홈네트워크 보안 표준화 동향

Trend of Home Network Security Standardization

u-IT839의 정보보호 이슈 특집

이윤경 (Y.K. Lee) 홈네트워크보안연구팀 연구원
한종욱 (J.W. Han) 홈네트워크보안연구팀 책임연구원
정교일 (K.Y. Chung) 정보보호기반그룹 그룹장

목 차

홈네트워크는 이종의 유무선 네트워크와 프로토콜이 합해져서 하나의 네트워크를 형성하기 때문에 많은 보안 헛점이 존재할 수 있다. 설사 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. 이러한 홈네트워크에서의 보안 취약성을 해결하기 위하여 최근 국내외에서 다양한 표준이 제정되고 있고, 또한 많은 표준안들이 논의되고 있다. 본 고에서는 홈네트워크 보안에 관한 국내외 표준화 진행 현황에 대하여 소개하고, 각 표준 및 표준안의 주요 내용에 대하여 기술하고자 한다.

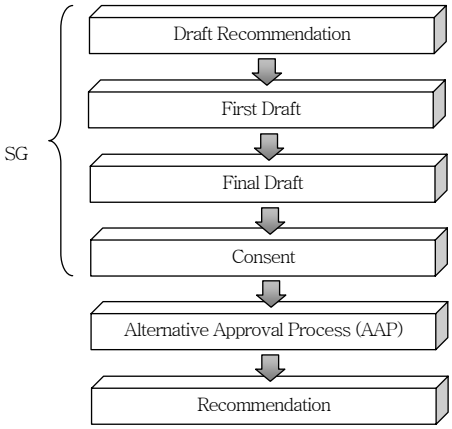
Ⅰ. 서론

홈네트워크에 대한 관심이 높아지면서 홈네트워크에서의 보안에 관한 관심도 함께 높아지고 있다. IEEE 802.15(WPAN)에서 개발된 기술들이 홈네트워크의 일부로 자리매김 하게 됨에 따라, 이들 기술들에 적용된 보안 기술이 홈네트워크에서의 보안으로 인식된 적도 있었다. 그러나, 홈네트워크 서비스를 실생활에 적용하고자 하는 움직임이 나타나면서 구체적인 서비스 모델이 나오게 되었고, 이들에 대한 보안이 고려되게 되었다. 그 결과물로 2005년 ISO에서 홈네트워크 보안 요구사항과 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 있고, 홈네트워크 보안관련 표준 개발도 시작단계에 있다[1].

한편 국내에서는 HNSF와 TTA를 중심으로 홈네트워크 보안에 관한 표준이 개발되고 있는데, 2004년부터 표준이 꾸준히 발표되고 있다. 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 표준안을 발표하였다. 특히, '홈네트워크 보안 기술 프레임워크' 표준안은 2006년 12월 ITU-T 제네바 회의에서 국가별 의견수렴 과정인 consent 과정을 완료하였다.

Ⅱ. 국외 표준화 동향

홈네트워크 보안에 대한 국외 표준화는 ISO에서 2005년에 표준안이 한 건 있었고, ITU-T에서 진행중인 표준안이 3건이 있다. ITU-T에서 진행중인 표준안들은 SG17의 Question9에서 진행중이다.



(그림 1) ITU-T 표준화 절차

Question9은 X-homesec-1, X-homesec-2, X-homesec-3의 세 부분으로 나뉘어져 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 제목 아래 표준화가 진행중이다[2]. 본 장에서는 ISO에서 2005년에 표준화가 완료된 표준과 ITU-T SG 17 Question9에서 진행중인 표준안들에 관해 기술하고자 한다. 또한 ITU-T 표준화 절차[2]-[4]는 (그림 1)과 같다.

1. 홈네트워크 보안

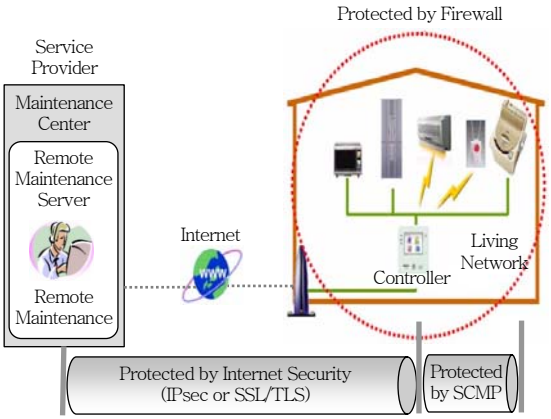
홈네트워크 보안 전반에 관하여 다룬 표준이다. ISO/IEC에서 2005년 6월 표준으로 발표되었고, "Home network security"라는 주제 하에 세 부분으로 나뉘어 표준이 완성되었다: security requirements, internal security service, external security service[5].

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 2)는 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 SSL혹은 TLS를 이용한다. 이들 메커니즘과 방화벽의 조합을 통한 댁외 보안은 'low cost', 'low complexity', 'moderate inconvenience'를 제공한다. (그림 2)에서는 댁내의 보안은 SCMP, 댁외의 보안은 SSL/TLS와 IPsec을 이용할 수 있음을 나타낸다.



(그림 2) 댁내 및 댁외 보안

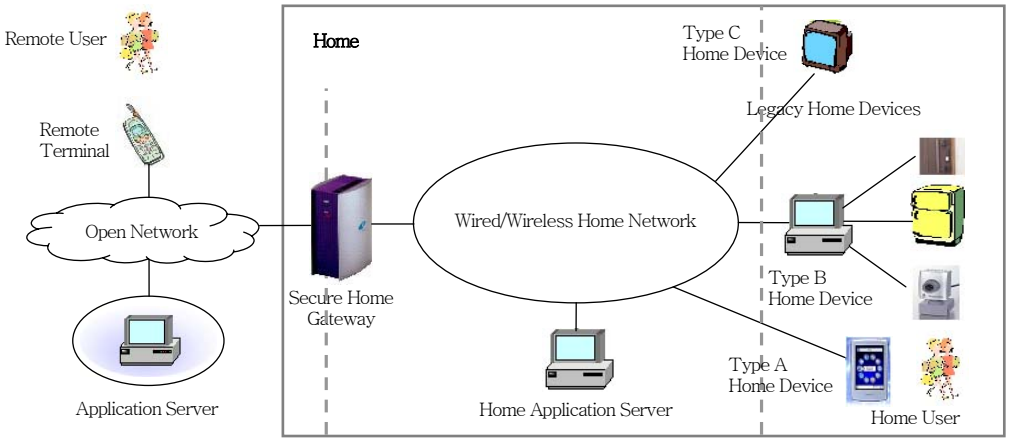
2. 홈네트워크 보안기술 프레임워크

홈네트워크 보안기술 프레임워크는 국내 표준화 기관인 TTA에서 표준으로 채택되었고, 현재 ITU-T에서 표준화 과정에 있다. 앞서 기술하였듯이 ITU-T SG17 Question9의 X-homesec-1에서 논의중인 이 표준안은 댁내 및 댁외에서의 홈네트워크 사용자에 대한 보안위협, 보안요구사항, 보안위협 해결방안 등을 다루고 있다. 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 완료하였다.

이 표준안은 유무선 전송기술을 고려한 홈네트워크 보안위협, 보안요구사항, 보안기능을 정의하고, 원격사용자, 원격 터미널, 응용서버, 보안 홈게이트웨이, 홈 응용서버, 홈사용자, 홈디바이스의 7개 개체로 구성된 홈네트워크 일반모델과 3가지 홈디바이스 모델을 제안하고 있다. 또한 홈네트워크에서의 보안위협 및 보안요구사항에 관하여 기술하고 있는데, 이 부분은 X.1121[1][1]과 X.805[6][2] 표준에 기반을 두고 있다[3],[4]. 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[7].

(그림 3)은 이 표준안에서 제안한 홈네트워크 보안 모델을 보여주는데, 이 그림은 ITU-T SG17 Question9의 다른 표준안들에서도 기본 모델로 사용하고 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



(그림 3) 홈네트워크 보안 기본 모델

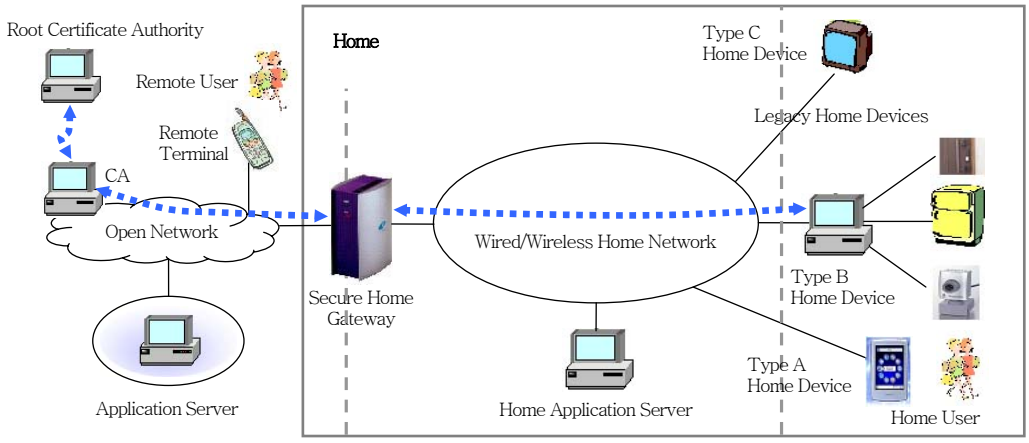
이 표준에서는 홈네트워크가 전력선, 무선통신, 유선 케이블 등 다양한 전송 매체를 사용하고, 이들은 유선 및 무선 매체가 섞여 있으므로 유선뿐만 아니라 무선 네트워크상의 위협까지도 고려해야 한다는 특성이 있음을 강조하고, 이에 대한 보안 위협 및 보안요구사항들을 정의하고 있다. 이 표준에서 기술하고 있는 일반적인 보안 위협에는 도청, 폭로, 가로채기, 통신방해, 통신교란, 데이터 삽입 및 수정, 비인가된 접근, 부인, 패킷 비정상 포워딩 등이 있고, 모바일 통신상에서의 보안위협으로는 도청, 폭로, 가로채기, 통신방해, 통신교란, 어깨너머보기, 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, 보안 기능으로 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 보안 기능들을 Y(해당 보안 기능을 반드시 적용), K(표시된 보안 기능으로 강화), X(선택적 보안 기능 추가)의 세 가지 단계로 표시하고 있다.

3. 홈네트워크용 디바이스 인증서 프로파일

홈네트워크용 디바이스 인증서 프로파일 표준안은 현재 ITU-T SG17의 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 보안요구사항 추가, 참조표준 변경, ASN.1 표현방식 변경 등의 표준안 수정에 대한 요구사항을 반영하여 TD를 작성, 차기 회의인 2006년 12월 제네바 회의에서 first draft를 제안할 것을 협의하였다.

이 표준안에서는 (그림 4)와 같은 디바이스 인증 모델 하에서 디바이스를 인증하기 위한 디바이스 인증서 프로파일을 제시하고, 디바이스 인증서 발급 및 폐지 프로토콜, 보안요구사항을 기술하였다. (그림 4)에서 나타나 있듯이, 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.



(그림 4) 디바이스 인증 모델

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, 확장 필드의 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 프로토콜로써 디바이스 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[8].

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.

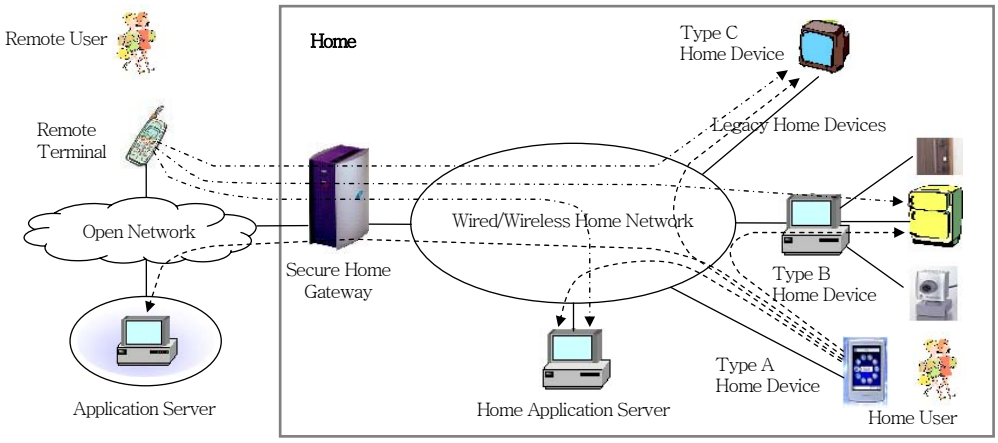
4. 홈네트워크 사용자 인증 메커니즘

홈네트워크 사용자 인증 메커니즘 표준안은 현재 ITU-T SG17의 Question9에서 표준화를 진행중이다. 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 서비스구조, 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 홈네트워크 일반 모델을 고려하여 개발하기로 결정하였다.

(그림 5)에서는 (그림 3)의 홈네트워크 보안 일반 모델을 기반으로 홈네트워크 서비스 구조를 정의하고, 이에 맞춰 사용자 인증 메커니즘을 제시할 것을 보여주고 있다. (그림 5)에는 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.

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[9].

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



(그림 5) 사용자 인증을 위한 홈네트워크 서비스 구조

정이다. 이때 사용자 인증 데이터는 사용자의 ID/PW, 인증서, 생체정보 등 다양한 정보가 될 수 있음을 기술하고 있다.

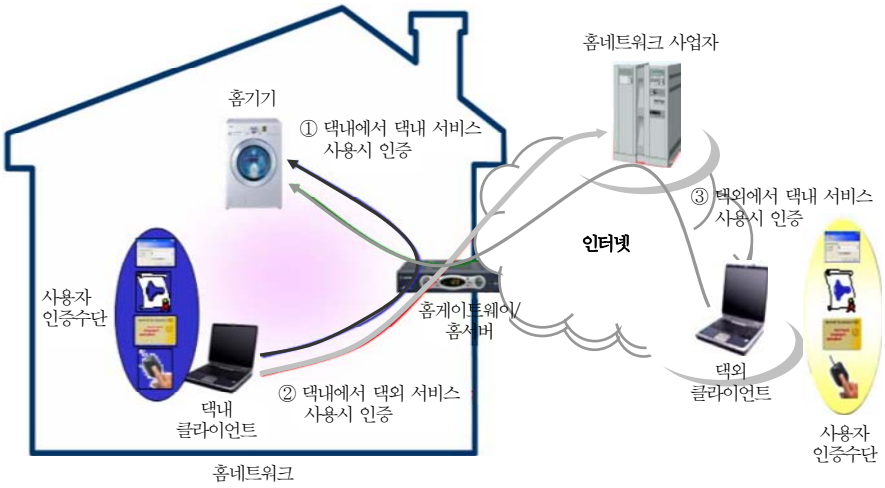
Ⅲ. 국내 표준화 동향

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.

1. 홈네트워크 사용자 인증 메커니즘

홈네트워크 사용자 인증 메커니즘은 2005년에 TTA[10] PG101과 HNSF[11]에서 표준안으로 채택되었고, 표준화가 완료되었다. 현재 ITU-T SG17 Question9에서 X.homesec-3에서 국제 표준으로 진행중에 있고, 국제 표준안 내용은 SG에서의 회의 결과에 따라 국내 표준의 내용에서 수정이 있을 수도 있을 것이다.

이 표준은 안전한 홈네트워크 서비스 제공을 위해 필요한 사용자 인증 메커니즘과 홈게이트웨이와 홈네트워크 사업자 인증서버간 디바이스 인증메커니즘에 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 6) 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.

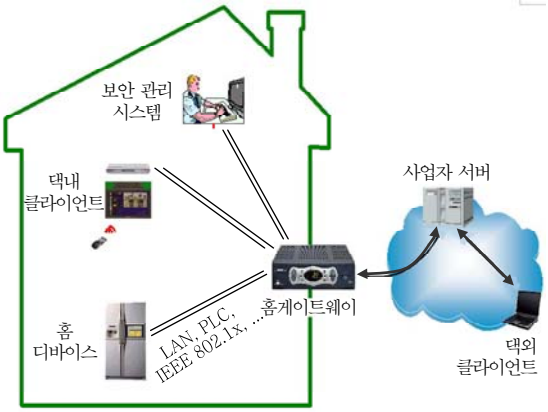


(그림 6) 세 가지 사용자 인증 메커니즘

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 제 3자가 사용자 인증정보를 알 수 없게 함은 물론이고, 현재 홈네트워크 서비스를 이용하는 사람이 누구인지 모르게 함으로써 프라이버시 보호 효과도 얻을 수 있음을 기술하고 있다.

2. 홈네트워크 보안 정책 기술 언어

홈네트워크 보안 정책 기술 언어에 관한 표준안은 TTA PG101과 HNSF을 통해서 각각 표준화를 추진하여, 2006년 12월 표준으로 제정되었다. 이 표준안은 홈네트워크 보안 서비스에 필요한 접근제어 및 다양한 보안 정책 등을 기술하는 XML 기반의 언어로써, xHDL이라 부른다. xHDL이 적용되는 홈네트워크 모델은 (그림 7)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.



(그림 7) xHDL을 위한 홈네트워크 모델

〈표 1〉 xHDL Element

Combining_rule element	- 접근 허용 정책, 우선순위 적용 정책 등 정책간 충돌 처리요소
Authentication element	- Method, encAlgs 등 사용자 인증 메커니즘과 관련된 정책을 기술
User element	- ID/PW, 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

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

3. 홈네트워크를 위한 보안기술 프레임워크

홈네트워크를 위한 보안기술 프레임워크에 관한 표준안은 TTA PG101에서 표준화를 추진중에 있고, 2006년 12월 표준으로 제정되었다. 앞서 기술하였듯이, 현재 ITU-T SG17 Question9에서 X.homesec-1에서 국제 표준으로 진행중에 있다.

표준안 내용은 국외 표준화 현황의 2절에서 기술한 바와 비슷하다. 홈네트워크 보안을 위한 기본 모

델을 정립하고, 유무선 전송기술을 고려하여 홈네트워크에서의 보안위협, 보안요구사항, 보안기능을 정의하고 있다. 또한 홈네트워크의 구성 요소를 7개의 개체로 구분하고, 홈디바이스의 특성에 따라 3개의 모델로 구분하여 각 특성에 따른 보안요구사항을 기술하고 있다. 또한 ITU-T X.1121[1]과 X.805[6] 표준을 이용하여 홈네트워크에서의 보안위협 및 보안요구사항을 기술하고 있다.

Ⅳ. 결론

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 표준화 과정이 진행중인 표준안의 내용에 대하여 간략히 기술하였다. 현재까지의 표준화 움직임에 더해서 홈디바이스의 인증 및 인가에 대한 표준 제정이 필요할 것으로 본다. 또한 홈디바이스 인증서에서는 기존의 사용자 인증 체계와의 호환성을 고려하여 X.509 기반으로 가되, 홈디바이스의 특성을 포함할 수 있는 확장 필드를 추가하는 방향으로 나아가는 것이 바람직할 것으로 본다.

현재는 우리나라가 홈네트워크 보안에 관한 표준화 활동이 가장 활발하고, 홈네트워크 보안에 관한 표준을 이끌어 가고 있다. 홈네트워크 및 홈네트워크 보안에 관한 종주국으로 내세우기에 손색이 없도록 더욱 활발한 표준화 활동이 이루어지고, 현재 표준화 과정에 있는 표준안들이 표준으로 발표될 날을 기대해본다.

● 용 어 해 설 ●

SSL/TLS (Secure Socket Layer/Transport Layer Security): SSL은 Netscape사에서 Netscape 웹브라우저 보안을 위해 고안한 프로토콜로써, 그 후 IETF에서 SSL의 취약점을 보완하여 SSL 3.0을 Internet Draft로 제안하였다. 그 후 SSL 3.0을 수정하여 SSL 3.1에 해당하는 TLS 1.0을 RFC 2246으로 발표하였다. SSL/TLS는 디지털 서명을 통하여 서버와 클라이언트를 인증하고, 비밀키 교환 및 메시지 인증코드를 이용하여 데이터 암호화 및 위/변조를 막기 위해서 사용하는데, 현재 대부분의 웹브라우저에서 지원하고 있다.

약 어 정 리

AAA	Alternative Approval Process
CA	Certificate Authority
CMP	Certificate Management Protocol
CRL	Certificate Revocation List
HNSF	Home Network Security Forum
ITU-T	International Telecommunication Union-Telecom Standardization
OCSP	Online Certificate Status Protocol
SG	Study Group
TD	Temporary Document
TTA	Telecommunications Technology Association, 한국정보통신기술협회
WPAN	Wireless Personal Area Network
xHDL	eXtensible Home security Description Language

참 고 문 헌

[1] 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.
[2] ITU-T, http://www.itu.int/ITU-T
[3] HNSF, “제 3회 홈네트워크 시큐리티 워크숍,” *in Proc. of HNSF*, July 2006.

[4] HNSF, "제3회 홈네트워크 정보보호 표준 심포지움," *in Proc. of HNSF*, Nov. 2006.
[5] P. Walter, "Home Network Security-Part 1: Security Requirements," ISO/IEC, June 2005.
[6] Draft ITU-T Recommendation X.805, Security architecture for systems providing end-to-end communications, 2003.
[7] 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.
[8] 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.
[9] 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.
[10] TTA, http://www.tta.or.kr
[11] HNSF, http://www.hnsf.org