등 댁내망으로 구성된다. 접근망은 기존에 사용하던 네트워크 망으로서 주로 인터넷 망이나 케이블, 광전송 장치 및 위성 등을 통하여 홈네트워크로 접근한다. 댁내망은 유선과 무선으로 구분되며 유선망으로는 Ethernet, HomePNA, PLC(Power Line Carrier), IEEE1394, USB(Universal Serial Interface)등이 있으며, 무선망으로는 홈RF(Home Radio Frequency), 블루투스(Bluetooth), IrDA(Infared Data Association), 무선 LAN (Local Area Network), UWB(Ultra Wideband), IEEE 802.11x 등이 있다.

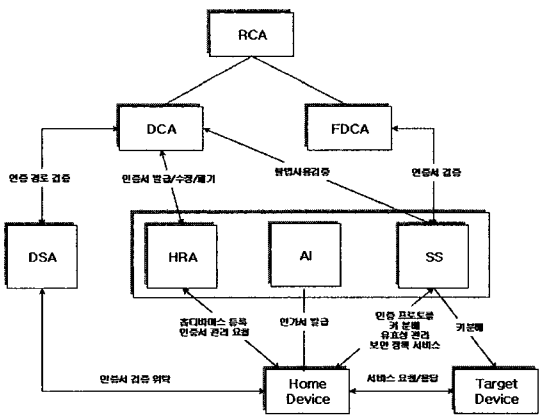
홈네트워크 기술은 크게 홈플랫폼 기술, 유/무선 홈네트워킹 기술, 정보가전 기술, 지능형 미들웨어 기술로 분류될 수 있다[8].

이러한 기술을 기반으로 한 유비쿼터스 홈네트워크 서비스의 기본 조건은 크게 세가지로 구분할 수 있다. 첫째, 디바이스의 존재를 인식하지 않으면서도 컴퓨터를 사용할 수 있도록 컴퓨터를 자연스럽게 주변 상황에 파고 들게 하여야 한다. 둘째, 사용자 개입을 최소화하여야 한다. 사용자 개입을 최소화하기 위해서는 사용자가 디바이스의 사용이나 네트워크의 존재에 주의를 기울이지 않는 기술을 구현하여야 한다. 셋째, 디바이스 협업을 통한 서비스를 제공하여야 한다.

Ⅲ. 홈디바이스 인증/인가 기술

홈서버 중심의 중앙집중형 인증/인가 시스템은 홈서버의 부하로 인하여 다양한 사용자와 디바이스를 포함하는 유비쿼터스 환경에서 사용하기에는 많은 문제점을 내포하고 있다. 유비쿼터스 홈서비스 환경에서 안전한 서비스를 제공하기 위해서는 비IT 사용자를 포함한 다양한 사용자와 경량화 된 디바이스를 고려한 보안 기술로서 디바이스 인증/인가 기술이 필요하다. 디바이스 인증/인가 기술이란 사용자가 개입하지 않고 디바이스들 간에서 이루어지는 인증 및 인가를 의미한다. 홈네트워크 서비스의 진화 방향을 고려하면 홈네트워크 댁외에서는 홈디바이스 인증서를, 댁내에서는 홈디바이스 인가서를 사용하는 방법이 제안되고 있다[5][6]. 홈디바이스 인증에서는 인증서를 사용하고, 홈디바이스 인가 서비스는 대칭키 기반의 인가서를 이용하여 계산 능력이 작은 디바이스를 통하여 서비스를 제공할 수 있도록 하고 있다.

[그림 1]은 인증/인가 기능들이 홈네트워크 내에서 동작하는 과정을 나타낸 것이다[6]. 디바이스 인증서 발급을 위한 등록은 댁내에 위치한 HRA(Home Registration Authority)를 통해 이루어지며, 댁내 서비스에 대한 인가서는 AI(Authoricate Issuer)를 통해 직접 발급된다. HRA는 댁외에 위치한 인증기관에 디바이스 인증서 발급 요청을 위한 등록 기관으로서의 역할을 하며, DCA (Domain CA)와 연계하여 홈디바이스에 인증서를 전



〔그림 1〕 홈네트워크 인증/인가 구성도

달, 설치하도록 하는 역할까지 담당한다. RA(Register Authority), AI, SS(Security Server) 등은 일반적으로 홈서버에 탑재되며, 다른 시스템에서 독립적으로 동작이 가능하다.

사용자 편리성을 위해 HRA를 두어 사용자 개입 없이 홈디바이스 관련 인증서 발급 절차를 수행하며, 다른 홈이나 타 도메인으로 이동시 자동적으로 디바이스 인증 절차를 수행할 수 있도록 SS를 둔다. 또한 DSA (Deligate Security Agent)를 두어 인증서 검증 절차를 자동적으로 위탁함으로써 저성능 디바이스를 위한 절차도 포함하고 있다.

3.1 유비쿼터스 환경에서의 홈디바이스 인증

홈네트워크에서 디바이스 인증에 대한 인증체계는 크게 외부 인증기관이 홈디바이스 인증서를 발급하고 관리하는 체계와 홈 내에 하나의 인증기관을 두고 홈 내에서만 사용가능한 인증서를 발급하고 관리하는 체계로 나눌 수 있다. 외부 인증기관에서 인증서를 발급하고 관리하는 체계는 인증 기관을 댁외에 두고 이 인증 기관은 자신이 발행한 인증서에 대한 검증 및 관리와 책임을 진다. 그리고 홈 내에 RA의 기능을 하는 디바이스인 HRA를 두어 홈디바이스들에 대한 인증서의 발급을 돕는다. HRA는 새로운 홈디바이스가 등록되면 이 디바이스에 대한 확인 작업을 거쳐 외부 인증 기관에 홈디바이스 인증서 발급을 요청한다. 외부 인증 기관이 해당 홈디바이스의 인증서를 발행하여 HRA에 배포하면 HRA는 이를 받아서 해당 홈디바이스에 인증서를 전송한다.

홈 내부에서의 인증서 발급과정은 홈 내부에 별도의 인증 기관을 두고 홈 내부 및 외부에 존재하는 홈디바이스에게 인증서를 발급한다. 이 경우 댁내 인증기관은 외부 인증 기관으로부터 발급받은 디바이스 인증서 이외에 홈디바이스용 인증서 발급을 위한 인증서를 소유하고 있어야 하며 댁내의 인증 기관은 홈 내부 또는 외부의 디바이스들에게 홈디바이스용 인증서를 발급하고, 해당 인증서에 대한 검증 및 관리를 수행한다.

3.2 유비쿼터스 환경에서의 홈디바이스 인가

3.2.1 홈디바이스 인가 모델

홈디바이스 인가 모델은 인가 서버, 홈디바이스, 홈서비스로 구성된다. 인가 서버는 인가 정책을 관리하고 인가서를 발급하며, 홈디바이스는 인가 서버로부터 발급 받은 인가서를 통해서 홈서비스에 접근한다. 홈서비스는 인가서를 검증하여 서비스를 제공한다. 이 모델은 인가 서버와의 연동 없이 디바이스들이 독자적으로 인가를 수행할 수 있어 대규모 네트워크에서도 효율적으로 적용할 수 있고, 각 홈디바이스는 한번의 인가서 발급만으로 서비스에 여러 번 접근할 수 있다. 또한, 인가서의 안전성 보장을 위해 대칭키 암호를 사용함으로써 연산을 줄이고 replay 공격에 대응할 수 있다. 홈네트워크를 위한 홈디바이스 키 관리 시스템은 마스터 키와 그룹키로 나누어 구성된다. 마스터 키는 초기 홈디바이스에 제공되며 디바이스 비밀 정보와 그룹키를 보호한다. 그룹키는 서비스를 제공하는 홈디바이스들의 그룹에 대해 동일한 그룹키를 제공함으로써, 서비스를 이용하고자 하는 디바이스의 인가서를 보호하고 검증한다.

홈디바이스가 홈 서비스를 이용하기 위해서는 인증을 받고 서비스를 제공하는 디바이스에 대해 사용 권한이 설정되어 있는 인가서를 소유하고 있어야 한다. 인가서버는 인가서에 디바이스 ID 정보, 인가서 유효 기간, 접근 제어 정보를 기본적으로 포함하여 서비스를 요청하는 디바이스에 발급하며 그룹키로 인가서를 암호화하여 전송한다. 또한 홈디바이스와 홈서비스 간의 안전한 세션을 위해서 인가 서버가 설정한 세션키도 동시에 전송되며, 발급되는 세션키는 인가 서버와 홈서비스만이 알고 있어 수정이 불가능하여 제3자에 의한 불법 사용을 방지할 수 있다.

인가서를 발급받은 디바이스는 홈서비스를 받기 위해 홈서비스에 접근 요청 메시지를 전송하고 그룹키로 암호화된 자신의 인가서를 보낸다. 그룹키로 암호화된 인가서를 받은 홈서비스는 자신이 속한 그룹의 키로 인가서를 복호하여 인가서의 접근 권한을 열어 홈디바이스가 자신의 기능과 서비스에 접근하여 사용할 수 있도록 허가한다. 홈디바이스가 발급받는 인가서는 해당 홈도메인 내에서만 유효하며 유효 기간도 짧게 설정된다[6].

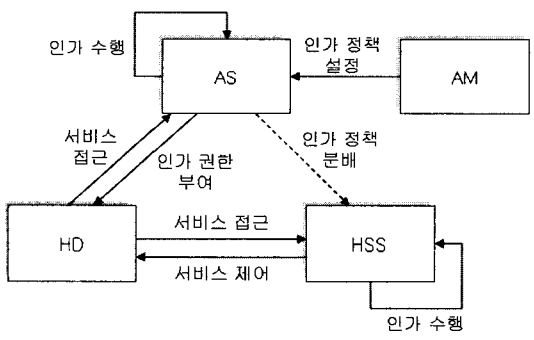
3.2.2 홈디바이스 인가

홈디바이스 인가서는 내, 외부의 불법 접근과 서비스 사용을 방지함으로써 자원을 보호하고 개인 정보 유출을 방지하며 침입 사고가 발생했을 경우 피해를 최소화할 수 있는 보안 기능을 제공한다. 인가서를 구성하는데

있어서 기본적으로 요구되는 사항은 접근 주체 식별 정보와 접근제어 정보, 발급 개체 정보를 포함하여야 하며, 인가서를 사용하는데 있어 안전성을 보장해야 한다. 또한 공개된 암호 알고리즘을 사용하여야 하며 저성능의 홈디바이스에서도 유용하게 사용될 수 있어야 하며, 유효기간을 제공하여야 한다.

홈디바이스 인가를 수행하기 위한 구성은 홈서비스를 이용하고자 하는 HD(Home Device)와 홈네트워크 서비스를 제공하고 인가를 수행하는 HSS(Home Service Server), 인가 정책을 저장하고 분배하고 인가를 수행하는 AS(Authorization Server) 및 인가 정책을 관리하기 위한 AM(Authorization Manager)로 구성된다.

홈디바이스 인가를 위하여 디바이스를 등록하고 각 디바이스에게 인가서를 만들어 전송할 인가 서버에 인가 정책을 설정한다. 인가 정책 설정을 마친 후 홈디바이스에게 권한을 부여하기 위하여 인가 서버에서 인가서를 생성하여 암호화한 후 전송한다. 서비스를 제공하는 홈서비스 서버에게는 인가서를 복호할 수 있도록 인가 서버에서 키를 전송하고 인가서에서 접근 권한에 관한 필드를 참조하여 자신의 서비스를 사용할 수 있도록 허가한다. [그림 2]는 홈디바이스의 인가 과정을 나타낸 것이다.



〔그림 2〕 홈디바이스 인가 구성도

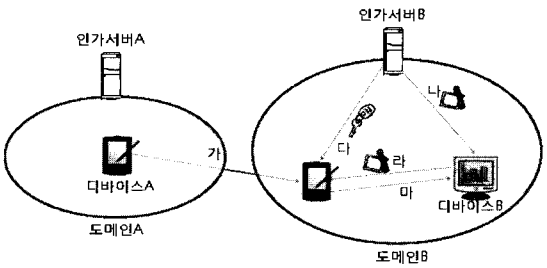
Ⅳ. 홈디바이스 인증/인가에 대한 프라이버시 문제 및 대책

3장에서 홈디바이스 인증/인가 기술에 대하여 기술하였으나 이들 기술만으로 사용자의 개인 정보를 보호할 수 있는지 살펴보고 홈디바이스 인증/인가에서 발생할 수 있는 프라이버시 문제를 고찰하고 그 대책을 제안한다.

4.1 게스트 디바이스 인가에 대한 문제점 및 대응 방안

서비스를 제공받기 원하는 디바이스는 서비스를 제공하는 디바이스를 이용하기 위하여 인가서를 사용한다. 인가서는 인가 관리자에 의해 인가서버에 설정된 내용을 바탕으로 만들어 지며 서비스를 제공받는 디바이스와 서비스를 제공하는 디바이스에서 사용할 수 있는 권한이 설정되어 있다.

홈디바이스 인가 시스템에서 다른 홈 도메인으로부터 온 게스트 디바이스가 서비스를 제공 받을 경우, 인가 시스템은 문제없이 작동한다. 그러나, 게스트 디바이스가 서비스를 제공해야 할 경우 게스트 디바이스는 방문한 홈 도메인의 인가 서버에 등록되고, 이때 인가 서버가 자신의 홈 도메인 내에 존재하는 디바이스에게 게스트 디바이스의 모든 것을 사용하도록 인가서 권한을 설정 할 수 있다. 이 경우 홈 도메인의 디바이스는 게스트 디바이스의 기능을 서비스 받을 수 있을 뿐 아니라 게스트 디바이스에 기록된 문서, 사진, 영상 등 사용자의 정보를 읽거나 복사, 수정할 수 있게 되며 이로 인한 프라이버시 침해 문제가 발생할 수 있다. [그림 3]은 게스트 디바이스 인가에 대한 문제점을 도식화한 것이다.



〔그림 3〕 게스트 디바이스 인가

가. 디바이스 A가 도메인 B로 이동 한다.
나. 디바이스 A가 인가 서버 B에 등록된 후, 인가 서버 B는 설정된 그룹에 맞는 인가서를 작성한다. 이때 서비스를 제공하는 게스트 디바이스의 모든 것을 사용할 수 있도록 인가서에 권한 설정하여 디바이스B에게 전송한다.
다. 인가 서버 B가 디바이스 A에게 인가서를 복호할 수 있는 그룹키를 전송한다.
라. 디바이스 B가 디바이스 A에게 인가서를 전송하면서 서비스를 요청한다.
마. 디바이스 A의 모든 기능을 디바이스 B가 사용할 수 있도록 허가 된다.

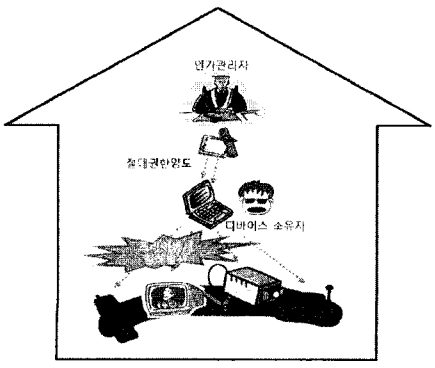
이처럼 타 도메인으로부터 이동해온 디바이스가 서비스를 제공해야 하는 경우, 도메인의 인가 관리자가 위

의 시나리오처럼 인가서에 권한 설정을 한다면, 이동해 온 디바이스의 모든 권한 및 기능에 접근이 가능하여 이동해온 디바이스 안에 존재하는 데이터를 유출시켜 프라이버시를 침해할 수 있다. 즉, 게스트 디바이스 소유자의 동의 없이 홈디바이스 인가 관리자가 인가서에 권한 설정을 하고, 그 인가서를 가진 홈디바이스가 게스트 디바이스에 접근하는 데에 문제가 있다. 이 문제점에 대응하기 위한 방안으로는 도메인을 이동한 디바이스, 즉 게스트 디바이스에 대해서는 반드시 소유자에 대한 인증을 하여야 한다. 홈 도메인 디바이스가 게스트 디바이스에 서비스를 요청할 때 게스트 디바이스의 소유자에게 인증을 요구하고, 디바이스 소유자의 동의가 이루어지고 나면 게스트 디바이스에 대한 권한 정책에 따라 권한이 결정된다.

4.2 인가 관리자의 절대 권한으로 인한 문제점 및 대응 방안

홈네트워크에서 인가 관리자의 권한은 절대적이다. 인가 관리자는 디바이스에 모든 서비스를 이용할 수 있는 절대 권한을 가진 인가서를 발급할 수 있다. 이 인가서가 삽입된 디바이스는 절대 권한을 갖게 되며 결국 디바이스를 소유한 누구라도 모든 서비스를 이용할 수 있는 권한을 갖게 된다. [그림 4]는 인가 관리자의 권한이 디바이스에 인가되면서 발생할 수 있는 시나리오이다.

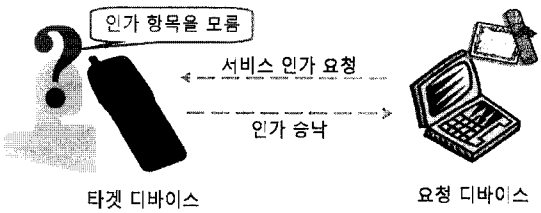
이 문제는 위에서 언급하였던 게스트 디바이스 인가에 대한 문제와도 관계가 있다. 인가관리자의 정책에 따라 인가서가 발급되고, 인가서가 다양한 디바이스로 양도 되면서 디바이스를 소유한 악의적인 사용자로 인해 프라이버시 침해가 발생할 수 있다. 이 문제를 해결하기 위하여 인가 관리자의 절대 권한을 축소시킬 필요가 있다. 인가 정책에 따른 인가서를 발급할 때 프라이버시와 직간접적으로 관련이 되는 항목의 사용 및 접근에 대해서는 해당 디바이스의 소유자 동의를 받아야 한다. 게스트 디바이스에 대한 소유자 동의는 반드시 필요하며, 같은 홈 도메인의 디바이스라도 홈 구성원이 각자의 디바이스를 소유하고 있을 경우에는 소유자 동의가 필요하다. 소유자 동의는 소유자 인증으로 가능하며 인증에 대한 방법은 기존의 사용자 인증 방법들을 응용할 수 있다.



[그림 4] 인가관리자의 인가 권한으로 인한 프라이버시 침해

4.3 허가된 인가 정보에 대한 은닉 문제 및 대응 방안

서비스 요청 디바이스가 인가서를 가지고 타겟 디바이스에 서비스를 요청할 때 타겟 디바이스의 소유자는 서비스 요청 디바이스가 어떤 인가정책을 가지고 어떤 서비스를 이용할 수 있는지 알 수 없어 타겟 디바이스의 소유자도 모르는 사이에 타겟 소유자의 개인 정보가 다른 디바이스로 유출될 수 있다. [그림 5]는 승낙된 인가 항목에 대한 은닉의 문제점을 보여주고 있다.



[그림 5] 승낙된 인가 항목에 대한 은닉

타겟 디바이스 소유자가 요청 디바이스의 인가 정책 사용할 수 있는 서비스의 종류 등에 대한 인가 정보를 모르면 요청 디바이스가 접근하였을 때 타겟 디바이스가 가지고 있는 어떤 정보에 접근 가능한지 알 수 없어 프라이버시 침해가 발생하더라도 인지하지 못할 가능성이 있다. 이 문제는 요청 디바이스가 인가서를 가지고 접근할 때마다 타겟 디바이스가 요청 디바이스에 제공할 수 있는 서비스 및 기능 등을 표시하여 사용자에게 알려주는 방법으로 해결 가능하다.

4.4 다수의 그룹키를 복호할 경우 생기는 문제점 및 대응 방안

홈디바이스 인가 시스템은 디바이스 인가를 그룹별

로 관리하며 인가서를 그룹키로 암호화하여 같은 그룹에 해당하는 디바이스 간에 통신이 가능하도록 한다. 그러므로 소규모의 그룹이 많이 생기거나 특정 디바이스가 복수의 그룹에 포함되어 있을 경우 디바이스가 다수의 그룹키를 소유하게 되며, 서비스를 요청하기 위하여 이 디바이스로 인가서를 보내면 소유하고 있는 모든 키를 대입하여 인가서를 복호한다. 이 경우, 컴퓨팅 파워가 부족한 디바이스에서는 복호하는 시간이 길어지거나 많은 부하가 발생할 수 있다. 이 문제를 해결하기 위하여 인가서를 그룹키로 암호화 하여 전송할 때 디바이스를 구별할 수 있는 고유의 값을 암호화된 인가서와 함께 보내어 디바이스를 판별할 수 있도록 하면 복호를 위하여 모든 키를 대입하여 생기는 부하 문제를 해결할 수 있다.

V. 결 론

홈네트워크는 향후 발전 가능성이 매우 높은 IT 융합 서비스 중의 하나로서 홈엔터테인먼트, 교육, 의료 등 다양한 분야를 포함하고 있다. 홈네트워크의 발달된 형태인 유비쿼터스 홈네트워크에서는 다양한 디바이스를 이용하여 다양한 서비스를 제공받을 수 있고, 자신의 집뿐만 아니라 다른 사람의 집에서도 서비스를 제공 받을 수 있을 것으로 예상된다. 그러나 여러 도메인에서 디바이스를 사용하기 위해서는 올바른 디바이스로 인증된 기기에 대하여 서비스를 제공하거나 제공받을 수 있도록 하여야만 개인정보를 보호할 수 있다. 인증/인가가 이루어지지 않을 경우 디바이스에 저장되어 있는 사진 및 문서 등과 같은 개인의 정보가 사용자가 인식하지 못하는 사이에 유출될 수 있기 때문이다. 홈디바이스 인증/인가 서비스 모델이 제안되면서 기존의 중앙에서 인증/인가를 처리하던 구조에서 인가의 중심이 디바이스로 이동되어 사용자의 개입을 최소화할 수 있게 되었다. 또한, 각 디바이스가 소유하고 있는 암호화된 인가서와 그룹키를 이용하여 디바이스 간의 접근 권한을 설정하여 부하를 분산 시켜 서비스의 품질을 향상시킬 수 있게 되었다. 그러나 사용자의 개입 없이 이루어지는 인증/인가 기술이 안전한지 검토할 필요가 있다. 본 논문에서는 홈디바이스 인증/인가 서비스의 프라이버시 취약점을 분석하여 인가 정책 관리자가 인가 서버의 정책을 악의적으로 설정 하여 게스트 디바이스의 모든 권한을 사용하도록 허가할 수 있다는 문제점을 발견하였고 그에 대한 대응 방안으로서 게스트 디바이스 소유자의 인증을 받은 후 서비스를 제공하도록 하는 방법을 제안하였다. 또, 다수의 그룹키를 가지는 디바이스의 경우 모든 그룹키를 대입해서 인가서를 복호함으로서 많은 부하가 발생할 수 있고, 이 점을 이용하여 개인 정보가 유출될 수 있음을 밝혔고, 이에 대한 대응방안으로서 디바이스의 고유값을 이용하여 디바이스를 판별하고 그에 따른 그룹키를 빠르게 선택하도록 하는 방법을 제안하였다. 요약하면, 기존에 유비쿼터스 홈네트워크를 위해 제안되어 있는 디바이스 인증/인가 방법을 이용하였을 경우 디바이스 인증/인가만으로는 유비쿼터스 홈네트워크 내에서 개인의 프라이버시를 보호하는데 한계가 있으므로 소유자의 인증이라는 사용자 인증 기술이 병행되어야만 안전한 홈네트워크 서비스가 가능하다고 결론내릴 수 있다.

참고문헌

[1] 서운석, 신순자, 구자동, 임진수, "유비쿼터스 컴퓨팅 환경에서 보안 및 인증 서비스 방향 연구", 한국전산원, 2004년 10월.

[2] 김정태, 범민준, 박혜경, 백의현, "유비쿼터스 홈 서버 보안 요구사항 및 구현 방안", 전자통신동향분석, 제20권 제2호, 2005년 4월.

[3] 고훈, "홈네트워크 취약점 분석 및 인증 분석", 한국정보보호학회지, 제16권 제6호, pp. 19-32, 2006년 12월.

[4] 황지온, 엄윤식, 김용, 박세용, "홈네트워크 환경에서의 지식기반 서비스를 위한 보안 및 정책 연구", 한국정보보호학회지, 제16권 제6호, pp. 19-32, 2006년 12월.

[5] 한종욱, 이덕규, 정교일, "홈디바이스 인증/인가 기술 동향", 한국정보보호학회지, 제16권 제6호, pp. 33-41, 2006년 12월.

[6] 정보보호연구단 홈네트워크보안연구팀, "유비쿼터스 홈디바이스 인증/인가 가술", 한국전자통신연구원, 2006년 11월.

[7] Jin-Bum Hwang, Hyung-kyu Lee, Jong-Wook Han, "Efficient and User Friendly Inter-domain Device Authentication/Access Control for Home Networks", EUC 2006, pp.131-140, 2006. 8.

[8] 이선영 외, "홈디바이스 인증/인가 서비스에서의 프라이버시 대책 연구", 한국전자통신연구원, 2007년 11월.

〈著者紹介〉

이 선 영 (Sun-Young Lee)
종신회원

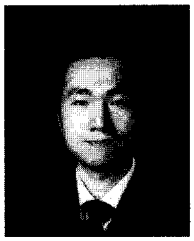
1993년 : 부경대학교 전자계산학과 이학사
1995년 : 부경대학교 전자계산학과 이학석사
2001년 : 일본 동경대학교 전자정보공학과 공학박사
2004년~현재 : 순천향대학교 정보보호학과 교수
<관심분야> 암호이론, 정보이론, DRM, 정보보호

임 강 빈 (Kangbin Yim)
종신회원

1992년 2월 : 아주대학교 전자공학과 학사
1994년 2월 : 아주대학교 전자공학과 석사
2001년 2월 : 아주대학교 전자공학과 박사
2003년 3월~현재 : 순천향대학교 정보보호학과 교수
2005년 3월~현재 : 한국정보보호학회 이사
<관심분야> 시스템보안, 운영체제보안, 임베디드시스템보안, 영상보안

배 광 진 (Kwang-jin Bae)
학생회원

2005년 2월 : 순천향대학교 정보보호학과 학사
2007년 2월 : 순천향대학교 정보보호학과 석사
2007년 3월~현재 : 순천향대학교 정보보호학과 박사과정
<관심분야> 시스템보안, 운영체제보안



정 태 영 (Taeyoung Jeong)
학생회원

2007년 2월 : 순천향대학교 정보보호학과 학사
2007년 3월~현재 : 순천향대학교 정보보호학과 석사과정
<관심분야> 시스템보안, 운영체제보안, 임베디드시스템보안

한 종 욱 (Jong-Wook Han)

1985년 : 광운대학교 공과대학 전자공학과 공학사
1991년 : 광운대학교 전자공학과 공학석사
2001년 : 광운대학교 전자공학과 공학박사
1991년~현재 : 한국전자통신연구원 융합서비스보안연구팀 팀장
<관심분야> 융합보안, 물리보안, Optical Security