ITU-T SG17 회의 유치 및 표준화 활동

진병문 TTA 표준화본부 본부장
김 선 TTA 표준화본부 정보통신팀 팀장
오흥룡 TTA 표준화본부 정보통신팀 과장

정보보호 및 소프트웨어 분야의 국제표준화를 담당하는 ITU-T 제17연구반(SG17) 회의가 지난 4월 19일부터 28일까지 김치동 MIC 전파연구소 소장, 김홍구 TTA 사무총장, 이홍섭 KISA 원장, 임주환 ETRI 원장을 비롯한 110여 명의 국내외 표준 전문가가 참석한 가운데 제주시 그랜드 호텔에서 성황리에 개최되었다.

한국은 이번 회의에 SG17 부의장인 진병문 TTA 표준화본부장을 대표단장으로 40여 명의 표준화 전문가가 참석하여 멀티캐스트, 보안관리, 생체인식, 안전한 통신서비스, 스팸대응 등의 분야에서 국제표준화를 주도하였으며, 총 35건의 사항을 국제표준에 반영하고, 1명의 부-라포처 및 5명의 에디터를 추가로 임명받는 성과를 올렸다.

1. 회의 개요

- ㅇ 회의명 : ITU-T SG17 국제표준화 회의
- ㅇ 회의장소 : 한국, 제주 그랜드 호텔

○ 회의기간 : 2006년 4월 19일 ~ 28일
○ ITU-T SG17 회의 한국대표단 : 총 42명(섹터멤버 포함)
○ 회의 참가자 : ITU-T 회원국 등 총 112명

2. 회의 주요 내용

가. SG17 전체(Plenary) 회의 주요내용

○ 향후, SG17에서 제정될 정보보호 표준들에 대한 표준번호를 다음과 같이 할당하기로 논의함
- 보안구조 및 프레임워크(X.805~809)
- 일반적인 보안개념(X.1000~1099)
- 안전한 응용 및 서비스(X.1100~1199)
- 사이버 보안(X.1200~1299)

○ 차기 ITU-T SG17 회의(2006. 12. 6~15, 제네바)에서 한국 주도로 개발되고 있는 RMCP-2(중계 전송방식 멀티캐스트 통신), X.homesec-1(홈네트워크를 위한 보안기술 프레임워크)을 consent(의견수렴) 단계로 추진키로 함

나. WP1(Frame Relay and Data Communication) 회의 주요내용

1) Q.1(품질서비스 관리향상을 위한 종단간 멀티캐스트 통신) 회의 결과

○ Q.1은 ISO/IEC JTC1/SC6/WG7과 공동으로 다음과 같은 이슈들을 토의하였음
- 향상된 통신 전송 프로토콜(ECTP)
  • ECTP-5의 프로토콜, 세부스펙, 구현 결과물을 업데이트 했으며, 차기 회의에서 데이터 복구 메커니즘, 추가되는 API의 필요성들에 대해 검토키로 함
- 중계 멀티캐스트 전송 프로토콜(RMCP)
  • 한국 주도하에 추진되고 있는 RMCP-2는 JTC1에서 최종 CD 단계를 통과한 후, 차기 SG17 미팅에서 consent를 추진키로 함
  • RMCP-3을 위한 향상된 트리 구성 메커니즘과 실시간 데이터 복구 메커니즘을 업데이트 함
  • RMCP-2를 위한 보안 프로토콜(RMSP)을 개발키로 하였으며, 현재 Draft Rec. X.603.1의 부속서(Amendment)로 추진키로 합의하였고 main-editor로 윤미영 선임(KISA)이 임명됨
- 모바일/무선 환경을 위한 RMCP를 새로운 표준화 아이템으로 개발키로 하였으며, 기본 개념, 기능 요구사항, 보안 요구사항들을 정의하였고 main-editor로 박주영 선임(ETRI)이 임명됨

2) Q.2(디렉토리 서비스/시스템, 공개키/속성 인증서) 회의 결과

○ X.500 Series 대부분이 ISO/IEC JTC1에서 FDIS로 통과되었으며, X.519에서는 잘못된 부분이 발견되어 차기회의에서 계속해서 검토키로 함
○ X.509의 권한 관리 기반구조(PMI)를 개정하기로 하였으며, 새로운 연구아이템으로 ID 관리를 위한 디렉토리 지원 작업을 연구하기로 함
○ E.115(Computerized Directory Assistance)의 유지보수가 완료되어, consent로 추진함

3) Q.3(개방형 시스템 상호연동)은 회의가 개최되지 않았음

4) Q.16(국제 도메인 네임) 창설에 대한 회의 결과

○ 이번 회의에서는 폴란드, 일본, 페르시아에서 각 국가별로 IDN이 구축되어 상용화되고 있는 결과물들에 대한 발표가 있었으며, 이를 기반으로 Question text 및 Action Plan을 수정함
○ 또한, 다양한 IDN 구축 현황을 분석하기 위하여, 각

국가별로 설문지를 배포하여 조사하기로 함

5) 차기 WP1 미팅

○ Q.1: 2006.6.12~16일까지, 체코 프라하에서 멀티캐스트 이슈로 JTC1/SC6/WG7과 공동으로 interim 회의를 개최키로 함

다. WP2(Telecommunication Security) 회의 주요내용

1) Q.4(통신시스템 보안 프로젝트) 회의 결과

○ 정보통신기술(ICT) 로드맵과 지난 10월에 개최된 'New Horizons for Security Standardization' 워크숍의 리포트가 on-line으로 서비스되고 있음을 공지

- 로드맵: http://www.itu.int/ITU-T/studygroups/com17/ict/index.html
- 워크숍 리포트: http://www.int.int/ITU-T/worksem/security/200510/index.html

○ WTSA-2004 Resolution 50(Cyber Security)과 관련하여, ITU-T 내의 각 보안 활동에 대해 요약정리가 필요하다는데 의견을 같이 하고 각 SG에서 개발되고 있는 표준들을 분석키로 함

○ 개발도상국(카메론 등) 및 경제 변화를 추구하는 국가들을 위해 Mr. Nlend가 계속해서 활동하기로 하였으며, 핸드북에 IMT-2000을 포함키로 함

2) Q.5(보안 구조 및 프레임워크) 회의 결과

○ 패스워드 인증 키교환 프로토콜(PAK)는 Diffie-Hellman 알고리즘 파라미터 선정 방법 등의 가이드를 추가했으며, 차기회의에서 consent로 추진키로 함

○ 한국 주도하에 개발되고 있는 X.spn(네트워크 보안을 위한 정책의 생성, 저장, 분배 및 실행을 위한 프레임워크)은 다양한 네트워크 환경에서의 각 장비들에 적용될 수 있을 것으로 검토되었으며, e-mail로 계속해서 검토하기로 함

○ 한국 주도하에 개발되고 있는 X.ngn-akm(NGN을 위한 인증 및 키관리 프레임워크)은 NGN에서의 EAP 프로토콜의 선별 방법을 제공하고 있으며, Q.15/13으로 liaison 문서를 발송하여 공동으로 표준화 작업을 추진키로 함

3) Q.6(사이버 보안) 회의 결과

○ Q.6에서는 개인식별(Identity, Identity management) 이슈를 SG17 내에서 Lead Question으로 연구키로 함

4) Q.7(보안 관리) 회의 결과

○ 한국에서 제안한 보안사고 관리(X.sim)가 새로운 연구 아이템으로 채택되어 main-editor로 김정덕 교수(중앙대)가 임명되었고 Q.7의 새로운 부-라포처로도 임명됨

○ 중국에서 제안한 '정보보안관리 플랫폼(ISMP)'은 기술적인 측면에서 ISMS 구현을 위한 제안이였으나, 내용이 불분명하고 상호 일관성도 없으며, 범위가 명확하지 않아 차기회의에서 좀더 검토하기로 함

5) Q.8(생체인식) 회의 결과

○ TMMF(Telebiometrics Multimodal Model Framework) 검토 결과

- X.physiol에 생체인식 코드와 템플릿을 추가하기로 하였으며, 분산형 정보공유 기법을 부록에 기입하기로 하였으며, 국제적인 과학단체들이나 세계건강기구들에게도 본 표준(안)에 많은 참여를 유도하기 위하여 ITU-T SG17 홈페이지에 본 결과물을 게재하기로 함

○ TSM(Telebiometrics System Mechanism) 검토 결과
- 다중생체 정보를 이용하여 다른 개체(clinet, server, TTP)들에 적용하는 메커니즘은 아직 미흡한 것으로 검토되었고 향후 이를 개선하기 위한 연구를 계속하기로 함
- X.tsm에서 생체인증 메시지 정의와 관련하여, ISO/IEC JTC1 SC37에서 추진중인 인터페이스 국제규격 BioAPI를 이용한 바이오 정보통신 프로토콜인 BIP(BioAPI Interworking Protocol)과의 중복성 문제가 제기됨
- 따라서, 이를 해결하기 위하여 미국, 영국, 프랑스, 일본, 한국 등 JTC1 SC37과 ITU-T SG17 전문가 그룹(Q.8, 10)이 공동으로 X.bip을 새롭게 개발하기로 결정함

○ TAI(Telebiometircs Authentication Infra-structure) 검토 결과
- TAI에 사용되는 생체인증서와 TSM에 사용되는 생체인증 템플릿은 같은 기능을 하지만, 다른 형식으로 되어 있으므로, 향후 이를 통일시키기로 함
- 생체인식 알고리즘 인증서는 X.509의 속성인증서를 사용하기로 함

○ TPP(Telebiometirics Protection Procedures) 검토 결과
- X.ttp-1에서 TLS 메시지 확장을 위해 RFC3456이 검토되었고 향후 에러 코드 수정방법에 대한 검토 및 샘플 데이터의 품질값과 관련된 표준들을 찾아 비교하여 정의키로 함
- X.ttp-1에서 생체 정보처리 평가기준을 위하여 SC27 N4834, ISO/IEC 19792 등 추가적인 정보를 수집하여 반영하기로 하였으며, Replay attack으로부터 보호하기 위하여, 시도-응답(challenge-response) 프로토콜을 사용하기로 함
- X.ttp-2는 X.ttp-1과 중복되지 않게 하기 위하여, scope를 명확히 하였고, 다중생체 정보들의 컴포넌트 구조와 정책, 보호되어야할 디바이스들을 정의하였음
- X.ttp-2에서는 다중생체 정보를 보호하는 방법과 Replay attack으로부터 생체정보를 보호하는 방법을 연구키로 하였으며, Least Significant Bit를 사용하여 생체정보가 일그러지는 현상을 해결하는 방법도 포함키로 함

○ 한국에서 제안한 "생체정보 기반의 암호학적 인증(X.tdigik)" 검토 결과
- 본 표준(안)은 생체정보를 이용한 다양한 통신환경에서 중요하게 활용될 것으로 검토되었으며, X.509, X.tsm에서의 인증모델, SC37의 BIP 등을 고려하여 연구키로 함
- Q.8에서는 본 표준화 아이템을 새롭게 연구하기로 합의하였고 main-editor로 이형우 교수(한신대)와 co-editor로 박해룡 선임(KISA), 김재성 팀장(KISA)을 차기 회의에서 임명키로 함

6) Q.9(모바일 보안) 회의 결과

○ 홈네트워크 보안 이슈 검토
- 홈네트워크를 위한 보안기술 프레임워크(X.homesec-1)를 최종적으로 검토했으며, 차기회의에서 consent로 추진키로 함
- 홈네트워크를 위한 디바이스 인증서 프로파일(X.homesec-2)은 국제적으로 입증된 암호 알고리즘을 부록에 추가하기로 하였으며, 자국내의 암호알고리즘 사용방법도 고려하여 추진키로 함
- 또한, 인증서의 유효성 판단을 위하여 IETF SCVP를 사용할 경우, IETF DPD/DPV의 요구사항을 참조키로 함
- 홈네트워크를 위한 사용자 인증 메커니즘(X.homesec-3)은 클라이언트 인증과 사용자 인증의 차이점에 대해 검토가 이루어졌으며, 2006년 12월에 first draft recommendation으로 추진키로 함

○ 모바일 보안 이슈 검토
- 중국에서 제안한 모바일 보안정책(X.msec-3) 관련해서는 OMA 스펙 일부를 informative reference로 추가하였고 그림 3, 5를 수정하였음. 또한, 차기

제네바 미팅에서 final draft recommendation으로 추진키로 함

- 중국에서 제안한 상호연동 가능한 시스템(X.crs)은 특별한 코멘트가 없었으며, 각 장별로 혹은 세부 절별로 부족한 점을 보완하여, 차기 제네바 미팅에서 final draft recommendation으로 추진키로 하였으며, Q.5와 공동으로 검토키로 함
- 중국에서 제안한 모바일 보안을 위한 인증 구조(X.msec-4) 검토결과
  - 모바일 통신에서 사용자 인증을 위해 USIM과 같은 토큰 사용 방법, USIM의 각 기능들에 대해 토의가 이루어짐
  - USIM에서나 사용자 단말기에서의 SS(Service Subscriber) 기능성을 위한 적절한 위치, 보안 취약점, X.msec-4를 위한 USIM의 용어들을 정의함

○ 안전한 응용서비스

- 일대일, 일대다중 통신을 위한 보안 요구사항(X.p2p-1)은 P2P 서비스 시나리오, 분산된 컴퓨터 통신, 익명자의 인증구조에 대한 요구사항 등을 정의함
- X.p2p-1에 overlay P2P 네트워크, 모델, 기본요구사항 등을 고려하여 개발키로 했으며, 안전한 라우팅 사용방법과 관련된 표준들을 informative reference에 반영키로 함
- 구조화된 P2P 네트워크 기반의 DHT를 위한 reputation system 이슈는 X.p2p-1에 일부 요구사항과 기본 정의, 취약점 분석 등을 반영키로 하였으며, X.p2p-2에 세부적인 메커니즘과 프로토콜을 반영키로 함
- P2P 네트워크를 위한 신뢰된 모델, 인증구조, P2P 차단 및 제어를 위한 프레임워크에 대해 검토한 결과 X.p2p-1, 2의 연구영역에 반영하여 표준을 개발키로 함
- 일본에서 제안한 '제3의 신뢰모델(TTP)을 이용한 안전한 서비스를 위한 요구사항(X.p2p-2)' 은 표준(안)의 범위를 좀더 구체화하기로 함
- 한국에서 제안한 '강한 패스워드 인증 프로토콜을 위한 가이드라인' 은 공격 방법 등에 대한 추가적인 검토와 5.4 항목을 부록으로 이동키로 함

○ OASIS의 XML 보안(SAMLv2.0, XACMLv2.0)

- OASIS의 요청으로 표준화하고 있는 XML 보안(SAMLv2.0, XACMLv2.0)은 일부 항목들을 수정하여, 이번 회의에서 consent로 추진하였음

○ 프라이버시/RFID 보안

- 멀티미디어 통신에서의 콘텐츠 프라이버시 보호, 주민등록 대체기술(개인식별 관리), RFID 응용서비스를 위한 프라이버시 보호기반의 프레임워크 등은 EPCGlobal 기구와의 중복성 문제로 프랑스에서 반대하여, 신규 아이템으로는 채택되지 못하였으며, 차기 Interim 미팅에서 계속해서 검토하기로 함

○ 웹서비스 보안

- 한국에서 제안한 '모바일 웹서비스에서의 메시지 보안을 위한 구조' 는 다른 표준화기구(OMA, 3GPP, 3GPP2)와 중복성 문제가 제기되어, 향후 이들에 대한 중복성 문제를 해결하면서 표준을 개발키로 하였고 main-editor에 이재승 선임(ETRI)이 임명됨
- 한국에서 제안한 '모바일 웹 환경에서의 싱글 사인온(Single Sign-On) 및 접근제어' 는 X.websec-1, 2를 위한 좋은 시나리오 예가 될 것으로 검토되었으며, Liberty alliance와 OMA에 중복성 검토를 의뢰키로 함

7) Q.17(기술적 방법에 의한 스팸 대응) 회의 결과

○ TSB, 영국, 프랑스의 제안에 따라, Question text의 4장 'Relationships' 에서는 SPU(ITU Strategy and Policy Unit)를 삭제하고 3장 'Tasts' 에서는 SPU를 유지키로 함

○ 중국에서 제안한 '스팸 대응을 위한 기술적인 프레임워크 설계' 는 다른 표준화기구에서 개발되고 있는 표준들과 상호호환성이 적합한 것으로 검토되어, X.tcs의 5장에 반영키로 함

○ X.fcs 표준(안)에서는 스팸 대응을 단일 관리 방법에서 다중 관리 방법으로 변경하기로 함
○ X.csreq에서는 연구범위를 수정, OECD 리포트를 반영, 그림 1을 삭제하고 이를 설명하기 위한 새로운 문장을 삽입키로 함

8) 차기 WP2 Interim 미팅

○ Q.4를 제외한 Q.5~9, 17의 interim 회의를, 2006. 9. 11~15일까지 캐나다 오타와에서 개최키로 함

라. WP3(Language and Telecommunication Software) 회의 주요내용

1) Q.10(ASN.1과 기타 언어) 회의 결과

○ SG17에서는 ISO, IEC, ITU-T, UNECE 및 다른 표준화 기구와의 MoU MG(Management Group)와의 협의를 위한 대표로 Mr. John Larmoth와 Mr. M Oliver Dubuisson을 재임명함
○ SG17를 대표하여, ISO/IEC JTC1/SC37(생체인식) 협의 대표로 Mr. John Larmoth를 임명함
○ ASN.1의 표준(안)과 부속서를 TD3212로 수정하였으며, X.891 Cor.1의 AAP 결과를 X.891에 반영되도록 SG17 TSB에 요청함
○ SG17 웹페이지에 객체 식별자(OID: Object IDentifier) 할당 등록을 위한 페이지가 개설된 이후, 현재 80,000개의 OID가 등록됨
○ X.680과 X.690 series의 모든 표준들을 유지보수하기로 결정함

2) Q.11(언어 스펙과 구현) 회의 결과

○ SDL(Specification and Description Language)을 위한 UML 프로파일을 수정하여 Z.100에 반영함
○ Z.130(extended Object Definition Language Implementer's Guide v1.0), Z.130 Annex E (eODL to CIDL mapping) 표준(안)은 eODL과 UML의 공통사항들에 대한 비교 검토가 완료되어, 이번 회의에서 consent로 추진키로 함

3) Q.12(언어 요구사항) 회의 결과

○ GRL(Goal oriented requirement language), UCM(Use case map notation), URN(User Requirement Notation) 메타 모델(metamodel)에 대해 검토가 이루어졌음
○ URN, GRL, UCM을 지원하기 위한 툴이 서비스되고 있음
- http://cserg0.site.uottawa.ca/twiki/bin/view/ProjetSEG/WebHome

4) Q.13(시스템 설계 언어 프레임워크와 단일화된 모델링 언어) 회의 결과

○ X.689, Z.109, Z.119, Z.129, Z.149, Z.159를 UML2.0에 맞게 계속해서 유지보수하기로 함

5) Q.14(언어 평가, 방법론, 프레임워크) 회의 결과

○ 한국과 ETSI가 공동으로 추진하고 있는 'Z.itfm: Interoperability testing framework and methodology' 표준(안)은 이번 회의에서 검토되지 않았지만, ETSI의 IOP 특별작업에서 본 이슈에 대한 검토가 완료되면 추진이 가능할 것으로 검토됨

6) Q.15(개방형 분산 처리) 회의 결과

○ X.901-904 표준들에 대한 유지보수와 X.906 표준(안)에 대해, ISO/IEC JTC1/SC7에 추진되고 있는 결과들과 비교 검토하였음

7) 차기 WP3 Interim 미팅

- ㅇ Q.10은 2006. 6. 12~16일까지, 체코 프라하에서 JTC1/SC6 그룹과 공동으로 개최키로 함
- ㅇ Q.10은 2006. 6~11월까지 계속해서 ISO 표준화 작업 관련하여, e-mail 회의를 개최키로 함
- ㅇ Q.11, 13은 2006. 5. 30~6. 3일까지, Kaiserslautern 대학에서 개최키로 함
- ㅇ Q.11, 12, 13은 2006. 9월 중순에 Tele-confernce 회의를 개최키로 함
- ㅇ Q.11, 13은 2006. 10월에 ETSI에서 개최키로 함
- ㅇ Q.10~15는 2006. 5~11월까지 계속해서 LC 이슈로 e-mail 회의를 개최키로 함

마. ITU-T SG17 차기회의 일정

- ㅇ 2006.12.6 ~ 15일까지, 스위스 제네바에서 개최키로 함

3. 맺음말

이번 ITU-T SG17 회의는 다른 어느 나라에서 개최될 때 보다 더 많은 국내외 표준화 전문가들이 참석하였고, 모든 참가들이 회의준비와 전체적인 회의운영에 있어 훌륭하다고 평가한 회의였다. 한국은 다른 어느 나라보다, 많은 참가자와 많은 기고서를 제출하여 국내 기술을 국제 표준에 반영시키는 성과를 올렸으며, 새롭게 Q.7의 부-라포처를 김정덕 교수가 임명받았고 새로운 연구 아이템(모바일 멀티캐스트, 중계방식 멀티캐스트 통신보안, 보안사고 관리, 바이오 정보를 이용한 전자서명 생성방법, 웹서비스 메시지 보호를 위한 구조)에 대해 main-editor로 임명받아 해당 분야의 국제표준을 주도하기에 좀더 유리한 발판을 마련하였다.

ITU-T SG17은 ITU-T 내의 '정보통신 보안 선도그룹' 으로서 정보보호 관련 국제표준을 중점적으로 개발하고 있는 바, 한국은 이번 회의의 성과를 바탕으로 정보통신 보안 분야의 국제표준화를 지속적으로 선도해 나아갈 예정이다. TTA