情 報 保 護 學 會 誌
第17卷 第1號, 2007. 2

안전한 통신 서비스 표준화 동향 및 향후 전망

오흥룡*, 염흥열**

요 약

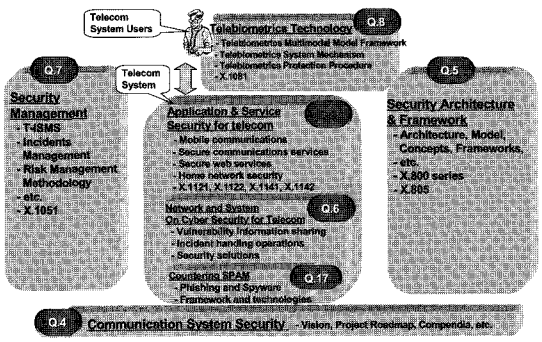
국제표준화기구 ITU-T SG17 WP2에서는 정보통신 보안에 관한 표준을 주도하는 연구그룹으로, 산하 7개의 연구과제(Question)를 구성하여 정보보호 표준화 작업을 진행하고 있다. 이 연구과제들 중 Q.9/17에서는 안전한 통신 서비스라는 이름으로 모바일 보안, 홈네트워크 보안, 웹 서비스 보안, 그리고 안전한 응용 프로토콜 등에 대한 표준을 개발 중에 있다. 현재, Q.9/17에서 제정된 표준은 한국과 일본이 공동으로 제안하여 2004년 3월에 제정된 모바일보안 2건(X.1121, X.1122)과 OASIS의 제안으로 2006년 6월에 제정된 웹서비스 보안 2건(X.1141, X.1142)이 표준으로 제정된 바 있다. 그리고 Q.9/17에서 작업중에 있는 표준초안은 모바일 보안 3건, 홈네트워크 보안 3건, 웹서비스 보안 1건, 안전한 응용 프로토콜 2건, P2P 보안 2건 및 RFID 보안 1건에 대해서 개발중에 있다. 특히, 이번 12월 제네바 회의에서는 한국 주도로 개발된 홈네트워크를 위한 보안기술 프레임워크(X.homesec-1) 표준초안이 SG17 총회에서 승인되어 국가별 의견수렴(consent)을 추진키로 합의되었다. 본 논문에서는 Q.9/17에서 수행되고 있는 표준초안들에 대해 간단히 소개하고, 2006년 9월 캐나다 오타와 회의와 2006년 12월 스위스 제네바 회의에서의 주요쟁점사항 및 토론 결과, 그리고 향후 추진방향을 제시하고자 한다.

Ⅰ. 서 론

급속도로 발전하는 유비쿼터스 환경에서는 이동성과 휴대성이 편리한 모바일 네트워크와 사용자들이 집안에서 편리하게 다양한 컨텐츠를 이용할 수 있는 홈네트워크가 발전할 것으로 예측되며, 이러한 환경에서 응용서비스들이 안전하고 신뢰성 있게 제공되기 위해서는 모바일 환경에서의 보안 기술, 홈네트워크 환경에서의 보안기술, 이를 위한 안전한 응용 프로토콜, 그리고 안전한 웹 서비스를 위한 인프라 보안 등의 표준 개발이 요구되고 있다. ITU-T SG17에서는 정보통신 보안에 관한 표준을 선도하는 그룹으로 〔그림 1〕과 같이 WP2 산하에 통신 시스템 보안 프로젝트, 보안 구조 및 프레임워크, 사이버 보안, 보안 관리, 바이오인식, 안전한 통신서비스, 기술적인 스팸대응 등의 7개 연구영역으로 보안 표준들을 개발하고 있다. ITU-T SG17은 이번 연구회기(2005년-2008년)동안 정보통신 보안 관련하여 총 7회의 국제표준화 회의를 개최한 바 있다[22]. 본 논문에서는 ITU-T SG17 WP2 Q.9에서 수행하고 있는 최근 표준화 동향, 현재의 주요 표준화 항목, 각 표준화 항목당 주요 쟁점사항, 그리고 향후 표준화 추진 계획을 중심으로 살펴본다.

Ⅱ. ITU-T SG17 연구과제 9의 표준화 현황 및 전망

Q.9에서 개발되어 완료된 표준은 모바일 보안(X.1121, X.1122), 웹서비스 보안(X.1141, X.1142) 총 4건이 표



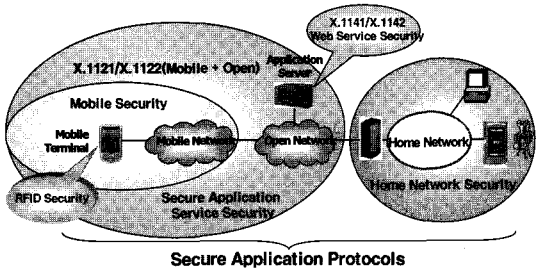
〔그림 1〕 ITU-T SG17 WP2 연구영역

* 한국정보통신기술협회 표준화본부 (hroh@tta.or.kr)
** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

준으로 존재하고 있으며[1,2,5,6], 〔표 1〕과 같이 홈네트워크 보안, 모바일보안, 안전한 응용서비스, 웹서비스 보안 등의 표준화가 추진되고 있다.

2.1 Q.9의 표준화 연구영역

Q.9의 표준화 연구영역은 〔그림 2〕와 같이 크게 안전한 응용서비스 보안, 홈네트워크 보안 및 안전한 응용 프로토콜 보안으로 표준화를 추진하고 있다. 다시 안전한 응용서비스 보안영역은 모바일 단말기와 모바일 네트워크 간에 요구되는 모바일 보안, 사용자 단말기와 RFID 태크 간에 요구되는 RFID 보안, 서비스 제공자(ISP)가 사용자에게 안전하게 서비스를 제공하기 위한 웹서비스 보안으로 세분화된다. 기존의 X.1121 및 X.1122 표준은 모바일 보안 영역과 웹서비스 보안영역 간에 요구되는 표준이며, X.1141 및 X.1142는 웹서비스 보안을 지원하기 위한 표준이다. 또한, 홈네트워크 보안은 댁내에 존재하는 보안사항과 개방형 네트워크를 통하여 서비스되는 구간까지의 영역을 다루고 있다. 끝으로 안전한 응용프로토콜 보안은 이들 전체영역에서 안전하게 응용 가능한 프로토콜을 표준화하기 위한 연



〔그림 2〕 Q.9의 표준화 연구영역

구영역으로 프로토콜의 취약점 및 선정기준 등을 연구하고 있다[25].

2.2 기존 표준안(X.1121, X.1122, X.1141, X.1142)

ITU-T X.1121과 X.1122는 한국과 일본이 공동으로 제안하여 지난 연구회기 동안 표준화된 표준이다[1,2]. X.1121에서는 모바일 종단간 데이터통신을 위한 프레임워크를 제시하고 있으며, 두 가지 통신 모델을 정의하여, 모바일 환경에서 발생하는 다양한 취약성을 분석하고, 이 취약성을 대비할 수 있는 보안 서비스를 정의하였으며, 보안서비스를 구현하는 구체적인 보안 메커니

〔표 1〕 ITU-T SG17 WP2 Q.9에서 개발 중인 표준초안 현황

표준 약어	제 목	에디터	기반 문서	완료시기
X.msec-3	General security value added service (policy) for mobile data communication	F. Zhang, J. Chen	TD2515	2008. 4
X.msec-4	Authentication architecture in mobile end-to-end data communication	Z. Zheng, J. Wei	TD2446 Rev.1	2007. 9
X.crs	Correlative reacting system in mobile network	S. Liu, J. Wei	TD2442 Rev.1	2007. 9
X.homesec-1	Framework for security technologies for home network	H. Y. Youm, H. R. Oh	TD2512 Rev.1	2007. 2
X.homesec-2	Certificate profile for the device in the home network	D. Y. Yoo, J. H. Baek	TD2514	2008. 4
X.homesec-3	User authentication mechanisms for home network service	H.K.Lee	COM77	2008. 4
X.sap-1	Guideline on secure password based authentication protocol with key exchange	H. Y. Youm	TD2507	2007. 9
X.sap-2	Secure communication using TTP service	T. Kaji	TD2511	2008. 4
X.p2p-1	Requirements of security for P2P communications	Y. Miyake	TD2520	2008. 4
X.p2p-2	Security architecture and protocols for peer to peer network	J. H. Nah	COM72	2008. 4
X.websec-3	Security architecture for message security in mobile web services	J. S. Lee	TD2513	2008. 4
X.rfidsec-1	Privacy protection framework for networked RFID services	D. H. Choi	COM96	2008. 4

즘을 도출하고, 이 보안 메커니즘이 통신 모델에서 어느 보안 요소에 실현되어야 하는지에 대하여 정의하고 있다. X.1122는 PKI 기반의 안전한 모바일 시스템 구현을 위한 가이드라인 표준이다. X.1122에서는 게이트웨이 기반의 PKI 모델과 일반적인 PKI 모델을 정의하고, 이 두 가지 모델에 기반을 둔 인증서 발행, 인증서 취소, 인증서 유효성 검증 등의 인증서 관리 절차 등을 정의하였고, 사용자 인증 및 서버 인증, 그리고 무결성 서비스 등으로 구성되는 세션 레벨 보안 서비스와 인증, 무결성, 디지털 서명 등의 응용 레벨 보안 서비스가 요구됨을 정의하였다. 세션 레벨 보안 기능을 위하여 사용자 인증 및 응용 서비스 인증 절차, 암호와 무결성 서비스 제공 절차가 기술되었고, 응용 레벨 보안을 위하여 서명과 암호 기능을 제공하기 위한 구체적인 절차가 기술되었다[19].

ITU-T X.1141과 X.1142는 OASIS에서 제정된 XML 보안 표준(SAMLv2.0, XACMLv2.0)을 2005년 7월에 ITU-T SG17로 제안하여 2006년 6월에 제정된 웹서비스 보안 표준이다[5,6]. X.1141 표준은 보안 정보를 교환하기 위한 XML 기반의 프레임워크를 정의하는 표준이다. 즉, 통신 주체들(사용자, 컴퓨터, ISP 등) 간에 요구되는 보안주장들을 XML 언어로 표현하기 위한 방법을 정의하고 있으며, 이들 주장들은 인증, 권한부여, 속성들의 서로 다른 정보들로 구성되어 있다. 또한, X.1141 표준은 통신주체간에 교환되는 메시지들의 형식을 XML로 정의하고 있으며, 이들 간에 사용되는 프로토콜을 정의하고 있다. X.1142 표준은 통신주체간에 요구되는 접근제어 정책들을 XML 언어로 표현하기 위한 방법을 정의하고 있다. 즉, 임의의 어떤 자원에 접근하고자하는 개체들에게 일정한 권한을 부여하는 정책과 이들 정책을 평가하는 규칙, 이를 XML로 표현하는 방법들을 정의하고 있다.

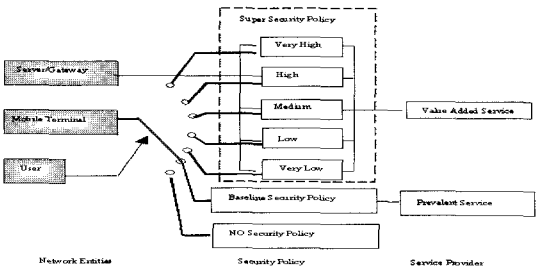
2.3 모바일 보안 표준화 동향 및 쟁점사항

2.3.1 개요

모바일 보안 표준화는 2004년에 제정된 X.1121, X.1122 표준 이후 3건의 표준초안이 중국을 중심으로 개발되고 있다.

첫 번째로 모바일 환경에서 보안 서비스(정책) 표준(X.msec-3)은 보안 서비스를 새로운 부가가치 서비스로 개발하기 위한 일반적인 보안 모델과 관련 보안 절차, 보안 정책, 보안 정책관련 보안 요소 집합, 그리고 이를 위한 정보 요소를 정의하고 있다[10]. 모바일 보안 정책의 이점은 순수한 이동 네트워크 환경 또는 이동 네트워크와 고정 네트워크가 상호 연동되는 환경에서 사용자에게 부가가치 서비스로 보안 서비스를 제공함으로써, 네트워크 제공자에게 새로운 서비스 모델을 창출케 하고, 사용자에게 안전한 모바일 서비스를 이용 가능케 한다는 점이다.

X.msec-3에서는 이동망에서 다양한 등급화된 보안 서비스를 제공하기 위한 기본 프레임워크로 [그림 3]을 정의하였다. 보안 정책 프레임워크는 크게 3 부분으로 구성된다. 첫 번째 부분은 보안 정책이 적용되는 개체가 어디냐에 따라서 보안 게이트웨이, 모바일 단말, 그리고 사용자 등으로 구성되는 "네트워크 개체" 요소이고, 두 번째 부분은 특정 개체에 적용되는 보안 정책이 어느 등급이냐에 따라서 상위 보안정책(super security policy), 기본 보안 정책(baseline security policy), 그리고 무보안 정책(no security policy) 으로 구분되는 "보안 정책" 요소이며, 세 번째 부분은 제공되는 보안 서비스가 어느 서비스에 속하느냐에 따라 부가 가치 서비스(value added service)와 일반 서비스(prevalent service)로 구분되는 "서비스 제공자" 요소이다. 보안 정책 요소 중에서 상위 보안 정책은 다시 여러 개의 세부 보안 계층으로 구분된다. 여러 개의 세부 보안 정책 중 "최상위 보안 정책(High)"은 가장 강력한 암호 알고리즘과 가장 긴 암호 키를 사용하여 높은 수준의 보안 기능을 제공하는 세부 보안 정책 계층이다. 무보안 정책은 모바일 보안과 응용 서비스 서버에서 보안 기능이 필요치 않은 환경에서 이용되며, 모바일 단말 또는 응용 서비스 제공자가 외부에서 제공되는 보안 서비스를 이용하거나, 통신 환경이 높은 수준으로 안전한 경우에 사용될 수 있다. 기본 보안 정책은 일방향 인증,



[그림 3] 보안정책 프레임워크

신분 관리, 유용성 등과 같이 기본 보안 서비스만을 제공하는 반면, 상위 보안 정책에서는 이보다 종류가 많고 암호 강도 측면에서도 강력한 인증, 기밀성, 무결성, 익명성, 접근제어, 부인방지, 그리고 프라이버시 보안 서비스 등 까지를 제공하도록 하였다. 기본적으로 모바일 단말을 포함한 모든 네트워크 요소는 기본 보안 정책 이상을 제공해야 한다고 권고되고 있다. 이외에 모바일 단말과 응용 서비스 제공자간에 정책 협상 절차에 대한 내용을 포함하고 있다.

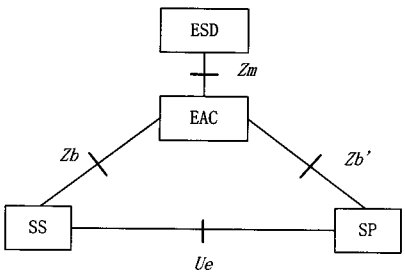
두 번째로는 모바일 종단간 데이터 통신에서의 인증 구조(X.msec-4)로 모바일 사용자와 다양한 응용서비스 제공자 간에 효율적인 인증 방법을 제공하기 위한 표준이다[11]. 특히, 응용서비스 제공자의 유형과 형태에 무관하게 일반적인 인증 모델을 통하여 인증 서비스를 제공하는 것은 매 응용 서비스 제공자마다 인증 서비스를 개발해야 하는 부담을 덜고 통일화된 인터페이스를 통하여 인증 서비스를 네트워크 제공자가 제공할 수 있다는 측면에서 매우 유용하다.

〔그림 4〕의 X.msec-4 인증 모델에서 SS(Service Subscriber)는 서비스 가입자, SP(Servics Provider)는 서비스 제공자, EAC(Entity Authentication Center)는 인증센터, ESD(Entity Subscrption Database)는 사용자 및 서비스 제공자의 인증정보를 보관하는 데이터베이스, AP(Authentication Proxy)는 대리 인증 서버를 의미한다. 모바일 통신을 하기 위해서 사용자 및 서비스 제공자는 사전에 인증정보를 EAC에게 등록함으로써, 통신을 시작할 때 서로 간에 안전한 상호인증이 가능하다. X.msec-4에서는 인증 서비스 시나리오로 3가지 방법이 고려되고 있으며, 첫 번째는 SS가 SP에게 서비스를 요청할 때, 자신의 인증정보를 SP에게 전달함으로써, SP는 이를 EAC에게 검토 의뢰하고, SS가 사전에 인증된 SS일 경우 서비스를 제공하는 방법이다. 두 번째는 SS가 임의의 SP로부터 서비스를 이용하고자 할 때, 직접 자신의 인증정보를 EAC에게 전달하여 본인에 대한 인증을 요청하고, EAC로부터 보증된 인증정보를 받아 SP에게 전달함으로써 성립되는 방법이다. 세 번째는 SS가 임의의 SP로부터 서비스를 이용하고자 할 때, EAC를 통하여 SP에게 서비스를 요청하는 방법이다. 즉, SP는 EAC를 신뢰기관으로 인증함으로써 SS를 인증하고, 본인의 인증정보 또한 EAC를 통하여 SS에게 전달함으로써, 향후 서로 간에 신뢰된 서비스가 가능하게 되는 방법이다.

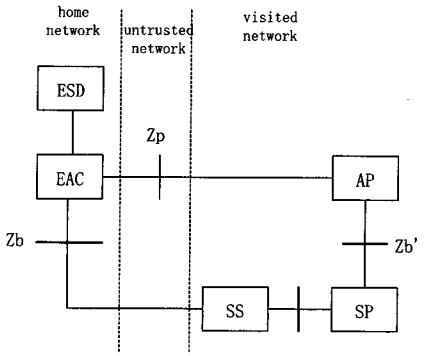
〔그림 4〕의 오른쪽에 있는 인증모델은 서비스 가입자가 외부 네트워크로 이동되었을 때, AP를 이용하여 상호인증하기 위한 모델이다. 현재, X-msec-4는 아래와 같은 모델을 기반으로 각각의 구간(Ue, Zb, Zb', Zm, Zp)에서 발생되는 인증협약절차, 인증방법, 보안요구사항 등에 대한 표준화를 추진하고 있다.

세 번째로는 모바일 데이터 통신에서의 상호연동 시스템(X.crs) 표준으로 최근 모바일 단말을 대상으로 하는 웜과 바이러스가 증가되고 있어, 이동환경에서 단말과 네트워크간의 협력을 통하여 모바일 단말의 보안 상태를 파악하여 잠재적인 공격을 제어하기 위한 표준이다[12].

상호연동 시스템의 기본원리는 〔그림 5〕와 같이 단말에서 보안 관련 정보를 수집하는 보안 상관 에이전트, 단말로부터 보안 관련 정보를 수집하여 단말의 보안 등급을 결정하는 보안 상관 서버, 그리고 단말의 보안 등

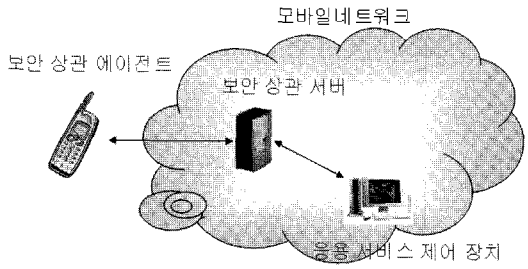


< 모바일 인증 모델 >

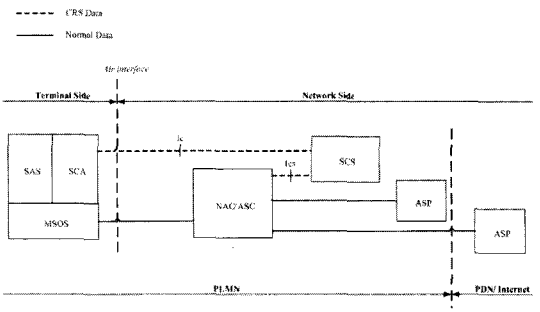


< 외부 네트워크와 인증 모델 >

〔그림 4〕 X.msec-4 인증 모델



〔그림 5〕 상호연동 시스템의 기본 원리



〔그림 6〕 상호연동 시스템 구조

급을 저장하고 있는 응용서비스 제어 장치로 구성된다. 모바일 단말에 보안 상관 에이전트를 두고, 보안 단말 에이전트는 단말의 보안 관련 정보(운영체제의 버전, 안티 바이러스 소프트웨어의 버전, 단말에 존재하는 응용서비스 목록)를 수집하여 모바일 네트워크에 있는 보안 상관 서버에 전송하며, 보안 상관 서버는 수신된 정보를 근거로 이 단말에 대한 보안 등급을 평가하여 접근을 위한 범위, 접근 가능한 응용, 송수신 속도 등을 제어한다. 또한, 보안 상관서버는 단말로 하여금 최신 바이러스 백신 또는 운영체제에 대한 업데이트를 담고 있는 사이트로 이동하여 새로운 버전의 백신 또는 운영체제 업데이트 버전을 다운로드 받도록 유도하는 등의 행위도 수행할 수 있다. 이렇게 함으로써, 네트워크가 단말의 보안 상태를 실시간으로 제어할 수 있고, 이를 근거로 바이러스 또는 웜에 오염된 단말의 행위가 네트워크에 바로 영향을 미치지 않게 할 수 있다. 〔그림 5〕의 기본원리를 구체화한 상호연동 시스템 구조는 〔그림 6〕과 같다. 단말은 보안 응용프로그램을 담당하고 있는 SAS, 단말의 운영체제를 담당하는 MSOS, 상관 서버로 단말의 정보를 전송하기 위한 보안 상관 에이전트 SCA로 구성된다. 그리고 여기서 SCA는 일종의 응용프로그램으로 구현될 수도 있고, 아니면 별도의 하드웨어로도 구현이 가능할 것이다. 하지만, 다양한 종류의 단말과 각 지역마다의 특성을 고려하여 실시간으로 업데이트가 가능한 응용소프트웨어로 구현하는 것이 편할 것이다. 즉, SCA가 내장된 단말은 임의의 상관 서버가 존재하는 네트워크에 접속하게 되면, 우선 자신의 SCA가 해당 SCS와 연동이 가능한 지를 체크하여, 필요시 SCS에게 제공되는 SCA 응용프로그램을 다운받음으로 통신이 가능하게 된다. 그리고 〔그림 6〕에서는 제외되었지만, 단말의 내부에는 각 영역 간에 상호정보를 체크하기 위한 별도의 인터페이스가 존재하고 있다. SCS는 IC 인터페이스를 통해 단말의 보안정보를 평가하게 되고, 평가 결과에 따라 네트워크 접근제어기(NAC), 응용서비스 접근제어기(ASC)에게 해당 단말의 보안정책이나 접근 가능한 범위를 할당할 수 있게 된다.

본 표준은 〔그림 6〕의 구조를 바탕으로 각각의 영역에서 존재할 수 있는 보안위협과 이를 해결하기 위한 보안요구사항, 각 구간에서의 동작절차 및 효율적인 상호연동 시스템 구현 방법들에 대해서 개발중에 있다.

2.3.2 2006년 오타와 및 제네바 회의의 주요 이슈, 쟁점 사항, 향후 추진방향

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

- X.msec-4는 USIM과 사용자 단말기에서 SS 기능성에 대한 가능한 위치를 text로 설명키로 하였으며, 사용자 단말기에 SS가 존재할 경우, 잠재적으로 존재하는 보안 취약점을 고려키로 함, 또한, USIM과 같은 토큰에서 SS가 존재할 경우, 사용자 인증에 대한 필요성을 text로 설명키로 하였으며, USIM 용어에 대해 명확히 정의키로 하고, information reference에 Kerberos 기술에 대한 문서들을 일부 삽입키로 합의되었다. 그리고 본문 내용 중에 'public-private key pair' => 'asymmetric key pair', 'certificate repository' => 'certificate depository'으로 수정키로 하였고, 기존 네트워크(home network)와 방문된 네트워크(visited network) 사이에 AP의 가능한 위치를 text로 설명키로 하였고, TLS를 기반으로 B.3의 그림을 수정키로 하였으며, B.3에 절차 4, 5, 6을 수정키로 하였다.

- X.crs는 CRS 메시지 무결성에 대한 이름과 'OS/platform version' => 'OS version' 변경키로 하였으며, CRS 시스템에 설치되는 패치들의 이름을 일반적인 예로 리스트하는 방법을 추가키로 하였다.

오타와 회의 결과를 바탕으로 수정된 기고서를 2006년 12월 제네바 회의에 제안하였으며 주요결과는 다음과 같다.

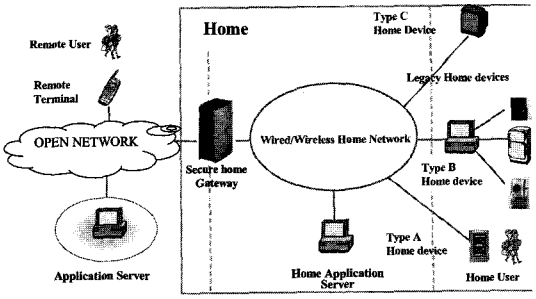
- X.msec-3는 3.2 절에 "security domain"을 정의하기로 하고, [그림 1]의 모델과 다른 그림들에 있는 모델들 간의 차이점을 명확히 정의하기로 하였다. 또한, [그림 5]를 수정하기로 하고, [그림 5]와 [그림 6] 사이에 있는 step 3과 [그림 5]와 [그림 7] 사이에 있는 step 5에 대한 관계를 명확히 정의하였다. 그리고 보안게이트 간에 세부적인 협약 과정은 X.msec-3 연구범위에서 벗어나므로 일부 문장으로만 설명을 다루기 검토되었고, Appendix A, B를 Annex A, B로 변경될 가능성을 검토키로 하였으며, 한국에서 제안한 X.msec-3 코멘트 기고서의 모든 항목들을 받아들이기로 합의되었다.
- X.msec-4는 오타와 회의에서 지적된 코멘트를 반영하여 최종 TD2446Rev.1표준초안을 개발하여, 이를 3GPP, 3GPP2, SG19, OMA에 검토 의뢰키로 합의되었다.
- X.crs는 13장의 주요 내용이 CRS 시스템의 구현을 위한 전형적인 예이므로, Appendix A로 이동하고, [그림 18]은 본문에 포함시킬 것에 대해 추가 검토키로 하였으며, 11.2절에 정의된 "large scale update" 항목은 유용성 유/무에 대해 재검토키로 하였다.

2.4 홈네트워크 보안 표준화 동향 및 쟁점사항

2.4.1 개요

2004년 11월 일본 동경 회의에서 처음으로 홈네트워크 보안 연구의 필요성을 한국에서 제안하여 채택되어, 현재 Q.9에서 한국을 중심으로 총 3건의 표준이 추진되고 있으며, 2006년 12월 제네바 회의에서 신규 표준화 아이템으로 홈네트워크 보안을 위한 인가 프레임워크 표준을 제안하여, Q.9에서 그 중요성을 인정받았다.

첫 번째는 홈네트워크를 위한 보안기술 프레임워크



[그림 7] 홈네트워크를 위한 보안 모델

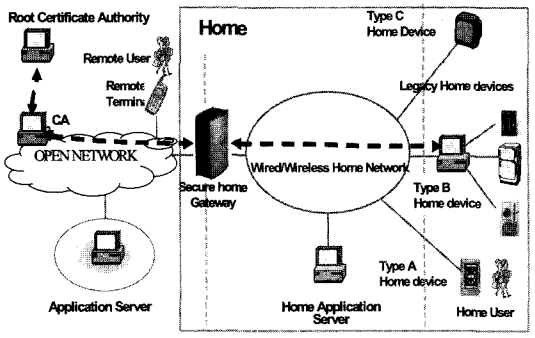
(X.homesec-1) 표준은 유/무선 전송기술을 고려하고 있으며, 홈네트워크 사용자 및 원격사용자의 보안적 측면에서 보안위협과 보안요구사항들을 정의하였다. 그리고 홈네트워크에서 응용 가능한 보안기술과 보안위협들을 해결하기 위한 보안 기능들을 정의하였으며, 이런 보안 기능들에 대한 구현 가능한 계층들을 정의하였다[7].

[그림 7]은 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 기

능을 가지고 있는 장치들이다. C는 단지 디스플레이 기능만을 가지고 있는 보안카메라, A/V 장치 등이 이에 해당한다.

홈네트워크를 위한 보안 모델에서는 원격유저와 원격터미널, 원격터미널과 안전한 홈게이트웨이, 원격터미널과 홈응용서버, 원격터미널과 홈디바이스 A, 원격터미멀과 홈디바이스 B/C, 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 13가지의 관계에 존재하는 보안위협과 보안요구사항, 이를 해결하기 위한 보안기능들을 정의하고 있다. 또한 보안이 실현되어야 할 계층을 확인하고, 이를 위한 구체적인 요구사항을 정의하고 있다.

두 번째로는 "홈네트워크를 위한 디바이스 인증서 프로파일(X.homesec-2)" 표준으로 홈네트워크 디바이스들을 인가받은 사용자만이 이용할 수 있도록 하기 위한 표준이다[8]. 홈네트워크 원천기술을 개발하고 있는 ITU-T 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 불편



〔그림 8〕 안전한 홈게이트웨이를 위한 디바이스 인증 모델

함이 있다. 따라서 X.homesec-2에서는 이런 불편한 점을 해결하기 위하여 ITU-T 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, 케이블 서비스에도 적용 가능하며, 홈디바이스 고유식별자(CPU Serial Number, LAN Card MAC 등)를 고려키로 하였다. 또한, 보안알고리즘의 인증서 프로파일을 위해서 국제적으로 입증된 알고리즘이

〔표 2〕 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

나 국제적으로 활용되고 있는 알고리즘을 정의키로 하였으며, 특수한 경우에 국가별로 사용되는 특정 알고리즘에 대해서도 고려키로 하였다. 이외에도 일반적인 응용 보안프로토콜과 홈네트워크 디바이스에 의해서 발생할 수 있는 다양한 서비스들을 고려하여 개발하고 있다.

〔그림 8〕은 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 2와 같이 반드시 있어야 할 기본필드와 추가적인 정보를 담고 있는 확장필드로 구성되어 있다.

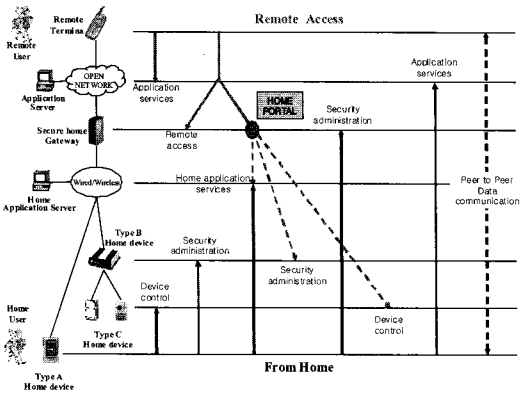
홈네트워크 환경에서 인증서를 활용하여 안전한 서비스를 제공하기 위해서는 다음의 사항들이 고려되어야 한다.

- 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

홈네트워크에서 디바이스 인증서 관리는 안전한 홈게이트웨이가 인증서의 발급, 폐기, 유효성 검증을 수행한다. 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 대리인증기관으로부터 등록코드(reference code/authorization code)를 부여 받고, 이를 이용하여 자신의 홈디바이스들에게 표 2의 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 디바이스의 경우 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 8〕의 모델에서 원격터미널과 홈게이트웨이 구간, 응용서버와 홈게이트웨이 구간, 홈디바이스와 홈게이트웨이 구간에서 사용되며, 링크계층과 응용계층에서 주로 사용될 것이다.

세 번째로 "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[9].

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 9〕와 같은 서비스 구조를 정의하였다. 홈포탈(Home Portal)은 일종의 대행 서버(Proxy Server)로 사용자가 직접적으로 서비스를 받을 수 없을 때 중간매개체 역할을 수행하는 개체로써 사용자를 인증하고 사용자가 요구하는 명령들을 모아 해당 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 9〕에서와 같이 원격사용자는 댁내서비스를 이용하기 위하여 홈포탈을 이용하여 접근할 수 있고, 홈유저들은 홈포탈 없이 직접적으로



〔그림 9〕 홈네트워크 서비스 구조

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 위한 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 3〕과 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

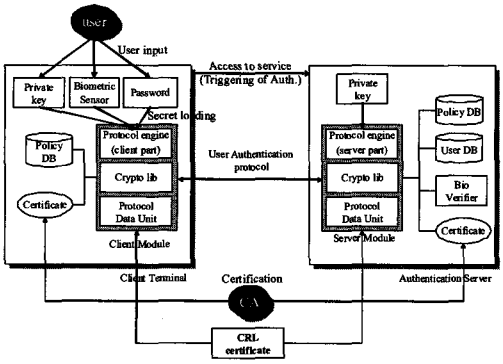
홈네트워크 사용자 인증을 위한 보안요구사항은 다음과 같다.

- 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 10〕은 홈네트워크 서비스를 위한 사용자 인증

〔표 3〕 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)	-



〔그림 10〕 사용자 인증메커니즘을 위한 보안 컴포넌트

메커니즘의 보안 컴포넌트로 클라이언트 터미널은 사용자의 인증정보를 입력할 수 있는 인터페이스가 존재하여야 하며, 서버 역할을 수행하는 홈 개체들은 각각의 사용자 인증정보와 대응할 수 있는 데이터베이스를 가지고 있어야 한다. 클라이언트와 서버의 프로토콜 모듈은 홈네트워크의 사용자와 관리자에 의해 구성된 정책에 따라 제어되어야 하며, 이는 정책 데이터베이스에 저장된다. 또한, 인증서를 이용한 사용자 인증을 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.

2.4.2 2006년 오타와 및 제네바 회의의 주요 이슈, 쟁점사항, 향후 추진방향

2006년 4월 제주 회의에서 검토되었던 이슈들을 중심으로 수정 및 보완된 기고서를 오타와 회의에 제출하였으며, 본 회의는 SG17 정기회의가 아닌 임시회의 이므로, X.homesec-3 기고서는 제출되지 않았다. 회의 주요결과는 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 키길이 안전성에 대한 내용을 추가하였다. 또한, ASN.1 코드를 표준 표기법으로 포맷을 수정하였다.

오타와 회의 결과를 바탕으로 수정된 기고서를 2006년 12월 제네바 회의에 제안하였으며 주요결과는 다음과 같다.

- X.homesec-1은 SG9의 코멘트 사항과 일본 전문가들의 코멘트 사항들을 모두 반영하여 최종 X.homesec-1 문서(TD2512)를 작성하고, 총회에서 승인되었으며, 이를 국가별 의견수렴(consent)으로 추진키로 하였다.
- X.homesec-2는 ITU-T X.500, X.501 표준들을 레퍼런스로 추가키로 하였으며, 용어 정의에서 중복적으로 정의된 "ASP, PDA, PIN" 용어는 삭제키로 하고, 각각의 용어들을 알바벳 순서로 정렬하여 정의키로 하였다. 또한, 7장의 마지막 문장을 수정키로 하고, 7.3절의 CN 형식을 수정키로 하였으며, 7.2.1절에 키 식별자 표현 방법을 수정키로 하고, 8.3절에 "on line certificate status validation protocol"에서 "status" 단어를 삭제키로 하였다.
- Xhomesec-3은 ITU-T 표준초안으로 개발중에 있는 X.pak와 X.tsm 등을 고려하여 사용 인증메커니즘에 적용할 수 있는 가능성을 검토키로 하였으며, 13장에 제안하고 있는 사용자 인증 세부프로토콜은 X.homesec-3 연구범위에서 벗어나므로 삭제키로 하였다. 만약, 홈네트워크를 위한 세부적인 인증 프로토콜 표준이 필요할 경우 신규 표준화 아이템 신설에 대해 검토키로 합의되었다.
- 한국에서 제안한 신규 표준화 아이템(authorization in the home network) 검토 결과 다음과 같은 사항들을 고려하여 차기회의에서 신규 아이템 채택 유/무를 재검토키로 하였다. 즉, 홈네트워크에서 권한부여를 위한 필요성 및 인가시나리오 사용 방법들을 포함하고, 인가 프레임워크, 세부적인 인가 메커니즘 및 프로토콜들을 포함하여 보완키로 하였다.

2.5 웹 서비스 보안 표준화 동향 및 쟁점사항

2.5.1 개요

Q.9에서 웹서비스 보안은 2006년 6월에 제정된

XML 보안 표준 2건(X.1141, X.1142)과 한국의 제안으로 추진되고 있는 모바일 웹서비스에서 메시지 보안을 위한 보안구조(X.websec-3) 표준이 개발중에 있다. 향후, OASIS에서는 XML 보안과 관련된 다양한 웹서비스 보안을 ITU-T로 제안할 예정에 있다.

X.websec-3은 모바일 웹서비스에서 메시지 보호를 위한 구조와 다양한 서비스 시나리오를 정의하고 있다. SOAP 메시지가 방화벽에 의해서 필터링이 되지 않기 때문에 메시지 필터링할 수 있는 메커니즘이 보안구조로 단일화되어야 하며, 이를 지원하기 위한 보안정책 메커니즘, 모바일 웹서비스 응용과 다른 응용간에 상호연동 가능한 메커니즘을 개발하려 하고 있다[17]. X.websec-3에서 정의하고 있는 웹서비스 보안 로드맵과 안전한 메시지 보안구조는 〔그림 11〕과 같다. 여기서 WS-Security란 SOAP Message Security를 의미한다.

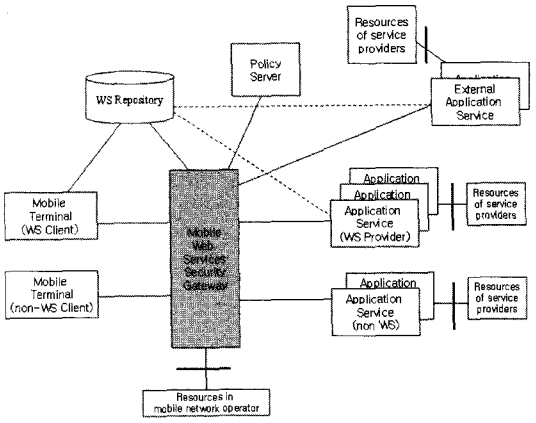
X.websec-3에서 논의되고 있는 모바일 웹서비스를 위한 보안 모델은 〔그림 12〕와 같다. 모바일 터미널은 모바일 서비스를 이용하고자 하는 사용자로써, 사용자 단말이 SOAP 프로토콜 지원 유/무에 따라 분류될 수 있고, 부가서비스를 제공자 또한 SOAP 프로토콜 유/무에 따라 분류된다. 보안정책 서버는 사용자와 서비스 제공자 간에 메시지 교환과 접근제어를 관리하기 위한 개체이며, 사용자가 모바일 환경이 아닌 외부 응용서비스 이용할 경우도 고려되고 있다. 이들에 대한 전체적인 관리와 제어 역할은 중간매개체인 보안게이트웨이에서 수행하게 된다. 현재, X.websec-3에서는 〔그림 12〕의 모델을 기반으로 보안게이트웨이의 컴포넌트 정의와 메시지의 필터링 방법, 사용자와 서비스 제공자 간에 발생할 수 있는 다양한 서비스 시나리오를 개발하고 있다.

2.5.2 2006년 오타와 및 제네바 회의의 주요 이슈, 쟁점 사항, 향후 추진방향

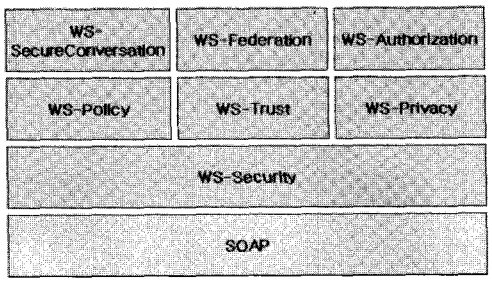
2006년 4월 제주 회의에서 검토되었던 이슈들을 중심으로 수정 및 보완된 기고서를 오타와 회의에 제출하여 검토된 결과는 다음과 같다.

- OMA의 스펙 OWSER(OMA Web Services Enabler)를 반영하고, 기술적으로 OMA 스펙과 동일하게 추진하되, X.websec-3과 OMA 스펙 간에 차이점을 설명하는 새로운 절을 만들기로 하였다. 또한, 모바일 웹서비스 보안을 위한 추가적인 일반 모델을 정의키로 합의되었다.

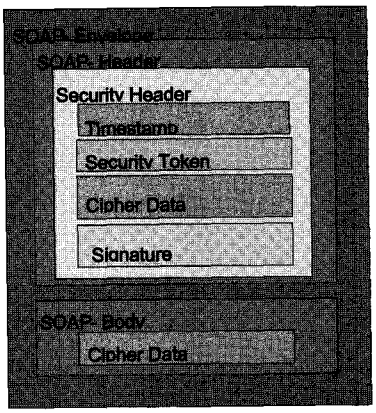
오타와 회의 결과를 바탕으로 수정된 기고서를 2006



〔그림 12〕 모바일 웹서비스를 위한 보안 모델



< 웹서비스 보안 로드맵 >



< 웹서비스 보안에 의한 안전한 메시지 구조 >

〔그림 11〕 X.websec-3의 보안 로드맵과 메시지 구조

년 12월 제네바 회의에 제안하였으며 주요결과는 다음과 같다.

- ITU-T X.805 표준의 보안요구사항을 반영하고, 보안위협들과 보안요구사항들 간의 관계를 명확히 정의키로 하였으며, 인도네시아에서 제안한 "로밍 서비스 시나리오 모델"을 X.websec-3에 정의하고 있는 서비스 시나리오 모델에 추가하여 반영키로 하였다.

2.6 안전한 응용 프로토콜 표준화 동향 및 쟁점사항

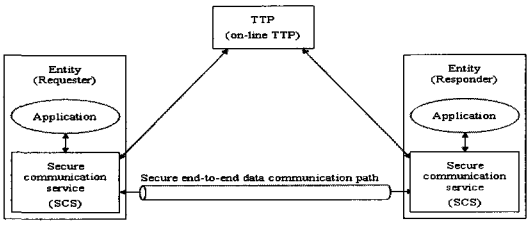
2.6.1 개요

한국 주도하에 추진되고 있는 안전한 패스워드 기반의 인증 및 키교환 프로토콜 가이드라인(X.sap-1)은 인간이 기억할 수 있는 작은 용량의 패스워드를 이용하여 안전하고 강한 인증서비스를 지원하기 위한 표준초안이다. 본 표준에서는 인증프로토콜의 요구사항, 안전한 프로토콜 선택하기 위한 선정기준과 가이드라인을 제시하고 있으며, 다양한 인증 및 키교환 프로토콜의 등급 선정 등에 대해 정의하고 있다[13]. X.sap-1에 정의하고 있는 패스워드 기반의 인증 및 키교환 프로토콜의 선정기준은 〔표 4〕와 같다.

일본 주도하에 추진되고 있는 TTP 서비스를 이용한 안전한 종단간 데이터통신 기술(X.sap-2)은 ITU-T X.842에 정의되어 있는 서비스 방법에 추가적인 방법들을 정의하고 있으며, 온라인상에서 제3의 신뢰기관(TTP: Trusted Third Party)을 이용하여 두개의 통신 주체간에 효율적인 통신을 하기 위한 방법으로 각 주체간에 사용되는 인터페이스, 상호연동절차 및 데이터전송절차 등을 정의하고 있다[14]. X.sap-2에서 기본적으로 정의하고 있는 모델은 〔그림 13〕과 같다.

2.6.2 2006년 오타와 및 제네바 회의의 주요 이슈, 쟁점사항, 향후 추진방향

2006년 4월 제주 회의에서 검토되었던 이슈들을 중심으로 수정 및 보완된 기고서를 오타와 회의에 제출하



〔그림 13〕 on-line TTP 기본 모델

〔표 4〕 패스워드 기반의 인증 및 키교환 프로토콜 선정기준 (M: MUST, S: SHOULD, O: MAY)

	High Level	Medium Level	Low Level
Perfect forward secrecy	M	M	M
Mutual authentication	M	M	M
Replay attack	M	M	M
Man-in-the-middle attack	M	M	M
Denning-Sacco attack	M	M	M
Online dictionary attack	M	M	M
A range of cryptographic algorithms support	M	M	M
Authenticity of server	M	M	M
Authenticity of client	M	M	M
Client-initiated authentication information (e.g., password) change	M	M	M
Offline dictionary attack	S	M	M
Server compromise attack	S	M	M
Server-compromised dictionary attack	S	S	M
Verifier-based SPAK	S	S	M
Simplicity	S	S	S
Minimal client configuration	S	S	S
Minimum storage and minimum computation	S	S	S
Sharing of secrets across multiple servers	O	O	S

여 검토된 결과는 다음과 같다.

- X.sap-1은 패스워드 인증 프로토콜의 고려사항, 선정기준, 비교 분석 등을 수정하였으며, ITU-T 저자 가이드라인(A.1500)을 반영하여 IETF RFC 레퍼런스 항목들을 수정키로 하였다.
- X.sap-2는 Liberty Alliance에서 연구되고 있는 결과들과의 중복성을 검토키로 하였으며, TTP 기반의 서비스 시나리오를 추가하기로 하고, 서비스 흐름도 1단계 전 상태에 대해 명확히 정의하고 부록 B에 요약을 수정하기로 합의하였다.

오타와 회의 결과를 바탕으로 수정된 기고서를 2006년 12월 제네바 회의에 제안하였으며 주요결과는 다음과 같다.

- X.sap-1은 레퍼런스에 RFC2119 표준이 중복되어 있어, 이를 삭제하고 최종 TD2511 문서를 first draft Recommendation으로 채택키로 합의하였다.
- X.sap-2는 Liberty Alliance에서 정의한 TTP 서비스 기술을 사용할 수 있는 가능성을 검토키로 하였으며, Annex A를 Appendix A로 수정하고, "ubiquitous" 용어를 좀더 적절한 용어로 대체하기로 합의되었다. 또한 이를 반영한 TD를 first draft Recommendation으로 채택키로 합의하였다.

2.7 P2P 및 RFID 보안 표준화 동향 및 쟁점사항

2.7.1 개요

P2P 보안으로는 일본 주도하에 추진되고 있는 P2P 통신을 위한 보안 요구사항(X.p2p-1)과 한국 주도하에 추진되고 있는 P2P 통신을 위한 보안구조 및 프로토콜(X.p2p-2)이 추진되고 있다. X.p2p-1는 P2P 기술을 기반으로 개발된 다양한 응용 통신기술과 서비스 시나리오 상에서 존재할 수 있는 보안 취약점들을 분석하여 정의하고 있으며, 이를 해결하기 위한 보안요구사항들을 도출하여 정의하였다[15]. 또한, X.p2p-2는 안전한 통신을 위한 프로토콜, 보안기술들을 정의하고 있으며, 효율적인 인증 및 권한부여 방법, 키 관리 및 분배방법, 그룹통신에서의 프레임워크 정의, P2P 통신에서의 개인 프라이버시 보호 방법 등을 정의하고 있다[16]. 현재, Q.9에서 논의되고 있는 P2P 모델은 Hybrid, Pure, Operable, Structured, Distributed, Computing 모델들이 논의되고 있다.

RFID 보안은 2005년 10월 제네바 회의에서 처음으로 한국 제안으로 Q.9에서 검토되었던 이슈로 다른 표준화기구들과의 중복성 문제 등으로 계속해서 보류되다가 2006년 9월 오타와 회의에서 처음으로 채택된 표준화 아이템이다. 오타와 회의에서 한국은 RFID 프라이버시 보호를 위한 가이드라인(X.rfpg)과 네트워크 기반의 RFID 서비스를 위한 프라이버시 보호 프레임워크(X.rfidsec-1) 2건을 제안하였지만, 현재 X.rfpg는 가이드라인 성격이 강해 Q.6 산하에서 개발키로 합의되었고, X.rfidsec-1만 Q.9 산하에서 개발중에 있다. X. rfidsec-1은 네트워크 기반의 RFID 서비스에서의 프라이버시 침해 분석, 프라이버시 보호를 위한 보안요구사항, 프로파일에 대한 프레임워크, 안전한 RFID 서비스를 지원하기 위한 모델 및 각 개체들의 정의, 각 개체 간에 이루어지는 서비스 시나리오들을 정의하고 있다. 그리고 X.rfidsec-1은 EPC global 및 다른 표준화기구들에서 연구하고 있는 RFID 보안 표준화 활동들을 조사하여 표준을 개발할 예정에 있다[18].

2.7.2 2006년 오타와 및 제네바 회의의 주요 이슈, 쟁점사항, 향후 추진방향

2006년 4월 제주 회의에서 검토되었던 이슈들을 중심으로 수정 및 보완된 기고서를 오타와 회의에 제출하였으며, 본 회의는 SG17 정기회의가 아닌 임시회의 이므로, X.p2p-2 기고서는 제출되지 않았다. 회의 주요결과는 다음과 같다.

- X.p2p-1은 12장에 보안기술에 대한 반영 유/무와 SETI@HOME에 정의된 분산된 컴퓨터 기반의 P2P 모델에 대한 사항들을 고려하여 수정키로 하였으며, P2P 환경에서 익명의 인증 구조 요구사항을 정의하기 위한 위협 및 취약점들을 연구하여 반영키로 하였다. 또한, X.p2p-1의 제목을 "Requirements of security for peer-to-peer communications"으로 변경키로 하였다.
- X.rfidsec-1은 RFID와 네트워크 RFID 간에 차이점을 정의하고, 네트워크 RFID를 명확히 정의키로 하였으며, Q.6와 JCA-NID 그룹과 협력하여 개발키로 하였고, 본 기고서를 X.rfidsec-1로 채택하고, main-editor로 최두호 선임(ETRI)이 임명되었다.

오타와 회의 결과를 바탕으로 수정된 기고서를 2006년 12월 제네바 회의에 제안하였으며 주요결과는 다음

과 같다.

- X.p2p-1은 유용성(usability) 요구사항에 대한 항목을 삭제하는 것에 대해 재검토키로 하였고, 12장에서 다루고 있는 세부적인 보안기술 사항은 X.p2p-2의 연구범위이므로 삭제키로 하였다. 또한, 10.1 절의 제목을 적절한 제목으로 변경키로 하였고, X.p2p-1에서 정의하고 있는 보안요구사항들에 대해 "필수", "권고", "옵션"으로 구분하여 정의하고, 서비스 모델과 요구사항들 간의 관계를 명확히 정의하기로 합의되었다.
- X.p2p-2는 이번에 제출된 기고서를 baseline 문서로 채택하고, X.p2p-1과 서로 조화되는 표준을 개발키로 합의되었다.
- X.rfidsec-1은 "RPS" 용어를 새롭게 정의하고, JCA-NID 그룹에 의해 정의된 프레임워크 모델이 있을 경우, X.rfidsec-1 모델을 JCA-NID 그룹의 모델을 참조하여 변경키로 합의되었다.
- 한국에서 제안한 신규 표준화 아이템 "네트워크 기반의 RFID 시스템에서 인증프로토콜의 보안요구사항"은 Q.9의 연구범위에 있다고 승인하였으나, 서버-클라이언트 모델에서의 인증프로토콜의 요구사항과 N-RFID 환경에서의 인증프로토콜의 요구사항과의 차이점을 명확히 정의하고, 다른 표준화 기구들과의 연구영역이 정확히 어떻게 다른지를 보완하여, 차기회의에서 신규 표준화 아이템 채택 유/무를 재검토키로 하였다.
- 한국에서 제안한 신규 표준화 아이템 "SIP 기반의 VoIP 서비스를 위한 인증 프레임워크"는 IETF, 3GPP 및 다른 표준화기구들과의 중복성 문제를 명확히 하고, 본 기고서의 연구범위에 맞는 세부적인 인증 메커니즘을 정의하여 차기회의에서 재검토키로 하였다.

V. 결 론

본 논문에서는 ITU-T SG17 WP2 산하 Q.9에서 진행하고 있는 모바일 보안, 홈네트워크 보안, 웹서비스 보안, 안전한 응용프로토콜 보안, P2P 보안, RFID 보안 분야의 표준화 동향에 대해서 살펴보았다. 한국은 2006년 12월 스위스 제네바 회의에서 다른 어느 나라 보다, 많은 참가자와 많은 기고서를 제출하여 국제표준에 국내 기술을 반영시키는 성과를 올렸으며, 보안 분야에서 국제표준을 좀더 주도하기 위한 유리한 입지를 확보하였다. 특히, 홈네트워크를 위한 보안기술 프레임워크(X.homesec-1)는 총회에서 승인되어, 2007년 1월 중순경에 국가별 의견수렴(consent)을 추진할 예정이며, 크게 문제가 없으면 2007년 2월말 경에 ITU-T 내에 최초로 홈네트워크 보안 표준(X.1111)으로 채택될 예정이다. 현재, Q.9에 참여하고 있는 국내 대표단은 이번 연구회기가 2008년 4월 회의를 끝으로 마감됨으로 각각의 표준초안 에디터들과 협력하여 한국 주도로 개발되고 있는 표준초안들이 모두 마무리될 수 있도록 대응할 예정이다. Q.9 산하에서 개발되고 있는 모바일 보안과 홈네트워크 보안, 그리고 웹서비스 보안 등은 매우 중요한 표준이 될 것으로 예측되는바 향후 이들 표준들을 국내 표준으로 도입시기와 국내 환경에 적합한 지에 대한 검토가 추가적으로 필요할 것을 생각된다. 보안은 이제 선택사항이 아니며, 시스템 설계 초기부터 개입되어야 할 핵심 기능이므로, 이들 분야의 표준화가 조속히 완성되어야 할 것으로 생각된다.

참고문헌

[1] ITU-T Recommendation X.1121, "X.1121: Framework of security technologies for mobile end-to-end data communication", ITU-T SG17, March 2004.

[2] ITU-T Recommendation X.1122, "X.1122: Guideline for implementing secure mobile systems based on PKI", ITU-T SG17, March 2004.

[3] ITU-T Recommendation J.190 "Architecture of MediaHomeNet that supports cable based services" defines a reference model of home network based on cable network and describes security requirements for the reference model.

[4] ITU-T Recommendation J.192 "Residential Gateway to support the delivery of cable data services" describes home gateway security.

[5] ITU-T Recommendation X.1141, "X.1141: Security Assertion Markup Language(SAML 2.0)", ITU-T SG17, June 2006.

[6] ITU-T Recommendation X.1142, "X.1142: eXtensible Access Control Markup Language (XACML 2.0)", ITU-T SG17, June 2006.

[7] Heung-Youl Youm, Heung-Ryong Oh, "ITU-T Candidate Recommendation X.homesec-1-Framework of security technologies for home network", ITU-T SG17, TD2512Rev.1, December 2006.

[8] Jong-Hyun Baek, Dong-Young Yoo, Heung-Youl Youm, "X.homesec-2 : Device certificate profile for the home network", ITU-T SG17, TD2514, December 2006.

[9] 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, COM17-C77-E, December 2006.

[10] Jianyoung Chen, Feng Zhang, "First draft-General security service (policy) for secure mobile end to end data communication, X.msec-3", ITU-T SG17, TD2515, December 2006.

[11] Zheng Zhibin, Wei Jiwei, "Proposed updated draft text of X.msec-4 from Editors", ITU-T SG17, TD2446Rev.1, December 2006.

[12] Liu Shuling, Wei Jiwei, Zheng Zhibin, "Proposed updated draft text of X.crs: Correlative Reacting System in mobile data communication", ITU-T SG17, TD2442Rev.1, December 2006.

[13] Heung-Youl Youm, "ITU-T First Draft Reommendation on X.sap-1: Guideline on secure password-based authentication protocol with key exchange", ITU-T SG17, TD2507, December 2006.

[14] Tadashi KAJI, "The first draft Recommendation x.sap-2", ITU-T SG17, TD2511, December 2006.

[15] Yutaka Miyake, "First draft Recommendation X.p2p-1", ITU-T SG17, TD2520, December 2006.

[16] Jae-Hoon Nah, "Proposed first draft of X.p2p-2: Security architecture and protocols for peer-to-peer network", ITU-T SG17, COM17-C72-E, December 2006.

[17] Jae-Seung Lee, Ki-Yoong Moon, Kyo-IL Chung, "First Draft Recommendation on X.websec-3, Security Architecture for Message Security in Mobile Web Services", ITU-T SG17, TD2513, December 2006.

[18] Doo-Ho Choi, Ho-Won Kim, Kyo-IL Chung, Heung-Youl Youm, "Updated draft text on a new study item X.rfidsec-1: Privacy protection framework for networked RFID services", ITU-T SG17, COM17-C96-E, December 2006.

[19] 오흥룡, 염흥열, "ITU-T SG17 정보보호 표준화 동향과 Mobile Security 표준 분석", 한국정보보호진흥원, 정보보호기술 표준화 동향지, 2004.12.

[20] 염흥열, "ITU-T SG17 WP2 Q.9(안전한 통신 서비스) 표준화 동향 및 향후 전망", 한국정보보호진흥원, 정보보호기술 표준화 동향지, 2005.12.

[21] 오흥룡, 염흥열, "ITU-T SG17 WP2 Q.9(안전한 통신 서비스) 표준화 동향 및 향후 전망 - 상반기", 한국정보보호진흥원, 정보보호기술 표준화 동향지, 2006.6.

[22] 오흥룡, 염흥열, "ITU-T SG17 WP2 Q.9(안전한 통신 서비스) 표준화 동향 및 향후 전망 - 하반기", 한국정보보호진흥원, 정보보호기술 표준화 동향지, 2006.12.

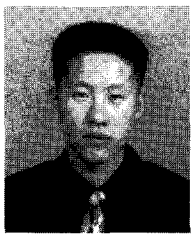
[23] 진병문, 오흥룡, 염흥열, 강신각, "2005년 ITU-T SG17 연구동향", TTA, ITU-T 연구활동 보고서, 2005.12.

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

[25] 오흥룡, "Secure Communication Services(Q.9) 표준화 동향", 제7회 정보보호기술 표준 워크샵 (ISSW2006), KISA, 2006.11.

[26] 오흥룡, 염흥열, "ITU-T SG17 홈네트워크 보안 표준화 동향 및 향후전망", 한국정보보호학회 학회지 제16권 제6호 pp7~16, 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, 정보보호 표준

염 흥 열 (Heung-Youl Youm)
종신회원

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, (현)상임부회장
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