情 報 保 護 學 會 誌
第 16 卷 第 1 號, 2006. 2

안전한 통신 서비스 표준화 동향 및 향후 전망

염 흥 열

요 약

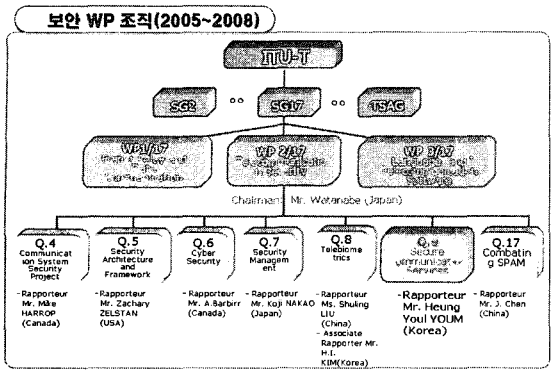
국제표준화기구인 ITU-T의 SG17 WP2는 정보통신 보안에 관한 표준화를 다루는 연구그룹이며, 7개의 연구과제(Question)를 두고 통신망을 위한 정보보호 표준화 작업을 진행하고 있다. 이 연구과제들 중 연구과제 9에서는 안전한 통신 서비스라는 이름으로 홈네트워크 보안 표준, 모바일 보안 표준, 웹 서비스 보안 기술, 그리고 안전한 응용 프로토콜 등에 대한 표준을 개발 중에 있다. 현재 연구과제 9가 제정한 표준은 2004년 3월 한국과 일본이 공동으로 제안한 X.1121, X.1122 표준이 존재하며, 2005년도 10월 제네바회의를 통하여 홈네트워크 보안 분야의 3개의 표준과제, 모바일 보안 관련 3개의 표준과제, 안전한 응용 프로토콜 관련 4개의 표준과제, 그리고 웹서비스 보안 관련 2개의 표준과제들이 개발되고 있다. 2005년 3월 모스코바 회의와 2005년 7월 중국 센젠회의에서 OASIS(Organization for the Advancement of Structured Information Standards.)는 각각 SAML(Security Assertion Markup Language) 표준과 XACML(Extensible Access Control Markup Language) 표준을 ITU-T 표준으로 이전할 것을 제안하였고, 이번 회의를 통해 이를 위하여 해결해야 할 여러 문제들이 논의되고 해결방안이 도출되었으며, 이를 위한 향후 추진 일정을 확정하였다. SAML과 XACML 표준은 홈네트워크 및 모바일 보안, 그리고 안전한 프로토콜 표준시에 유용하게 활용될 수 있을 것으로 기대된다. 본 논문에서는 연구과제 9에서 수행되고 있는 지난 2005년도 제네바 회의에서 합의된 주요 표준화 동향을 살펴보고, 현재 논의되고 있는 주요 쟁점사항을 살펴보며, 쟁점사항과 토론 결과, 그리고 향후 추진방향을 제시한다.

Ⅰ. 서 론

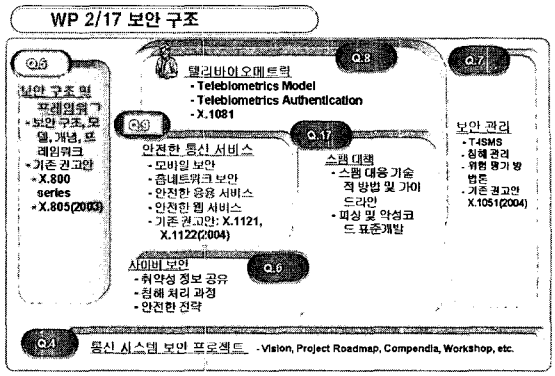
고속 서비스가 가능한 무선 단말기의 출현과 더불어 통신망과 홈 네트워크를 위한 다양한 응용 서비스가 나타날 것으로 예측되며, 이러한 응용 서비스들이 안전하고 신뢰성 있게 제공되기 위해서는 모바일 환경에서의 보안, 홈네트워크 환경에서의 보안, 안전한 응용 프로토콜, 그리고 안전한 웹 서비스를 위한 보안 기술과 표준의 개발이 요구되고 있다. ITU-T SG17에서는 통신 보안(Telecommunication Security)에 관한 WP2 산하에 보안 구조 및 프레임워크, 사이버 보안, 통신 시스템 보안, 안전한 통신 서비스, 보안 관리, 텔리바이오메트릭 등의 NGN(Next Generation Network) 보안, 모바일 보안 등의 연구과제(Question)가 존재했으나, "기술적 수단에 의한 SPAM 대응"이라는 연구과제가 지난 2005년 3월 모스코바 회의에서 제안되어 2005년 10월 제네바 회의에서 신설하기로 합의하여 전체 7개의 보안 관련 연구과제가 현재 존재하고 있다. ITU-T SG17은 '보안, 언어, 소프트웨어' 분야의 표준화 연구를 추진하고 있으며, 특히 보안 분야는 ITU-T LSG (Lead Study Group)으로 활동하고 있다. 한국은 '모바일보안' 관련 2건의 국제표준(2004.3)을 제정한바 있으며, WP2 의장단으로 연구과제 8 부라포처(김학일, 인하대), 연구과제 9 라포처(염흥열, 순천향대)로 활동하고 있다. 이의 역할과 구성을 자세히 나타내면 그림 1과 표 1과 같다.[39-41] 각 연구과제의 역할은 그림 2와 같다.[41] ITU-T SG17은 이번 연구회기(2005년-2008년)동안 최초의 회의가 2005년 3월 러시아 모스코바에서 개최되었고, 2005년 7월 SG17 WP2 산하의 보안 관련 연구과제들이 중국 센젠에서 인터림 회의가 개최되었으며, 2005년도 마지막 회의가 2005년 10월 제네바에서 개최되었다.

본 고에서는 ITU-T SG17 WP2 연구과제 9에서

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 결과로 수행되었음
* 순천향대학교 공과대학 정보보호학과(hyyoum@sch.ac.kr)



〔그림 1〕 ITU-T SG17 연구과제 구성



〔그림 2〕 ITU-T SG17 WP2 연구과제 개요

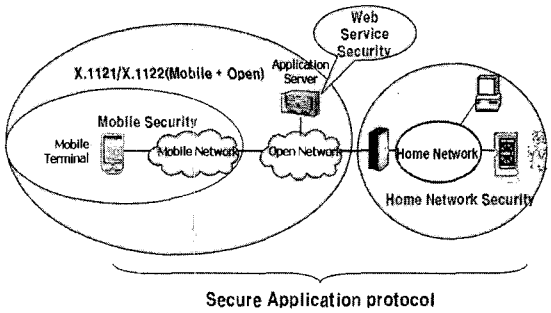
2005년 10월에 수행된 최근 표준화 동향, 현재의 주요 표준화 항목, 각 표준화 과제당 주요 쟁점사항, 그리고 향후 표준화 추진 계획을 중심으로 살펴본다.[14,41]

II. ITU-T SG17 연구과제 9의 표준화 현황 및 전망

모바일 보안을 위한 표준으로는 한국과 일본이 공동으로 작성한 X.1121(X.msec-1)과 X.1122(X.msec-2) 두 종류의 표준이 완성되었고,[1,2] 그림 3과 표 2와 같이 2005년 3월 이후 모바일 보안 분야에서 3개의 표준과제, 홈네트워크 보안 분야에서 3개의 표준과제, 안전한 응용 프로토콜 분야에서 4개의 표준과제, 그리고 웹 서비스 보안 분야에서 2개의 표준과제가 개발되고 있다.

2.1 유지보수되고 있는 기존 표준안(X.1121, X.1122)

ITU-T X.1121과 X.1122는 한국과 일본이 공동으로 제안하여 지난 연구회기 동안 표준화된 표준이다.[1,2,35] X.1121 에서는 모바일 종단간 데이터통신



〔그림 3〕 연구과제 9의 주요 표준화 분야

을 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 메커니즘을 도출하고, 이 보안 메커니즘이 통신 모델에서 어느 보안 요소에 실현되어야 하는지에 대하여 설명하고 있다. X.1122는 PKI(Public-key Infrastructure) 기반의 안전한 모바일 시스템 실현을 위한 가이드라인 표준이다. X.1122에서는 게이트

〔표 1〕 ITU-T SG17 WP2 연구과제 개요

연구과제	연구과제 제목	기존 표준안
4/17	통신 시스템 보안 프로젝트(Communications systems security project)	
5/17	보안 구조 및 프레임워크(Security architecture and framework)	X.800, X.802, X.803, X.805, X.810, X.811, X.812, X.813, X.814, X.815, X.816, X.830, X.831, X.832, X.833, X.834, X.835, X.841, X.842, X.843
6/17	사이버 보안(Cyber security)	E.409
7/17	보안 관리(Security management)	X.1051
8/17	텔리바이오메트릭(Telebiometrics)	X.1081
9/17	안전한 통신 서비스(Secure communication services)	X.1121, X.1122
17/17	기술적 수단에 의한 SPAM 대응(Countering SPAM by technical means)	

〔표 2〕 ITU-T SG17 Q.9에서 개발 중인 표준안 내용

분야	약어	제목	에디터
홈네트워크 보안	X.homesec-1	Framework for security technologies for home network	H.Y.Youm,H.R. Oh
	X.homesec-2	Certificate profile for the device in the home network	D.Y. Yoo
	X.homesec-3	User authentication mechanisms for home network service	H.K. Lee
모바일 보안	X.msec-3	General security value added service (policy) for mobile data communication	F. Zhang,J. Chen
	X.msec-4	Authentication architecture in mobile end-to-end data communication	Z. Zheng,J.W. Wei
	X.crs	Correlative reacting system in mobile network	S. Liu,J.W. Wei
안전한 응용 보안 프로토콜	X.p2p-1	Anonymous authentication architecture in community communication	Y. Miyake
	X.p2p-2	Security architecture and protocols for peer to peer network	J.H. Nah
	X.sap-1	Guideline on strong password authentication protocols	H.Y. Youm
	X.sap-2	Secure communication using TTP service	T. Kaji
웹 서비스 보안	X.websec-1	Security Assertion Markup Language	A. Barbir
	X.websec-2	eXtensible Access Control Markup Language	A. Barbir

웨이 기반 PKI 모델과 일반 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 확인하였다. 세션 레벨 보안 기능을 위하여 사용자 인증 및 응용 서비스 인증 절차, 암호와 무결성 서비스를 제공하기 위한 절차가 기술되었고, 응용 레벨 보안을 위하여 서명과 암호 기능을 제공하기 위한 구체적인 절차가 기술되었다.

2.2 2005년 10월 회의 기고서 현황

2005년 10월 제네바 SG17 회의는 지난 모스크바 회의(2005.3.30~4.8) 이후, 진척된 표준화 기술들에 대해 토의하는 회의로써, 한국은 표 3과 같이 연구과제 9에 14건의 표준화 기고서를 제출하여 새로운 표준과제로 3건에 대해 새로운 신규 에디터로 임명받았으며, 4건의 기술을 표준에 반영시켰으며, 8건의 기고서는 금번 제출된 기고서를 기반으로 차기회의에서 보다 상세히 논의키로 합의하였다.

2.3 모바일 보안 분야 표준화 동향 및 쟁점사항

가. 개요

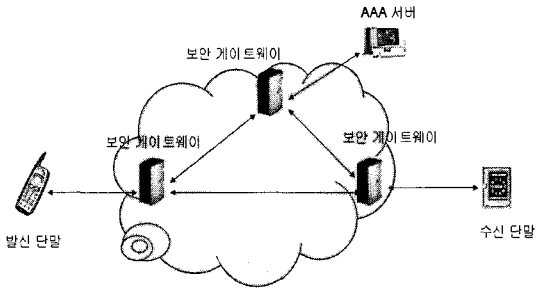
모바일 환경에서 모바일을 통하여 제공받는 서비스 이용 요금에 대한 사용자 저항이 인터넷의 경우보다 낮아지고 있는 경향이 있다. 따라서, 모바일 환경에서 각 사용자에게 특성화되고 유료화된 보안 서비스를 제공함으로써 모바일 네트워크 제공자(mobile network provider)에게 새로운 부가가치를 제공할 수 있다.[5-9,18-23,35-36,38]

모바일 환경에서 보안 정책(서비스) 표준(일명, X.msec-3로 통칭됨)은 보안 서비스를 새로운 부가가치 서비스를 개발하기 위한 일반적인 보안 모델과 관련 보안 절차, 보안 정책, 보안 정책관련 보안 요소 집합, 그리고 이를 위한 정보 요소를 정의하고 있다.[5] 모바일 보안 정책에 대한 표준 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. 모바일 보안 정책을 위한 구성요소는 호를 요청하는 발신 단말, 단말과 보안 알고리즘과 보안 수준을 협상하는 보안 게이트웨이, 호를 수신하는 수신 단말, 그리고 보안 서비스 사용 요금 정보를 수집하는 AAA(Authentication, Authorization, Accounting) 서버 등이다.

기본적으로 X.msec-3는 이동망에서 다양한 등급화된 보안 서비스를 제공하기 위한 기본 프레임워크를 제공함에 그 목적을 두고 있다. X.msec-3는 그림 4와 같이 발신 단말(caller), 보안 게이트웨이(security gateway), 수신 단말(callee) 사이에 안전한 모바일 통신을 관리하기 위한 보안정책 프레임워크를 제시하고 있다. 종단간 이동 통신망을 위한 보안 서비스는 주로 이동 통신망에 부착되어 있는 모바일 단말(mobile

〔표 3〕 한국 기고서 14건 제안 및 결과

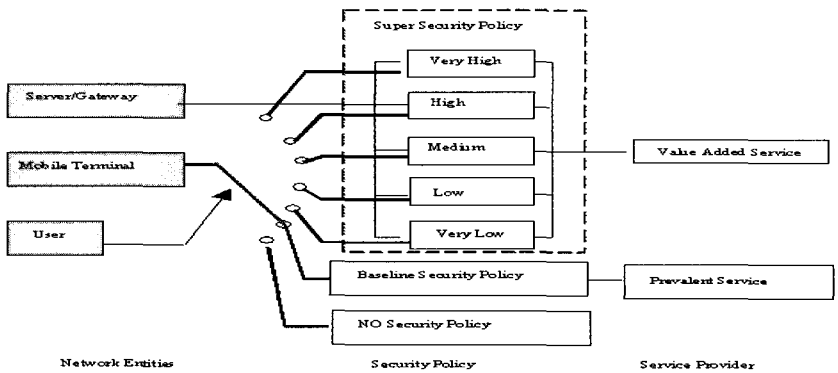
	기고서 명	문서번호	결과
1	Proposal about classification of authentication and key establishment model (키성립 모델과 인증 분류법에 대한 제안)	D77/Q.9	반영 (X.msec-4에 키성립 모델, TTP 모델 사용 유/무에 대해 반영됨)
2	Proposal for studying P2P network security (P2P 네트워크 보안 연구를 위한 제안)	D78/Q.9	반영 (새로운 연구아이템(X.p2p-2)으로 채택되었으며, main-editor로 나재훈 팀장이 임명됨)
3	Contribution on the guideline for the protection of personal information and privacy on web (웹에서의 개인정보 및 프라이버시 보호를 위한 가이드라인)	D84/Q.9	채택 (본 기고서를 기반으로 차기회의에서 상세히 논의키로 함)
4	Proposal on the guideline for the architecture supporting single sign-on in mobile web environment (모바일 웹 환경에서 싱글사이온 지원 구조를 위한 가이드라인 제안)	D89/Q.9	채택 (본 기고서를 기반으로 차기회의에서 상세히 논의키로 함)
5	Access control methods for UDDI in web services using XACML (XACML을 이용한 웹서비스에서 UDDI를 위한 접근제어 방법)	D90/Q.9	채택 (본 기고서를 기반으로 차기회의에서 상세히 논의키로 함)
6	Updated framework of security technologies for home network (업데이트된 홈네트워크를 위한 보안기술 프레임워크)	D91/Q.9	반영 (first draft Recommendation 문서로 확정됨)
7	Guideline on strong password authentication protocols (강한 패스워드 인증프로토콜 가이드라인)	D92/Q.9	반영 (새로운 연구아이템(X.sap-1)으로 채택되었으며, main-editor로 염흥열 교수가 임명됨
8	Device certification profile for the home network (홈네트워크를 위한 디바이스 인증서 프로파일)	D93/Q.9	반영 (X.homesec-2에 인증서 발행 절차, 사용범위 등을 정의함)
9	Proposal on user authentication mechanisms for home network service (홈네트워크 서비스를 위한 사용자 인증메커니즘 제안)	D95/Q.9	반영 (새로운 연구아이템(X.homesec-3)으로 채택되었으며, main-editor로 이형규 선임이 임명됨)
10	Security roadmap for the future mobile environment (미래 모바일 환경을 위한 보안 로드맵)	D97/Q.9	채택 (본 기고서를 기반으로 차기회의에서 상세히 논의키로 함)
11	Proposal of security considerations for ubiquitous networking environment based on web services (웹서비스 기반 유비쿼터스 네트워크 환경을 위한 보안 고려사항 제안)	D98/Q.9	채택 (본 기고서를 기반으로 차기회의에서 상세히 논의키로 함)
12	Proposal of guideline on security architecture for message security in mobile web services (모바일 웹서비스에서의 메시지 보안을 위한 보안구조 가이드라인 제안)	D99/Q.9	채택 (본 기고서를 기반으로 차기회의에서 상세히 논의키로 함)
13	Proposal for the study on a security framework for mobile RFID applications as a new work item on mobile security (모바일보안의 새로운 연구아이템으로 모바일 RFID 응용을 위한 보안 프레임워크 연구를 위한 제안)	D116/Q.9	채택 (본 기고서를 기반으로 차기회의에서 상세히 논의키로 함)
14	Considerations for the guideline on the protection of personal information and privacy for RFID (RFID를 위한 개인정보와 프라이버시 보호 가이드라인을 위한 고려사항)	D117/Q.9	채택 (본 기고서를 기반으로 차기회의에서 상세히 논의키로 함)



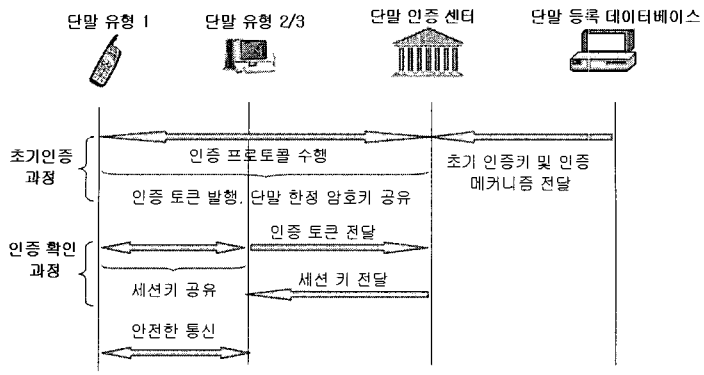
〔그림 4〕 모바일 보안 정책 모델

terminal)과 응용 서비스 제공자(application service provider)에 의하여 제공된다. 한편, 모바일 단말이 갖는 낮은 계산능력과 낮은 메모리 능력, 그리고 이동 통신망이 제공하는 낮은 대역폭 등의 특성은 이동 통신 환경에서 유선망과 같이 하나의 보안 등급을 갖는 일관적인 보안 서비스의 제공을 매우 어렵게 한다. 따라서, 다양한 이동 통신 환경에 따른 다양한 보안 서비스가 요구되게 되었으며, 결과적으로 이들 다양한 등급의 보안 서비스를 제공하기 위한 보안 정책의 개발이 필요하게 되었다. 보안 정책은 보안 서비스를 제공하기 위한 기준의 집합으로 정의되며, 보안 정책은 이동 통신망의 각 네트워크 개체(모바일 단말, 응용 서비스 제공자, 보안 게이트웨이) 내에 존재하여 관련 보안 서비스에 대한 융통성을 제공하고 있다. 이동 환경에서 보호해야 할 자산으로 크게 저장 및 전송되는 데이터를 나타내는 정보 자산, 응용 프로그램에 의하여 제공되는 서비스 자산, 그리고 물리적 하드웨어 개체인 시스템 자산 등으로 구분하였다. 종단간 이동 통신을 위한 보안 정책 프레임워크는 그림 5와 같다. 보안 정책 프레임워크는 크게 3 부분으로 구성된다. 첫 번째 부분은 보안 정책이 적용되는 개체가 무엇이냐에 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" 요소다. 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, 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 다른 모바일 단말과 응용 서비스 제공자간에 정책 협상 단계에 내용을 포함하고 있다.

모바일 환경에서 인터넷 서비스 제공과 각종 금융 거래를 위한 응용이 다양하게 증가하고 있다. 모바일 환경에서 응용을 위하여 모바일 단말과 응용서비스 서버 간에 인증은 매우 중요하다. 특히 응용 서버스 제

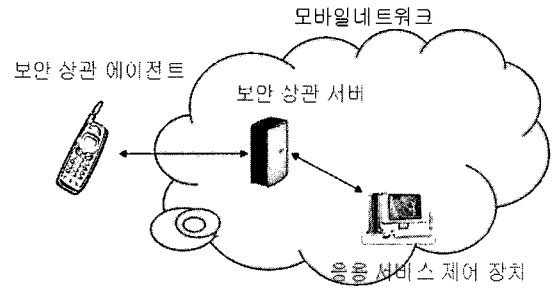


〔그림 5〕 보안정책 프레임워크



〔그림 6〕 인증과정 및 인증 확인 과정

공자의 유형과 형태에 무관하게, 일반적인 인증 모델을 통하여 인증 서비스를 제공하는 것은 매 응용 서비스 제공자마다 인증 서비스를 개발하야 하는 부담을 덜고 통일화된 인터페이스를 통하여 인증 서비스를 네트워크 제공자가 제공할 수 있다는 측면에서 매우 필요하다.[6,7,8] 모바일 환경을 위한 인증 구조(일명, X.msec-4로 통칭됨)의 경우, 모바일 단말을 세 가지 유형으로 구분하였다. 단말 유형 1은 다른 모바일 서버로부터 서비스를 제공받는 일반적인 모바일 단말이고, 단말 유형 2는 서비스 제공자 역할과 서비스 사용자 역할을 동시에 수행하는 단말이며, 단말 유형 3은 네트워크 운영자 네트워크 내에 존재하는 응용 서버이다. 인증을 위하여 정의된 개체는 3가지 개체로 구성된다. 하나는 단말이고, 다른 하나는 단말 인증 센터, 그리고 단말 등록 데이터베이스 등이다. 개체 인증 센터는 제삼의 신뢰기관이며, 단말 등록 데이터베이스는 모바일 가입자 정보(단말의 초기 키, 단말을 인증하기 위한 인증 메커니즘의 유형 등의 정보 보관)를 보관한다. 인증을 위한 과정은 그림 6과 같이 초기 인증과정(Initial authentication procedure)과 인증 확인 과정(authentication confirmation procedure)으로 구성된다.



〔그림 7〕 모바일 환경에서 침해 대응을 위한 구성요소

초기 인증 과정에서는 사용자와 인증 센터 간에 특정 인증 프로토콜을 수행하고 이 과정의 부산물로 단말 한정 키를 단말과 개체 인증센터가 공유하며, 더불어 단말에게 인증 토큰을 전달한다. 사용자 인증 확인 과정에서는 초기 인증에서 공유한 단말 한정 키를 이용하여 두 사용자간에 안전한 통신을 위한 세션키를 생성하는 과정으로 구성되어 있다.

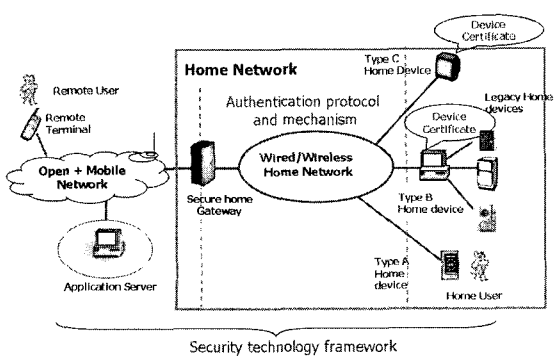
최근에 모바일 단말을 대상으로 하는 웜과 바이러스가 보고되고 있다. 모바일 환경에서 상관 침해 대응 시스템은 이동환경에서 단말과 네트워크간의 협력을 통하여 모바일 단말의 보안 상태를 파악하여 잠재적인 공격을 제어하는데 목적을 두고 있다.[9,21] 상관 침해 대응시스템(일명 X.crs 로 통칭됨)을 위한 구성요소는 그림 7과 같이 단말에서 보안 관련 정보를 수집하는 보안 상관 에이전트, 단말로부터 보안 관련 정보를 수집하여 단말의 보안 등급을 결정하는 보안 상관 서버, 그리고 단말의 보안 등급을 저장하고 있는 응용 서비스 제어 장치 으로 구성된다. 모바일 단말에 보안 상관 에이전트를 두고, 보안 단말 에이전트는 단말의 보안 관련 정보(운영체제의 버전, 안티 바이러스 소프트웨어의 버전, 단말에 존재하는 응용 서비스 목록)를 수집하여 모바일 네트워크에 있는 보안 상관 서버에 전송하며, 보안 상관 서버는 수신된 정보를 근거로 이 단말에 대한 보안 등급을 판단하여 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 감시 제어할 수 있게 판단하게 하고, 이를 근거로 바이러스 또는 웜에 오염된 단말의 행위가 네트

워크에 바로 영향을 미치지 않게 할 수 있다. 이 표준은 이러한 시스템을 개발하기 위한 보안 모델을 정의하고, 여기서 필요한 정보 요소의 구조와 의미를 정의하며, 각 구성 요소의 기능과 역할을 개발한다.

나. 쟁점사항 및 결정사항

중국에서 제안한 모바일 보안정책(X.msec-3) 관련 D110, WD4 기고서는 3GPP에서 검토된 의견을 반영하여 수정되었으며, 차기 2006년도 4월 제주도 미팅에서 first draft recommendation을 만들기로 합의하였다. 중국에서 제안한 상호연동 가능한 시스템(X.crs) 관련 D118 기고서는 각 개체간에 정보교환을 위해 XML을 사용하는 방법과 암호화하는 방법, 다양한 전송 모델, 이때 사용되는 응용프로토콜들을 추가하여 차기회의에서 재검토키로 하였으며, 공동 에디터로 Mr. Jiwei Wei를 추가로 임명하였다. 중국에서 제안한 모바일 보안을 위한 인증 구조(X.msec-4) 검토결과는 다음과 같다. 첫째, 인증 및 키성립 모델(D77) 기고서는 키성립 절차와 X.msec-4의 다양한 인증 모델(TTP 모델을 사용할 때와 사용하지 않을때)을 추가하여 차기회의에서 재검토키로 하였으며, X.msec-4의 공동 에디터로 Mr. Jiwei Wei를 임명하였다. 인증구조(D113, 114) 기고서는 로밍과 관련된 이슈들, 인증메커니즘에서 필요한 보안요구사항들, X.msec-4에서의 중재모델(mediation)과 커버러스 모델(Kerberos) 등을 고려하여 차기회의 재검토키로 하였다.

또한, 이외에도 한국에서 제안한 "웹서비스 기반의 유비쿼터스 네트워크 환경을 위한 보안 고려사항(D98)"은 Q.9의 연구범위 웹서비스 보안과 유비쿼터스 환경은 다르다는 지적이 있었지만, 연구과제 9에서는 본 기고서를 기반으로 새로운 연구아이템 선정에 대해 차기회의에서 재검토키로 하였다.[33] 한국에서 제안한 "모바일 RFID(D116(WD3), 117)"는 정확한 개념 정의가 필요하고, 프레임워크 및 가이드라인에 대한 명확한 연구범위를 정의하여, 본 기고서를 기반으로 차기회의에서 연구과제 9의 새로운 연구아이템 선정에 대해 검토키로 하였다.[28] 한국에서 제안한 "모바일 환경을 위한 보안 로드맵(D97)"은 CDMA, WLAN, 3GPP 등의 다양한 네트워크 환경을 고려하여, 본 기고서를 기반으로 차기회의에서 계속적으로 논의키로 하였다.[23]



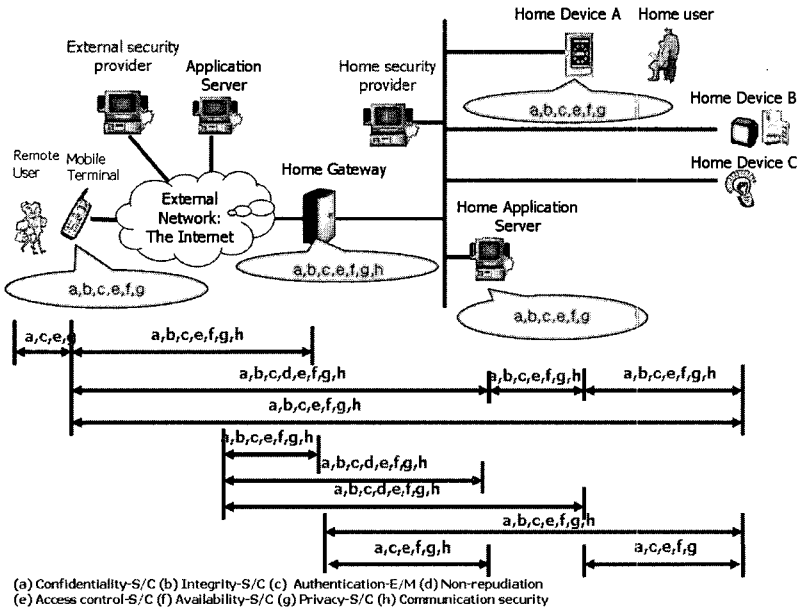
(그림 8) 홈네트워크 보안 참조모델

2.4 홈네트워크 보안 분야 표준화 동향 및 쟁점사항

가. 개요

현재 ITU-T SG17 연구과제 9에서 추진 중인 홈네트워크 보안 표준은 홈네트워크 보안 프레임워크, 홈네트워크를 위한 디바이스 인증서 프로파일 이 존재하며[10,-17], 이외에 인가 인증서 프로파일, 홈게이트웨이를 위한 운영 가이드라인 등의 향후 표준화 항목에 대한 표준화를 추진하기로 2003년 3월 모스코바 회의에서 합의한바 있다.[12,37]

홈네트워크 보안 프레임워크 표준(일명 X.homesec-1)과 디바이스 인증 표준은 한국(에디터: 염흥열, 오흥룡)에서 각각 제안되었으며, 홈네트워크 보안 프레임워크 표준은 원격 사용자와 홈 사용자 관점에서 본 보안 취약성과 보안 요구사항을 도출하고, 보안 서비스를 구현할 구체적인 보안 메커니즘을 정의하며, 이 보안 메커니즘의 적용 위치를 정의하고 있다.[10,15] 홈 네트워크 보안 프레임워크는 기본적으로 그림 8과 같은 홈 네트워크 보안 참조 모델을 정의하고 이 참조 모델을 근거로 하여 보안 위협을 정의하고, 이 보안 위협에 적합한 보안 서비스를 정의하며, 이 보안 서비스를 구현할 구체적인 보안 메커니즘을 구현하고, 어떤 보안 메커니즘의 집합이 홈 네트워크 보안 서비스를 위하여 요구되는 망 요소 또는 망 요소간의 관계에 적용될 것인지를 제시하기 위한 표준이다. 홈 디바이스가 기능 측면에서 오디오/비디오(audio/video) 디바이스, PC(personal computer) 디바이스, 텔렉스/팩스(telex/fax) 디바이스, 그리고 홈 가전(home appliance) 디바이스로 구분될 수 있다. 보안 관점에서 홈 디바이스는 크게 보안 명령을 전달하는 디바이스와 보안 명령을 받는 디바이스, 그리고 동시에 송수신하는 디바이스로 구분될 수 있다. 홈 네트워크를 위한 디바이스는 그림 8과 같이 보안 관점에서 세 가지 유형으로 정의되고 있고, 디바이스 유형 A는 유형



〔그림 9〕 홈 네트워크를 위한 보안 서비스

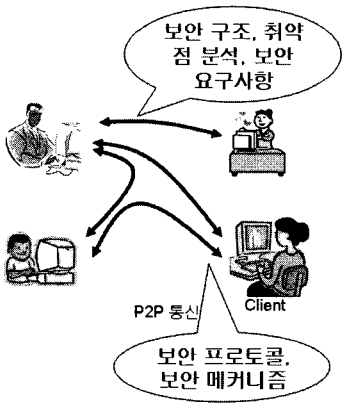
B와 유형 C 디바이스에게 제어 명령을 내리는 디바이스이고, 유형 B는 기존 통신 기능이 없는 홈네트워크 디바이스와 네트워크를 연결하는 디바이스이며, 유형 C는 오직 제어명령 만을 수신하여 서비스를 제공하는 디바이스 이다. 홈 네트워크를 위하여 정의된 보안 서비스는 그림 9에서 알 수 있듯이 기밀성, 무결성, 인증, 접근 제어 또는 인가, 부인 방지, 통신 흐름 보안, 프라이버시 보안, 가용성 등이 있으며, 원격 사용자, 원격 터미널, 홈 디바이스, 홈 사용자, 보안 홈 게이트웨이, 그리고 홈 응용 서버 등의 6개의 망요소와 모바일 터미널과 모바일 사용자간의 관계 등으로 구성되는 12개의 보안 관계 간에 이들 보안 서비스들이 적절하게 배치될 것이다. 이 보안 표준은 현재 "first darft recommendation" 상태에 있으며, 앞으로 나타날 모든 홈 네트워크 보안 표준의 기본 문서로 활용될 것이며, 고차원의 기본 기능을 설계하기 위한 가이드라인 문서로 활용될 것이다.[15]

홈 네트워크에서 활용 가능한 디바이스 인증서(일명 X.homesec-2)는 기존의 사람에게 발행되는 공개키 인증서가 아닌 홈 네트워크 디바이스에게 발행되는 인증서라고 볼 수 있다.[13,16] 이 디바이스 인증서는 홈 네트워크 디바이스(특히 홈게이트웨이)가 외부 응용 서버나 내부 홈 서버에게 인증되도록 하기 위하여 이용될 수 있으며, 인증뿐만 아니라 안전한 콘텐츠 다운로드 및 코드 다운로드용으로 활용될 인증서 이다. 디바이스 인증서 프로파일의 에디터 역시 한국(유동영, KISA) 이다. 이 인증 프로파일은 기존의 오픈케이블 표준과 호환을 이루며, 기본적으로 ITU-T X.509 v3 표준을 근거로 결정될 것이다. 정의될 프로파일은 IETF RFC 3280과 ITU-T J.192 디바이스 인증서 표준 등을 참조로 결정될 것이다.

홈네트워크를 위한 인증 프로토콜 및 메커니즘 개발 표준(일명 X.homesec-3)에서는 지난 10월 회의에서 표준화 과제로 처음 선정되었으며, ID/PW, 생체, 인증서 등 다양한 사용자 인증 수단을 지원하여 사용자에게 편리한 인증방식을 사용할 수 있도록 하는 통합 사용자 인증 메커니즘의 개발 및 표준화를 목표로 하고 있다. 이의 첫 드래프트 표준을 2006년 4분기까지 만들기로 결정하였다. 에디터로 한국의 이형규 선임이 임명되었다.[17]

나. 쟁점사항 및 결정사항

지난 중국 미팅이후, SG9의 표준 J.190과 J.192를 반영하여 제안한 "D91: Updated framework of security technologies for home network(X.homesec-1)" 기고서는 부록의 홈디바이스 분류방법을 J.192 방법과 UPnP 방법으로 분류키로 하였으며,[3,4] 본 기고서를 이번 회의를 통하여 초안이 아닌 "first draft recommendation"으로 채택키로 합의하였다.[15] 한국에서 제안한 "D93: Device cer-



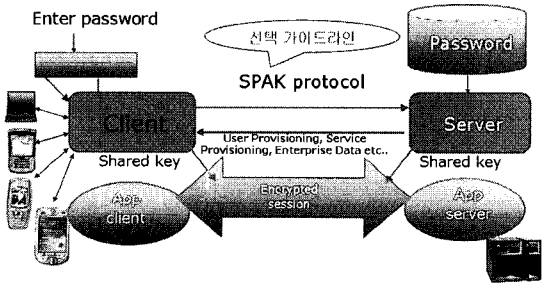
〔그림 10〕 P2P 보안 분야

tificate profile for the home network(X.home-sec-2)" 기고서는 정확한 연구범위 정의와 디바이스 인증서를 XML로 표현하는 방법, 디바이스 인증서를 관리하기 위한 프로토콜에 대해 추가적으로 연구키로 하였다. 한국에서 제안한 "D95: User authentication mechanisms for home network" 기고서는 홈네트워크 보안을 위한 향후 연구아이템 중 하나로 홈게이트웨이를 이용하여 사용자 인증 및 디바이스들을 대상으로 적용할 것이다.[17]

2.5 안전한 응용 프로토콜 표준화 동향 및 쟁점사항

가. 개요

이번 제네바 회의를 통하여 4개의 신규 표준과제가 제안되었다.[24-27] P2P 통신은 일반적으로 불법 공유 파일과 연관되지만, 파일 전송의 즉시성, 사용자 편리성 등의 많은 이점이 존재한다. P2P 서비스를 이용한 파일의 공유는 영화산업, 방송 사업, 케이블 사업의 비즈니스 모델을 위협하고 있다. P2P 응용은 그림 10과 같이 컴퓨터간의 데이터 전달을 위하여 직접적인 통신을 이용하고 있다. 또한 TTP 를 이용한 키 분배와 공유, 그리고 사용자 인증이 요구되고 있고, 패스워드를

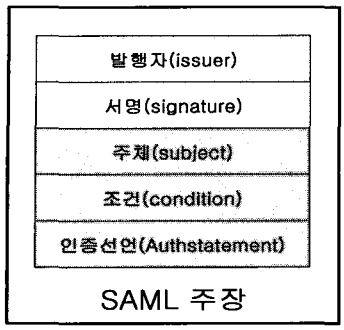


〔그림 11〕 강한 패스워드 인증 프로토콜

이용한 강한 인증 기법에 대한 연구가 수행되고 있다. 안전한 응용 프로토콜에서는 4개의 표준과제가 이번에 신설되었다. 이들 4개의 표준과제는 P2P 보안을 위한 보안 요구사항과 위협 요인, P2P 보안을 위한 보안 메커니즘, TTP(Trust Third Party)를 이용한 보안 프로토콜, 그리고 강한 패스워드 인증을 위한 가이드라인이다. 강한 패스워드 인증 프로토콜은 그림 11과 같이 패스워드를 이용하여 인증과 키 공유를 동시에 수행하는 프로토콜이다. 강한 패스워드 인증 프로토콜 가이드라인은 패스워드 인증 프로토콜을 위한 프레임워크 요구사항, 프로토콜 요구사항, 선택 가인드라인, 여러 방식 비교, 선택을 위한 가이드라인을 제시하고자 하며, 2007년 말에 표준을 완료할 예정이다. TTP를 이용한 보안 프로토콜은 보안 서비스 정의, 서비스 구조, 구조 및 인터페이스 정의, 구체적인 보안 프로토콜에 대하여 표준화하고, 표준화 완료 시점은 2007년 12월이다. P2P 보안 요구사항은 P2P 보안 취약성, 보안 요구사항, 보안 구조, 인터페이스를 정의하며, 2007년 말에 표준화를 완료할 예정이다. P2P 보안 프로토콜 및 메커니즘은 P2P 보안 프로토콜, 보안 메커니즘, P2P 보안을 위한 가이드라인, 그리고 P2P 응용 프로토콜을 정의하며, 2007년 말에 표준화를 완료할 예정이다.

나. 쟁점사항 및 결정사항

일본에서 제안한 "P2P 보안(D74)"은 P2P 환경에서의 위협요소들을 분석하고 있으며, Q.9에서는 이 기고서를 기반으로 위협 분석, 요구사항 도출, 기본 프레임워크 연구 등으로 구성되는 "P2P 보안 요구사항(X.p2p-1)" 표준을 개발키로 하고, 에디터로 Mr. Y.Miyake를 임명하였다. 한국에서 제안한 "P2P 보안 연구의 필요성 제안(D78)"은 IEEE802.11i의 활동 현황을 고려하여야 하여 세부 보안 프로토콜 설계 및 보안 메커니즘과 가이드라인을 제공하는 것을 포함하는 "P2P 보안 세부기술(X.p2p-2)" 표준을 개발키로 하고, 에디터로 나재훈 팀장(ETRI)이 임명되었다. 한국에서 제안한 "강한 패스워드 인증프로토콜을 위한 가이드라인(D92)"은 인증기반의 시도-응답(challenge-response)과 강한 패스워드 인증의 차이를 고려하여 사용자 관점에서 개발키로 하였으며, X.sap-1의 에디터로 염흥열 교수(순천향대)가 임명되었다. 일본에서 제안한 "제3의 신뢰모델(TTP)을 이용한 안전한 통신(D75)"은 구현 가능한 위치와 제안된 프로토콜의 응용영역 등을 고려하여, Q.9의 새로



〔그림 12〕 SAML 인증 주장의 고차원 구조

운 연구아이템으로 개발키로 하였으며, X.sap-2의 에디터로 Mr. T. Kaji가 임명되었다.

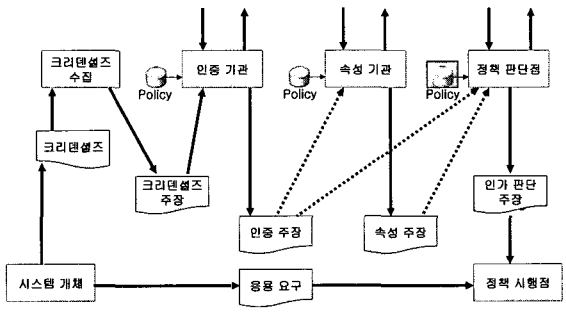
2.6 웹 서비스 보안 표준화 동향 및 쟁점사항

가. 개요

웹 서비스 보안은 OASIS 제안 2건의 표준 과제와 4건의 신규 연구아이템이 선정되었다. 먼저, OASIS 제안 2개의 표준을 살펴보자. OASIS 제안 SAML과 XACML은 웹 환경 하에서 인증과 권한 정보 등의 보안 정보를 전달하기 위한 데이터 구조를 정의하는 표준이다. 2005년 3월 버전 2.0으로 진화된 SAML은 XML 기반으로 동작한다. 보안 정보는 주체에 대한 주장(assertion)의 형태로 표현되며, 주체는 하나의 보안 영역 내에서 신원을 갖는 개체이다. 주체의 대표적인 사례는 사람 또는 컴퓨터이며, 사람은 일반적으로 특정 인터넷 DNS 영역에서 자신의 전자메일 주소에 의하여 확인된다. 주장은 SAML 기관, 인가 기관, 또는 정책 판단 점에 의하여 발행되는 하나 이상의 선언(statement)을 담고 있는 정보 패키지이다. 주장 선언은 주체에 대하여 사전에 수행된 인증 선언, 주체에 대한 속성 선언, 그리고 주체가 특정 자원에 접근할 수 있도록 허용되는지를 결정하는 인가 판단 선언으로 구분된다. 다시 말해, 인증 주장 선언의 경우 특정 주체가 특정한 시점에 특정한 인증 수단으로 SAML 인증기관에 의하여 인증되었음을 나타내며, 속성 선언은 특정 주체와 관련되는 신분 및 직위 등의 속성 정보를 포함하며, 인가 판단 정보는 특정 자원에 대한 특정 주체에 대한 접근 허용 여부를 나타내는 선언을 나타낸다. 그림 12는 SAML 인증 주장의 전형적인 구조를 나타내고 있다.

SAML은 클라이언트가 SAML 인증기관으로부터 주장을 요청하고, 이들로부터 응답을 수신하는 프로토콜을 정의하고 있다. XML 기반의 요구와 응답 메시지 형태로 구성되는 이 프로토콜은 많은 서로 다른 기반 통신 및 전송 프로토콜과 결합될 수 있으나, 현재는 HTTP 상의 SOAP로의 바인딩 만을 정의하고 있다. SAML 기관은 응답을 생성하기 위하여 여러 발신지들의 정보를 이용할 수 있다. SAML은 주로 SSO에 이용될 수 있으며, SSO는 하나의 보안 영역에서 인증 받은 주체가 다른 보안 영역에서 재인증 과정 없이 서비스를 제공받게 한다. SAML의 여러 프로파일들이 SSO를 위한 시나리오에 활용될 수 있고, 전자거래를 위한 분산 처리와 분산된 접근 제어를 가능케 하는 다른 응용에서도 활용 가능하다.

XACML(eXtensible Access Control Markup Language) 은 접근 제어 정책을 표현하기 위한 XML 표현이다. 접근 제어는 요구된 자원 접근이 허용되어야 하는지에 대한 판단 정보와 접근 결정을 시행하기 위한 정보들로 구성되어 있다. 접근 제어 정책은 접근 제어 결정을 위한 기준이 된다. XACML 핵심 규격은 인가 정책을 평가하기 위한 문법과 규칙으로 정의되고 있다. XACML은 대규모 환경에서 동작하며, 접근 제어용으로 이용되는 정보가 자동화된 주체에 의하여 관리되는 응용을 위해 효율적으로 동작하도록 설계되어 있다. XACML 정책은 그림 13과 같은 원리로 동작하며, 요구의 일시와 같은 환경 정보, 자원의 특성과 내용, 활동의 임의의 주체의 신원과 속성을 포함하여 인가 결정하기 위하여 필요한 모든 가용한 정보를 포함하고 있다. XACML은 풍부한 불리안 연산자와 데이터 조작 연산자를 규정하고 있다. XACML은 특정 접근 제어 판단에 적용할 수 있는 여러 가지 정책들을 고려하고 있고, 상충되는 판단 결과를 해결하기 위한 확장 가능한 조합 집합을 제공하고 있다. XACML은 또한 접근이 허용되고 거부될 때 취해져야 할 추가적인 행동을 규정하기 위한 광범위한 메커니즘을 제공하고 있다.



〔그림 13〕 인가 원리

나. 쟁점사항 및 결정사항

이번 회의의 주요 쟁점사항은 다음과 같다. 표준화 방법으로 두 가지 대안이 선택될 수 있는데, 하나는 단순히 OASIS에서 개발한 표준들을 참고만 하고 몇 페이지의 참조만을 담는 방법으로 ITU-T 표준을 구성하는 방법이고, 다른 하나는 기존 OASIS표준을 ITU-T 버전 표준으로 전면 개조하는 방법이다. 이번 회의를 통하여 후자의 방법을 선택하기로 결정하였고, 에디터로 캐나다의 A.Barbir를 임명하고, 다음 Q.9 회의까지 ITU-T 버전 표준을 개발하기로 합의하였다. 두 번째 문제는 ITU-T를 위한 이용 시나리오를 개발할 필요가 있는 것이었는데, 이번 회의에서 ITU-T에 적용되는 이용 시나리오를 개발하기로 합의하였다. 그 다음은 OASIS와 관련된 특허 선언과 관련된 문제점을 도출하는 것이다. 토의 과정에서 OASIS 와 ITU-T의 특허 문제는 매우 유사하여 큰 문제를 초래할 것 같지는 않지만, 지속적으로 문제점을 확인키로 하였다. 표준화 이후 누가 ITU-T 버전 표준을 유지보수 할 것인지도 중요한 문제였다. 이는 ITU-T에서 유지보수하기로 하였고, 만약 OASIS 표준이 업그레이드된다면 이에 동기를 이루어 ITU-T 표준도 업그레이드하기로 결정하였다. 만약 기존 OASIS 표준에 오류가 발견되면, ITU-T 표준에도 반영될 것이고, 이를 OASIS에 피드백하여 최종적으로 OASIS 표준에도 반영하기로 하였다. 또한 수많은 네임 스페이스에 대한 문제가 매우 중요하게 대두되었다. SAML과 XACML에는 많은 이름 공간이 존재한다. 만약 이를 모두 ITU-T 이름 공간으로 이전한다면, 관련 표준과

〔표 4〕 SAML/XACML 표준 집합

SAML	SAML 버전 2.0을 위한 인증 환경/〔SAML2Auth〕	면대면 등의 초기 인증 방법, 크리덴셜 타협을 최소화하기 위한 메커니즘(크리덴셜 갱신 주기, 클라이언트 키 생성), 크리덴셜 저장 및 보호방법(스마트카드, 패스워드 기반), 그리고 인증 방법 (패스워드, 인증서-기반 SSL) 등을 포함하는 인증 환경을 정의
	바이딩(Bindings)/〔SAML2Bind〕	SAML 요구와 응답을송수신하기 위하여 SOAP 을 사용하는 방법을 정의하고 있음
	호환성 프로그램 규격/〔SAML2Conf〕	SAML V2.0과 호환을 주장하는 구현에 대한 강제적인 특징과 선택적인 특징을 정의하고 있음
	주장과 프로토콜/〔SAML2Core〕	SAML 주장과 관련 프로토콜의 구조를 정의하고 있음
	용어(Glossary)/ 〔SAML2Gloss〕	SAML 규격과 관련 문서에서 사용되는 용어를 정의하고 있음
	메터 데이터/〔SAML2Meta〕	확인자, 바인딩 지원과 최종점, 인증서와 키 등에 관한 시스템 개체간의 합의를 정의하고 있음
	프로파일/〔SAML2Prof〕	SAML 주장을 어떻게 프레임워크나 프로토콜에 삽입하고 추출하는지에 대한 방법에 대한 규칙을 정의하며, 발신 주체에 의하여 다른 객체(파일 또는 PDU)로 어떻게 SAML 주장이 삽입되는지와 수신지에서 어떻게 처리되는지에 대해 기술하고 있음
	보안 고려사항/〔SAML2Secc〕	SAML이 어떻게 프라이버시 보호 문제를 다루는지, 위협과 보안 위험은 무엇인지, 다루어지지 않은 보안 위험은 무엇인지, 그리고 이 보안 위험을 감소시키는 대응책에 대한 대응방안을 제공하고 있음
	스키마 파일/〔SMAL2Schema〕	SAML 관련 스키마를 포함하고 있음
XACML	XACML핵심 XACML 버전 2.0 규격/〔XACML2Core〕	언어의 문법과 정책 평가를 위한 법칙을 정의함
	XACML의 SAML 2.0 프로파일 /〔XACML2SAML〕	정책 조회, 분산된 판단 요구를 위하여 SAML 스키마 요소를 확장함
	XACML의 디지털 서명 프로파일/〔XACML2DSIG〕	디지털 서명이 XACML 정책에 어떻게 적용되는지를 정의함
	XACML 프라이버시 정책 프로파일/〔XACML2Priv〕	XACML이 프라이버시 정책을 어떻게 시행하는지를 정의함
	XACML 계층적 자원 프로파일/〔XACML2Hier〕	계층적 구조를 갖는 자원에 적용되는 자원에 대하여 어떻게 접근제어 정책과 접근판단 요구가 이루어지는지를 정의함
	XACML을 위한 다중 자원 프로파일/〔XACML2Mult〕	하나 이상의자원에 대하여 동시에 어떻게 접근제어가 이루어질 수 있는지를 정의함
	XACML을 위한 계층적 역할 기반 제어(RBAC)프로파일/〔XACML2RBAC〕	XACML이 어떻게 역할 기반 접근 제어를 시행하는지를 정의함
	XML 스키마/〔XACML2Schema〕	XACML 관련 스키마 파일을 정의하고 있음

스키마를 저장하기 위한 별도의 웹 서버를 운영해야 하는 문제가 발생한다. 이 문제는 매우 중요한 관리차원의 문제를 포함하여 다음 Q.9 회의까지 지속적으로 연구하기로 결정하였다. 대부분의 국가 대표들은 현재 OASIS 개발 두 가지 핵심 표준을 ITU-T 표준으로 만드는 것에 대하여 찬성하고 있는 것으로 판단된다. 이는 이의 활용성과 이를 추진하기 위한 지난 2년간의 OASIS 측의 노력이 평가를 받고 있는 것으로 판단된다. 현재 ITU-T로 이전하고자 하는 SAML/XACML 관련 표준 프로파일은 표 4와 같다.

기존의 OASIS 표준을 기술적으로 검토할 기술 검토위원회를 두기로 합의하였다. 기술 검토위원회에는 일본 T.Kaji, 캐나다 A.Barbir, 한국 이재승 박사, 그리고 저자(위원장)로 구성되었고, 2006년 1월 제네바 인터림 회의까지 관련 기술 사항을 메일링 리스트를 통하여 기존 표준의 문제점 분석과 이전 고려사항을 검토하기로 하였다. 또한, ITU-T 표준으로 수용하기 위한 대략적인 로드맵을 합의하였다. 지금부터 2006년 인터림 회의까지 기술 검토위원회에서 기존 표준의 기술적 오류와 네임 스페이스 재배정 문제 등을 포함한 기술적인 문제를 검토하기로 하였고, 다음 제네바 인터림 회의까지 에디터인 A. Barbir가 드래프트 표준을 만들기로 하였고, 이에 대한 세부 기술사항을 검토하고, SG16 Q.25에 협력 문서를 보내 이에 대한 회신을 고려하여 최종적으로 2006년 4월에 제주에서 개최 예정인 차기 SG17 회의에서 최종 동의 과정을 획득한 후 라스트 콜 상태로 들어가기로 합의하였다.

이외에도, 한국에서 제안한 "웹에서의 개인정보와 프라이버시 보호를 위한 가이드라인(D84)"의 경우, W3C의 개인정보플랫폼(P3P: Platform for Privacy Preference)과 차이를 명확히 하여야 하며, 본 기고서의 목적 및 연구과제 7과의 중복성 등을 고려해야 하며, 사용자 관점에서 개발이 필요하며, 이 기고서를 기반으로 차기회의에서 재검토키로 했다.[30] 한국에서 제안한 "모바일 웹환경에서의 싱글사이온(Single Sign-On) 지원 구조를 위한 가이드라인(D89)"의 경우, SAML을 이용하는 좋은 시나리오 예가 될 것으로 인식되었고, 다른 표준화 기구에서 연구되고 있는 활동과의 차이를 명확히 하여야 하고, 이 기고서를 기반으로 차기회의에서 재검토키로 했다.[31] 한국에서 제안한 "XACML을 이용한 웹서비스에서의 UDDI를 위한 접근제어 방법을 위한 가이드라인(D90)"의 경우, XACML을 이용한 좋은 시나리오 예가 될 것으로 판단되고, XACML을 위한 개인 URL 할당방법과 모바일 웹보안을 위한 네임 스페이스 할당 방법을 고려하여야 하며, 본 기고서를 기반으로 차기회의에서 재검토키로 했다.[32] 한국에서 제안한 "모바일 웹환경에서의 메시지보안을 위한 보안구조 가이드라인(D99)"의 경우, 여러 가지 토의 내용을 고려하여 이 기고서를 기반으로 차기회의에서 재검토키로 했다. 또한, 코어 네트워크 서비스에 접근을 위해 Parlay-X 게이트웨이를 사용하고 있어, Parlay 작업과는 차이가 있음을 확인했다.[34]

III. 결 론

본 고에서는 ITU-T SG17 WP2 연구과제 9에서 진행하고 있는 모바일 보안, 홈네트워크 보안, 그리고 웹서비스 보안 분야의 표준화 동향에 대해서 살펴보았다. 현재 홈네트워크 보안 프레임워크는 2006년 말을 목표로, 웹서비스 보안 표준(SAML, XACML)은 2006년도 상반기를 목표로, 안전한 응용 보안 프로토콜 관련 표준과제는 표준은 2007년도 말을 목표로, 모바일 보안은 2007년 말을 목표로 표준화 작업이 진행 중이다. 모바일 보안 분야와 홈네트워크 보안 분야, 그리고 웹서비스 보안 분야는 매우 중요한 표준이 될 것으로 예측되는바 국내에서도 많은 관심과 참여가 필요한 시점이다. 보안은 이제 선택사항이 아니며, 시스템 설치 초기부터 개입되어야 할 핵심 기능이므로, 이들 분야의 표준화 주도할 필요가 있다고 생각된다.

참 고 문 헌

[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 "Residential Gateway to support the delivery of cable data services" describes home gateway security.
[5] Jianyong Chen, Feng Zhang, "Proposed modification of baseline document for X.msec-3", ITU-T SG17, CHN-Doc-010, July, 2005
[6] Zheng zhibin, Liu Shuling, "Proposal for requirement of authentication architecture in mobile end-to-end data communication", ITU-T SG17, COM 17 D 53 E, March 2004.
[7] Zheng zhibin, Liu Shuling, "Proposal of an authentication architecture in mobile end-to-end data communication", ITU-T SG17, COM 17 D 54 E, March 2004.
[8] Tadashi KAJI, Proposal on the discussion items related to COM 17-D 53 and COM 17-D 54, ITU-T SG17, CHN-Doc-003, July, 2005
[9] Shuling Liu, Jiwei Wei, Zhibin Zheng, "Correlative reacting system in mobile data communication", ITU-T SG17, CHN-Doc-009, July 2005.
[10] Heung-Youl Youm, Heung Ryong Oh, Kyo Il Chung, Framework for security technologies for home network, ITU-T SG17, CHN-Doc-006, July, 2005
[11] Tadashi KAJI, Proposal on the security framework for home network, ITU-T SG17, CHN-Doc-002, July, 2005
[12] Heung-Youl Youm, Byung 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, COM 17 D-19-E, March 2004.
[13] Dong-Young Yoo, Yoo-Jae Won, Heung Youl Youm, Proposal for studying certificate profile for the device in the home network, ITU-T SG17, COM 17 D-23-E, March 2004.
[14] H.Y.Youm, IReport of Q.9 Meeting, Geneva, 5-14 October 2005, ITU-T, TD2178Rev.1, 2005.10.
[15] H.Y. Youm, etc, Updated framework of security technologies for home network, ITU-T SG17, COM 17-D91, October, 2005
[16] D.Y. Yoo, etc, Device certificate profile for the home networks, ITU-T SG17, COM 17-D93, October, 2005
[17] H.K. Lee, etc, Proposal on user authentication mechanisms for home network service, ITU-T SG17, COM 17-D95, October, 2005
[18] J. Chen, etc, Proposed modification of section 7 for X.msec-3, ITU-T SG17, COM 17-D110, October, 2005
[19] Zheng Zhibin, etc, Draft text for X.msec-4: Authentication architecture in mobile end-to-end data communication, ITU-T SG17, COM 17-D113, October, 2005
[20] Wei Jiwei, Proposal on the discussion items related to the authentication architecture in study item X.msec-4, ITU-T SG17, COM 17-D114, October, 2005
[21] L. Shuling, etc, Correlative reacting system in mobile data communication, ITU-T SG17, COM 17-D118, October, 2005
[22] K.W. Kim, etc, Proposal about classification of authentication and key establishment model, ITU-T SG17, COM 17-D77, October, 2005
[23] K.W. Kim, etc, Security roadmap for the future mobile environment, ITU-T SG17, COM 17-D97, October, 2005
[24] Yutaka Miyake, Proposal for studying anonymous authentication architecture in community communication, ITU-T SG17, COM 17-D74, October, 2005
[25] Tadashi KAJI, Proposal on the new study item about secure communica-

tion using TTP services, ITU-T SG17, COM 17-D75, October, 2005
[26] J.H. Nah, etc, Proposal for studying P2P network security, ITU-T SG17, COM 17-D78, October, 2005
[27] H.Y. Youm, Guideline on strong password authentication protocols, ITU-T SG17, COM 17-D92, October, 2005
[28] B.H. Chung, etc, Proposal for the study on a security framework for mobile RFID applications as a new work item on mobile security, ITU-T SG17, COM 17-D116, October, 2005
[29] D.I. Seo, Considerations for the guideline on the protection of personal information and privacy for RFID, ITU-T SG17, COM 17-D117, October, 2005
[30] H. Ryu, Contribution on the guideline for the protection of personal information and privacy on web, ITU-T SG17, COM 17-D84, October, 2005
[31] D.K. Shin, etc, Proposal on the guideline for the Architecture supporting Single Sign-On in Mobile Web Environments, ITU-T SG17, COM 17-D89, October, 2005
[32] D.K. Shin, etc, Access Control Methods for UDDI in Web Services using XACML, ITU-T SG17, COM 17-D90, October, 2005
[33] J.S. Lee, etc, Proposal of Security Considerations for Ubiquitous Networking Environment based on Web Services, ITU-T SG17, COM 17-D98, October, 2005
[34] J.S. Lee, etc, Proposal of Guideline on Security Architecture for Message Security in Mobile Web Services, ITU-T SG17, COM 17-D99, October, 2005
[35] 염흥열, "ITU-T 모바일 보안 표준 분석 및 전망", TTA IT Standard Weekly, April 2004.
[36] 염흥열, 오흥룡, ITU-T SG17 정보보호 표준화 동향과 Mobile Security 표준 분석, 정보보호진흥원, 2004.12.
[37] 염흥열, ITU-T가 홈 네트워크 보안 표준을 주도할 수 있을까?, TTA IT Standard Weekly, 2005.6.
[38] 염흥열, ITU-T SG17 종단간 이동 통신 보안을 위한 보안 정책 및 홈 네트워크 보안 프레임워크에 관한 표준화 동향 , TTA IT Standard Weekly, 2005.1.
[39] 진병문, 오흥룡, 염흥열, 정교일, ITU-T SG17 모스크바 회의, TTA, TTA 저널, 99호, 2005.6.
[40] 진병문, 오흥룡, 염흥열, 정교일, ITU-T SG17 제네바 회의, TTA, TTA 저널, To be published, 2005.12.
[41] 염흥열, "Secure Communication Services," ISSW2005, 한국정보보호진흥원, 2005.11.30

〈著 者 紹 介〉

염 흥 열 (Heung Youl Youm)

1981년 2월 : 한양대학교 전자공학과 졸업(학사)
1983년 2월 : 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월 : 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~현재 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사
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
〈관심분야〉 네트워크보안, 전자상거래보안, 공개키 기반구조, 부호이론, 이동통신보안