情 報 保 護 學 會 誌
第 16 卷 第 6 號, 2006. 12

ITU-T SG17 홈네트워크 보안 표준화 동향 및 향후 전망

오 흥 룡*, 염 흥 열**

요 약

국제표준화기구 ITU-T SG17 WP2(Security)에서는 정보통신 보안에 관한 표준을 주도하는 연구그룹으로 산하 7개의 연구과제(Question)를 구성하여 정보보호 표준화 작업을 진행하고 있다. 이 연구과제들 중 Q9/17에서는 안전한 통신 서비스라는 이름으로 홈네트워크, 모바일, 웹 서비스, P2P, 안전한 응용 프로토콜 및 RFID 보안에 대한 표준을 개발 중에 있다. 본 논문에서는 이들 표준화 아이템들 중에 홈네트워크 보안 표준(안)들을 분석하고, 최근 개최되었던 국제회의 주요결과 및 향후 대응전략을 소개하고자 한다.

Ⅰ. 서 론

홈네트워크 기술은 가정 내의 모든 정보가전기기가 유/무선으로 연결되어 누구나 기기, 시간, 장소에 구애받지 않고 다양한 홈 디지털 서비스를 제공받을 수 있는 미래지향적인 가정 환경을 제공함으로써, 삶의 질을 향상시키고 국민의 정보수요 격차를 해소하기 위한 수단을 제공하는 기술이다. 이런 홈네트워크 기술은 액세스망과 홈네트워크를 연결하기 위한 홈버서/홈게이트웨이 기술, 사용자의 편의성 제공을 위한 미들웨어기술, 그리고 가정정보화인프라 구축을 위한 유/무선 홈네트워크 기술 등으로 분류되어 개발되고 있으며, UPnP, IEEE, ISO 등에서 표준화 작업이 추진되고 있다. 그리고 ITU-T내에서는 홈네트워크 원천기술과 관련된 부분은 SG9에서 표준화가 추진되고 있으며, SG17에서는 보안적인 관점에서 필요한 홈네트워크 보안 표준을 개발하고 있다. SG17의 홈네트워크 보안은 지난 일본 동경 회의(2004.11.)에서 한국을 중심으로 홈네트워크 보안을 연구키로 합의되었으며, 현재 표 2과 같이 3건의 표준(안)이 한국 주도하에 개발되고 있으며, 이번 스위스 제네바 회의(2006.12.)에서 인가 프레임워크와 관련된 표준(안)을 제안할 예정이다.

본 논문에서는 SG17 산하 Q.9에서 개발되고 있는 홈네트워크 보안 표준(안) 3건을 분석하고, 최근에 개최되었던 주요회의 결과와 향후 홈네트워크 보안에 대한 전망 및 국내 대응전략을 제시하고자 한다.

Ⅱ. SG17(개방형시스템기술, 보안, 언어 및 소프트웨어)

ITU-T 내에 SG17은 LSB(Lead Study Group)으로 정보통신 시스템 상에서 정보보호 분야의 표준들을 개발하고 있다. 주요임무로는 정보보호 관련 다른 표준화기구 및 ITU-T 내 SG들의 보안 관련 대응, 전반적인 ITU-T 보안 프레임워크 및 협력방안 검토, 보안 표준화 아이템에 대한 SG들의 운선순위 결정, 보안메뉴얼, 보안요약물, 보안워크샵 및 사이버심포지엄 등의 업무를 수행하고 있다. SG17 산하 보안 영역인 WP2는 총 7개의 연구과제로 분류되어 표 1과 같은 영역으로 보안 표준을 개발하고 있다.

Ⅲ. 홈네트워크 보안 표준(안)

SG17에서 개발되고 있는 홈네트워크 보안 표준(안)은 표 2와 같으며, 이중에 X.homesec-1은 이번

본 연구는 2006년 11월 1일 이전까지 수행된 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었습니다. (IITA-2005-(C1090-0502-0020))
* 한국정보통신기술협회 표준화본부 (hroh@tta.or.kr)
** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

제네바 회의에서 국가별 의견수렴(consent)으로 추진할 예정이다.

〔표 1〕 SG17 WP2 Question별 연구활동 영역

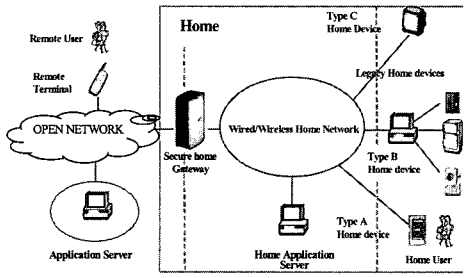
연구과제	제목	연구활동 영역
Q.4	통신 시스템 보안 프로젝트	- 보안 비전, 로드맵 - 보안 관련된 요약물 - 보안 워크샵 및 행사
Q.5	보안 구조 및 프레임워크	- 보안구조 및 모델 - 보안개념 및 프레임워크 - X.800 series, X.805
Q.6	사이버 보안	- 취약점 공유 방법 - 인터넷 침해사고 관리 - 사이버 보안 솔루션
Q.7	보안관리	- 정보보호관리시스템 - 침해사고 관리 방법론 - 위협 및 취약점 관리 방법 - X.1051
Q.8	바이오인식	- 바이오인식 프레임워크 - 바이오인식 메커니즘 - 바이오인식 정보 보호방안 - X.1081
Q.9	안전한 통신 서비스	- 모바일, 홈네트워크 보안 - 웹서비스, P2P, RFID 보안 - 안전한 응용프로토콜 보안 - X.1121, 1122, 1141, 1142
Q.17	스팸대응	- IP 멀티미디어 스팸대응 - e-mail 스팸대응 - 스팸대응을 위한 기술사항

〔표 2〕 SG17 홈네트워크 보안 표준(안) 현황

No.	표준(안)	에디터	완료시기
X.homesec-1	Framework for security technologies for home network	염흥열 오흥룡	2007/1Q
X.homesec-2	Certificate profile for the device in the home network	유동영 백종현	2007/3Q
X.homesec-3	User authentication mechanisms for home network service	이형규	2008/4Q
제안예정	Framework of authorization in home network	김건우	2008/4Q

1. X.homesec-1[1]

홈네트워크 보안 표준의 첫 번째는 "홈네트워크를 위한 보안기술 프레임워크(X.homesec-1)" 표준으로 유/무선 전송기술을 고려하고 있으며, 홈네트워크 사용자 및 원격사용자의 보안적 측면에서 보안위협과 보안요구사항들을 정의하였다. 그리고 홈네트워크에서 응용 가능한 보안기술과 보안위협들을 해결하기 위한 보안 기능들을 정의하였으며, 이런 보안 기능들을 구현 가능한 계층들을 정의하였다.



〔그림 1〕 홈네트워크를 위한 보안 모델

그림 1은 홈네트워크를 위한 보안 모델로 원격사용자, 원격터미널, 응용서버, 안전한 홈게이트웨이, 홈응용서버, 홈디바이스, 홈유저 등 7개의 개체들로 구성된다. 여기에서 홈디바이스는 Type A, B, C로 재분류하였다. 원격사용자는 홈네트워크에 있는 디바이스를 제어하기 위하여 원격터미널을 이용하는 사용자이다. 원격터미널은 외부에서 댁내에 있는 디바이스에 연결하기 위해 사용되는 장치이다. 응용서버는 외부에서 제공되는 다양한 멀티미디어 서비스 및 응용 서비스들을 댁내에 제공하는 역할을 한다. 안전한 홈게이트웨이는 보안적 관점에서 정의한 댁내 게이트웨이로써, 외부 네트워크와 댁내 네트워크 사이에서 주어진 보안정책에 따라 데이터 패킷 전송, 보안 파라미터 변환, 사용자 인증, 패킷 필터링, 침입차단 등의 보안 기능을 수행한다. 홈응용서버는 원격터미널과 홈디바이스들을 연결하게 하며, 원격사용자 및 홈유저들에게 댁내에 존재하는 멀티미디어 서비스나 다양한 응용서비스들을 제공한다. 홈유저는 댁내에서 홈네트워크 디바이스나 외부 네트워크의 다양한 서비스에 접근하고자 하는 사용자이다. 홈디바이스는 댁내에 존재하는 개체로써 홈유저들에게 편리한 서비스를 제공하기 위한 장치들이다. 이는 보안적 관점에 따라 다시 Type A, B, C로 분류되는데, A에는 다른 홈디바이스들을

제어하는 기능을 가지고 있는 PC, PDA 등이 이에 해당하고, B는 브리지 역할을 하는 홈디바이스로 통신 인터페이스가 없는 홈디바이스 C와 연결해주는 역할을 한다. 즉, Bluetooth, HAVi 등의 기능을 가지고 있는 장치들이다. C는 단지 디스플레이 기능만을 가지고 있는 보안카메라, A/V 장치 등이 이에 해당한다.

홈네트워크 일반 모델에서는 원격유저와 원격터미널, 원격터미널과 안전한 홈게이트웨이, 원격터미널과 홈응용서버, 원격터미널과 홈디바이스, 응용서버와 안전한 홈게이트웨이, 응용서버와 홈응용서버, 응용서버와 홈디바이스, 안전한 홈게이트웨이와 홈디바이스, 홈응용서버와 홈디바이스, 홈디바이스와 홈유저, 홈디바이스와 다른 홈디바이스, 안전한 홈게이트웨이와 홈응용서버 간의 관계들을 고려하여야 한다. 본 프레임워크에서는 총 12가지의 관계에 존재하는 보안위협과 보안요구사항, 이를 해결하기 위한 보안기능들을 정의하고 있다.

홈네트워크 환경에서 고려되어야 할 특징들은 다음과 같다.

- 다양한 전송매체 기술이 사용되고 있음(전력선, 유/무선 통신, 전화 케이블 등이 사용됨에 따라 도청, 가로채기, 서비스거부공격, 중간자공격 등에 노출되기 쉬움)
- 홈네트워크는 유/무선 네트워크로 구성되어 있음(보안위협으로부터 유/무선 네트워크를 모두 고려해야 함)
- 홈네트워크는 보안 관점에서 다양한 환경으로 구성됨(개인 혼자 살고 있는 환경, 자녀들과 함께 살고 있는 환경, 룸메이트들로 구성된 환경 등 다양한 환경이 존재함)
- 원격터미널은 원격사용자에 의해서 이동됨(외부 네트워크에서 댁내에 존재하는 디바이스들을 제어하기 위하여 항상 휴대됨)
- 홈디바이스들은 특징에 따라 다양한 보안 등급이 적용되어야 함(Type A, B, C에 따르거나, 서비스되는 특징들에 따라 차별화됨)

홈네트워크에 존재하는 보안 위협들은 ITU-T X.1121(모바일 종단간 데이터통신을 위한 보안기술 프레임워크) 표준에서 정의한 일반적인 보안위협들과 모바일 원천적으로 존재하는 보안 위협들, X.805(종단간 데이터통신을 위한 보안구조)에서 정의한 보안위협들에서 도출하여 정의하였다. X.1121과 X.805에서 도출한 보안위협들은 도청, 폭로, 가로채기, 통신방해, 데이터 변경이나 삽입, 비인간된 접근, 부인방지, 불규칙한 패킷 등의 일반적인 보안위협과 모바일 원천적으로 존재하는 어깨 넘어 도청, 단말기 분실, 예기치 못한 셧다운, 입력 에러 등의 보안위협을 도출하였다. 그리고 이들의 보안위협들과 홈네트워크를 위한 보안 모델과의 관계를 재정의 하였다. 그리고 X.1121과 X.805에서 보안요구사항으로 데이터 비밀성, 데이터 무결성, 인증성, 접근제어, 권한부여, 부인방지, 통신흐름보안, 프라이버시보안, 유용성을 도출하였으며, 보안위협과 보안요구사항과의 관계를 재정의 하였고, 이를 기반으로 홈네트워크 일반 모델에서 각 개체들간에 요구되는 보안요구사항들을 정의하였다. 다음으로는 홈네트워크 보안요구사항들을 만족하기 위한 보안기능들을 정의하였다. 즉, 암호화 기능, 디지털 서명 기능, 접근제어 기능, 데이터 무결성 기능, 인증성 기능, 공증 기능, MAC 기능, 키관리 기능들을 정의하였고, 홈네트워크에서 보안기능들과 보안요구사항들과의 관계를 정의하였다. X.homesec-1에서는 지금까지 정의된 각각의 관계 및 분석을 통하여 표 3과 같은 홈네트워크를 위한 보안 모델과 보안 기술들의 관계를 정의하였으며, 본 모델에서 각 개체간에 보안 구현이 필요한 계층과 홈네트워크를 위한 보안기능 요구사항으로 총 13가지의 요구사항을 정의하였다.

① 홈네트워크를 구성하는 모든 개체들은 중요한 정보들을 안전하게 유지하여야 하며, 비인가된 사용자들로부터의 접근, 변조, 삭제를 막아야 함
② 원격터미널은 적절한 사용자 인증방법을 통하여, 원격사용자의 인증을 수행하여야 함
③ 원격터미널과 안전한 홈게이트웨이 구간은 네트워크 계층이나 섹션 계층에서 개체인증, 키관리, MAC, 무결성 기능을 가져야 함
④ 원격터미널과 홈응용서버 구간은 응용계층이나 네트워크 계층에서 개체인증, 키관리, 암호화, MAC, 무결성 기능을 가져야 함
⑤ 원격터미널과 홈디바이스 B, C 구간은 응용계층에서 개체인증, 키관리, 전자서명, 암호화, MAC, 무결성 기능을 가져야 함
⑥ 홈디바이스 A는 홈사용자에 대한 적절한 방법으로 인증을 수행하여야 함
⑦ 홈디바이스 A와 홈디바이스 B, C 구간은 응용계층에서 개체인증, 키관리, 암호화, MAC, 무결성 기능을 가져야 함

〔표 3〕 홈네트워크를 위한 보안 모델과 보안기술들과의 관계
(Y: 보안서비스는 보안기능에 의해 제공됨, K: 보안서비스는 보안메커니즘에 의해 제공됨, X: 보안서비스는 선택가능한 보안기능에 의해 제공됨)

보안기능 / 개체나 개체간의 관계		암호화	무결성	MAC	개체인증	디지털서명	공증	접근제어		키관리	유용성	
								물리적	기술적		물리적	기술적
저장된 데이터	원격터미널	Y	X	Y	Y	Y	Y	K	Y	Y		Y
	홈디바이스	Y	X	Y	Y	Y	Y	K	Y	Y		Y
	안전한 홈게이크웨이	Y	X	Y	Y	Y	Y	K	Y	Y		Y
	홈응용서버	Y	K	Y	Y	Y	Y	K	Y	Y		Y
통신 데이터	원격사용자와 원격터미널	Y		X	Y	Y		K	Y	Y		
	원격터미널과 안전한 홈게이트웨이	Y	X	X	Y	Y	Y	X		Y	X	Y
	원격터미널과 홈응용서버	Y	X	X	Y	Y	Y	X		Y	X	Y
	원격터미널과 홈디바이스 B, C	Y	X	X	Y	Y	Y	X		Y	X	Y
	응용서버와 안전한 홈게이트웨이	Y	X	X		X	X	X		Y	X	Y
	응용서버와 홈응용서버	Y	X	X		Y	Y	X		Y	X	Y
	응용서버와 홈디바이스	Y	X	X	Y	Y	Y	X		Y	X	Y
	안전한 홈게이트웨이와 홈디바이스	Y	X	X	Y	Y	Y	X		Y	X	Y
	홈응용서버와 홈디바이스	Y	X	X	Y	Y	Y	X		Y	X	Y
	홈디바이스 A와 홈디바이스 B, C	Y	X	X	Y	Y	Y	X		Y	X	Y
	홈디바이스 A와 홈유저	Y		X	Y	Y		K	Y	Y		
	안전한 홈게이트웨이와 홈응용서버	Y	X	X	Y	Y	Y	X		Y	X	Y
	원격터미널과 홈디바이스 A	Y		X	Y	Y	Y	X		Y	X	Y

⑧ 홈디바이스 B, C와 홈응용서버/응용서버 간에는 네트워크 계층, 세션 계층, 응용계층에서 개체인증, 키관리, MAC, 무결성 기능을 가져야 함

⑨ 홈디바이스 B, C와 안전한 홈게이트웨이 간에는 네트워크 계층, 세션 계층에서 개체인증, 키관리, MAC, 무결성 기능을 가져야 함

⑩ 안전한 홈게이트웨이와 홈응용서버/응용서버 간에는 네크워크 계층에서 개체인증, 키관리, MAC, 무결성 기능을 가져야 함

⑪ 홈네트워크 관리자는 사용자 허가 하에 원격 및 로컬로 홈게이트웨이나 홈응용서버를 관리하여야 함

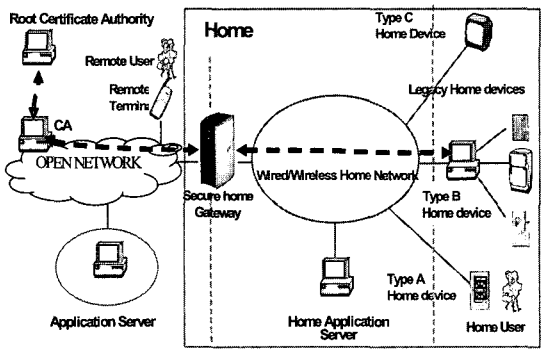
⑫ 홈게이트웨이는 방화벽, 침입차단, 데이터 필터링과 옵션 기능으로 유지보수를 위한 원격접근 인터페이스를 가져야 함

⑬ 안전한 홈게이트웨이를 관리하기 위하여, 로그인/메시지 기능을 통하여 관리자하게 모니터링 되어야 함

2. X.homesec-2[2]

홈네트워크 보안 표준의 두 번째로는 "홈네트워크를 위한 디바이스 인증서 프로파일(X.homesec-2)" 표준으로 홈네트워크 디바이스들을 인가받은 사용자만이 이용할 수 있도록 하기 위한 표준이다. 홈네트워크 원천기술을 개발하고 있는 SG9에서는 J.192(A Residential Gateway to support the Delivery of Cable Data Services, 2004) 표준에서 홈디바이스 인증서 프로파일을 정의하였지만, 본 표준에서는 오픈케이블 기반의 케이블 서비스만을 지원할 수 있게 정의되어, 이를 일반적인 서비스에 적용하기 위해서는 인증서 프로파일을 변환해야 하는 불편함이 있다. 따라서 X.homesec-2에서는 이런 불편한 점을 해결하기 위하여 X.509v3을 기반으로 홈디바이스 인증서 프로파일을 정의하게 되었다. 홈디바이스 인증을 위한 고려사항으로는 외부의 비인가된 사용자가 홈게이트웨이의 보안 소프트웨어를 불법적으로 다운로드하여, 댁내의 홈디바이스를 사용하거나 비밀정보를 습득하지 못하도록 해야한다. 또한, 홈디바이스 제조업체들은 제품을 생산하는 시점에서부터 인증서를 삽입할 수 있어야 하고 인증서 프로파일이 한번 설치 후 재설치 없이 다른 홈디이바스들 간에도 사용가능하도록 명확히 정의되어야 한다. X.homesec-2는 J.192와도 모순되지 않도록 하기위하여, 케이블 서비스에도 적용가능하며, 홈디바이스 고유식별자(CPU Serial Number, LAN Card MAC 등)를 고려키로 하였다. 또한, 보안알고리즘의 인증서 프로파일을 위해서 국제적으로 입증된 알고리즘이나 국제적으로 활용되고

있는 알고리즘을 정의키로 하였으며, 특수한 경우에 국가별로 사용되는 특정 알고리즘에 대해서도 고려키로 하였다. 이외에도 일반적인 응용 보안프로토콜과 홈네트워크 디바이스에서 의해서 발생할 수 있는 다양한 서비tm들을 고려하여 개발하고 있다.



〔그림 2〕 안전한 홈게이트웨이를 위한 디바이스 인증 모델

그림 2는 홈디바이스 인증 모델이며, 홈네트워크에서 디바이스 인증서를 활용하는 방법은 크게 2가지로 분류된다. 첫 번째는 안전한 홈게이트웨이가 직접 서명한 인증서를 모든 댁내 디바이스들에게 나누어 주고, 안전한 홈게이트웨이는 외부의 인증기관으로부터 인증서를 발급받아 추후 홈게이트웨이를 통하여 인증서를 활용하는 방법이다. 두 번째는 홈네트워크에 존재하는 모든 디바이스들을 외부의 인증기관을 통해서 인증서를 발급받아 활용하는 방법이다. 두 번째 방법은 SG9의 J.192에서 정의하고 있는 방법이고 X.homesec-2에서는 첫 번째 방법에 대해 정의한다.

홈디바이스 인증서 프로파일은 ITU-T X.509와 IETF RFC3280을 기반으로 정의하고 있으며, 표 4와 같이 반드시 있어야 할 기본필드와 추가적인 정보를 담고 있는 확장필드로 구성되어 있다.

인증서의 구별자 이름(DN) 형식은 다음과 같다.

- 인증기관의 인증서(C={country}, O={home network}, OU={division}, CN={author})
- 홈디바이스 인증서(C={country}, O={home device vender}, OU={device model}, CN={certification information}

홈네트워크 환경에서 인증서를 활용하여 안전한 서비스를 제공하기 위해서는 다음의 사항들이 고려되어야 한다.

- RSA 알고리즘의 경우에는 1024비트 이상의 키를 사용해야 함
- 서명 알고리즘의 경우에도 1024비트 이상이 키를 사용해야 함
- 홈디바이스 인증서의 유효기간은 10년 이상 사용되어야 함
- 안전한 홈게이트웨이와 홈디바이스 간에는 정기적으로 세션키 갱신이 가능해야 함
- 안전한 홈게이트웨이는 안전하게 홈디바이스들의 인증서를 발급하고 관리할 수 있어야 함
- SHA-1에 대한 취약점이 발견됨에 따라, 해쉬함수를 사용할 경우는 SHA-256 알고리즘을 사용하여야 함

〔표 4〕 X.homesec-2 홈디바이스 인증서 프로파일

인증서 필드		설 명
기본 필드	Version	PKI 인증서 포맷을 구분하기 위한 인코딩 버전
	Serial Number	인증기관에 의해 할당받은 각 개체들의 고유 넘버
	Signature	인증서를 서명하기 위한 것으로 인증기관에 의해 사용되고 있는 해쉬함수나 알고리즘의 식별자
	Issuer	인증서의 발급자 정보로 X.500의 구별자 이름(DN)
	Validity	인증서의 유효기간
	Subject	인증서에 저장된 공개키의 주체로 각각의 홈디바이스
	Subject Public Key Info	공개키와 함께 사용될 알고리즘 식별정보(RSA, DSA, ECDSA 등)
확장 필드	Authority Key Identifier	인증서 서명에 사용되는 개인키에 대응되는 인증기관의 공개키 식별정보
	Subject Key Identifier	각 주체가 특별한 공개키를 사용할 경우에 사용되는 공개키 식별정보
	Key Usage	각 인증서에서 공개키가 사용되는 목적을 기입(암호화, 서명 등)
	Basic Constraint	CA 인증서의 최대 길이를 명시하기 위한 필드이며, 홈디바이스 인증서는 해당되지 않고 홈게이트웨이를 위함
	Certificate DN Format	인증서의 구별자 이름 형식

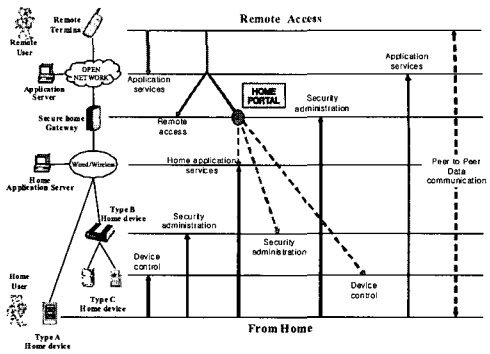
홈네트워크에서 디바이스 인증서 관리는 안전한 홈게이트웨이가 인증서의 발급, 폐기, 유효성 검증을 수

행한다. 또한 인증서를 발급 방법으로는 외부에서 직접적으로 등록하는 방법과 온라인으로 등록하는 방법이 있다. 홈디바이스들 중에 PC, PDA 등과 같이 직접으로 연산이 가능한 디바이스들은 2가지 방법으로 등록이 가능하나, 연산 능력이 없는 디바이스들은 관리자에 의해서 직접적으로 등록되어야 한다. 또한 이런 디바이스들은 인증서를 사용할 수 있도록 적절한 인터페이스가 요구된다. 안전한 홈게이트웨이는 자신의 인증서를 인증기관에 등록하기 전에 인증기관이나 대래인증기관으로부터 등록코드(reference code/ authorization code)를 부여 받고, 이를 이용하여 자신의 홈디바이스들에게 표 4의 인증서 프로파일로 인증서를 발행하고 이를 외부 인증기관에 등록하여야 한다. 인증서 폐기 절차는 인증서 유효기간이 길게 발급되므로 빈번이 일어날 일은 없지만, 만약에 발생된다면 연산 가능한 홈디바이스들은 직접적으로 CMP (인증서 관리 프로토콜) 모듈을 사용하고 연산 능력이 없는 디바이스들은 관리자에 의해 폐기될 수 있다. 인증서 유효성 검증은 온라인으로 상태 유효성 서버를 통하여 검증하는 방법과 인증기관에 의해 주기적으로 발급되는 CRL(인증서 폐기 리스트)를 통하여 검증하는 방법이 있다. 여기서 CRL은 ITU-T X.509에 정의된 방법을 이용한다. 이렇게 발급된 홈디바이스 인증서는 그림 2의 모델에서 원격터미널과 홈게이트웨이 구간, 응용서버와 홈게이트웨이 구간, 홈디바이스와 홈게이트웨이 구간에서 사용되며, 링크계층과 응용계층에서 주로 사용될 것이다.

3. X.homesec-3[3]

홈네트워크 보안 표준의 세 번째는 "홈네트워크 서비스를 위한 사용자 인증 메커니즘(X.homesec-3)" 표준으로 외부에서 댁내로 접속하는 원격사용자와 댁내에서 홈디바이스 및 외부서비스에 접속하기 위한 홈유저들에 대한 적절한 인증수단(패스워드, 인증서, 바이오인식 정보 등)을 통한 인증방법을 제공하기 위한 표준이다.

홈네트워크에서는 다양한 사용자(노인, 부모, 아이 등)가 이용하기 때문에 쉬운 방법으로 서비스를 지원할 수 있어야 하며, 이를 위하여 각 구간의 서비스 인터페이스 정의가 필요하므로 그림 3과 같은 서비스를 구조를 정의하였다. 홈포탈(Home Portal)은 일종의 대행 서버(Proxy Server)로 사용자가 직접적으로 서비스를 받을 수 없을 때 중간매개체 역할을 수행하



〔그림 3〕 홈네트워크 서비스 구조

는 개체로써 사용자를 인증하고 사용자가 요구하는 명령들을 모아 해당하는 홈디바이스에 맞는 프로토콜로 변경하는 역할을 수행하다. X.homesec-1 모델에서 이 역할은 안전한 홈게이트웨이나 홈응용서버가 수행할 수 있으나 X.homesec-3에서는 안전한 홈게이트웨이에서 홈포탈을 수행하는 것으로 가정하였다. 또한, 그림 3에서와 같이 원격사용자는 댁내서비스를 이용하기 위하여 홈포탈을 이용하여 접근할 수 있고, 홈유저들은 홈포탈 없이 직접적으로 댁내 및 댁외서비스에 접근할 수 있다고 가정하였다.

홈네트워크 환경은 실제적으로 클라이언트와 서버 시스템 개념으로 구성되어 서비스를 이용하는 사용자와 서비스를 제공하는 서비스 제공자로 구성된다. 따라서 사용자는 서버에서 제공되는 서비스만을 이용하기 때문에 별도의 데이터를 저장하거나 그것들을 유지하기 위하 비용은 필요하지 않는다. X.homesec-3의 사용자 인증 메커니즘도 이와 같은 개념이며, 홈디바이스 A는 클라이언트 역할을 수행하고, 홈응용서버나 홈게이트웨이가 서버 역할을 수행한다. X.homesec-3에서는 홈네트워크를 위한 각 개체들 간의 고려사항들을 정의하고 있으며, 다음의 표 5와 같이 사용자 인증을 위한 홈네트워크 개체들의 역할 및 특징들을 분류하였다. 예로 원격터미널은 사용자 인터페이스 성능이 높아야하고, 네트워크 이용성 또한 높고, 컴퓨팅 파워는 중간 정도이며, 홈서비스 능력은 낮고, 저장능력은 중간, 네트워크 상에서의 보안능력은 높아야하고, 클라이언트 인증이 수행되어야 한다.

홈네트워크 사용자가 서비스에 접근할 때, 사용자 인증을 위해 수행되는 절차는 다음과 같다.

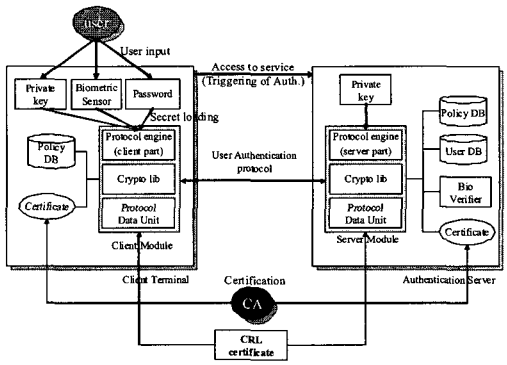
- 서버인증 절차가 초기화 되고, 사용자 인증을 요청
- 서버인증이 성공되면, DH(Diffie-Hellman)

키동의 프로토콜에 의해 세션키가 만들어지고, 클라이언트 인증이 수행

- 클라이언트 인증을 위해 사용자는 인증 수단으로 패스워드, 인증서, 바이오인식 정보 등을 선택
- 사용자가 선택한 인증 정보와 함께 클라이언트 화면에 자신의 ID를 입력
- 클라이언트 인증 절차가 초기화되고, 앞에서 발급받은 세션키로 인증을 수행
- 클라이언트 인증이 성공하면, 사용자는 서비스에 접근이 가능

홈네트워크 사용자 인증을 위한 보안요구사항은 다음과 같다.

- 서버인증 후에는 클라이언트 인증과 함께 상호인증이 수행되어야 함
- "simple flooding attack"에 저항성이 있어야 함
- 사용자의 바이오인식 정보나 ID가 보호되어야 함
- 다양한 사용자 인증 수단이 지원되어야 함



〔그림 4〕 사용자 인증메커니즘을 위한 보안 컴포넌트

그림 4는 홈네트워크 서비스를 위한 사용자 인증 메커니즘의 보안 컴포넌트로 클라이언트 터미널은 사용자의 인증정보를 입력할 수 있는 인터페이스가 존재하여야 하며, 서버 역할을 수행하는 홈 개체들은 각각의 사용자 인증정보와 대응할 수 있는 데이터베이스 가지고 있어야 한다. 클라이언트와 서버의 프로토콜 모듈은 홈네트워크의 사용자와 관리자에 의해 구성된 정책에 따라 제어되어야 하며, 이는 정책 데이터베이스에 저장된다. 또한, 인증서를 이용한 사용자 인증하기 위하여 CA 서버 및 CRL 서버와도 상호 연동되어야 한다. 사용자 인증을 위한 중간매개체 수단으로 안전성을 고려하여 스마트카드를 사용하는 것을 권장하나, 다양한 인증수단을 지원하기 위해 인터페이스가 요구된다.

X.homesec-3에서는 사용자 인증 프로토콜을 위한 서버인증 방법과 클라이언트 인증 방법(패스워드, 바이오인식 정보, 인증서)에 대한 세부 프로토콜을 정의하고 있으나 본 논문에서는 정의하지 않도록 한다.

4. 신규 표준화 아이템(New work item)[4]

12월, 제네바 회의에서 제안할 신규 표준화 아이템은 "홈네트워크 환경을 위한 인가(권한부여) 프레임워크" 이다. 본 아이템의 주요사항으로 홈네트워크를 위한 인가 요구사항, 인가 프레임워크, 인가 메커니즘을 주로 다룰 계획이며, 다음과 같은 사항을 고려하여 개발할 계획이다.

- 정당한 인가 발급은 서비스 도메인 간에 적용되어야 함
- P2P 서비스 모델에서 인가의 복잡성과 비효율

〔표 5〕 사용자 인증을 위한 홈네트워크 개체들의 역할 및 특징

홈네트워크 개체	홈네트워크 개체들의 특징						사용자 인증을 위한 역할	
	사용자 인터페이스	네트워크 이용성	컴퓨팅 파워	홈 서비스	저장	보안 (네트워크)	클라이언트	서버
원격터미널	높음	높음	중간	낮음	중간	높음	수행	
응용서버	낮음	높음	높음	높음	높음	높음		수행
안전한 홈게이트웨이	낮음	높음	중간	낮음	낮음	높음		수행
홈응용서버	낮음	높음	높음	높음	높음	높음		수행
홈디바이스 A	높음	높음	중간	낮음	중간	높음	수행	
홈디바이스 B	낮음	높음	낮음	낮음	낮음	낮음		수행 (보안컨솔)
홈디바이스 C	중간 (보안컨솔)	낮음	낮음	중간	낮음	중간	수행 (보안컨솔)	

성을 고려
- 홈디바이스들의 연산량과 컴퓨팅 파워를 고려

Ⅳ. 2006년 SG17 주요회의 결과

본 장에서는 2006년 개최되었던 SG17 미팅에서 홈네트워크 보안과 관련되어 토의되었던, 주요회의 결과를 소개한다.

1. SG17 정기회의(2006.04.19~28, 제주)[9]

2005년 10월 제네바 회의에서 검토되었던 이슈들을 중심으로 수정 및 보완된 기고서를 제출하였으며, 주요결과는 다음과 같다.

- X.homesec-1은 주요 용어와 본문에서의 오타 등을 수정하여 기고서를 제출하였으며, 제주회의에서 최종적인 표준(안) 검토를 하였다. 또한, 본 회의결과로 확정된 표준(안)이 차기회의에서 더 이상의 문제가 없다고 판단되면, 12월 제네바 회의에서 국가별 의견수렴(consent)으로 추진키로 합의하였다.
- X.homesec-2는 국제적으로 입증된 암호알고리즘(RSA, DSA 등)을 중심으로 OID로 정의하였으며, J.192와 호환되도록 홈디바이스 인증서 프로파일을 정의하였다. 또한, 홈게이트웨이를 이용한 홈디바이스 인증서 관리 방법을 명확하게 정의하였다. 차기회의에서는 인증서의 유효성 판단을 위하여 IETF SCVP를 사용할 경우, IETF DPD/DPV의 요구사항 등에 대해 논의키로 합의하였다.
- X.homesec-3은 X.homesec-1을 기반으로 용어 수정 및 정의를 보완하였으며, 사용자 인증 메커니즘의 영역과 서비스구조 및 사용자 인증을 위한 고려사항을 검토하였다. 또한, 클라이언트 인증과 사용자 인증의 차이점에 대한 검토가 이루어졌으며, 12월 제네바 회의에서 첫 번째 권고초안(first draft recommendation)으로 추진키로 합의하였다.

2. SG17 WP2 Interim 회의(2006.09.11~15, 오타와)[10]

2006년 4월 제주 회의에서 검토되었던 이슈들을 중심으로 수정 및 보완된 기고서를 제출하였으며, 본 회의는 SG17 정기회의가 아닌 임시회의 이므로, X.homesec-3 기고서는 제출되지 않았다. 회의 주요 결과는 다음과 같다.

- X.homesec-1은 SG9에서 추가적인 검토의견을 받아 용어, 보안요구사항, 보안요구사항과 보안기능과의 관계 표를 수정하였다. 또한, 일본에서 X.homesec-1의 독자들을 고려하여 일부내용을 쉽게 설명하자는 제안을 받아들려 최종적인 표준(안)을 확정하였다.
- X.homesec-2는 홈디바이스 인증서 프로파일을 기본필드와 확장필드로 구분하여 정의하였으며, 국제적으로 입증된 알고리즘을 사용해야 된다는 의견에 따라, KCDSA, HAS-160을 제외하고, RSA, ECDSA, DSA 등으로 변경하였으며, 보안고려사항으로 서명알고리즘 등의 키 길이 안전성에 대한 내용을 추가하였다. 또한, ASN.1 코드를 표준 표기법으로 포맷을 수정하였다.

Ⅴ. 결론 및 향후 대응전략

본 논문에서는 ITU-T SG17에서 한국 주도로 개발되고 있는 홈네트워크 보안 표준에 대해 분석하였다. 현재, X.homesec-1은 SG9에서 추가적인 검토의견을 주어 이를 반영하여 방화벽, Malware라는 용어를 추가하였으며, 이에 따른 보안고려사항 및 보안기능과의 관계 등 일부 내용을 수정하였다. X.homesec-1은 크게 문제가 없다고 하면, 이번 제네바 회의에서 국가별 의견수렴으로 추진할 계획이며, 문제없이 통과가 되면 빠르면 2007년 상반기에 ITU-T 처음으로 홈네트워크 보안 국제표준이 한국에 의해 제정될 예정이다. X.homesec-2는 홈디바이스 인증서 프로파일을 IETF RFC3280에서 ITU-T X.509 기반으로 변경하여 제안하였으며, 빠르면 2007년 9월에 국가별 의견수렴으로 추진할 예정이다. X.homesec-3은 실제적인 사용자 인증 메커니즘의 세부프로토콜 수행절차를 제안하였으며, 기존의 표준(안)에 불명확한 문장들을 수정 및 보안하였다. X.homesec-3은 2008년 4월에 국가별 의견수렴으로 추진할 예정이다. 이번 12월 제네바 회의에서 신규로 제안할 예정인 홈네트워크를 위한 인가 프레임워크는 Q.9/17의 신규 표준화 아이템으로 채택되도록 유도할 예정이다.

ITU-T SG17은 한국, 중국, 일본에서 많은 표준화 전문가가 참석하고 있는 상황이며, 특히, 홈네트워크

보안은 앞에서 보는 바와 같이 한국이 주도적으로 개발하고 있는 표준화 아이템이다. 따라서, 국내에서 개발되고 있는 홈네트워크 보안기술을 국제표준에 반영하기 좋은 시점이므로, 국내 정보보호 산업체 및 홈네트워크 산업체에서도 지속적인 관심과 적극적인 참여가 필요하다고 생각된다. 현재, ITU-T SG17 대응은 국내 ITU-T SG17 분과위원회(의장 진병문 본부장, TTA)를 중심으로 20명 표준화 전문가와 SG17 회의에 참석하고 있는 참가자 및 에디터들이 함께 대응하고 있다.

참 고 문 헌

[1] Heung-Youl Youm, Heung-Ryong Oh, "Final Draft Recommendation X.homesec-1 - Framework of security technologies for home network", ITU-T SG17 Meeting, Swiss Geneva, 6-15 Dec 2006.

[2] Jonghyun Baek, Dong-Young Yoo, Heung-Youl Youm, "Proposal for first draft recommendation of X.homesce-2 : Device certificate profile for the home network", ITU-T SG17 Meeting, Swiss Geneva, 6-15 Dec 2006.

[3] Hyung-kyu Lee, Yun-kyung Lee, Jong-wook Han, Kyo-il Chung, Dae-hun Nyang, Heung-Youl Youm, "Proposal for the first draft recommendation of X.homesec-3 - User authentication mechanism for home network services", ITU-T SG17 Meeting, Swiss Geneva, 6-15 Dec 2006.

[4] Geon-woo Kim, Jong-wook Han, Kyo-il Chung, "Proposal of a new item for authorization in the home network", ITU-T SG17 Meeting, Swiss Geneva, 6-15 Dec 2006.

[5] Heung-Youl Youm, Byoung-Moon Chin, Dong-Young Yoo, Jong-wook Han, "Proposal of future study items for developing the security standard of the home network", ITU-T SG17 Meeting, Russia Moscow, 30 Mar - 8 Apr 2005.

[6] 오흥룡, 염흥열, "ITU-T SG17 WP2 Q.9(안전한 통신 서비스) 표준화 동향 및 향후 전망", 한국정보보호진흥원, 정보보호기술 표준화 동향지, 2006.7.

[7] 진병문, 오흥룡, 염흥열, 정교일, "ITU-T SG17 모스크바 회의", TTA 저널, 99호, 2005.6.

[8] 진병문, 오흥룡, 염흥열, 정교일, "ITU-T SG17 제네바 회의", TTA 저널, 102호, 2005.12.

[9] 진병문, 김선, 오흥룡, "ITU-T SG17 회의 유치 및 표준화활동(제주)", TTA 저널, 제105호, 2006.6.

[10] 오흥룡, 염흥열, "ITU-T SG17 WP2 국제표준화 회의 참가보고(오타와)", TTA 저널, 제107호, 2006.10.

[11] 진병문, 오흥룡, 염흥열, 강신각, "2005년 ITU-T SG17 연구동향", TTA, ITU-T 연구활동 보고서, 2005.12.

[12] 진병문, 오흥룡, 염흥열, 강신각, "2006년 ITU-T SG17 연구동향", TTA, ITU-T 연구활동 보고서, 2006.12.

〈著者紹介〉

오 흥 룡 (Heung-Ryong Oh)
정회원
2002년 2월 : 순천향대학교 전자공학과 졸업
2004년 2월 : 순천향대학교 정보보호학과 석사
2004년 2월~현재 : 한국정보통신기술협회(TTA) 표준화본부
2004년 11월~현재 : X.homesec-1 Associate Editor
2005년 3월~현재 : ITU-T SG17 국내 분과위원회 간사
관심분야 : 보안프로토콜, 정보보호표준

염 흥 열 (Heung-Youl Youm)
정회원
1981년 2월 : 한양대학교 전자공학과 졸업
1983년 2월 : 한양대학교 전자공학과 석사
1990년 2월 : 한양대학교 전자공학과 박사
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국통신정보보호학회 총무이사, 학술이사, 교육이사, 현 총무이사
2004년 1월~현재 : 한국인터넷정보학회 이사, 논문지 편집위원
2004년 1월~현재 : OSIA 이사
2003년 9월~2004년 3월 : ITU-T SG17/Q10 Associate Rapporteur
2004년 3월~현재 : ITU-T SG17/Q9 Rapporteur
2006년 11월~현재 : 정보통신부 정책자문단 정보보호 PM
관심분야 : 네트워크 보안, 전자상거래 보안, 공개키 기반 구조, 부호이론, 이동통신보안