情 報 保 護 學 會 誌
第 16 卷 第 6 號, 2006. 12

홈디바이스 인증/인가 기술 동향

한 종 욱*, 이 덕 규*, 정 교 일*

요 약

홈네트워크 기술이 유비쿼터스 홈네트워크로 진화되어 감에 따라 다양한 서비스 도메인에 걸쳐 홈디바이스의 이동이 증가하게 되고 홈디바이스 간의 협업에 의한 새로운 홈서비스가 증가할 것이다. 이러한 유비쿼터스 환경에서는 안전한 홈디바이스의 이동과 seamless한 서비스의 제공을 위해 경량화된 홈디바이스에 적합한 인증/인가 기술이 필요하다. 그러나 현재까지는 유비쿼터스 홈네트워크 환경에 적합한 디바이스 인증 및 인가 기술은 개발된 사례가 없다. 따라서 본고에서는 유비쿼터스 홈네트웨크에서의 홈디바이스 인증/인가 기술을 위한 보안 요구사항을 설명하고, 유비쿼터스 홈네트워크에 적합한 디바이스 인증/인가 개념에 대해 설명한다.

Ⅰ. 서 론

홈네트워크 기술은 통신과 방송 융합, 유비쿼터스 사회로의 빠른 이동 등 IT 전반적인 환경에서 빠른 변화와 함께 사용자의 특성을 고려해야함으로, 다양한 분야의 기술들이 융합되어 IT 분야 통합과 같은 성격을 가지고 있다. 기간통신사업자를 축으로 기간망의 고도화로 시작된 네트워크 인프라는 이제 최후의 실핏줄인 홈네트워크로 발전하고 있으며, 홈네트워크 기술은 유선뿐 아니라 무선 부분에서도 급속한 발전을 이루고 있다. 이러한 홈네트워크가 발전하게 되는 가장 중요한 이유는 인터넷의 급격한 발전으로 이뤄지고 있으며, 현재, 초기에 비해 다양한 서비스는 물론 지능형 서비스를 통해 브로드밴드 서비스가 이뤄지고 있다[1-4].

또한 언제 어디서나 컴퓨팅이 가능한 유비쿼터스 컴퓨팅 사회에서는 개인의 컴퓨팅 환경 의존도가 증가함에 따라 사이버공격뿐 아니라 홈네트워크 및 홈디바이스의 취약성을 이용한 댁내 홈네트워크에 대한 불법적인 접근이 가능함으로 인해, 홈디바이스에 대한 안전성 확인을 통해 유효한 홈디바이스만 홈네트워크에 접근할 수 있어야 한다. 또한 불법적인 서비스의 접근을 차단하기 위해 사용자 인증기술이 사용되고 있으나, 최근 들어 디바이스 인증기능을 추가하여 유효한 디바이스를 통해서만 서비스를 제공 받을 수 있게 하는 한 단계 강화된 보안의 필요성이 제기되고 있으나, 이를 위해 먼저 보안 고려사항을 선행하여 점검해야 한다.

또한 유비쿼터스 홈네트워크로의 진화는 다양한 서비스 도메인에서 홈디바이스 이동이 증가될 것이며, 홈디바이스간의 협업에 의한 새로운 홈서비스가 증가할 것이다. 이와 같은 기술의 진화에 따라 유비쿼터스 환경에서 안전한 이동과 seamless한 서비스를 제공할 수 있도록 경량화된 홈디바이스 인증/인가 기술이 필요하다. 유비쿼터스 홈네트워크 환경에서는 단순한 네트워크 인증이나 미들웨어레벨의 인증만으로 안전하게 홈네트워크가 보호될 수 없기 때문에 유비쿼터스 홈네트워크 디바이스 인증기술 개발이 필요하다. 따라서 홈네트워크 구성 요소들의 여러 가지 사항들을 고려하여, 댁내와 댁외 모두 사용할 수 있도록 인증 및 인가서로써 디바이스 인증 및 인가 기능을 제공하여야 한다. 본 논문에서는 먼저 홈네트워크 기술 동향 및 보안 기술 동향에 대해 살펴보고 홈디바이스 인증 및 인가시 고려되어야할 홈디바이스에 필요한 요구사항을 살펴보고, 인증서 및 인가서를 이용한 홈디바이스 인증/인가 기술에 대해 설명한다. 마지막으로 인증 인가 기술의 기대 효과를 살펴본다.

* 한국전자통신연구원 정보보호연구단(hanjw@etri.re.kr, deokgyulee@etri.re.kr, kyoil@etri.re.kr)

II. 홈네트워크 기술 동향

홈네트워크의 기본 개념은 집안의 정보가전기기를 네트워크로 묶고 이를 외부의 인터넷 망과도 연결하여 집 내부 및 외부 어디서나 사용자의 위치에 관계없이 정보가전기기를 제어할 수 있도록 하고 각종 편의를 위한 홈서비스를 제공하겠다는 것이다.

홈네트워크 기술은 크게 4개의 중점 기술로 분류될 수 있다. 이중에서 홈플랫폼 기술은 외부 망과 가정을 연결하고 가정 내 다양한 서비스를 제공하여 유무선 통합 홈네트워크 환경 및 고품질의 융합서비스를 가능케 하는 홈서버/게이트웨이, 홈네트워크 보안 및 개방형 서버 기술로 구성된다. 우선 홈플랫폼 기술은 외부 인터넷과 연결을 위한 가입자망으로 xDSL, Cable, FTTH(Fiber To The Home), PLC(Power Line Communication), IEEE802.11 등 다양한 유·무선망의 사용이 가능하다. 홈네트워크는 적용 대상에 따라 여러 대의 PC 및 컴퓨터 관련 장비간의 통신을 위한 정보 네트워크, 가전 장비 제어를 위한 자동화 네트워크, 음향 및 영상기기나 게임기 등의 오락 또는 문화생활을 위한 엔터테인먼트 네트워크 3가지 네트워크로 나눌 수 있다.

정보 네트워크는 컴퓨터 및 그 관련 장비간의 통신을 위한 네트워크로 블루투스, 무선랜, HomeRF (Home Radio Frequency) 등을 이용한 무선통신과 이더넷, 전화선 (HomePNA : Home Phoneline Networking Alliance), 전력선(PLC : Power Line Communication) 등을 이용한 유선 통신으로 구성이 가능하다. 장비 제어를 위한 미들웨어로는 마이크로소프트 진영이 중심이 되어 TCP/IP 프로토콜을 활용한 UPnP(Universal Plug and Play)와 자바 진영이 중심이 된 Jini라는 프로토콜이 있다. 자동화 네트워크는 보안장비, 조명, 환기, 에어컨 등의 가전 장비 제어를 위한 네트워크로서 2Mbps 이하의 저속의 통신으로 가능하며, 주로 전력선을 활용하여 통신을 한다. 여기에는 LonWorks, HnCP (Home Network Control Protocol) 등의 미들웨어가 이용되고 있다. 엔터테인먼트 네트워크는 가전 장비나 음향 및 영상기기 (TV, VTR, DVD Player, Audio, 게임기 등)에 적용되며, 100-400Mbps 정도의 고속으로 동영상이나 음악, 게임 등을 실시간으로 전송하는 네트워크이다. 여기에는 UPnP AV나 HAVi(Home Audio Video interoperability)라는 음향 및 영상 장비간의 통신 및 제어를 위한 미들웨어가 사용 가능하다. 대부분의 가정에서는 이러한 3가지 네트워크 모두를 필요로 하므로 백색가전기기, 컴퓨터 관련 장비, 음향 및 영상 장비 등을 효과적으로 엮을 수 있도록 다양한 네트워크 및 미들웨어들을 브릿지 할 수 있는 홈게이트웨이를 개발하고 있으며, ETRI에서는 다양한 미들웨어간의 연동을 가능하게 해주는 통합미들웨어를 개발하고 있다.[5-7,17-21]

〔표 1〕은 홈네트워크 기술에 대한 분류이다

〔표 1〕 홈네트워크 기술 분류

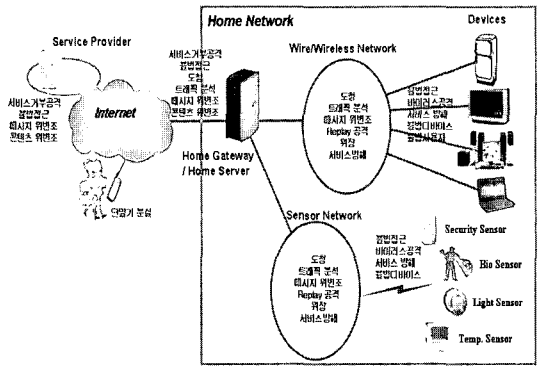
대분류	중분류	소분류
홈네트워크 기술	홈플랫폼 기술	홈서버/홈게이트웨이 기술
		홈네트워크 보안
		개방형 서버 기술
	유/무선 홈네트워킹 기술	유선 홈네트워킹 기술(Ethernet, PLC, IEEE 1394)
		무선 홈네트워킹 기술(WLAN (802.11a/b/g/n), WPAN (UWB, Zigbee)
	정보가전 기술	지능형 정보가전
		홈센서 기술(RFID, 센서)
	지능형미들웨어 기술	홈네트워킹 미들웨어 기술
		상황적응형 미들웨어 기술
		멀티 모달 인터페이스 기술

III. 홈네트워크 디바이스 인증/인가 기술 동향

본 장에서는 홈네트워크 디바이스 인증/인가 기술 동향에 대하 살펴본다. 홈네트워크 보안 취약성, 홈디바이스 인증 기술 동향, 홈디바이스 인가 기술 동향과 보안 기술 표준화 동향에 대해 설명한다.

1. 홈네트워크 보안 취약성

홈네트워크에서는 다양한 유·무선 네트워크와 프로토콜 등의 혼재로 기존 인터넷 등에서 발생되던 보안취약성외에도 추가적으로 고려해야할 보안취약성이 존재하고 있다. 즉, 홈네트워크의 모든 정보기기들은 인터넷과의 연결로 다양한 사이버공격의 대상이 될 수 있으며, 홈네트워크내의 정보기기의 다양성과 기기간 자원의 공유 등으로 보안측면에서 고려해야할 요구사항은 더욱 복잡하고 다양한 특성을 지니게 된다. 더욱이 홈네트워크의 정보가전기기들은 상대적으로 컴퓨팅 능력이 낮아 강력한 보안기능의 탑재가 어려우므로 사



〔그림 1〕 홈네트워크의 보안취약점

이버공격에 이용되거나 목표가 될 가능성이 더욱 높다고 할 수 있다. 홈네트워크에는 Ethernet, Home-PNA, PLC, IEEE 802.1x, Bluetooth, UWB (Ultra Wide Band) 등 다양한 홈네트워킹 기술이 사용 가능하나 홈네트워크 측면에서 매체의 보안취약성을 해결할 수 있는 대응기술을 갖고 있지 못하며, 미들웨어의 경우에도, 각 미들웨어들이 요구하는 보안기능을 모두 만족할 수 있고 개별 미들웨어를 통합한 통합미들웨어 환경에서도 유연하게 보안기능을 제공할 수 있는 보안인프라가 아직 개발되지 못하고 있다 [16-18].

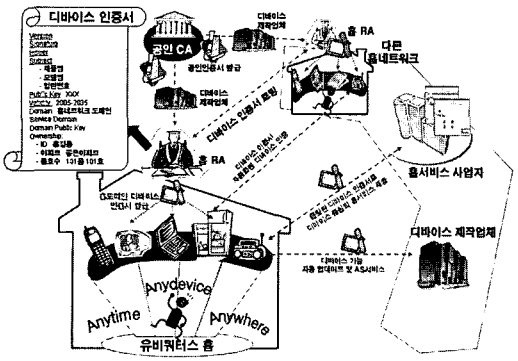
〔그림 1〕은 홈네트워크에서 발생될 수 있는 보안취약성을 정리한 것이다. 인터넷 등에서 발생되던 취약성이 홈네트워크 내부망에서도 그대로 발생됨을 알 수 있으며, 내부망의 복잡함을 고려할 때 우선적으로 종합적인 보안프레임워크를 정립하는 것이 필요하겠다. 홈네트워크에서 디바이스가 가지는 보안 취약성은 이동성(Mobility), 개체인증, 동일 개체 인증, 데이터 발신처 인증, 접속/비접속 기밀성 등이 있다. 이와 같은 사항에 대해 각 디바이스의 보안이 유지되지 못한다면, 사용자의 정보가 유용될 소지를 가지고 있다. 위와 같은 홈디바이스 인증에 대한 문제점들은 동일 네트워크나 동일 미들웨어에서만 사용 가능한 디바이스 인증 기술의 한계를 가지고 있으므로 홈네트워크 환경에 적합하고 호환이 가능한 디바이스 인증 기술이 개발이 필요로 하다. 또한 홈디바이스에 대해 인증 절차 후 서비스 접근을 위한 인가 절차가 필요하다. 그러나 모든 홈디바이스에 대해 동일한 서비스 제공이 아닌 사용자에 따라 서비스가 변경되어야 한다. 따라서 이에 대한 각 사용자의 접근을 정의 할 수 있는 인가서에 대한 개발이 필요하다.

2. 홈디바이스 인증 기술 동향

유비쿼터스 홈네트워크로의 진화는 다양한 서비스 도메인에서 홈디바이스 이동이 증가될 것이며, 홈디바이스간의 협업에 의한 새로운 홈서비스가 증가할 것이다. 이와 같은 기술의 진화에 따라 유비쿼터스 환경에서 안전한 이동과 seamless한 서비스를 제공할 수 있도록 경량화된 홈디바이스 인증 기술이 필요하다. 그러나 현재까지 디바이스 인증은 미들웨어 레벨에서 제공되고 있다. UPnP의 경우, 디바이스 마다 부여된 Security ID로 디바이스의 홈네트워크 등록과정에서 디바이스 인증이 이루어지고 있으며, HAVi의 경우에는 디바이스마다 고유한 인증서를 발행하여 디바이스 인증 수행시 사용하고 있다. 그러나 기존 업체의 경우, 기존 인증서를 그대로 이용하여 소형화되고, 컴퓨팅 능력이 부족한 디바이스에서 그대로 이용하기에 많은 문제점을 가지고 있다. 실 예로, x.509 기반의 PKI 인증 솔루션이 홈게이트웨이용 인증기술로 활용하고 있으나 일반적으로 사설인증서 형태로 제공 운영되고 있다. 홈디바이스가 다양한 서비스 및 유비쿼터스 환경에서 사용되기 위해서는 경량화된 홈디바이스가 다수의 인증서를 가져야 하고, 또 서비스 도메인이 변경될 때마다 사용자들이 불편한 과정을 통해 별도의 인증서를 발급받아야 하는 등 홈네트워크 환경에 그대로 적용하기에는 적합하지 않다고 할 수 있다.[13,22-24]

향후, 홈네트워크 서비스는 디바이스간의 협업을 통해 디바이스가 서비스의 주체가 되어 디바이스들이 판단하여 사용자 상황에 맞는 최적의 서비스를 제공하는 형태로 진화할 것이다. 또한 홈네트워크는 유비쿼터스 서비스의 한 도메인으로서 홈네트워크 간에, 홈네트워크와 사이버오피스 간에, 홈네트워크와 텔래메틱스 도메인 간에 다양한 서비스 도메인간의 seamless한 홈서비스를 제공하게 될 것이다. 따라서 향후에는 홈디바이스간의 신뢰관계 구축이 매우 중요한 보안이슈가 될 것이며, 현재 〔그림 2〕와 같이 PKI기술을 기반으로 한 동일 홈네트워크 인증기술이 아닌 서비스 도메인간의 인증기능 로밍이 가능한 멀티 홈네트워크 인증기술이 요구될 것이다. 위와 같은 seamless한 홈서비스 제공을 위해서는 여러 다른 홈네트워크 특성에 적합하고 사용자 편의성이 강화된 인증 프로토콜과 함께 홈디바이스의 특성을 고려한 관련 작업도 필요하다. 이를 위해 댁내와 댁외의 구분으로 댁내에서는 대칭키 기반의 인가서를 이용하고, 댁외에서는 홈네트워크 서비스 환경에 맞도록 변형한 x.509기반의 인증서를 이

용한다면 경량화된 홈디바이스로도 안전하게 다양한 유비쿼터스 홈서비스 사용이 가능하겠다.



〔그림 2〕 디바이스 인증서 개념

3. 홈디바이스 인가 기술 동향

유비쿼터스 홈네트워크로의 진화는 다양한 서비스 도메인에서 홈디바이스 이동이 증가될 것이며, 홈디바이스간의 협업에 의한 새로운 홈서비스가 증가에 따라 안전한 이동과 seamless한 서비스를 제공할 수 있도록 경량화된 홈디바이스 인증 기술의 필요성을 설명하였다. 이와 함께 중요한 것은 댁내에서 안전하게 서비스를 제공받을 수 있도록 하는 인가 기술이 필요하다.

현재까지의 인가기술로는 한정된 서비스 환경에서만 작동하는 단점을 가지고 있다. SPKI(Simple PKI)의 경우, 객체의 ID정보가 아닌 공개키 자체에 대한 인증을 통해 서비스 접근 권한을 제어하며, PMI(Privilege Management Infrastructure)는 신원확인을 제공하는 PKI보다 사용자 또는 디바이스 속성 정보를 제어하기 위한 연구가 진행되었으나 별도의 처리기관을 두어야 하는 등 홈네트워크 환경에 적용하기에는 단점을 갖고 있어, 현재 홈네트워크를 위한 홈디바이스 인가 기술은 개념 정립 및 일부 서비스에 대한 초기 기술 개발단계로 이뤄지고 있다[8,9,25].

따라서 홈네트워크 환경에서 사용자의 편의성과 안전성을 증대 시킬 수 있는 인가서가 필요하며, 대칭키 기반의 인증서로써 댁내 환경에서 안전하게 유비쿼터스 홈서비스의 이용이 가능하다.

4. 홈네트워크 보안 기술 표준화 동향

현재 홈네트워크 서비스 산업은 시장 형성을 위한 초기 단계로 국내외를 막론하고 모든 사용자들이 널리 이용할 수 있는 표준화된 보안기술이 없는 실정이다. 각 가전 제조사나 홈네트워크 서비스 업체들은 저마다의 기술을 이용하여, 이종의 유무선 네트워크상에서 홈오토메이션과 같은 제한된 홈서비스 및 홈기기 개발에 초점을 맞추고 있으나 보안기능은 고려가 되고 있지 않다. 현재, 보안기능의 고려 없이 서비스가 전개되고 있지만, 해킹에 의한 보안사고가 발생할 경우 재산의 피해뿐 아니라 생명의 위협까지 발생될 수 있으므로, 궁극적으로 보안 기능의 미비는 홈네트워크의 활성화에 큰 장애물로 작용할 것이다. 국내에서는 SKT와 KT를 중심으로 홈네트워크 시범서비스를 위한 컨소시엄이 구성되었지만, 실제 정보보호 대책은 사용자의 아이디와 패스워드를 이용한 단순한 인증 방식에 그치고 있다. 따라서 통일된 홈네트워크 모델이 없는 상황에서 적용되는 다양한 네트워크나 미들웨어에 따라서 제공 가능한 보안기술도 상이할 수밖에 없으므로 표준화 관점에서 우선적으로 종합적인 보안요구사항을 정의하고 이를 반영한 보안프레임워크 모델 표준화를 추진하고 있다.

국제 표준화의 경우는, ITU-T SG17의 Q.9에서 추진되고 있으며 3개의 표준화 프로젝트가 수행 중에 있다. Xhomesec-1은 홈네트워크 보안 프레임워크의 정립을 Xhomesec-2는 홈네트워크에서 디바이스 인증을 제공하기 위한 인증서 프로파일(Device Certificate Profile)에 대한 정의를 목표로 하고 있으나, 기존 PKI 인증서에 디바이스 관련 프로파일을 추가 정의가 목표이며, 사용자 속성정보와의 연계성, 디바이스 유효성 확인을 위한 통일화된 정보, 사용자 편의성 증대를 위한 멀티 도메인 인증 개념 등에 대한 고려는 없다. ETRI에서 제출한 Xhomesec-3은 사용자에게 편리한 인증방식을 사용할 수 있도록 하는 통합 사용자 인증 메커니즘의 개발 및 표준화로 진행되고 있다.

국내 표준화의 경우, ETRI가 제안한 홈네트워크 사용자 인증메커니즘이 2005년 1월 홈네트워크 시큐리티 포럼의 사실표준으로 채택되었고, 2005년 12월 TTA 국내표준으로 제정되었다. 그리고 홈네트워크 접근제어기술에 대한 표준화를 위해 ETRI에서 개발한 보안정책 언어에 대한 표준안이 TTA와 홈네트워크 시큐리티 포럼에서 12월 재정 예정이다.

Ⅳ. 홈디바이스 인증/인가 보안 요구사항

이 장에서는 인증서를 이용한 홈디바이스 인증과 대

칭키를 이용한 인가 메커니즘을 위한 고려사항 및 보안 요구사항들을 살펴본다[10,12].

1. 홈디바이스 인증 요구사항

홈디바이스 인증은 홈네트워크 환경에서 다양한 디바이스들이 통일된 인증체계를 가지도록하기 위해 디바이스 인증서를 이용한 인증메커니즘으로 동작하며 다음과 같은 사항들이 필요하다.

- 홈디바이스 인증은 다양한 서비스 도메인에서의 유연성을 고려하여 인증서를 기반으로 동작해야 한다.
- 홈디바이스 인증서는 홈디바이스를 유일하게 결정 및 식별할 수 있어야 한다.
- 홈디바이스 인증서는 서비스 인가를 결정하기 전에 디바이스의 Identity를 인증하기 위해 사용된다.
- 홈디바이스 인증서는 유비쿼터스 또는 멀티홈 환경에서 서로 다른 디바이스들이 인증 가능하도록 동작해야 한다.
- 홈디바이스 인증서에 대한 발급/수정/폐기 등의 관리 기능을 제공해야 한다.
- 홈디바이스 인증서에 대한 불법 사용이나 변조를 방지할 수 있어야 한다.
- 홈디바이스 인증서는 공개키 방식을 지원해야 한다.
- 홈디바이스 인증서 자체의 유효성을 판별할 수 있어야 한다.
- 홈디바이스 인증서의 사용시 사용자 개입을 최소화해야 한다.
- 홈디바이스 인증서의 유효성 검증을 위해 위탁서버를 운영할 수 있다.
- 홈디바이스 인증서에 대한 연산은 디바이스에서 충분히 동작할 수 있도록 경량화 되어야 한다.
- 홈디바이스 인증서는 디바이스 소유권에 대한 정보를 포함할 수 있다.

2. 홈디바이스 인가 고려사항

홈디바이스 인가 서비스는 대칭키 기반의 디바이스 인가서를 이용한 인가메커니즘으로 동작하며 다음과 같은 사항들이 필요하다.

- 홈디바이스 인가는 Private 도메인에서만 유효한 인가서를 기반으로 동작한다.
- 홈디바이스 인가는 홈서비스에 대한 접근 권한 정보를 안전한 방식을 통해서 포함해야 한다.
- 인가서에 대한 발급/수정/폐기 기능을 제공해야 한다.
- 인가서에 대한 불법 사용이나 변조를 방지할 수 있어야한다.
- 홈디바이스 인가서는 대칭키를 지원해야 한다.
- 인가서는 인증서보다 유효기간이 짧아야 한다.
- 홈디바이스 인가는 사용자 개입을 최소화해야 한다.
- 인가서 검증은 인가서를 발행한 서비스도메인에서만 수행되어야 한다.

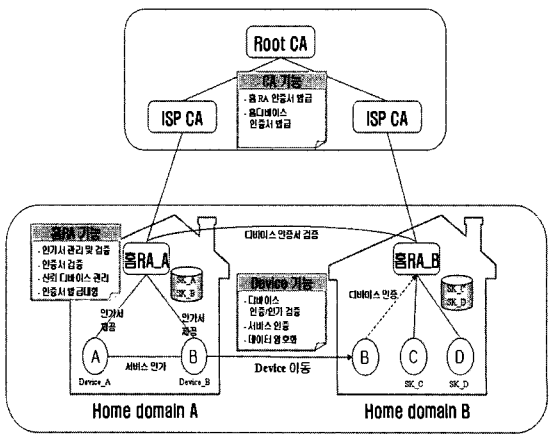
V. 유비쿼터스 환경을 고려한 홈디바이스 인증/인가 기술

본 장에서는 동일 네트워크나 동일 미들웨어에서만 사용 가능한 기존 디바이스 인증 기술의 한계를 해결하는 유비쿼터스 홈네트워크 환경에 적합한 디바이스 인증/인가 기술에 대해 살펴본다[14,15].

1. 홈디바이스 인증/인가 기술 개념

1.1 홈디바이스 인증/인가 체계도

홈네트워크에서 홈디바이스의 인증/인가 구조는 홈네트워크의 특성을 고려하여 설계될 필요가 있다. 따라서 홈네트워크 서비스 구조에 적합한 인증 및 인가 구조를 가지기 위해 홈네트워크 구성 요소의 특성에 따라 인증 및 인가 관련 기능을 재배치할 수 있다. 아래 [그림 3]은 인증/인가 기능들이 홈네트워크 내에서 동작 체계도이다.



[그림 3] 홈네트워크 인증/인가 체계

홈디바이스 인증서 발급을 위한 등록은 댁내에 위치한 홈RA를 통해 이루어지며, 댁내 서비스에 대한 인가서는 홈RA가 직접 발급된다. 홈RA는 댁외에 위치한 인증기관(CA)에 디바이스 인증서 발급요청을 위한 등록기관으로서의 역할을 하며, CA와 연계하여 홈디바이스에 인증서를 전달, 설치하도록 하는 역할까지 담당한다. 홈RA, 보안 서버 등은 일반적으로 홈게이트웨이/홈서버에 탑재되며, 다른 시스템에서 독립적으로 동작할 수도 있다.

일반적으로 홈네트워크에서는 비IT사용자들과 다양한 성능의 디바이스들이 존재할 수 있으므로 사용자 편리성과 알고리즘 경량화에 중점을 두어야 한다. 또한 홈디바이스의 편리한 이용을 위해 댁내 홈네트워크에서는 인증서의 사용이 아닌 인가서를 통한 홈디바이스의 접근제어가 이뤄져야한다. 이와는 다르게 댁외 홈네트워크에서는 사용자의 홈디바이스가 위치한 곳에서 디바이스에 대한 인증을 수행하여야 하기 때문에 인증서를 이용하는 형태가 되어야 한다. 이는 사용자 편리성을 위해 홈RA를 두어 사용자 개입 없이 홈디바이스 관련 인증서 발급절차를 수행하며, 다른 홈네트워크나 타 도메인으로 이동시 자동적으로 디바이스 인증 절차를 수행할 수 있도록 홈RA를 둔다. 또한 인증서 검증 절차를 자동적으로 이뤄지게 함으로써 저성능 디바이스를 위한 절차도 포함하고 있다. [그림 3]에서 인증을 요하는 디바이스가 외부 도메인으로부터 댁내로 들어왔을 경우, 먼저 홈RA는 홈네트워크에 위치한 디바이스를 인증한 후 인가서를 발급하기 위한 절차를 수행하게 된다.

1.2 홈디바이스 인증 구조

홈디바이스 인증은 유비쿼터스 및 멀티홈 환경에 적합하도록 설계된다. 따라서 여러 도메인의 다양한 단말들이 서로를 신뢰할 수 있도록 상위에 CA를 가지는 계층적 인증구조를 가진다. 이러한 계층적 인증 구조는 홈네트워크 사업자 모델이나, 단지의 이동 등에 폭넓게 적용할 수 있는 장점을 가진다. [그림 4]는 홈디바이스 인증 구조를 나타낸다.

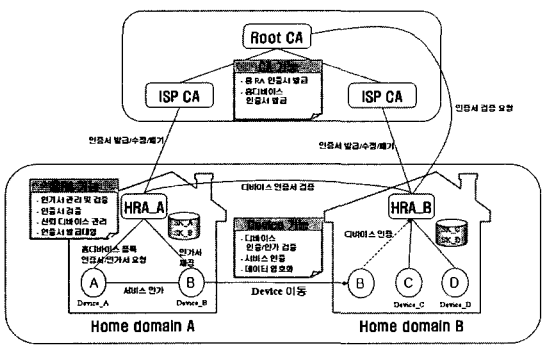
홈RA는 홈디바이스의 관련정보를 CA에 통보하여 인증서를 등록하고, 인증서 발급 및 폐기 등에 대한 관리 요청을 수행한다. CA는 타 도메인의 홈디바이스를 인증하고, 홈디바이스의 불법사용여부를 판단하며 기타 보안에 필요한 키분배, 보안 정책 등에 대한 관리 기능을 수행한다. 홈RA는 홈디바이스의 인증서 검증 시 신뢰경로 검증, CRL 검증 등의 기능을 위탁받아 검증대행기능을 제공하기 위해 사용된다.

1.3 홈디바이스 인가 구조

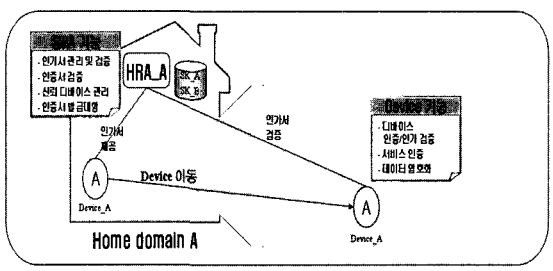
홈디바이스 인가 구조는 사용자 정보를 포함하는 홈디바이스에 대한 인가 정책을 수립하고 적용하기 위한 구조를 정의하며, 홈RA를 중심으로 동작한다. 홈디바이스들중에는 운영체제가 없는 8비트 프로세서 기반의 가전기기가 다수 존재하므로 본 고에서 제시하는 대칭키 기반의 인가서를 활용하는게 사용자 편의성 및 경량성을 이루는데는 적합하다고 할 수 있다.

사용자가 홈디바이스를 사용해서 홈네트워크 서비스를 제공받기 위해서는 먼저 해당 서비스 도메인의 홈RA로부터 도메인 내에서의 권한을 명시하는 대칭키 기반의 인가서를 발급받아야 한다. 홈디바이스는 홈RA로부터 발급받은 인가서를 통해서 접근 권한이 있는 서비스나 디바이스에 접근할 수 있으며, 실시간 인가서 검증 기능을 제공한다. [그림 5]는 홈디바이스 인가 구조를 나타낸다.

홈네트워크 인가 서비스를 제공하기 위해서 홈RA(AI: Authority Issuer)는 홈서비스를 제공하는 자원과 미리 인가에 사용되는 대칭키를 공유해서



[그림 4] 홈네트워크 인증 구조도



[그림 5] 홈네트워크 인가 구조도

분배해야 한다. 인가에 사용되는 키는 단일 서비스나 디바이스를 기반으로 할 수도 있으며, 홈네트워크의 특성을 고려해서 유사한 특성의 홈서비스에 대한 그룹 키 특징을 나타낼 수도 있다.

홈디바이스가 발급받은 인가서는 해당 홈 도메인 내에서만 유효하며, 키관리 허용범위에서 서비스 사업자 혹은 텔레매틱스 도메인으로 확장되어 사용될 수 있다. 또한 인증서와 달리 유효 기간을 짧게 설정해야 한다. 인가서는 홈RA와 접근하고자 하는 자원간 미리 설정된 대칭키를 사용한 서명을 포함한다. 따라서 홈디바이스는 홈RA로부터 발급받은 인가서를 통해서 해당 홈서비스를 요청하며, 안전한 검증 과정을 거친 후 서비스 제공 여부를 결정한다.

Ⅵ. 디바이스 인증/인가 기대효과

앞서 언급한 보안요구사항을 바탕으로 유비쿼터스 홈네트워크 환경에 적합하고 호환이 가능한 디바이스 인증/인가 기술 개발시 얻을 수 있는 기대효과는 다음과 같다.

- 홈디바이스가 안전하게 사용자를 대신할 수 있다.
  : 홈디바이스에 발급된 인증서 및 인가서의 활용으로 사용자의 개입없이 디바이스 스스로가 판단하여 사용자에게 최적의 서비스를 제공할 수 있게 한다. 즉, 디바이스간의 안전한 신뢰관계를 구축하게 하여 사용자는 디바이스가 제공하는 서비스를 안심하고 제공받을 수 있게 되는 것이다.
- 보안기능 제공시 사용자 편의성의 강화
  : 인증서에서 있어서 개인키 보호를 위한 암호화 키를 사용자가 입력하는게 아니라 디바이스내의 주요정보보호를 위한 메커니즘을 활용하여 보호함으로써 비IT 사용자도 별도의 동작없이 서비스를 제공받을 수 있으며, 통일된 홈디바이스 인증체계를 제공함으로써 이종의 서비스 도메인으로 디바이스가 이동하는 경우에도 추가적인 인증서 발급과정이 요구되지 않으므로 편의성은 한층 강화된다고 할 수 있다.
- 홈디바이스 분실 또는 도난 방지
  : 홈디바이스 분실시 CA서버로 분실신고를 하면, 불법 사용되는 경우 디바이스가 동작되는 서비스 도메인의 정보를 CA서버에서 알 수 있게 되므로 분실된 디바이스에 대한 대응책 마련이 가능하게 된다.
- 유비쿼터스 디바이스로 확장 사용 가능
  : 현재의 홈네트워크 도메인에서 뿐 아니라 다양한 서비스 사업자도메인(홈서비스 사업자, 텔레매틱스 사업자, u-Works 등)까지 확장 사용할 수 있다. 특히, 인가서의 경우, 키관리가 가능한 범위까지 도메인 확대가 가능하겠지만 복잡한 연산이 필요없으므로 경량화된 유비쿼터스 디바이스에도 활용이 가능하겠다.
- 서비스 호환 및 연동성 제공.
  : 유비쿼터스 환경으로 인해 사용자가 사용하고자 하는 서비스는 다양하게 증가할 것이다. 이에 통일된 홈디바이스 인증/인가 체계를 적용한다면 다양한 서비스간의 호환 및 연동성을 제공할 수 있겠다.

Ⅶ. 결 론

우리나라는 세계수준의 네트워크 인프라와 전자/반도체 기술 등이 있으므로 PC 보급과 광대역 통신과 같은 인프라 보급이 뒷받침 된다면 홈네트워크 수요가 활성화 될 것이다. 또한, 정보통신부에서는 "디지털 라이프 실현을 위한 디지털 홈 구축계획"을 발표하면서 가정을 누구나 기기 시간 장소에 구애받지 않고 다양한 홈서비스를 제공받을 수 있는 디지털 생활공간으로 전환하고, 2007년까지 천만가구에 디지털홈 구현을 위한 홈네트워크를 구축할 것이라는 비전을 제시했다. 정부의 홈네트워크 시장 육성의지와 맞물려 관련 업체들이 적극적으로 시장에 참여하고 있어 신성장동력으로서 홈네트워크 시장에 대한 기대감은 매우 높다고 할 수 있다.

하지만 홈네트워크 홈디바이스의 취약성은 존재하고 있으며, 불법적인 접근에 대해 신뢰된 홈디바이스만 홈네트워크에 접근할 수 있게 하는 보안대책이 마련되어야 한다. 유비쿼터스 홈네트워크 및 홈디바이스 경량화 추세 등 IT 환경의 변화로 인해 기존 정보보호 기술을 홈네트워크 환경에 그대로 적용하기 어렵다. 이에 본고에서는 유비쿼터스 홈네트워크 환경에 필요한 홈디바이스 인증/인가 기술에 대해 살펴보았으며, 그에 따른 고려 사항 및 보안 요구사항에 대해 살펴보았다. 따라서 본고에서 정의한 홈디바이스 인증/인가 기술에 대한 요구사항 등을 모두 반영한 홈네트워크 기술을 개발한다면 홈네트워크 분야를 통해 예상되고 있는 세계시장 선점을 통한 경제적 기대효과 및 미래 지향의 가정환경 구현이 가능해지리라 생각된다.

참 고 문 헌

[1] 박광로, 송영준, "홈네트워킹", TTA저널, 제78호, pp.101-109, 2001.

[2] 전호인, "디지털홈기술 및 표준화동향", TTA저널, 제88호, pp.59-73, 2003.

[3] 윤철, "최근의 홈네트워크 기술동향 및 시장전망", 주간기술동향, 제1098호, pp.22-33, 2003.

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

[5] "Home Network Control Protocol(HNCP) Prespec. Ver. 1.5", PLC 포럼 디지털 가전 위원회, 2003.

[6] 박광로, "IT839 전략 표준화: 홈네트워크", TTA저널, pp78-84, 2005

[7] 서대영, "표준기술동향: 홈네트워크를 위한 Open Services Framework", TTA저널, pp98-106, 2005

[8] Russ Housley and Tim Polk, "Planning for PKI", John Wiley & Sons, Inc.

[9] http://www.ist-shaman.org, "Initial report on PKI requirements for heterogeneous roaming and distributed Terminals", Shaman Project

[10] Jin-Bum Hwang, Do-Woo Kim, Yun-Kyung Lee and Jong-Wook Han, "Two Layered PKI Model for Device Authentication in Multi-Domain Home Networks", Proc. of 10th International Symposium on Consumer Electronics (ICSE), June 2006

[11] 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

[12] 황진범, 한종욱 "홈네트워크에 적합한 접근제어 방식에 대한 고찰," 한국해양정보통신학회종합학술대회, vol.9 no.1, pp.323-327, 2005. 5

[13] Carl M.Ellison, "Interoperable Home Infrastructure Home Network Security." Intel Technology Journal, Vol 6., pp.37-48, 2002.

[14] Jin-Bum Hwang, Jong-Wook Han, "A Security Model for Home Networks with Authority Delegation," ICCSA-4. 2006, pp 360-369, 2006. 5

[15] 한종욱, 이덕규, 정교일, "홈네트워크 보안기술 동향", 한국통신학회학회지, pp 113-124, 2006.9

[16] MIT Media Lab, Things That Think-Consortium, http://ttt.media.mit.edu

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

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

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

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

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

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

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

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

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

〈著者紹介〉

한 종 욱 (Jong Wook Han)

1985년 광운대학교 공과대학 전자공학과 공학사
1991년 광운대학교 전자공학과 공학석사
2001년 광운대학교 전자공학과 공학박사
1991년~현재 한국전자통신연구원 홈네트워크보안연구팀 팀장
관심분야 : 홈네트워크보안, 네트워크보안, Optical Security

이 덕 규 (Deok Gyu Lee)
정회원

2001년 순천향대학교 공과대학 컴퓨터공학과 공학사
2003년 순천향대학교 전산학과 공학석사
2006년 순천향대학교 전산학과 공학박사
2006년~현재 한국전자통신연구원 홈네트워크보안연구팀 Post-doc
관심분야: 홈네트워크 보안, 키관리, 콘텐츠 보안

정 교 일 (Kyo Il Chung)
정회원

1981년 한양대학교 전자공학과 공학사
1983년 한양대학교 전자계산학과 공학석사
1997년 한양대학교 전자공학과 공학박사
1982년~현재 한국전자통신연구원 정보보호기반그룹 그룹장
관심분야: Security, Biometrics, 홈네트워크보안, RFID