홈네트워크 보안

염 흥 열 | 순천향대 정보보호학과 교수
정보통신부 IT 정책자문단 정보보호 PM

요 약

홈네트워크 보안 기술은 디지털 생활의 질을 향상하고 신뢰성있고 상호연동이 가능한 홈네트워크 디바이스 및 서비스의 구현을 위해 요구되는 핵심 기술이다. 홈네트워크 보안과 연관된 국제표준화 기구 또는 사실표준화 단체는 ITU-T, UPnP, DSL 포럼 등을 들 수 있다. 본 고에서는 홈네트워크 보안 표준과 연관되는 이들 국제 표준화 기구와 사실 표준화 단체의 동향을 살펴본다.

I. 서론

홈네트워크 기술은 가정 내 정보 가전기기들이 서로 유/무선으로 연결되어 기기의 종류, 시간, 장소에 무관하게 다양한 홈 디지털 서비스를 제공받아 홈네트워크 사용자는 물론 원격 사용자에게 디지털 삶의 질을 향상시키기 위하여 요구되는 기술이라고 할 수 있다. 이런 홈네트워크 기술이 안전하고 신뢰성있게 제공되기 위해서는 정보보호 기술이 채용되어야 하고, 신뢰/호환/상호 연동성이 가능한 홈네트워크를 실현하기 위해서는 정보보호 기술에 대한 표준화도 수행되어야 한다.[12, 13] 현재 홈네트워크를 위한 보안 표준을 개발했거나 수행 중에 있는 중요한 국제 표준화 기구나 사실 표준화 단체는 ITU-T, DSL 포럼, DLNA 포럼, 그리고 UPnP 표준을 들 수 있다. ITU-T에서는 주로 보안 프레임워크, 인증/인가 기술의 표준화, DSL 포럼에서는 ADSL 환경에서 망 관리자와 홈네트워크 게이트웨이 간에 관리를 위한 통신을 위해 요구되는 보안 요구사항에 대한 표준화, DLNA 포럼에서는 엄밀하게 보안 표준은 아니지만 홈네트워크 상호 연동을 위한 프레임워크 표준화, 그리고 UPnP 포럼에서는 홈네트워크 디바이스 단위의 인증 및 인가 표준화를 중심으로 추진하고 있다.

본 고에서는 이러한 표준화 기구에서 추진하고 있는 주요 표준안의 내용과 향후 추진방향을 살펴본다.

II. 홈네트워크 보안 표준화 동향

본 장에서는 주요 국제 표준화 기구나 사실 표준화 단체에서 수행되고 있는 표준화 동향을 살펴본다.

2.1 DSL 표준화 동향

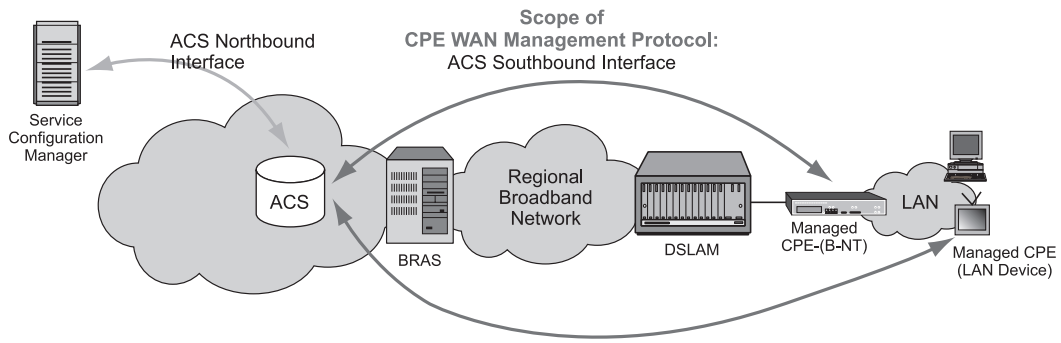
DSL(Digital Subscriber Line) 포럼에서 산출된 홈 네트워크 보안과 연관되는 기술문서는 표 1과 같다.[1, 2, 3] DSL 표준은 주로 원격 관리자에 의한 홈네트워크 내에 디바이스인 CPE(Customer Premise Equipment)의 원격 설정 및 관리를 위해 필요한 보안 기능을 정의하고 있다. 표 1과 같이 세 가지 표준이 존재하면, 그림 1과 같은 네트워크 환경에 기반을 두고 있다.

가. TR-069

홈네트워크에 존재하는 다양한 디바이스에 대한 초기 CPE 설정과 초기 설정이후 임의 시간에 자동 설정 및 능동적인 서비스 제공 기능, 버전 확인, 설정 파일 다운로드 초기화, 그리고 설정 파일 다운로드 초기화의 성공/실패 표시 등을 포함하는 자동화된 소프트웨어 다운로드 기능, CPE의 로그 파일 등의 제공을 통한 디바이스의 성능 및 상태 감시 기능, 그리고 원격 자동 진단 기능을 제공하고 있다. 자동 설정 구조는 그림 1과 같이 네트워크에 존재하는 ACS(Automatic Configuration System)와 홈네트워크 내에 존재하는 디바이스 간에 관리 프로토콜로 정의되고 있다.

이러한 관리 프로토콜은 규모가 가변적이면서 높은 수준의 보안을 제공하며, 다음과 같은 보안 목표를 갖고 있다.

- ACS와 CPE간에 안전한 설정 및 신뢰적인 메시지 교환 기능 제공
- 교환 메시지의 기밀성 제공



[그림 1] 원격 자동 설정 및 관리를 위한 구조(DSL TR-069)

[표 1] DSL 보안 표준 개요

문서 번호	문서 제목	표준화 일시	보안 주요 내용
TR-064	DSL CPE 설정	2004. 5.	– CPE에 대한 비인가된 설정을 막기 위한 보안 기능 규정 • 접근 제한, 패스워드 기반 인증, 패스워드 초기화 • 설정 보안 서비스로의 접근은 암호화된 https 링크를 이용함
TR-069	CPE WAN 관리 프로토콜	2004. 5.	– 원격에 존재하는 자동 설정 서버와 홈네트워크에 존재하는 홈디바이스 간의 설정을 위해 요구되는 보안 기능 규정 • 보안 목표 정의 • 보안 메커니즘 정의 • SSL/TLS 프로토콜 이용
TR-094	홈네트워크 다중 서비스 제공 프레임워크	2004. 8.	– 홈네트워크에서 다중 서비스 제공을 위해 요구되는 보안 요구사항을 정의함

- 교환 메시지에 대한 인증 기능의 제공
- 서비스 도용의 방지

관리 메시지 프로토콜을 위하여 사용된 보안 메커니즘은 다음과 같다.

- SSL/TLS 프로토콜을 이용하여 기밀성, 무결성, 인증서-기반 디바이스 인증 기능이 수행되어야 한다.
- HTTP 계층은 별도의 비밀 공유 방식에 기반한 디바이스 인증 기능을 제공해야 한다.

SSL/TLS 관련 보안 요구사항은 다음과 같이 정의되었다.

- SSL/TLS가 지원된다면, SSL 3.0이거나 TLS 1.0 이어야 한다.
- 대칭 암호알고리즘의 키의 길이는 128 비트 이상이어야 한다.
- 디바이스 인증을 위하여 사용되는 인증서는 ACS에 의하여 제공되어야 한다.
- ACS는 CPE가 제공하는 유효한 인증서를 받아들일 수 있으나, CPE가 인증서가 없을 경우라도 SSL/TLS 보안 세션은 설정되어야 한다.

ACS/CPE가 SSL/TLS를 이용하지 않을 경우, ACS는 HTTP를 이용하여 CPE를 인증해야 한다. 또한 SSL/TLS가 암호화를 위하여 이용되는 경우, ACS는 기본 HTTP 인증 또는 다이제스트 HTTP 인증을 이용할 수 있다. 만약 SSL/TLS가 이용되지 않을 경우, ACS는 다이제스트 인증을 이용해야 한다.

나. TR-094

TR-094는 홈네트워크에서 제공되는 여러 서비스를 위해 요구되는 다음과 같은 보안 요구사항을 정의하고 있다.

- 홈네트워크는 외부로부터 내부로의 원하지 않은 연결을 막아야 한다.
- 홈네트워크는 트로이목마, 백도어 및 원격 관리 프로그램, 서비스 공격, 타 공격의 중계자 등의 다양한 공격으로부터 보호되는게 바람직하다.
- 홈네트워크는 비인가된 디바이스 설정으로부터 보호되는게 바람직하다.
- 홈네트워크는 불법 콘텐츠로부터 자녀를 보호하기 위한 부모 제어와 콘텐츠 필터링 기능이 제공되는게 바람직하다.
- 홈네트워크는 링크 레벨에서 한정 제어시스템과 응용 레벨에서 디지털 권한관리 기능을 제공하는게 바람직하다.
- 홈네트워크는 원격 접근 VPN 클라이언트를 지원해야 한다.
- 홈네트워크는 네트워크 내와 외부로 암호 기능을 제공해야 한다.

다. TR-064

TR-064는 홈네트워크에 존재하는 CPE 설정을 위해 요구되는 보안 기능을 정의하고 있다. CPE에 대한 비인가된 설정을 막기 위해 다음과 같은 보안 기능을 규정하고 있다.

- 접근 제어: 민감한 CPE 정보에 대한 접근은 언제나 읽혀지지 않아야 하고, 상태 및 통계와 같은 CPE 정보는 읽기만 가능해야 하고, 설정 내용의 변경 메시지는 암호로 보호되어야 한다.
- 인증: 패스워드 보호된 접근은 HTTP 다이제스트 인증을 사용해야 하고, 인증을 위한 패스워드는 접근 제어를 위한 패스워드와 패스워드 재설정을 위한 패스워드로 구분된다.
- 패스워드 초기화: 공장 설정 패스워드 상태와 정상

[표 2] UPnP 보안 표준 개요

문서 제목	표준화 일시	문서 주요 내용
UPnP 보안 세레모니 설계 문서	2003. 10.	– 보안 측면에서 디바이스의 유형 정의 – 디바이스간 보안 모델 정의 및 디바이스간에 메시지 보안을 위한 서비스 • 무결성, 디바이스 인증, 디바이스 인가, 재생공격방지 등 – 다양한 디바이스 보안 서비스 • 보안 요소 발견 프로토콜, 디바이스 소유권, 세션키 공유방법, ACL 편집, 인증서 캐쉬

문서 제목	표준화 일시	문서 주요 내용
디바이스 보안 : 1 서비스 템플릿	2004. 5.	– 디바이스 보안:1 서비스 플래폼에서 정의된 동작은 일반 디바이스와 보안 제어 디바이스에 의하여 호출되는 동작들과 보안 제어 디바이스에 의해서만 호출될 수 있는 동작 그룹으로 구분되며, 관련 동작과 연관되는 변수, 전송 방향, 그리고 관련 XML 요소를 정의하고 있음
보안 콘솔 : 1 서비스 템플릿	2004. 8.	– 홈네트워크에서 다중 도메인 보안 서비스를 제공하기 위하여 보안 제어 디바이스가 제공하는 다양한 보안 동작과 이에 대한 세부 동작을 설명하고 있음 • 보안 제어 디바이스에 의한 제어 디바이스 발견 • 보안 제어 디바이스가 다른 보안 제어 디바이스에 존재하는 로컬 디렉토리로의 접근 가능해야 함 • 다중 보안 도메인 간에 접근 제어를 처리하는데 이용될 수 있는 인가 인증서의 처리

패스워드 상태로 구분하였다.
- 암호: 암호는 SSL3.0 또는 TLS1.0을 사용한 암호화된 HTTPS 링크를 이용하도록 권고하고 있다.

2.2 UPnP 홈네트워크 보안 표준화 동향

UPnP에서는 홈네트워크 내에 여러 보안 도메인이 존재하고, 하나의 보안 도메인은 하나의 홈네트워크에만 한정되는 것이 아니라 여러 홈네트워크를 통하여 구성될 수 있는 다중 보안 도메인, 부모에 의한 자녀 제어, 그리고 물리적 공간을 뛰어 넘는 가상 홈네트워크 보안 도메인 등을 가능케 한다. 또한 여기서는 사용자가 아니라 디바이스 단위로 인증과 암호화를 수행하며, 보안 명령을 발행하는 제어 디바이스(CP, Control Point)와 보안 명령을 수신하여 해당 명령을 수행하는 일반 디바이스 간에 보안 서비스를 제공하기 위해 필요한 표준을 정의하고 있다.[4, 5, 6] 이 표준을 이용하면, 디바이스 인증체계를 이용하여, 다양한 멀티미디어 서비스와 오디오 서비스를 제공받을 수 있다. UPnP 홈네트워크 보안 표준은 디바이스를 사용하는 사용자 단위의 보안 서비스를 제공하는 것이 아니라, 홈네트워크 내에 존재하는 다양한 디바이스에 대한 인증 기능을 제공하고, 또한 디바이스 단위의 ACL(Access Control List) 또는 인가 인증서(Authorization Certificate)에 기반하는 접근 제어 기능을 제공하고 있으며, SOAP 메시지 단위의 선택적인 기밀성 서비스와 무결성 서비스를 제공하고 있다.

가. 보안 세레모니 설계 표준

UPnP에서는 프로토콜의 일종으로 간주될 수 있는 세레모니(ceremony)를 정의하고 있으며, 프로토콜과 다른 점은 사용자나 인간이 프로토콜 진행 과정에 개입한다는 점이다. 보안 관점에서 홈네트워크 내의 디바이스는 일반 디바이스와 제어 디바이스(CP, Control Point)로 구분된다. 또한 보안 제어 디바이스(SC, Security Console)는 사용자 인터페이스 기능을 갖고 제어 디바이스와 일반 디바이스의 기능을 동시에 수행하는 홈네트워크 디바이스로 정의되며, 특별히 사용자와 소통하기 위한 디스플레이 기능을 갖는 디바이스라고 할 수 있다. 일반 디바이스와 제어 디바이스 간에 제어 메시지 교환은 SOAP 메시지를 이용하며, 제어 메시지를 보호하기 위한 보안 서비스는 다음과 같다.

- 디바이스 식별: 송신 디바이스 공개키에 대한 해쉬값인 보안 ID(security ID)를 근거로 디바이스를 식별함
- 무결성: 서명문 기반으로 메시지 무결성 검사함
- 발신지 인증: 송신 디바이스의 서명문을 근거로 메시지 발신지 인증을 수행함
- 메시지 신선도: 메시지 내에 난수를 이용하여 메시지의 신선도를 결정함
- 접근제어: 디바이스 식별이 완료되고 나서, 해당 디바이스에 할당된 권한을 검증하여 해당 동작 수행 여부를 결정함
- 선택적인 기밀성: 메시지 도청을 막기 위하여 선택적으로 메시지 기밀성 기능을 제공함

디바이스에 대한 접근 제어는 디바이스의 ACL, 그룹 멤버십 인증서, 그리고 인가 인증서를 이용하여 수행된다. 디바이스의 ACL은 주체, 인가정보, 대리 여부, 그

리고 유효기간으로 구성되며, 각 디바이스에서 관리되고 있다. 디바이스 보안 서비스는 해당 디바이스에 대한 제어 권한을 가지고 있는 제어 디바이스를 규정하고 있는 디바이스 소유권 관련 동작, 제어 디바이스와 일반 디바이스 간에 세션키 공유 동작, 각 디바이스의 ACL 편집 관련 동작, 인가 인증서 관련 동작 등으로 구성된다.

나. 디바이스 보안:1 서비스 템플릿

이 표준은 디바이스 보안 서비스를 제공하기 위해 요구되는 동작과 관련되는 다양한 동작과 연관되는 변수, 전송 방향, 상태 변수 등을 정의하고 있고, 이들 보안 동작과 연관되는 ACL, 소유자 목록, 인증서, 공개키 등에 대한 XML 데이터 구조를 정의하고 있다. 예를 들어, 디바이스의 공개키를 획득하기 위해 정의되는 GetPublicKeys라는 동작은 디바이스가 갖는 공개키를 제어 디바이스가 획득하기 위한 동작이고, 이 동작은 일반 디바이스에서 제어 디바이스로 기밀성 공개키 또는 서명용 공개키를 전달한다. 여기서 기밀성 공개키는 제어 디바이스가 생성한 세션키를 암호화하는데 이용된다. 보안 동작은 제어 디바이스와 보안 제어 디바이스와 연관되는 동작과 보안 제어디바이스에만 연관되는 동작으로 구분된다. 또한 ACL에 대한 XML 요소는 주체, 위임 가능 여부 플래그, 접근 권한, 그리고 유효기간 등의 요소로 구성된다.

다. 보안 제어 디바이스:1 서비스 템플릿

보안 제어 디바이스는 디바이스에 대한 접근 제어를 관리하기 위한 사용자 인터페이스를 제공하고 있다. 이 표준에서는 보안 제어 디바이스가 지원해야 하는 세 가지 동작 그룹을 정의하고 있다. 하나는 보안 제어 디바이스에 의한 제어 디바이스의 발견이고, 다른 하나는 디바이스의 고유 이름과 사용자 친화 이름을 매핑을 저장하고 있는 로컬 디렉토리와의 통신이며, 세 번째는 디바이스가 ACL을 저장할 공간이 없을 경우, 인가 인증서를 발행하여 권한을 디바이스 소유자가 갖도록 하기 위한 인증서 처리 동작 그룹이 존재한다.

인증서 처리를 지원하는 두 가지 동작은 제어 디바이스가 보안 제어 디바이스에 의하여 발행된 인증서를 패치할 수 있게 하는 GetCertificates라는 동작과 제어 디바이스가 만료된 인증서의 갱신을 요구하도록 하는 RenewCertificate라는 동작이 정의되어 있다.

2.3 ITU-T SG9 보안 표준화 동향

ITU-T SG9에서는 케이블 기반 멀티미디어 서비스를 지원하는 멀티미디어 홈네트워크 구조(J.190)와 케이블 데이터 서비스를 제공하기 위한 홈네트워크 게이트웨이(J.192) 표준을 개발했다.[7, 8] ITU-T SG9에서는 케이블 기반 멀티미디어 서비스를 제공하기 위해 요구되는 보안 기능을 정의하고 있다. 먼저 이 세 표준의 개요는 표 3과 같다.

가. J.190 케이블-기반 서비스를 지원하기 위한 멀티미디어 홈네트워크 구조

본 표준은 케이블 네트워크를 통한 멀티미디어 서비스를 지원하기 위하여 홈네트워크 내에 디바이스의 유형을 정의하고, 기본 참조 모델을 정의했으며, 주요 기능 블록을 결정했다. 홈 디바이스는 액세스 네트워크와

[표 3] ITU-T SG9 보안 표준 개요

표준 약어	문서 제목	표준화 일시	문서 주요 내용
ITU-T J.192	케이블-기반 서비스를 지원하기 위한 멀티미디어 홈네트워크 구조	2002. 7	- 기본 요구사항(QoS, 보안 요구사항 포함) - 멀티미디어 홈네트워크 기본 구조 - 기능 참조 모델(보안 기능 및 참조 모델 포함) - 정보 참조 모델
ITU-T J.190	케이블 데이터 서비스의 전달을 지원하기 위한 홈네트워크 게이트웨이	2004. 3	- 참조 구조(관리, 보안 포함) - 관리, 설비, 패킷 처리 및 주소 변환, QoS, 보안, 관리 절차, 설비 절차 등

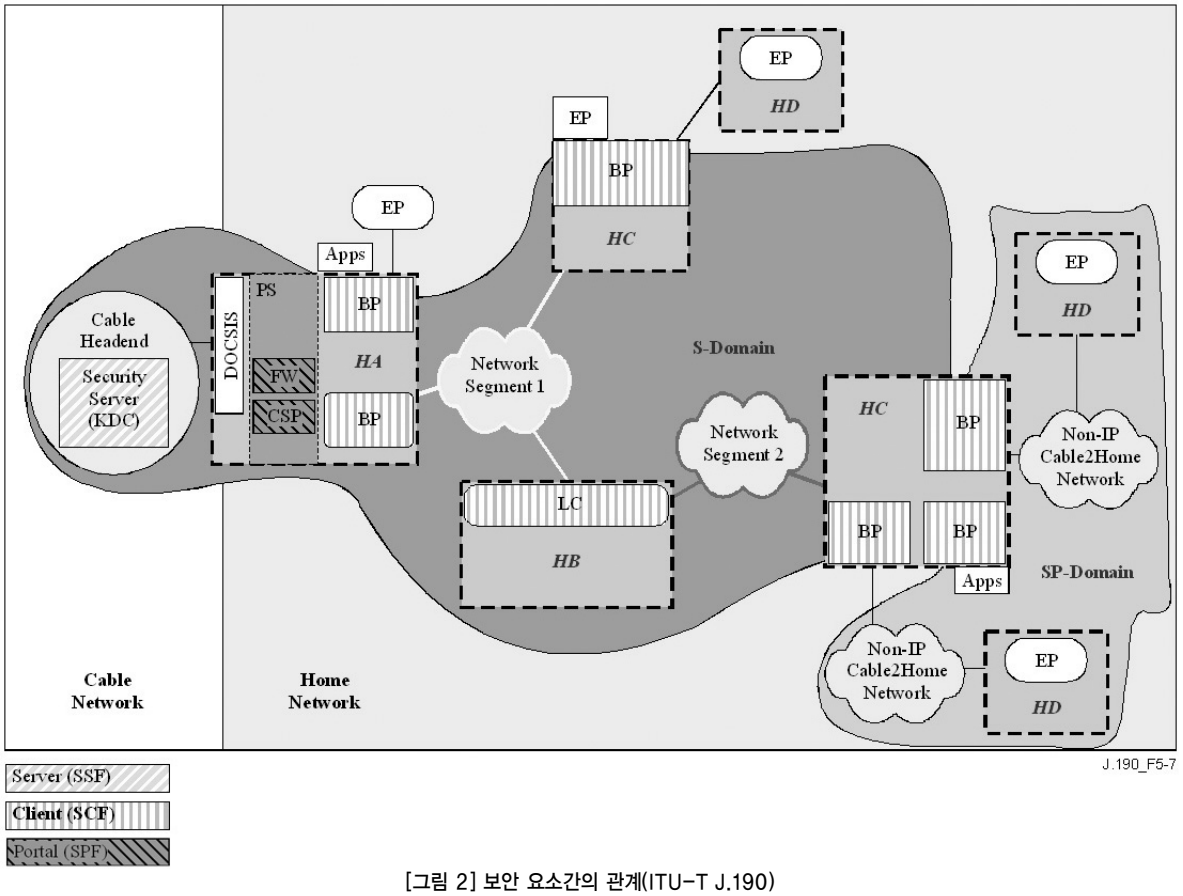
의 인터페이스 기능을 수행하는 HA 디바이스, 홈네트워크 내 요소 시스템간에 브리지 기능을 수행하는 HB 디바이스, 홈 네트워크와 디바이스 전용 통신과 인터페이스 하는 HC 디바이스, 그리고 전용 통신 프로토콜을 갖는 HD 디바이스로 구분하였다. HD 디바이스는 DVD 등의 기존 홈네트워크 내의 디스플레이 디바이스이고, HA 디바이스는 게이트웨이 디바이스, HC 디바이스는 전용 통신 프로토콜을 갖는 디바이스와 HB 디바이스를 연결하는 클라이언트 디바이스, HB 디바이스는 HC 디바이스와 HA 디바이스를 연결하는 브리지 디바이스이다.

보안 기능을 위해 그림 2와 같이 케이블 서비스 제공자 측에 존재하는 보안 서버, 홈네트워크 게이트웨이에 존재하는 방화벽 및 보안 포털, 홈네트워크 디바이스에 존재하는 보안 클라이언트 요소를 정의하고 있다.

보안 서버는 일반적으로 키분배 서버로 동작하며, 홈 네트워크 서비스를 위한 인증과 키분배 기능을 제공해야 한다. 보안 서버는 홈 게이트웨이에 존재하는 보안 포털과 통신하여 여러 다양한 보안 서비스를 제공한다. 방화벽은 악의적인 공격으로부터 홈을 보호하기 위한 기능을 수행한다. 이는 기존의 방화벽 기능의 경량화된 버전이라고 할 수 있다. 보안 포털은 홈 디바이스를 위한, 보안 기능을 위한, 보안 정보를 위한 포털 역할을 수행한다. 보안 포털은 키분배 서버와 통신한다. 보안 클라이언트는 일반적으로 기존의 홈 디바이스(HD)와 HC 디바이스에 존재하는 기능으로 원격 관리자에 의하여 제어된다.

더하여, 부록에 홈 게이트웨이를 인증하고 홈게이트웨이와 케이블 헤드엔드와의 관리 메시지를 안전하게 하기 위한 표준 메커니즘을 요구하고 있다. 이의 구체적인 내용은 다음과 같다.

- 서비스 제공자는 원격으로 사용자의 승인 하에 방



[그림 2] 보안 요소간의 관계(ITU-T J.190)

화벽을 관리할 수 있어야 한다.

- 방화벽은 서비스 제공자에게 방화벽의 로깅/관리자 인터페이스를 이용하여 방화벽의 활동을 관리하고 감시할 수 있게 해야 한다.
- 방화벽 관리 메시지는 인증되어야 하고, 선택적으로 암호화되어야 한다.
- 서비스 제공자는 홈네트워크 요소에 대한 정체성을 보장하기 위한 메커니즘이 제공되어야 한다.
- 홈네트워크 보안 수준은 평균적인 가입자가 비인가된 접근을 얻기가 쉽지 않을 정도의 수준이어야 한다.
- 홈 게이트웨이와 서비스 제공자 설비 시스템간의 인증은 자동적으로 이루어져야 한다.
- 관리자는 방화벽 룰셋이나 설정 파일, 그리고 소프트웨어 이미지를 홈네트워크 요소에 안전하게 다운로드 할 수 있어야 한다.
- 홈게이트웨이와 케이블 헤더엔드 간에 네트워크 관리 메시지는 인증되어야 하고, 선택적으로 암호화되어야 한다.

나. 케이블 데이터 서비스 전달을 위한 홈 게이트웨이

이 표준에서는 통합된 홈내의 보안, 관리, 설비, 주소화, 그리고 QoS 서비스를 제공하기 위한 논리적 요소인 포털 서비스(PS, Portal Service)를 정의하고 있다. 일반적으로 포털 서비스는 홈 게이트웨이 내에 존재하며, 홈게이트웨이는 포털 서비스와 케이블 모뎀 기능을 포함한다. 여기서는 포털 서비스 동작을 안전하게 하기 위해 필요한 보안 인터페이스, 프로토콜, 그리고 기능 요구사항을 정의하고 있다. 일반적으로 안전한 홈 게이트웨이의 목적은 신뢰적으로 IP 멀티미디어 서비스를 제공하는데 있다. 일반적으로 LAN 보안과 PS와 보안 서버간의 보안도 포함한다. 보안 구조를 개발하기 위한 가이드라인은 다음과 같다.

- 요소를 위한 인증 비밀키, 인증서 등의 인증 클리덴셜을 통신할 수 있어야 한다.
- PS와 보안 서버간에 인증 클리덴셜은 제공되어야 한다.
- 케이블 엔드와 PS간에 네트워크 관리 메시지는 인증되어야 하고, 선택적으로 암호화되어야 한다.
- 방화벽은 설정 파일을 수신할 수 있어야 한다.
- 케이블 운영자는 관리 파일이나 SNMP 명령을 통하여 방화벽을 원격으로 관리할 수 있어야 한다.
- 방화벽은 디폴트 정책 룰셋을 포함해야 한다.
- 방화벽을 통하여 필요한 지원을 수행해야 한다.
- 방화벽 필터링 능력 상에 최소한의 요구사항을 두어야 한다.
- 운영관리자는 세부적인 방화벽 사건 로깅 인터페이스의 방화벽 동작을 감시해야 하고 검토할 수 있어야 한다.
- 방화벽은 여러 네트워크 공격으로부터 홈네트워크와 원거리 통신망을 보호해야 한다.
- 방화벽 룰셋과 사건에 대한 관리 메시지는 세부적으로 보안 MIB로 정의되어야 한다.

또한, 구체적으로 다음과 같은 보안 표준 사항을 정의하고 있다.

- PS 디바이스 인증 구조: PS 인증을 위해서는 PKI를 이용하는 방안과 커버러스를 이용하는 방안을 정의하고 있다. 인증서 규격은 X.509 인증서 규격을 기본적으로 따르나, 케이블 제조업자 공개키 기반구조, 케이블 코드 검증 공개키 기반구조, 그리고 서비스 제공자 공개키 기반구조로 구분되어 있다. 또한 인증서에는 기본적으로 버전 3의 인증서 버전과, 공개키 종류와 공개키 값을 포함하며, 확장자로 주체키 확인자, 인증기관키 확인자, 키 용도, 기본 제한자, 서명 알고리즘 등의 확장 필드를 포함하고 있다.
- PS로의 관리 메시지 보호: 관리 메시지는 암호화되어야 하고, 반드시 인증되어야 한다.
- 방화벽: 방화벽은 설정 파일을 표준화된 형태로 수신할 수 있어야 하고, 원격으로 관리되어야 하며, 필터링을 위해 최소한의 요구사항을 가져야 하며, 방화벽의 동작을 원격으로 관리자에 의하여 관리되고 관찰되어야 하며, 보안 MIB를 정의해야 한다.
- 안전한 소프트웨어 다운로드: 케이블 운영자는 안전하게 PS 요소로 소프트웨어를 다운로드할 수 있어야 하며, 이때 PKCS #7 서명된 데이터 형식이 이용된다.
- 설정 파일의 안전한 전달: 운영자는 PS나 방화벽으로 설정파일을 인증하고 선택적으로 암호화하여 전달 할 수 있어야 한다. 이때 이용되는 보안 프로토콜은 TLS 프로토콜이다.

- 암호 알고리즘: 필수 암호 알고리즘은 메시지 인증을 위해 SHA-1 해쉬 알고리즘을 이용해야 한다.

2.4 ITU-T SG17 보안 표준

ITU-T SG17에서는 인터넷 기반 홈네트워크 원격 사용자와 홈네트워크 내부 사용자를 위한 보안 표준을 개발하고 있다. 현재 표 4와 같은 3가지 표준이 개발되고 있으며[9, 10, 11], 이를 이용하면, 안전한 인터넷 기반 홈네트워크 서비스를 제공할 수 있다[13].

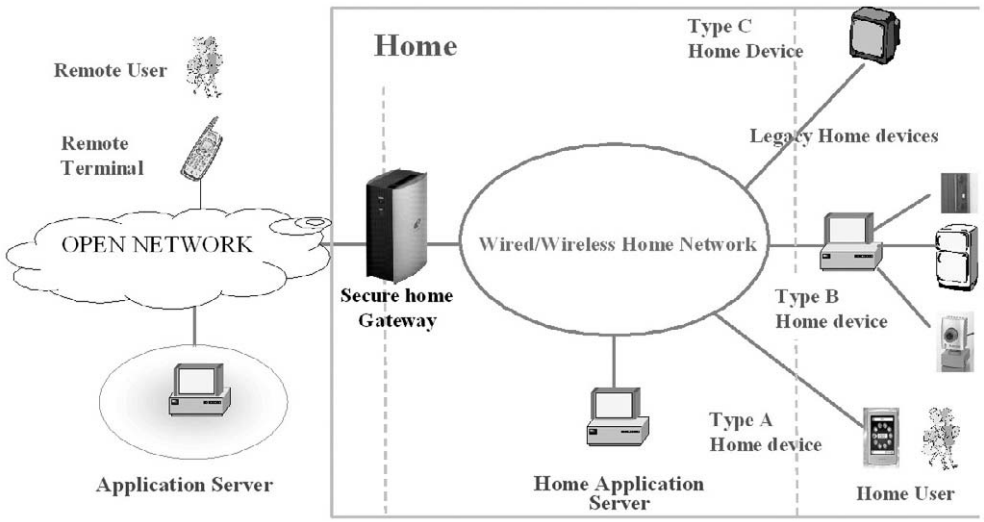
가. X.homesec-1

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 보안 요구사항들을 정의하였다. 그리고 홈네트워크에 응용 가능한 보안기술과 보안위협들을 해결하기 위한 보안 기능들을 정의하였으며, 이런 보안 기능들을 구현 가능한 계층들을 정의하였다.

[그림 3]은 홈네트워크를 위한 보안 모델로 원격 사용자, 원격 터미널, 응용서버, 안전한 홈게이트웨이, 홈 응용서버, 홈디바이스, 홈 사용자 등 7개의 개체들로 구성된다. 여기에서 홈디바이스는 보안 관점에서 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 보안 관점에서 정의한 댁내 게이트웨이로써,

[표 4] SG17 홈네트워크 보안 표준(안) 개요

표준 약어	표준 제목	완료시점
X.homesec-1(X.1111)	Framework for security technologies for home network	2007/1Q
X.homesec-2	Certificate profile for the device in the home network	2007/3Q
X.homesec-3	User authentication mechanisms for home network service	2008/4Q
제안 예정	Framework of authorization in home network	2008/4Q



[그림 3] 홈네트워크를 위한 보안 모델(ITU-T X.1111)

외부 네트워크와 댁내 네트워크 사이에서 주어진 보안 정책에 따라 데이터 패킷 전송, 보안 파라미터 변환, 사용자 인증, 패킷 필터링, 침입차단 등의 보안 기능을 수행한다. 홈 응용서버는 원격 터미널과 홈디바이스들을 연결하게 하며, 원격 사용자 및 홈 사용자들에게 댁내에 존재하는 멀티미디어 서비스나 다양한 응용서비스들을 제공한다. 홈유저는 댁내에서 홈네트워크 디바이스나 외부 네트워크의 다양한 서비스에 접근하고자 하는 사용자이다. 홈디바이스는 댁내에 존재하는 개체로써 홈 사용자들에게 편리한 서비스를 제공하기 위한 장치들이다. 이는 보안적 관점에 따라 다시 Type A, B, C로 분류되는데, Type A에는 다른 홈디바이스들을 제어하는 기능을 가지고 있는 PC, PDA 등이 이에 해당하고, Type B는 브리지 역할을 하는 홈디바이스로 통신 인터페이스가 없는 홈디바이스를 홈네트워크에 연결해주는 역할을 한다. 즉, Bluetooth, HAVi 등의 기능을 가지고 있는 장치들이다. Type B는 한쪽에 전용 통신 프로토콜로 기존 디바이스와 연결되고, 다른 쪽은 공통의 통신 프로토콜로 홈네트워크에 연결되어 있는 디바이스라고 볼 수 있다. Type C는 Type A 디바이스에 의하여 제어되는 디바이스로써 통신 기능이 있으며, 통상 보안 카메라, A/V 장치 등이 이에 해당한다.

X.homesec-1에서는 지금까지 정의된 각각의 관계 및 분석을 통하여 홈네트워크를 위한 보안 모델과 보안 기술들의 관계를 정의하였으며, 본 모델에서 각 개체간에 보안 구현이 필요한 계층과 홈네트워크를 위한 보안 기능 요구사항으로 총 13가지의 요구사항을 정의하였다.

① 홈네트워크를 구성하는 모든 개체들은 중요한 정보들을 안전하게 유지하여야 하며, 비인가된 사용자들로부터의 접근, 변조, 삭제를 막아야 함

② 원격 터미널은 적절한 사용자 인증방법을 통하여, 원격사용자의 인증을 수행하여야 함

③ 원격 터미널과 안전한 홈게이트웨이 구간은 네트워크 계층이나 섹션 계층에서 개체인증, 키관리, MAC, 무결성 기능을 가져야 함

④ 원격 터미널과 홈 응용서버 구간은 용용계층이나 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

⑧ 홈디바이스 B, C와 홈 응용서버/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 홈 응용서버/응용서버 간에는 네크워크 계층에서 개체인증, 키관리, MAC, 무결성 기능을 가져야 함

⑪ 홈네트워크 관리자는 사용자 허가 하에 원격 및 로컬로 홈게이트웨이나 홈 응용서버를 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 관리자에게 모니터링 되어야 함

현재 이 표준은 2006년 12월 ITU-T SG17 총회에서 ITU-T X.1111로 승인되었으며, 본 논문 작성 시점에 국가별 수렴 과정을 수행 중에 있다.

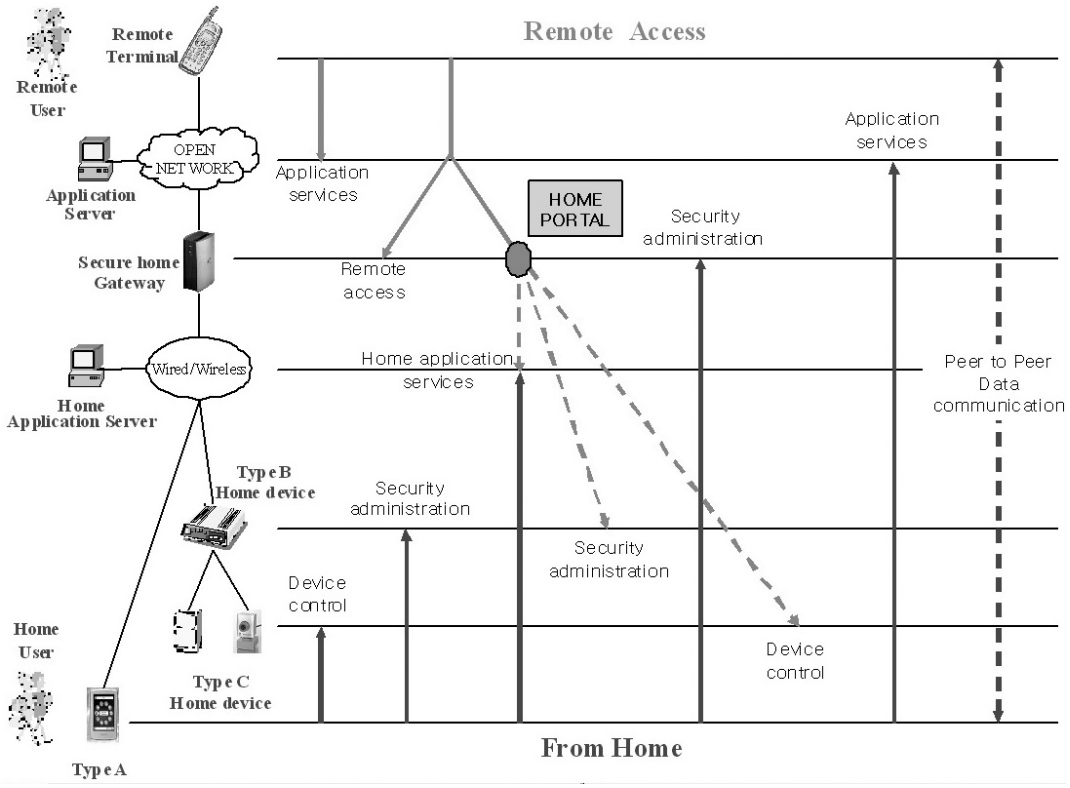
나. X.homesec-2

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 프로파

일을 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 해야 한다. 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 하기 위하여, 케이블 서비스에도 적용가능하며, 홈디바이스 고유식별자(CPU Serial Number, LAN Card MAC 등)를 고려키로 하였다. 또한, 보안 알고리즘의 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 서비스들을 고려하여 개발하고 있다.

홈디바이스 인증서 프로파일은 ITU-T X.509와 IETF RFC3280을 기반으로 정의하고 있으며, 기본필드와 추가적인 정보를 담고 있는 확장필드로 구성되어 있다. 기본 필드는 버전, 일련 번호, 서명 알고리즘, 발행자 필드, 유효기간, 주체, 주체 공개키 확장필드 등이며, 확장 필드는 인증기관 확인자, 주체 확인자, 키 용도, 기본 제한자 등이다.

홈네트워크에서 디바이스 인증서 관리는 안전한 홈게이트웨이가 인증서의 발급, 폐기, 유효성 검증을 수행한다. 또한 인증서의 발급 방법으로는 외부에서 직접적으로 등록하는 방법과 온라인으로 등록하는 방법이 있다. 홈디바이스들 중에 PC, PDA 등과 같이 직접으로 연산이 가능한 디바이스들은 2가지 방법으로 등록이 가능하



[그림 4] 홈네트워크 인증 서비스 구조(ITU-T X.homesec-3)

나, 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 대리 인증기관으로부터 등록코드(reference code/authorization code)를 부여 받고, 이를 이용하여 자신의 홈디바이스들에게 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 원격 터미널과 홈게이트웨이 구간, 응용 서버와 홈게이트웨이 구간, 홈디바이스와 홈게이트웨이 구간에서 사용되며, 링크계층과 응용계층에서 주로 사용될 것이다.

다. X.homesec-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 홈 사용자들에 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 4와 같은 인증 서비스 구조를 정의하였다. 홈포털(Home Portal)은 일종의 대행서버(Proxy Server)로 사용자가 직접적으로 서비스를 받을 수 없을 때 중간매개체 역할을 수행하는 개체로써 사용자를 인증하고 사용자가 요구하는 명령들을 모아 해당하는 홈디바이스에 맞는 프로토콜로 변경하는 역할을 수행하다. X.homesec-1 모델에서 이 역할은 안전한 홈게이트웨이나 홈 응용서버가 수행할 수 있으나 X.homesec-3에서는 안전한 홈게이트웨이에서 홈포털을 수행하는 것으로 가정하였다. 또한, 그림 5와 같이 원격 사용자는 댁내서비스를 이용하기 위하여 홈포탈을 이용하여 접근할 수 있고, 홈유저들은 홈포털 없이 직접적으로 댁내 및 댁외 서비스에 접근할 수 있다고 가정하였다.

III. 결언

본 논문에서는 홈네트워크 보안 표준을 위해 ITU-T SG9, SG17, UPnP, DSL 포럼 등에서 수행되는 표준화 동향을 살펴보았다. ITU-T SG9에서는 케이블 기반 멀티미디어 서비스를 제공하기 위한 보안 기능을, SG17에서는 일반적인 홈 원격 사용자와 홈 사용자를 위한 보안 기능을, DSL은 ADSL 기반 홈네트워크 내의 디바이스에 대한 원격 관리를 위해 요구되는 보안 기능을, ITU-T SG9 에서는 케이블 기반 멀티미디어 및 데이터 서비스를 제공하기 위해 요구되는 보안 기능을, ITU-T SG17에서는 인터넷 기반 원격 사용자 및 홈네트워크 내부 사용자를 위해 요구되는 보안 기능을 정의하고 있고, 관련 표준을 개발하고 있다.

따라서 이들 보안 표준들은 응용이나 환경에 따라 적절하게 적용되어야 할 것이다. 특히 SG17은 한국 주도로 보안 표준이 개발되어 있고, 향후 유비쿼터스 홈 네트워크 환경을 고려한 보안 표준을 계획하고 있어서, 국내의 많은 산업체나 표준 전문가의 관심이 요구되고 있다. 끝으로, 본고가 홈네트워크 보안 시스템을 설계하는 산업체나 연구자에게 도움이 되었으면 하는 바램이다.

참고문헌

[1] DSL TR-064, LAN-side DSL CPE Configuration, 2004. 5.

[2] DSL TR-069, CPE WAN Management Protocol, 2004. 5.

[3] DSL TR-094, Multimedia-Service Delivery Framework for Home Networks, 2004. 8.

[4] UPnP, UPnP Security Ceremonies Design Document, 2003. 10

[5] UPnP, DeviceSecurity:1 Service Template, 2003. 11.

[6] UPnP, SecurityConsole:1 Service Template, 2003. 11.

[7] ITU-T J.190, Architecture of MediaHomeNet that supports cable-based services, 2002. 7.

[8] ITU-T J.192, A Residential Gateway to Support the Delivery of Cable Data Services, 2004. 3.

[9] 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.

[10] 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.

[11] 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.

[12] 진병문, 오흥룡, 염흥열, 강신각, '2006년 ITU-T SG17 연구동향', TTA, ITU-T 연구활동 보고서, 2006. 12.

[13] 오흥룡, 염흥열, 'ITU-T SG17 홈네트워크 보안 표준화 동향 및 향후 전망,' 한국정보보호학회, 16권 6호, 2006. 12. TTA