홈네트워크 보안 기술 및 표준화 동향

Trend of Home Network Security Technology and Standardization

21세기를 대비하는 정보보호 특집

이덕규 (D.G. Lee) 융합서비스보안연구팀 선임연구원
김도우 (D.W. Kim) 융합서비스보안연구팀 선임연구원
한종욱 (J.W. Han) 융합서비스보안연구팀 책임연구원

목 차

홈네트워크는 기술의 통합적인 제공에 따라 높은 신뢰성이 필요하지만, 안전성이 확보되지 않는 홈네트워크는 사용자로부터 외면을 받을 수 밖에 없다. 또한 유무선 네트워크 및 프로토콜들 각각에 대한 보안이 고려되어 있다 하더라도 이들의 혼재로 인한 새로운 취약점이 생길 수 있고, 홈네트워크 서비스를 운용하는 과정에서 새로운 취약점이 드러나고 있다. 본 고에서는 안전한 홈네트워크 구축을 위해 최근 국내/외에서 다양한 표준이 제정, 논의되고 있으며, 홈네트워크 보안에 관한 국내/외 표준화 동향을 소개한다. 또한 홈네트워크 구축시 고려되어야 할 홈네트워크의 보안취약성 및 관련 보안기술 개발동향을 설명한다.

Ⅰ. 서론

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. 그러나 인터넷을 기반으로 한 사이버 해킹공격은 급격히 증가하고 있어 국내 해킹·바이러스 신고 접수 건수는 2005년 49,633건에서 2006년 34,579건, 2007년 27,728건으로 2005년도와 같이 인터넷 성숙단계의 진입에서는 폭발적으로 증가하였으나, 전년도 대비 2006년 바이러스 및 해킹은 20% 정도 감소하고 있다[1]-[3].

홈네트워크 서비스를 실생활에 적용하고자 하는 움직임이 나타나면서 구체적인 서비스 모델이 나오게 되었고, 이들에 대한 보안이 고려되게 되었다. 그 결과물로 2005년 ISO에서 홈네트워크 보안요구사항과 댁내 및 댁외 보안에 대한 표준이 나오게 되었고, ITU-T SG17에서도 2004년 WTSA 회의를 계기로 통신망에서의 정보보호에 대한 중요성을 크게 인식하고 NGN 보안, SPAM 메일 대책, 사이버 보안 등을 포함한 광범위한 범위의 보안관련 표준을 개발하고 있으며, 홈네트워크 보안관련 표준 개발도 시작단계에 있다[4].

한편 국내에서는 HNSF과 TTA를 중심으로 홈네트워크 보안에 관한 표준이 개발되고 있는데, 2004년부터 표준이 꾸준히 발표되고 있다. 2006년과 2007년에는 홈네트워크 보안 기술 프레임워크, 홈네트워크 사용자 인증 메커니즘, 홈네트워크 보안 정책 기술 언어 등의 표준안이 제정되었고, 이들 표준들 중 일부는 ITU-T SG17에서 국제표준으로 채택되기 위해 2006년 12월 제네바 회의에서 표준안으로 발표되었다. 특히, '홈네트워크 보안 기술 프레임워크' 표준안은 2006년 12월 ITU-T 제네바 회의에서 국가별 의견수렴 과정인 consent 과정을 거쳤으며, 현재는 의견을 반영하여 최종과정에 있다.

따라서 본 고에서는 홈네트워크 보안에 대한 국내/외 표준화 동향을 소개하고, 나아가 안전한 홈네트워크 구축을 통하여 홈서비스가 활성화 될 수 있도록 홈네트워크 구축시 고려되어야 할 홈네트워크의 보안취약성 및 관련 보안기술 개발동향을 살펴보고, 보안요구사항에 대하여 기술한다.

Ⅱ. 국내/외 표준화 동향

1. 국외 표준화 동향

홈네트워크 보안에 대한 국외 표준화는 ISO에서 2005년에 표준안이 한 건 있었고, 2005년에서 현재까지 ITU-T에서 진행중인 표준안이 3건이 있다. ITU-T에서 진행중인 표준안들은 Study Group17의 Question9에서 진행중이다. Question9은 X-homesec-1, X-homesec-2, X-homesec-3의 세 부분으로 나뉘어 있고, X-homesec-1은 "Framework of security technologies for home network", X-homesec-2는 "Device certificate profile for the home network", X-homesec-3는 "User authentication mechanism for home network service"라는 제목으로 표준화가 진행중이다[1].

가. 홈네트워크 보안

홈네트워크 보안 전반에 관하여 다룬 표준으로 ISO/IEC에서 2005년 6월 표준으로 발표되었고, "Home network security"라는 주제 하에 세 부분으로 나뉘어 표준이 완성되었다: security requirements, internal security service, external security service[5].

이 표준안에서는 홈게이트웨이 중심의 홈네트워크 모델을 정립하고, 이 모델에 적합한 보안 요구사항 및 보안 서비스들을 정의하였다. 또한 홈네트워크에서는 고려해야 할 사항들이 많고, 다양한 종류의 홈네트워킹 모델, 다양한 사용자 요구사항, 그리

고 많은 애플리케이션들이 존재하기 때문에 하나의 보안 솔루션으로 해결할 수 없음을 기술하고 있다. 또한 홈네트워크 보안시스템을 개발하는 데 있어서 'low cost', 'low complexity', 'easy to use', 'reliability'에 대해 고려하는 것이 중요함을 강조한다. (그림 1)은 이 표준안에서 제시하는 댁내 및 댁외 보안에 관한 개략도이다.

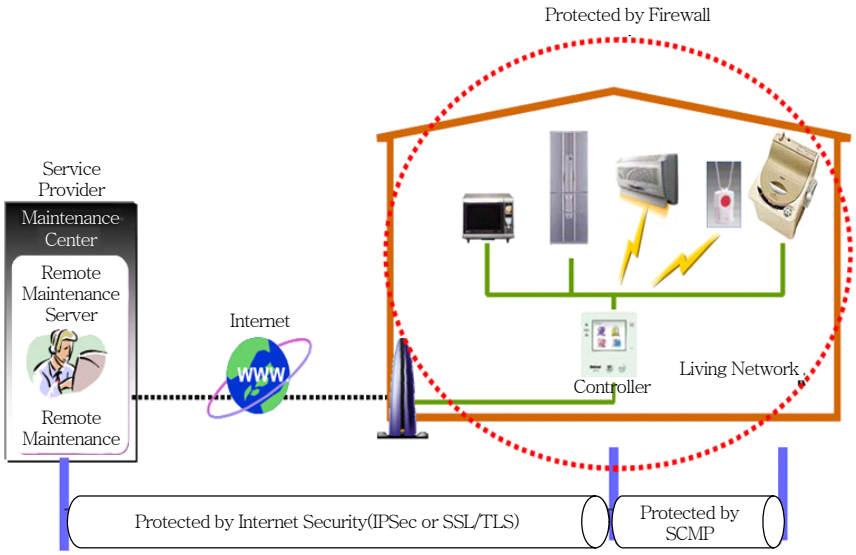
이 표준안에서, 댁내에는 다양한 종류의 디바이스 및 통신매체들이 있고, 외부 공격에 대해 안전성이 확보되지 않은 통신매체들이 있기 때문에 SCMP를 두어 댁내보안을 꾀하였다.

또한 댁외는 홈게이트웨이에서 서비스 프로바이더 혹은 댁외 클라이언트에 이르는 영역으로, 이들은 인터넷을 이용하여 연결되어 있으므로 새로운 프로토콜을 제시하지 않고, 기존의 인터넷 보안 프로토콜을 이용한다. 즉, 네트워크 계층의 보안을 위해서 IPSec을 이용하고, 세션 계층의 보안을 위해서 SSL 혹은 TLS를 이용한다. 이들 메커니즘과 방화벽의 조합을 통한 댁외 보안은 'low cost', 'low complexity', 'moderate inconvenience'를 제공한다. (그림 1)에서는 댁내의 보안은 SCMP, 댁외의 보안은 SSL/TLS와 IPSec을 이용할 수 있음을 나타낸다.

나. 홈네트워크 보안 기술 프레임워크

홈네트워크 보안 기술 프레임워크는 국내 표준화 기관인 TTA에서 표준으로 채택되었고, 현재 ITU-T에서 표준화 과정에 있다. 앞서 기술하였듯이 ITU-T Study Group17 Question9의 X-homesec-1에서 논의중인 이 표준안은 댁내 및 댁외에서의 홈네트워크 사용자에 대한 보안위협, 보안요구사항, 보안위협 해결방안 등을 다루고 있다[6]. 2005년 3월 모스크바 회의에서 권고안이 채택되었고, 2005년 10월 제네바 회의에서 first draft로 채택되었다. 이어 2006년 4월 제주 회의에서 final draft로 채택되었고, 2006년 9월 오타와 interim 회의에서 표준안 최종 수정이 이루어졌으며, 2006년 12월 제네바 회의에서 국가별 의견수렴을 하였다.

이 표준안은 유무선 전송기술을 고려한 홈네트워크 보안위협, 보안요구사항, 보안기능을 정의하고, 원격사용자, 원격터미널, 응용서버, 보안 홈게이트웨이, 홈응용서버, 홈사용자, 홈디바이스의 7개 개체로 구성된 홈네트워크 일반모델과 3가지 홈디바이스 모델을 제안하고 있다. 또한 홈네트워크에서의 보안위협 및 보안요구사항에 관하여 기술하고 있는



(그림 1) 댁내 및 댁외 보안

데, 이 부분은 X.1121[4][1]과 X.805[7][2] 표준에 기반을 두고 있다[2],[3]. 또한 홈디바이스를 A, B, C의 세 가지 타입으로 구분하여 타입별로 적용하는 시큐리티 레벨을 달리하였는데, 타입 A 디바이스는 PC 혹은 PDA처럼 사용자 인터페이스가 있어서 사용자 인증이 가능하고, 다른 디바이스들을 제어하는 디바이스들이 속하고, 타입 B 디바이스는 다른 디바이스들과 통신할 인터페이스가 없는 타입 C 디바이스들을 연결해주는 디바이스들이 속한다. 타입 C 디바이스는 A/V 기기, 웹 카메라 등 타입 B 디바이스가 전달하는 명령에 따라 제어되는 디바이스들로 이루어진다[8].

이 표준에서는 홈네트워크가 전력선, 무선통신, 유선 케이블 등 다양한 전송 매체를 사용하고, 이들은 유선 및 무선 매체가 섞여 있으므로, 유선뿐만 아니라 무선 네트워크상의 위협까지도 고려해야 한다는 특성이 있음을 강조하고, 이에 대한 보안 위협 및 보안요구사항들을 정의하고 있다. 이 표준에서 기술하고 있는 일반적인 보안 위협에는 도청, 폭로, 가로채기, 통신방해, 통신교란, 데이터 삽입 및 수정, 비인가된 접근, 부인, 패킷 비정상 포워딩 등이 있고, 모바일 통신상에서의 보안위협으로는 도청, 폭로, 가로채기, 통신방해, 통신교란, 어깨너머보기, 원격 터미널 분실 및 도난, 예기치 않은 통신 중단, 오독 및 입력오류 등이 있다. 또한 보안요구사항으로 데이터 기밀성 및 무결성, 인증, 접근제어, 부인방지, 개인정보보호 등이 있고, 보안기능으로 암호화 기능, 전자서명 기능, 접근제어 기능, 데이터 무결성 기능, 인증/공증 기능, MAC 및 키 관리 기능 등을 기술하고, 이들 보안요구사항을 만족하기 위해 필요로 하는 보안기능들을 Y(해당 보안기능을 반드시 적용), K(표시된 보안 기능으로 강화), X(선택적 보안 기능 추가)의 세 가지 단계로 표시하고 있다.

1) ITU-T에서 개발된 이동통신망 보안 관련 표준으로, 종단간 이동 통신을 위한 보안 프레임워크를 제시하고 있음
2) ITU-T에서 개발된 표준으로 종단간 데이터 통신을 위한 보안구조에 관하여 기술하고 있음

다. 홈네트워크용 디바이스 인증서 프로파일

홈네트워크용 디바이스 인증서 프로파일 표준안은 현재 ITU-T Study Group17의 Question9에서 표준화를 진행중이다. 이 표준안에서는 홈네트워크용 디바이스의 인증을 위한 디바이스 인증서 프로파일과 인증서 관리 프로토콜을 제안하고 있다.

이 표준안은 2005년 3월 ITU-T 모스크바 회의에서 권고안이 채택되었고, 2006년 1월 제네바 회의에서 일본이 security algorithm 선택에 관한 정책을 추가할 것을 제안하여 디바이스 인증서 프로파일을 수정하였고, 2006년 9월 오타와 회의에서 일본과 프랑스의 보안 요구사항 추가, 참조표 변경, ASN.1 표현방식 변경 등의 표준안 수정에 대한 요구사항을 반영하여 TD를 작성하였으며, 2006년 12월 제네바 회의에서 first draft를 제안하였다.

이 표준안에서는 디바이스 인증모델 하에서 디바이스를 인증하기 위한 디바이스 인증서 프로파일을 제시하고, 디바이스 인증서 발급 및 폐지 프로토콜, 보안요구사항을 기술하였다. 홈네트워크에서의 디바이스 인증 구조는 두 가지로 구분된다. 하나는 보안 홈게이트웨이가 댁내의 모든 디바이스들에 인증서를 발급하는 CA의 역할을 하는 것이고, 이때 보안 홈게이트웨이는 end-entity 디바이스 인증서를 발급하기 위해서 self-sign 인증서를 발행하여야 하고, 또한 외부 CA로부터 자신의 인증서를 발급받아야 한다. 이 홈게이트웨이 인증서는 홈게이트웨이와 홈네트워크 서비스 제공사업자 사이의 인증에 사용된다. 또 다른 하나는 외부의 독립적인 인증 시스템 내에 있는 CA가 댁내의 모든 디바이스에 인증서를 발급하는 구조이다.

디바이스 인증서 프로파일은 X.509 인증서에 기반하여 정의하였는데, 기본 필드의 경우 기존 X.509 V3를 준용하고, 확장필드의 경우 Authority Key Identifier, Subject Key Identifier, Key Usage, Basic Constraint의 네 가지 확장을 사용할 것을 권고하고 있다. 또한 기타 확장이 필요할 경우 X.509 인증서 표준안을 참고하여 추가 가능함을 언급하였다. 또한 디바이스 인증서 관리 프로토콜로서, 디바

이스 인증서 발급 절차, 디바이스 인증서 폐지절차, 디바이스 인증서 상태검증 절차에 관하여 기술하고 있다. 이 표준안은 ITU-T J.192 표준의 연장으로써, J.192 표준에서는 공인 인증체계 하에서 홈게이트웨이에 X.509 기반의 인증서를 발급 및 이에 대한 인증을 담당하고, 이 표준안에서는 댁내의 홈게이트웨이가 댁내의 디바이스에 대한 디바이스 인증서를 발급하고, 이에 대한 인증을 담당하기로 협의하였다. 따라서 이 표준안은 홈게이트웨이 및 홈디바이스에 대한 인증서 발급절차를 정의하고 있다. 이 표준안에 따르면, 홈게이트웨이에 최상위 인증기관 인증서를 우선 설치하여야 하고, 홈게이트웨이 인증서는 out-of-band 및 online으로 발급되고, 홈디바이스 인증서는 홈게이트웨이를 통해서 발급되거나 직접 발급될 수 있다고 기술하고 있다. 디바이스 인증서 폐지절차는 디바이스의 컴퓨팅 능력에 따라 CMP[3]를 통한 온라인 방식 및 out-of-band 방식을 사용할 수 있도록 하였다. 또한 인증서 상태 검증 절차로 OCSP[4] 또는 CRL[5] 방식을 정의하고 있다[9].

이 표준안에서 기술하는 보안요구사항은 다음과 같다.

- RSA 알고리듬의 경우 반드시 1024비트 이상의 키 길이 사용
- DSA, ECDSA 등 기타 서명 알고리듬 사용시 RSA 알고리듬과 동일한 보안 강도를 갖는 키 길이 사용
- 홈디바이스 인증서 유효기간은 디바이스 수명을 고려하여 10년 이상으로 설정
- CRYPTO2005에서 제기된 SHA-1 알고리듬 취약성에 따라 SHA-256 알고리듬 사용을 권고

3) 인증서 관리 프로토콜: 인증서를 인증기관-인증기관, 인증기관-end entity, end entity-end entity 등 각 개체 사이에서 전송하기 위한 프로토콜

4) 온라인 인증서 상태 프로토콜: 인증서 폐지 목록의 갱신 주기에 대한 문제를 해결하기 위해 폐지/효력정지 상태를 파악하여 사용자가 실시간으로 인증서를 검증할 수 있는 프로토콜

5) 인증서 폐기 목록: 폐기된 인증서를 이용자들이 확인할 수 있도록 그 목록을 배포, 공표하기 위한 메커니즘으로, 인증서와 함께 전달된다.

라. 홈네트워크 사용자 인증 메커니즘

홈네트워크 사용자 인증 메커니즘 표준안은 2007년 ITU-T Study Group17의 Question9에서 표준화되었다. 안전한 홈네트워크 서비스와 사용자 편의를 위해 다양한 인증 수단을 선택할 수 있는 표준화된 사용자 인증기술을 제안하는 것을 목표로 표준안을 제안하였다. 2005년 10월 제네바 회의에서 권고안이 채택되었고, 2006년 12월 제네바 회의에서 first draft로 채택되기 위해 표준안을 제안하였다. 2005년 제네바 회의에서 제출한 권고안에서는 패스워드, 인증서, 생체정보 등 다양한 인증수단을 사용하는 홈네트워크 사용자 인증 메커니즘을 정의할 것과, 사용자 인증 서비스 구조, 홈 개체 분류, 적용 시나리오, 홈 개체간 사용자 인증 고려사항, 사용자 인증의 기능적 요구사항, 사용자 인증의 보안 요구사항, 사용자 인증 프로토콜 등을 정의할 것을 제안하였다. 또한 사용자 인증 프로토콜은 X.homesec-1에서 제안한 홈 네트워크 일반 모델을 고려하여 개발하기로 결정하였다.

사용자 기준으로 두 가지의 홈네트워크 서비스 흐름이 표시되어 있는데, 하나는 원격 사용자가 댁내의 디바이스들에 접근하고자 하는 경우이고, 다른 하나는 댁내의 사용자가 댁내 혹은 댁외의 응용서버가 제공하는 홈서비스에 접근하는 경우이다[10]. 이 표준에서 사용자 인증을 위한 고려사항으로 인증 클라이언트와 홈 개체들간의 사용자 인증을 위한 고려사항을 정의하고, 원격 터미널과 타입 A 디바이스는 사용자 디바이스로 간주할 것, 원격터미널과 응용서버, 홈게이트웨이, 홈 응용서버, 타입 B, 타입 C 디바이스간 사용자 인증 고려사항을 정의하였으며, 타입 A와 응용서버, 홈게이트웨이, 홈 응용서버, 타입 B, 타입 C 디바이스간 사용자 인증 고려사항을 정의하였다[11].

이 표준안에서는 사용자 인증과정을 크게 세 부분으로 기술하고 있다: 서버(사용자 인증서버) 인증과정, 서버와 클라이언트 사이의 키 교환 과정, 보호된 사용자 인증 데이터 전송 과정. 서버인증 과정은

서버의 인증서를 클라이언트(사용자 단말)가 검증하는 과정이고, 서버와 클라이언트 사이의 키 교환 과정은 서버의 인증서 검증 과정의 연장선으로, 서버의 인증서를 클라이언트에 전달하는 과정에서 주고받은 메시지의 내용을 통해서 각자 키를 연산하는 과정이다. 보호된 사용자 인증 데이터 전송과정은 키 교환 과정에서 생성된 키를 이용하여 사용자 인증 데이터를 암호화하고, 이를 서버로 전송하는 과정이다. 이때 사용자 인증 데이터는 사용자의 ID/PW, 인증서, 생체정보 등 다양한 정보가 될 수 있음을 기술하고 있다.

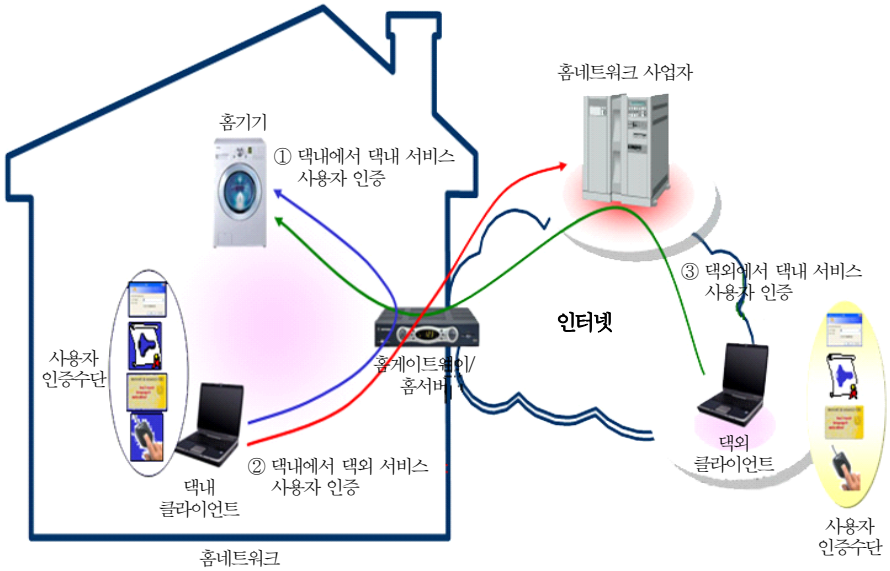
2. 국내 표준화 동향

국내에서의 홈네트워크 보안 표준화 작업은 2004년부터 시작되었다. TTA의 정보보호기반 프로젝트 그룹(PG101)과 HNSF을 중심으로 표준화가 진행되어 왔고, 진행중이다. 2004년 홈네트워크에서의 사용자 인증메커니즘에 관한 표준안이 HNSF에 제출된 것을 시작으로 홈네트워크 보안에 관한 국내 표준화 활동이 시작되었고, 홈네트워크에서의 사용자 인증 메커니즘에 관한 표준은 그 후 검토회의를 거쳐 2005년 TTA와 HNSF에서 표준으로 제정되었다. 2006년에는 홈네트워크 보안 정책 기술언어에 관한 표준안이 HNSF과 TTA PG101에 제출되었고, 2006년 12월 표준으로 제정되었다. 또한 홈네트워크를 위한 보안기술 프레임워크에 관한 표준안이 TTA PG101에 제출되었고, 2006년 12월 표준으로 제정되었다. 이 장에서는 국내에서의 홈네트워크 보안 표준화 현황 및 내용에 관하여 기술하고자 한다.

가. 홈네트워크 사용자 인증 메커니즘

홈네트워크 사용자 인증 메커니즘은 2005년 TTA [12] PG101과 HNSF[13],[14]에서 표준안으로 채택되었고, 표준화가 완료되었다. 현재 ITU-T Study Group17, Question9에서 X.homesec-3에서 국제표준으로 진행중에 있고, 국제표준안 내용은 Study Group에서의 회의 결과에 따라 국내표준의 내용에서 수정이 있을 수도 있을 것이다.

이 표준은 안전한 홈 네트워크 서비스 제공을 위해 필요한 사용자 인증 메커니즘과 홈게이트웨이와 홈네트워크 사업자 인증서버간 디바이스 인증메커



(그림 2) 세 가지 사용자 인증 메커니즘

니즘에 관하여 정의한다. 이 표준에서는 홈네트워크 서비스를 댁내 디바이스 제어, 홈네트워크 사업자 인증서버가 제공하는 서비스 이용, 댁외에서 댁내 디바이스 제어 등의 세 가지로 구분하고, 이들 서비스 이용에 필요한 사용자 인증 메커니즘을 제시하고 있다((그림 2) 참조). 또한 사용자 편의성을 위해서 인증서, 생체정보, ID/PW 등의 인증 수단을 사용자가 선택해서 인증 받을 수 있고, 사용자가 사용하고자 하는 인증수단과 홈네트워크 사업자 인증서버가 요구하는 인증수단이 상이할 경우 인증정보를 변환하는 기능을 제공하는 사용자 인증 메커니즘이 정의되어 있다.

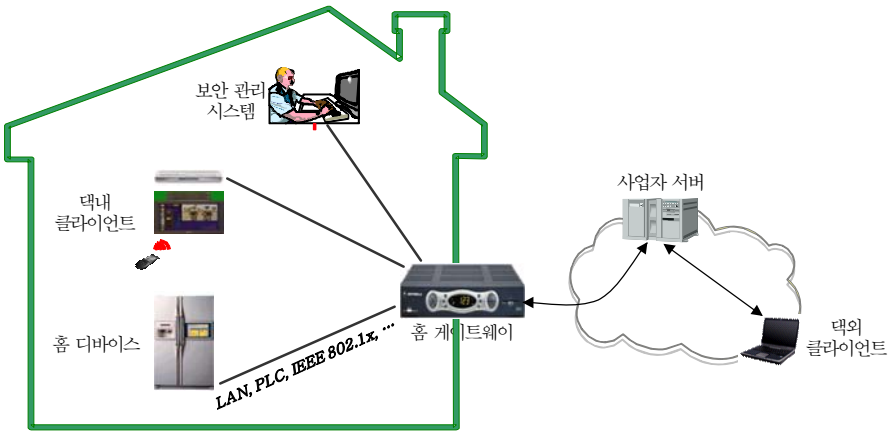
이 표준에서는 사용자 인증 정보를 보호하기 위해서 서버(사용자 인증서버)의 인증서로 서버를 인증한 후, 이 과정에서 서버와 클라이언트(사용자 단말) 사이에 나눠가진 키로 사용자 인증정보를 암호화하여 서버로 전송한다. 사용자 인증정보를 암호화하여 제3자가 사용자 인증정보를 알 수 없게 함은 물론이고, 현재 홈네트워크 서비스를 이용하는 사람이 누구인지 모르게 함으로써 프라이버시 보호 효과도 얻을 수 있음을 기술하고 있다.

나. 홈네트워크 보안 정책 기술 언어

홈네트워크 보안 정책 기술 언어에 관한 표준안은 TTA PG101과 HNSF을 통해서 각각 표준화를 추진중에 있고, 2006년 12월 중 표준으로 제정되었으며, 이 표준안은 홈네트워크 보안 서비스에 필요한 접근제어 및 다양한 보안 정책 등을 기술하는 XML 기반의 언어로서, xHDL이라 부른다. xHDL이 적용되는 홈네트워크 모델은 (그림 3)과 같다. 즉 홈네트워크는 제어의 대상이 되는 홈디바이스, 홈네트워크 서비스를 이용하는 데 사용하는 댁내/댁외 클라이언트, 보안관리를 위한 댁내의 보안관리 시스템, 댁내망과 댁외망을 연결하는 홈게이트웨이, 홈네트워크 서비스를 위한 콘텐츠를 제공하는 홈네트워크 사업자 서버로 구성되어 있다. 상황에 따라서 보안관리 시스템이 홈게이트웨이에 탑재될 수도 있을 것이다. xHDL 언어가 동작해서 홈네트워크의 보안 관련 정책을 제어하는 곳은 보안관리 시스템이다.

xHDL은 홈게이트웨이를 기반으로 하는 모든 홈네트워크 시스템에 적용 가능하고, XML 기반으로 인증 및 인가 정책을 기술할 수 있다. 또한 xHDL의 구성 요소를 정의하고 있으며, 각 구성요소에 대한 XML schema를 정의하고 있다.

xHDL의 구성요소에는 root element로써 xHDL element가 있고, 그 하위 element로써 combining_rule element, authentication element, user element, object element, object-group element, role element, rule element가 있다. 이들 element



(그림 3) xHDL을 위한 홈네트워크 모델

〈표 1〉 xHSDL Element

Combining_rule element	접근 허용 정책, 우선 순위 적용정책 등 정책간 충돌 처리 요소
Authentication element	Method, encAlgs 등 사용자 인증 메커니즘과 관련된 정책을 기술
User element	ID/Password, 보안수준, 이름, 성, 주소 등 홈네트워크 사용자의 정보 설정을 위한 요소
Object element	홈디바이스, 서비스, 센서 등 홈네트워크에서 사용 가능한 객체를 정의
Object-group element	홈디바이스, 서비스, 센서 등 홈네트워크에서 접근 가능한 자원을 그룹화 그룹을 하나의 자원으로 인식해서 접근제어와 같은 보안서비스를 제공
Role element	홈네트워크 사용자와 자원간 관계를 표현
Rule element	시간, 사용자 서비스 현황, 센서 이벤트, 홈서비스 접근 등 다양한 상황을 인지해서 해당 동작을 수행

중 object-group element와 rules element는 적용되는 정책의 환경에 따라서 생략이 가능하다. <표 1>은 각 element에 대해 간략히 설명한다.

다. 홈네트워크를 위한 보안 기술 프레임워크

홈네트워크를 위한 보안 기술 프레임워크에 관한 표준안은 TTA PG101에서 표준화를 추진중에 있고, 2006년 12월 중 표준으로 제정되었다. 앞서 기술하였듯이, 현재 ITU-T Study Group17, Question9에서 X.homesec-1에서 국제표준으로 진행중에 있다.

표준안 내용은 국외표준 현황의 2절에서 기술한 바와 비슷하다. 홈네트워크 보안을 위한 기본 모델을 정립하고, 유무선 전송기술을 고려하여 홈네트워크에서의 보안위협, 보안요구사항, 보안기능을 정의하고 있다. 또한 홈네트워크의 구성요소를 7개의 개체로 구분하고, 홈디바이스의 특성에 따라 3개의 모델로 구분하여 각 특성에 따른 보안요구사항을 기술하고 있다. 또한 ITU-T X.1121[4]과 X.805[7] 표준을 이용하여 홈네트워크에서의 보안위협 및 보안요구사항을 기술하고 있다.

Ⅲ. 홈네트워크 보안 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 홈 플랫폼 기술은 외부망과 가정을 연결하고 가정내 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, PLC, IEEE802.11 등 다양한 유/무선망의 사용이 가능하다. 홈네트워크는 적용 대상에 따라 여러 대의 PC 및 컴퓨터 관련 장비간의 통신을 위한 정보 네트워크, 가전장비 제어를 위한 자동화 네트워크, 음향 및 영상기기나 게임기 등의 오락 또는 문화생활을 위한 엔터테인먼트 네트워크 3가지 네트워크로 나눌 수 있다[15],[16].

정보 네트워크는 컴퓨터 및 그 관련 장비간의 통신을 위한 네트워크로 블루투스, 무선랜, HomeRF 등을 이용한 무선 통신과 이더넷, 전화선(Home PNA), 전력선(PLC) 등을 이용한 유선통신으로 구성이 가능하다. 장비 제어를 위한 미들웨어로는 마이크로소프트 진영이 중심이 되어 TCP/IP 프로토콜을 활용한 UPnP와 자바 진영이 중심이 된 Jini라는 프로토콜이 있다. 자동화 네트워크는 보안장비, 조명, 환기, 에어컨 등의 가전장비 제어를 위한 네트워크로서 2Mbps 이하의 저속의 통신으로 가능하며, 주로 전력선을 활용하여 통신을 한다[17]. 여기에는 LonWorks, HnCP 등의 미들웨어가 이용되고 있다. 엔터테인먼트 네트워크는 가전장비나 음향 및 영상기기(TV, VTR, DVD player, 오디오, 게임기

〈표 2〉 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)
	지능형 미들웨어 기술	홈네트워킹 미들웨어 기술
		상황적응형 미들웨어 기술
		멀티 모달 인터페이스 기술

등)에 적용되며, 100~400Mbps 정도의 고속으로 동영상이나 음악, 게임 등을 실시간으로 전송하는 네트워크이다. 여기에는 UPnP AV나 HAVi라는 음향 및 영상 장비간의 통신과 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 브리지 할 수 있는 홈게이트웨이를 개발하고 있으며, ETRI에서는 다양한 미들웨어간의 연동을 가능하게 해주는 통합미들웨어를 개발하고 있다.

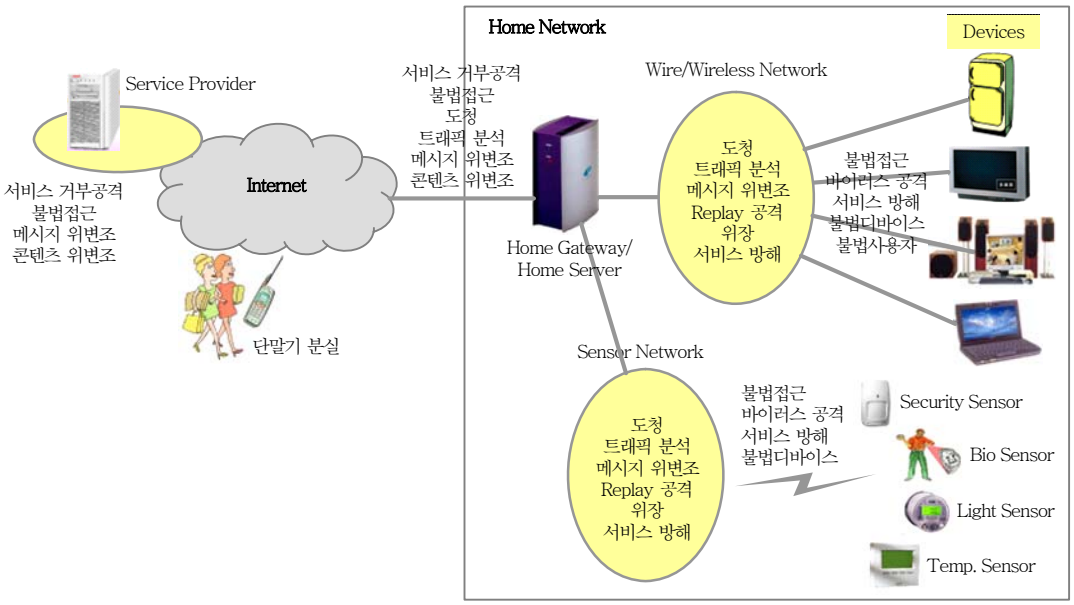
<표 2>는 홈네트워크 기술에 대한 분류를 나타내었다.

1. 홈네트워크 보안취약성

홈네트워크에서는 다양한 유·무선 네트워크와 프로토콜 등의 혼재로 기존 인터넷 등에서 발생되던 보안취약성 외에도 추가적으로 고려해야 할 보안취약성이 존재하고 있다. 즉, 홈네트워크의 모든 정보기기들은 인터넷과의 연결로 다양한 사이버공격의 대상이 될 수 있으며, 홈네트워크 내의 정보기기의 다양성과 기기간 자원의 공유 등으로 보안측면에서 고려해야 할 요구사항은 더욱 복잡하고 다양한 특성을 지니게 된다. 더욱이 홈네트워크의 정보가전기기들은 상대적으로 컴퓨팅 능력이 낮아 강력한 보안기능의 탑재가 어려우므로 사이버공격에 이용되거나 목표가 될 가능성이 더욱 높다고 할 수 있다. 홈네트워크에는 Ethernet, HomePNA, PLC, IEEE 802.1x, Bluetooth, UWB 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[18]-[21].

(그림 4)는 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.

각 디바이스의 보안이 유지되지 못한다면, 사용자의 정보가 유용될 소지를 가지고 있으며, 이와 같은 문제점은 아래의 사항과 연결하여 생각해 볼 수 있다. 홈네트워크에서는 헬스케어 서비스와 같이 생명과 직결된 바이탈신호들의 사용이 증가할 것으로 생각되고 있으며, 더욱이 생체정보를 이용한 사용자 확인으로 사용자에게 최적의 자동화된 홈서비스가 제공될 것이므로 주요 생체정보에 대한 노출이나 위변조를 통한 공격에 대비할 수 있는 보안기술개발이



(그림 4) 홈네트워크의 보안취약점

필요하겠다. 또한 개인의 행동특성이나 생활습관에 관련된 정보를 불법적으로 수집, 분석함으로써 개인에 대한 새로운 프라이버시 침해 가능성도 높다고 할 수 있다.

2. 홈네트워크 보안 기술 동향

홈네트워크는 인터넷과의 연결로 인하여 인터넷에서 발생되고 있는 다양한 사이버공격에 그대로 노출되어 있어 해킹, 악성코드, 웜 및 바이러스, DoS 공격, 통신망 도·감청 등에 보안취약성을 갖고 있다. 따라서 인터넷을 통한 사이버공격에 대응하기 위해서 대부분의 보안기능을 홈게이트웨이에 집중, 구현하여 안전성을 강화하는 형태로 기술개발이 이루어지고 있다. 현재까지 보안기능이 탑재된 다양한 상용 홈게이트웨이 제품이 개발되어 시판되고 있다. 홈게이트웨이는 댁외의 공중망과 댁내의 홈네트워크를 연결하는 입구로서 외부의 불법 침입에 대해 일차적인 대응 방안을 제공한다는 개념에서 최우선적으로 보안기능이 탑재되고 있으며, 홈게이트웨이에 탑재된 대표적인 보안기능에는 firewall, VPN 등이 있다[21]-[23].

〈표 3〉 홈게이트웨이 보안제품 현황

구분	업체 명
국내	ETRI, 알피에이네트웍스, 시큐베이, 디지스타, 지맥스테크놀로지, 기가링크
국외	Wipro, HotHardWare, FutureSoft, 2wire, linksys, 3com, 3eti, MaxGate, D-Link

<표 3>은 현재까지 개발 및 상용화된 보안기능이 제공되는 홈게이트웨이 제품 현황을 나타낸 것이다. 국외 제품의 경우, 대부분이 미국제품으로 보안측면에서 제공되는 기능은 firewall, VPN 등으로 대부분 제한적인 유사한 보안기능만을 제공하고 있다.

안전한 홈서비스 제공을 위해서는 홈네트워크 구성요소에 대한 접근제어 및 이를 위한 인증기능이 필요하게 된다. 따라서 홈게이트웨이 보안제품 외에 홈네트워크 자원에 대한 접근제어 및 인증기능 등이 제공되는 기술과 제품들이 국내외에서 개발되고 있다.

<표 4>는 현재까지 개발되었거나 개발중인 주요 홈네트워크 보안기술 개발 현황이다.

홈게이트웨이와 정보가전기기간의 제어를 위해 필요한 미들웨어들에서도 기본적인 보안기능이 제공되고 있다[4],[7]-[9],[11].

〈표 4〉 주요 홈네트워크 보안 기술 개발현황

구분	업체 명	관련 보안기능 개발현황
국내	ETRI	• 홈서비스 사업자가 요구하는 인증수단과 상이한 사용자가 원하는 인증수단을 사용해서도 인증을 받을 수 있게 하는 편의성이 강화된 안전한 통합인증 기술 개발 • 홈네트워크에 적합하고 편의성이 강화된 보안정책 기반의 경량화된 접근제어 기술개발 • 홈디바이스 환경에 적합한 경량화되고 편의성이 강화된 멀티홈 도메인용 디바이스 인증/인가 기술 개발
	안랩유비웨어	• 홈네트워크 자원에 대한 원격접근을 위한 PKI 기반의 홈네트워크 인증, 인가보안솔루션을 개발
	이니텍	• 디지털 방송을 위한 PKI 기반의 홈네트워크 보안 솔루션 개발
	소프트포럼	• 셋톱박스용 PKI 기반의 사용자 인증 기술 및 암호 기술개발
국외	MicroSoft	• PC를 홈엔터테인먼트의 중심으로 설정하여 디지털 서비스를 제공하는 e-Home을 추진중 • PC 접근을 위해 비밀번호 또는 지문 인식을 통한 사용자 인증을 연구
	CablesLabs	• 북/남미 케이블회사들로 구성된 CablesLabs에서 CableHome이라는 표준을 추진중 • 홈게이트웨이의 장치 인증, 컨트롤 데이터 및 다운로드 소프트웨어의 암호화 제공, 원격 홈게이트웨이의 firewall 기능 등을 지원
	NTT	• 일본 NTT 데이터, 후지쓰, 미쯔비시, 도쿄공업대 등에서 개인키를 포함한 스마트카드를 이용하여 원격지에서 홈네트워크를 관리하는 기술에 대해 연구중

특히 특허 분야에서 살펴보면, 국내 동향으로는 1998년까지 매년 2건 이하에 불과하던 홈네트워크 보안분야의 특허출원이 1999년 6건, 2000년 19건, 2001년 19건 등 2000년을 기점으로 출원건수가 급격히 증가하고 있다. 인증・무결성 분야 및 고성능 네트워크 보안분야의 특허출원은 활발하나, 센서네트워크 보안분야, 침입대응(침입탐지/침입감내) 기술 분야는 특허출원이 미흡하다. 한편, 국내에서는 LG전자, 삼성전자, 한국전자통신연구원이 홈네트워크 보안분야의 다출원인인 것으로 파악된다.

국제 동향을 살펴보면 홈네트워크 보안 기술의 특허 등록량이 1998년 이후부터 급격히 증가하는 추세이다. 미국 내에서 국가별 특허 등록비율은 미국이 69.8%, 일본 10.1%, 스웨덴 5.9%, 캐나다 5.3% 등이며, 우리나라는 0.6%(삼성전자 1건 등록)로 저조한 실정이다. 업체별로는 루슨트테크놀로지, 에릭슨, 노텔네트웍스, 모토롤라 등이 미국 내에서 다출원인인 것으로 조사되었다.

세부기술별로 분석해 보면 미국도 한국, 일본과 유사하게 인증・무결성 분야 및 고성능 네트워크 보안분야에서 특허출원이 가장 활발하며, 센서 네트워크 보안 기술, 침입탐지 및 침입감내 기술, 미들웨어 보안 기술은 특허출원이 미미한 것으로 나타났다.

Ⅳ. 결론

우리나라는 세계수준의 네트워크 인프라와 전자/반도체 기술 등이 있으므로 PC 보급과 광대역 통신과 같은 인프라 보급이 뒷받침된다면 홈네트워크 수요가 활성화 될 것이다. 유비쿼터스 컴퓨팅 환경 구현을 통해 창출될 시장규모가 580조 원을 상회할 것이라는 노무라종합연구소의 연구보고서만 보아도 유비쿼터스 컴퓨팅 환경의 시작점으로 인식되고 있는 홈네트워크가 가져올 기대효과는 엄청날 수 있다. 홈네트워크 서비스는 생소한 기술이 아니라, 우리의 실생활에 녹아 있다. 지금까지의 홈네트워크는 홈오토메이션 위주로 흘러왔지만, 앞으로는 홈오토메이션에서 한발 더 나아가 IPTV, VoD, 원격진료, 단지별 커뮤니티 형성 등 다양한 콘텐츠가 제공되는 폭넓은 서비스로 발전할 것이다. 또한 유비쿼터스 기술의 적용으로 지능화된 홈오토메이션 서비스가 제공될 것이다. 홈네트워크 서비스가 발전할수록 서비스 이용과정에서 사용자 정보를 많이 필요로 하므로 홈네트워크에 대한 보안의 중요성은 더욱 커지게 될 것이다.

따라서 국내외에서 홈네트워크에서의 보안에 관한 관심이 고조되고 있고, 활발한 표준화 활동이 진행되고 있다. 본 고에서는 현재 발표된 표준과 홈네

트워크 보안 기술동향 및 특허동향에 대해 간략히 기술하였다. 현재는 우리나라가 홈네트워크 보안에 관한 활동이 가장 활발하고, 홈네트워크 보안에 관한 표준을 이끌어가고 있다. 홈네트워크 및 홈네트워크 보안에 관한 종주국으로 내세우기에 손색이 없도록 더욱 활발한 연구가 이루어지고, 그 결과가 더욱 빛날 수 있기를 기대해 본다.

● 용 어 해 설 ●

보안 정책 기술 언어: 홈네트워크 내의 홈 디바이스의 접속에 따라 그 접근 범위가 결정되게 된다. 홈네트워크 디바이스 각각에 대한 보안정책을 XML 형태로 xDHL을 제공함으로써 각 홈디바이스의 접근제어를 용이하게 제공하는 언어이다.

보안관리 시스템: 홈디바이스 혹은 사용자에 따라 다양한 인증, 인가 방법이 존재하며, 각각의 홈디바이스, 사용자에 따른 보안 관리를 제공함으로써 용이한 접근을 수행할 수 있게 한다.

약 어 정 리

AAA	Alternative Approval Process
CA	Certificate Authority
CMP	Certificate Management Protocol
CRL	Certificate Revocation List
DoS	Denial of Service
FTTH	Fiber To The Home
HAVi	Home Audio Video interoperability
HnCP	Home Network Control Protocol
HNSF	Home Network Security Forum
HomePNA	Home Phoneline Networking Alliance
HomeRF	Home Radio Frequency
ITU-T	International Telecommunication Union-Telecom Standardization
OCSP	Online Certificate Status Protocol
PLC	Power Line Communication
SG	Study Group
TD	Temporary Document
TTA	Telecommunications Technology Association, 한국정보통신기술협회
UPnP	Universal Plug and Play
UWB	Ultra Wide Band
VPN	Virtual Private Network
WPAN	Wireless Personal Area Network
xHDL	eXtensible Home security Description Language

참 고 문 헌

[1] ITU-T, http://www.itu.int/ITU-T

[2] HNSF, "제 3회 홈네트워크 시큐리티 워크숍," *In Proc. of HNSF*, July 2006.

[3] HNSF, "제3회 홈네트워크 정보보호 표준 심포지엄," *In Proc. of HNSF*, Nov. 2006.

[4] 염흥열, "ITU-T SG17 종단간 이동 통신 보안을 위한 보안 정책 및 홈네트워크 보안 프레임워크에 관한 표준화 동향," *TTA IT Standard Weekly*, 2005-05호, Jan. 2005.

[5] P. Walter, "Home Network Security-Part 1: Security Requirements," ISO/IEC, June 2005.

[6] Jong Hyun Baek, Dong-Young Yoo, and Heung Youl Youm, "Proposal for Draft Recommendation of X.homesec-2: Device Certificate Profile for the Home Network," Nov. 2006.

[7] Draft ITU-T Recommendation X.805, Security architecture for systems providing end-to-end communications, 2003.

[8] Heung Youl Youm and Heung Ryong Oh, "Proposal for Final Draft Recommendation X.homesec-1 – Framework of Security Technologies for Home Network," ITU-T, Nov. 2006.

[9] Jonghyun Baek, Dong-Young Yoo, and Heung Youl Youm, "Proposal for Draft Recommendation of X.homesec-2: Device Certificate Profile for the Home Network," Nov. 2006.

[10] Geon Woo Kim, Jong Wook Han, and Kyo Il Chung, "Proposal of First Draft on X.homesec-4: Authorization Framework for Home Network," 2007. 9.

[11] Hyung-kyu Lee, Yun-kyung Lee, Jong-wook Han, Kyo-il Chung, Dae-hun Nyang, and Heung-youl Youm, "Proposal for the First Draft Recommendation of X.homesec-3 – User Authentication Mechanism for Home Network Services," Nov. 2006.

[12] TTA, http://www.tta.or.kr

[13] HNSF, http://www.hnsf.org

[14] 이윤경, 한종욱, 정교일, "홈네트워크 보안 표준화 동향," 전자통신동향분석, 제22권 제1권, 2007. 2., pp.73-82.

[15] 박광로, 송영준, "홈네트워킹," TTA 저널, 제78호, 2001, pp.101-109.
[16] 전호인, "디지털홈기술 및 표준화동향," TTA 저널, 제88호, 2003, pp.59-73.
[17] Carl M. Ellison, "Interoperable Home Infrastructure Home Network Security," *Intel Technology Journal*, Vol.6, 2002, pp.37-48.
[18] 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 Int'l Symp. on Consumer Electronics(ICSE)*, June 2006.
[19] Jin-Bum Hwang, Hyung-Kyu Lee, and Jong-Wook Han, "Efficient and User Friendly Inter-domain Device Authentication/Access Control for Home Networks," EUC 2006, 2006. 8., pp.131-140.
[20] Jin-Bum Hwang and Jong-Wook Han, "A Security Model for Home Networks with Authority Delegation," ICCSA-4, 2006. 5., pp.360-369.
[21] 김도우, 한종욱, 정교일, "홈디바이스 인증/인가 기술동향," 정보통신연구진흥원, 주간기술동향, 제 1326호, 2008, pp.1-11.
[22] 한종욱, 이덕규, 정교일, "홈네트워크 보안기술 동향," 한국통신학회학회지, 2006. 9., pp.113-124.
[23] 윤철, "최근의 홈네트워크 기술동향 및 시장전망," 주간기술동향, 제1098호, 2003, pp.22-33.