

ITU-T SG17(보안) 국제표준화 동향

오 흥 룡*, 염 흥 열**

요 약

국제전기통신연합(ITU)은 UN 산하에 신설된 국제기구로써, 산하에 전기통신표준화부문(ITU-T), 전기통신개발부문(ITU-D), 그리고 전파통신 부문(ITU-R) 등 3개의 부문으로 구성되어 있다[1],[2]. ITU-T는 역할과 임무에 따라 11개의 연구구반 (SG, study group)을 구성하고 있으며, 각 업무에 맞는 선두 그룹(Lead Study Group)을 지정하여 표준을 개발하고 있다. 이중 SG17(보안)은 전기통신 분야 정보보호 국제표준화를 담당하고 있다[2].

본 논문에서는 ITU-T 내에 정보보호 국제표준화 활동에 대한 상위수준의 PP-14 결의(Resolution) 분석과 SG17 국제표준화 활동의 최신 동향 및 차기 연구회기(2017-2020) 구조조정 방향에 대해 살펴본다.

※ 참고사항 (2015.6, TSAG 회의)

ITU-T SG20 신설 : Internet of Things (IoT) and its applications including smart cities and communities (SC&C)

I. 서 론

스마트폰의 등장으로 일상생활 속에서 정보통신(ICT) 기술 활용성이 증가하고 있고, 정보보호 관점에서는 보안 위협이 증가하게 되어 보호해야 될 대상이 더욱 증가하고 있다. 또한 비대면 인증 및 인터넷전문은행 등 새로운 부가서비스의 등장은 사용자에게 편리성을 제공하는 반면 악의적인 활동에 위협대상이 될 수 있어, 정보보호 관점에서는 더욱 신경을 써야 된다.

통신망(인터넷, 모바일 등)에서 피싱, 파밍, 스캔/침입, 홈페이지 변경, 비인가된 접근 등과 같은 사이버공격이 증가하고 있으며, 이를 해결하기 위한 방법도 단일 국가의 노력보다는 국가 간에 협업하는 형태로 진화되고 있다. 이에 대한 노력의 하나로 통신망에서의 정보보호 기술 표준화는 국가 간에 상호운용성, 보안 정책 및 신뢰성 확보를 위해 중요한 수단이며, ITU-T SG17 국제표준화 활동은 중요성이 점차 증가하고 있다.

본 논문 제2장에서는 ITU-T 내에 정보보호 국제표준화 활동에 대한 상위수준의 PP-14 결의(Resolution) 분석과 SG17 국제표준화 활동의 최신 동향 및 차기 연구회기(2017-2020) 구조조정 방향을 살펴보고, 제3장

에서는 결론 및 향후 대응방안을 제시한다.

II. ITU-T 정보보호 표준화 활동

ITU-T SG17 국제표준화 추진 방향은 매 4년마다 열리는 ITU 전권회의 (PP, plenipotentiary conference) 와 세계정보통신표준총회 (WTSA, world telecommunication standardization assembly) 의 정책 방향에 근거하고 있다. 본 장에서는 ITU-T SG17 활동의 근거가 되는 상위수준 PP-14 결의를 분석한다. 다른 WTSA-12 결의는 [정보보호학회지 제24권 제4호] 논문을 참고하기 바란다[3].

2.1. ITU PP-14 결의

ITU PP는 ITU에서 최고위급 정책 결정 회의로써, 산하 3개의 부문(sector)에 대한 연구 방향을 결정하고 각 부문의 운영을 담당할 고위직을 선출한다[3]. 2014년 한국 부산에서 열린 PP-14에서는 ITU-T 국장에 한국 이재섭 박사가 선출되는 쾌거를 남겼다. PP-14에서 산출된 정보보호 분야 결의는 Res.130, Res.179,

본 논문은 미래창조과학부의 지원을 받는 정보통신 방송표준 개발지원사업의 연구결과로 수행되었음

* 한국정보통신기술협회 표준화본부 (hroh@tta.or.kr),

** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

Res.181 등이 직접적으로 관련되며, 일부 다수 결의는 모든 연구반이 공동으로 고려해야 되는 결의들이다. SG17은 이 결의들을 바탕으로 표준화 정책 수립 및 국제표준화를 추진하고 있다[4], [5]. [표 1]은 정보보호와 관련된 주요 결의의 내용과 SG17 내 주요 활동 결과를 나타내고 있다.

2.2. SG17 국제표준화 동향

이번 연구회기(2013-2016)는 WTSA-12 회의에서 승인된 연구과제(Question)를 기능별로 나눠서 5개의 작업반(WP) 및 세부 연구과제 총 12개로 구성되어 운영되었다. 본 절에서는 각 연구과제별 중요 활동에 대한 정보를 제공하고자 한다.

2.2.1. 통신/ICT 보안 조정(Q1/17)

본 그룹에서 보안 전략, 비전, 계획, 로드맵 등의 보안 표준에 대한 총괄 업무를 수행하고 있으며, 이번 연구회기 동안에는 보안 표준들의 성공사례에 대한 기술 보고서(Technical Report)를 개발하고 있다.

2.2.2. 보안구조 및 프레임워크(Q2/17)

본 그룹에서는 보안구조, 모델, 전반적인 서비스 시나리오 등을 담당한다. 이번 연구회기 동안은 IPv6 구현을 위한 보안 표준(X.1037)과 IPv6 구현 지침 부속서(X.Sup23), 통신 사업자를 위한 보안지침(X.1033) 표준을 완료하였다. 현재는 전자상거래 환경에서 거래정보 등 데이터를 보호하기 위한 보안구조(X.salcm), SDN 보안 구조 및 요구사항(X.sdnsec-2), 모바일 가상 네트워크 운영자(별정통신사업자) 보안 지침(X.sgmvno), ITU-T X.805 구현 지침(정보보호 준비도), VoLTE 보안 구조 및 지침(X.voLTEsec-1)을 개발 중에 있다.

2.2.3. 통신부문 정보보호 관리체계(Q3/17)

본 그룹에서는 통신부문 보안관리 표준을 주로 다루고 있다. 이번 연구회기 동안은 ISO/IEC 27002 개정에 따른 통신조직을 위한 정보통신 보안관리(X.1051) 개정 작업을 완료하였다. 또한, 개인정보보호 관리체계

(PIMS) 국제표준화 작업을 ISO/IEC JTC1/SC27/WG5 그룹과 공통표준(Common Text) 작업(X.gpim)이 활발하게 진행되었다. 그리고 ISMS 관리체계를 중소기업에 적용하기 위한 지침(X.sgsm), PIMS 관리체계에 대한 구현 부속서(X.sup-gpim), X.1054(정보보호 거버넌스) 국제표준의 구현 사례 부속서(X.sup-gisb)가 개발 중에 있다.

2.2.4. 사이버보안(Q4/17)

본 그룹에서는 사이버공격 대응기술, 사이버보안 정보공유 방법, 사이버보안 전반적인 이슈를 다루고 있다. 이번 연구회기 동안은 사이버보안지수(X.1208), 사이버보안 역추적기술(X.1210), 웹기반공격 대응기술(X.1211), 재난경보 알림 프로토콜(X.1303 bis), 사이버보안 정보공유 프레임워크(X.1500) 시리즈 다수의 표준화 작업을 완료하였다. 현재는 세션정보 메시지 교환 포맷(X.simef), 사이버공간에서의 보안위협 평가 매트릭스(X.metric), 정보통신/ICT 네트워크 보안 평가기술(X.samtn), 스마트폰 봇넷 대응을 위한 보안 요구사항(X.sbb), 사용자 보호를 향상시키기 위한 설계 고려사항(X.cogent) 표준초안이 개발 중에 있다.

2.2.5. 스팸의 기술적 대응(Q5/17)

본 그룹에서는 스팸의 기술적인 대응 표준을 개발하고 있는 그룹으로 e-mail 스팸, IP멀티미디어 스팸, 보이싱 스팸, 모바일 메신저 스팸 등을 다루고 있다. 이번 연구회기 동안은 통신 조직 내에 보이싱 스팸 대응을 위한 기술(X.1246), 모바일 메신저 스팸 대응을 위한 기술적 프레임워크(X.1247), 모바일 폰 개발자를 위한 스팸 대응 지침(X.Sup25)을 완료하였다. 현재는 인스턴트 메신징 스팸 대응을 위한 기술 요구사항(X.cspim), 피싱 및 스미싱 대응 지침(X.gcsipi), 모바일 광고 스팸 대응을 위한 기술적 프레임워크(X.tfama), VoLTE 환경에서의 스팸 대응 부속서(X.ticsc)가 개발 중에 있다.

2.2.6. 유비쿼터스 통신 서비스 보안(Q6/17)

본 그룹에서는 IPTV 보안, USN 보안, 모바일 보안, 멀티캐스트 보안, 홈네트워크 보안, RFID 보안, 스마트

[표 1] ITU-T 정보보호 분야 PP-14 결의(2014)

결의 번호	제목	주요 내용 (SG 17관련)	SG17 관련활동
결의 130	(영문제목) Strengthening the role of ITU in building confidence and security in the use of information and communication technologies	<ul style="list-style-type: none"> 신뢰와 보안을 구축하기 위한 신규 보안 위협 및 취약점을 다룰 것 신규 보안 프로토콜 및 표준들에 대한 기술적 정보 교환 방법을 향상시킬 것 개발도상국을 위한 신뢰와 보안 구축 방법을 지원할 것 침해사고대응팀 (CIRT) 신설하기 위한 모범 사례를 식별하고, 참조 가이드를 준비할 것 관련 국제기구와 전문가와 협력해 침해사고대응팀 신설을 위한 모범사례를 개발할 것 	<ul style="list-style-type: none"> 연구과제 3(Q3/17) 보안사고 대응 지침 연구과제 4(Q4/17) 사이버보안 정보 교환 프레임워크 (CYBEX) 시리즈 연구과제 5(Q5/17) 사용자 신뢰성 확보를 위한 스팸대응
	(한글제목) 정보통신기술의 활용에 있어서 신뢰와 보안을 구축하기 위한 ITU의 역할 강화		
결의 179	(영문제목) ITU's role in child online protection	<ul style="list-style-type: none"> 온라인 아동보호를 위한 지식 및 모범사례를 공유하여 최적 플랫폼을 개발할 것 온라인 아동보호를 위한 기술적 구현방법에 대한 로드맵을 만들 것 온라인 아동보호를 위한 새로운 기술 개발 및 특정 방법에 대한 프레임워크를 만들 것 온라인 아동보호를 위한 글로벌 단일 전화번호의 도입 가능성을 SG2와 협력하여 연구할 것 	<ul style="list-style-type: none"> 2012년 3월 SG17 회의에서, 온라인 아동보호-조인트조정활동 (JCA-COP) 신설 현재, SG17 내에 기술적 관점에서 표준초안 개발 위한 연구가 진행 중
	(한글제목) 온라인 아동보호를 위한 ITU의 역할		
결의 181	(영문제목) Definitions and terminology relating to building confidence and security in the use of ICTs	<ul style="list-style-type: none"> ITU-T SG17이 정보통신 및 ICT 보안에 대한 핵심 국제표준을 개발하고, 권고 X.1205에 용어 “사이버보안”을 정의하고 있음을 고려해, ITU-T 국장에게 사이버보안 용어와 관련된 신규 또는 개정 권고를 ITU 이사회에 보고할 것 	<ul style="list-style-type: none"> SG17 회의에서 사이버보안 용어와 관련 신규 또는 개정 권고를 보고하고 있음 ITU-T X.1252, X.509, X.1500 시리즈 표준 활용
	(한글제목) 정보통신기술의 활용에 있어서 신뢰와 보안 구축과 관련된 용어 정의		
(정보보호 관련 간접 결의)			
<ul style="list-style-type: none"> - 결의 101 : Internet Protocol-based networks - 결의 123 : Bridging the standardization gap between developing and developed countries - 결의 136 : The use of tele-communication/ information and communication technologies for monitoring and management in emergency and disaster situations for early warning, prevention, mitigation and relief - 결의 174 : ITU's role with regard to international public policy issues relating to the risk of illicit use of information and communication technologies - 결의 177 : Conformance and interoperability - 결의 178 : ITU role in organizing the work on technical aspects of telecommunication networks to support the Internet - 결의 188 : Combating counterfeit telecommunication/information and communication technology devices - 결의 189 : Assisting Member States to combat and deter mobile device theft - 결의 197 : Facilitating the Internet of Things to prepare for a globally connected world - 결의 199 : To promote efforts for capacity building on software-defined networking in developing countries - 결의 200 : Connect 2020 Agenda for global telecommunication/ information and communication technology development - 결의 201 : Creating an enabling environment for the deployment and use of information and communication technology applications 			

그리드 보안, 사물인터넷 보안, ITS 보안 등의 표준을 다루고 있다. 이번 연구회기 동안은 IPTV 보안을 위한 가상 머신 기반 보안 플랫폼 iCAS(X.1198), 유비쿼터스 네트워킹을 위한 보안 요구사항 및 프레임워크(X.1314), 스마트폰 보안 기술 부속서(X.Sup19), 안전한 앱 배포 프레임워크 부속서(X.Sup24), 스마트 그리드 보안 기능 구조 부속서(X.sup.26)를 완료하였다. 현재는 IoT 환경을 위한 심플 암호화 절차(X.iotsec-1), IoT 보안 프레임워크(X.iotsec-2), ITS 통신 장비를 위한 안전한 소프트웨어 업데이트 방법(X.itssec-1), ITS 통신 시스템을 위한 보안 지침(X.itssec-2), 스마트폰 도난 시, 개인정보 등을 안전하게 섀다운 할수 있는 킬스위치(X.msec-9), 모바일 네트워크에서 감염된 단말의 부정적인 영향을 감소시키기 위한 지침(X.msec-11), SDN을 이용한 보안 서비스(X.sdnsec-1), ITS 보안 업데이트를 무선 방법으로 운영하기 위한 부속서(X.sotavsu)가 개발 중에 있다.

2.2.7. 안전한 응용 서비스(Q7/17)

본 그룹에서는 P2P 보안, 웹서비스 보안, 응용프로토콜 보안, 제3의 신뢰기관(Trusted Third Party) 기반 인증 기술 등을 다루고 있다. 이번 연구회기 동안은 XML 기반 접근제어 기술 XACML 3.0(X.1144), 다중 아이덴티티 제공자 환경에서 컴바인 인증 프레임워크(X.1154), 전자상거래 서비스를 위한 연결 가능한 인명 인증 지침(X.1155), 원타임 패스워드 기반 부인방지 프레임워크(X.1156), 상위 수준에서 이상거래 탐지 및 대응을 위한 기술적 요구사항(X.1157), 모바일 디바이스를 이용한 다중 인증 메커니즘(X.1158), ITU-T X.813 기반 방문자 부인방지 구조(X.1159), 정보통신 기반 P2P 보안요구사항 및 메커니즘(X.1163), 웹 매쉬업 서비스를 위한 보안 프레임워크(X.sup.21), XACML 3.0 내에 개선사항 및 신규 특징(X.sup.22) 부속서를 완료하였다. 현재는 클라이언트-서버 모델에서 하이브리드 인증 및 키관리 메커니즘 지침(X.hakm), 정보통신 서비스를 원활하게 지원하기 위한 보안 요구사항 및 프레임워크(X.websec-6), 온라인 분석 서비스를 위한 레퍼런스 모니터(X.websec-7), 통신 운영자를 위한 부가서비스 보호 지침(X.websec-8)을 개발 중에 있다.

2.2.8. 클라우드 컴퓨팅 보안(Q8/17)

본 그룹에서는 프레임워크, 메커니즘 등 클라우드 컴퓨팅 보안 전체를 다루고 있다. 이번 연구회기 동안은 클라우드 컴퓨팅을 위한 보안 프레임워크(X.1601), 소프트웨어 서비스(SaaS) 응용 환경을 위한 보안 요구사항(X.1602), 클라우드 서비스를 위한 ISO/IEC 27002 기반 정보보호 통제 구현 지침(X.1631), 클라우드 컴퓨팅 운영을 위한 보안 지침(X.1642)을 완료하였다. 현재는 클라우드 서비스 가입자 데이터 보안을 위한 지침(X.CSCDataSec), 클라우드 컴퓨팅 모니터링 서비스를 위한 데이터 보안 요구사항(X.dsms), 클라우드 컴퓨팅에서 퍼블릭 인프라 서비스(IaaS)를 위한 보안 요구사항(X.SRIaaS)을 개발 중에 있다.

2.2.9. 텔레바이오메트릭(Q9/17)

본 그룹에서는 네트워크 기반 바이오 정보를 이용한 인증 기술에 대한 표준을 다루고 있다. 이번 연구회기 동안은 이헬스 및 텔레메디슨에서 바이오정보를 보호하기 위한 통합 프레임워크(X.1092) 표준을 완료하였다. 현재는 바이오 하드웨어 보안 모듈을 이용한 텔레바이오 인증 프레임워크(X.bhsm), 텔레바이오인식에서 프라이버시 기반 접근제어(X.pbact), 모바일 디바이스를 이용한 텔레바이오 응용에서의 기술적 관리적 대응 지침(X.tam), 텔레바이오인식에 연관되는 학문적 정의(X.th Series) 표준초안들이 개발 중에 있다.

2.2.10. 아이덴티티 관리 구조 및 메커니즘(Q10/17)

본 그룹에서는 아이덴티티(Identity) 관리 기술과 기반 인증 서비스들에 대한 표준을 다루고 있다. 이번 연구회기 동안은 아이덴티티 관리 정보의 검색을 위한 프레임워크(X.1255), 어플리케이션 서비스에서 네트워크 인증 결과를 공유하기 위한 프레임워크(X.1256), 아이덴티티 및 통제 관리 분류체계(X.1257) 표준을 완료하였다. 현재는 실체 인증 보증 프레임워크(X.1254rev) 개정 작업과 수집된 속성 정보 기반 향상된 실체 인증(X.eaaa), 신뢰 개량(trust elevation) 프로토콜(X.te) 표준초안들이 개발 중에 있다.

2.2.11. 안전한 응용을 지원하기 위한 일반 기술(Q11/17)

본 그룹에서는 안전한 응용서비스를 지원하기 위한 디렉토리, PKI, PMI, ASN.1, OID 식별자 할당 등 업무를 수행하고 있다. 이번 연구회기 동안은 OSI 디렉토리 표준들에 대한 오류 정정 작업과 이기종 식별자 및 위치정보에 대한 OID 기반 해설 프레임워크(X.675), ANS.1 인코딩 규칙 표준들에 대한 유지보수, 우체국 간에 인증 및 인증된 메일 전송 프로토콜(X.1341), PKI 표준화를 위한 현재와 새로운 도전 기술보고서(XSTR-PKIS) 작업을 완료하였다. 현재는 PKI 유지보수 및 개선작업(X.pki-em), PKI 프로파일 정의(X.pki-prof), IoT 환경을 위한 객체식별자 활용 방법(X.oiddev), IoT 환경을 위한 객체식별자 활용 지침 부속서(X.oid-iot), JSON 스크립트 언어의 ASN.1 인코딩 규칙(X.jsoner), 암호 메시지 규격에 대한 ASN.1 응용 규칙(X.cms) 등 표준 개발과 OSI 디렉토리(X.500 series) 제8판에 대한 개정 작업이 진행 중에 있다.

2.2.12. 통신 소프트웨어와 시험을 위한 공식 언어(Q12/17)

본 그룹에서는 다양한 형식 언어 및 시험방법론에 대한 표준을 다루고 있다. 이번 연구회기 동안은 SDL-2010 기술 언어(Z.100 series), TTCN-3 시험 언어(Z.160 series), SDL 구현자 가이드(Z.Imp100) 유지보수 작업을 완료하였다. 현재는 ITU-T Z계열(형식 언어 및 시험방법론) 표준들에 대한 유지보수가 계속해서 진행되고 있다.

2.3. 차기 연구회기(2017-2020) 구조조정 방향

ITU-T 분야는 4년 주기로 WTSA 총회를 개최하여 전체 조직의 운영 효율성 및 전문 분야 등을 고려하여 조직을 재개편한다. 또한, WTSA 총회에서 최종 확정된 조직의 연구반(SG) 의장 및 부의장도 임명한다. 따라서 각 연구반에서는 현재 연구회기(2013-2016) 동안의 활동 실적과 차기 연구회기 구조 조정안을 상정하게 된다. SG17 연구반에서도 총 2회(2015.9월, 2016.3월) 정기회의를 통해 활동 실적 및 차기 구조 조정안을 확정하였다.

SG17 연구반 회의결과는 이번 연구회기 구조(12 Questions)를 유지하는 것으로 확정하였다. 단, Q6/17 그룹 명칭에 유비쿼터스 키워드를 삭제하기로 하고, Q11/17 그룹 명칭도 구체화하기로 확정하였다. 그리고 차기 연구회기 내에 일부 연구과제들의 연구범위를 다음과 같이 확장하기로 하였다[7], [8].

- Q2/17 : SDN, NFV, LTE/SAE 보안구조
- Q6/17 : 5G, SDN, NFV, eSIM 응용보안
- Q7/17 : 금융보안서비스, 데이터 분석 서비스
- Q10/17 : IoT 환경에서의 ID관리

한국은 차기 연구회기를 위한 또 다른 중요 사항으로 정보보호 분야를 총괄하는 SG17 연구반 의장 후보로 순천향대 엄홍열 교수를 미래부가 추천키로 결정하였다. WTSA-16 총회까지는 아직 시간이 남아 있어, 다른 국가들의 입후보 현황은 좀 더 지켜보아야 되지만, 정보통신 분야 정보보호를 총괄하는 의장을 한국이 수입하는 것은 정보보호분야 국제표준화 활동을 주도한다는 측면에서 큰 의미가 있다.

III. 결 론

본 논문에서는 이번 연구회기(2013-2016) 동안 SG17 연구반 국제표준화 활동 근거가 되는 ITU 상위 수준 회의의 관련 결의의 내용을 분석했다. 또한, 각 그룹 내에서 개발된 신규 권고와 현재 개발 중에 있는 표준초안들에 대해 살펴보았다.

현재 한국은 매 SG17 회의마다 많은 전문가로 구성된 대표단을 파견해 오고 있으며, 그 동안 SG17 부의장, WP 의장, 여러 연구과제의 라포처 등의 의장단 활동과 국제표준 개발을 책임지는 에디터 역할을 통해 SG17 국제표준화 활동에 크게 공헌해 오고 있으며, 미국, 일본, 중국 등 다른 국가에서도 인정받고 있다.

한국은 ITU-T SG17 국제표준화 활동에 더 큰 주도권 확보를 위해 차기 연구반 의장에 입후보한 만큼, 정부 및 정보보호 산업체, 학계, 공공기관 전문가가 서로 협력해 ITU-T 정보보호 분야에 한 단계 더 성장하는 발판을 마련해야 되는 시점이다.

참 고 문 헌

- [1] ITU-T 홈페이지, <http://www.itu.int>
- [2] 오홍룡, 김영화, 염홍열, “ITU-T SG17 국제표준화 동향 및 향후 전망”, 정보보호학회지, 제23권 제3호, 2013.06.
- [3] 염홍열, 오홍룡, “정보보호 기술 및 국제표준화 동향(ITU-T SG17)”, 정보보호학회지, 제24권 제4호, 2014.08.
- [4] ITU Plenipotentiary Conference 2014 : PP-14, <http://www.itu.int/plenipotentiary/2014/>
- [5] ITU PP-14, Final acts of the plenipotentiary conference (Busan, 2014), <http://www.itu.int/pub/S-CONF-ACTF-2014>
- [6] WTS-12, <http://www.itu.int/en/ITU-T/wtsa12/Pages/default.aspx>
- [7] ITU-T SG17 TD2240/R4, "ITU-T Study Group 17 REPORTS TO THE WTS-16 - PART I - GENERAL", 14-23 March 2016.
- [8] ITU-T SG17 TD2250/R4, "ITU-T Study Group 17 REPORT TO THE WTS-16 - PART II - QUESTIONS PROPOSED FOR STUDY DURING THE NEXT STUDY PERIOD (2017-2020)", 14-23 March 2016.



염 홍 열 (HeungYoul YOUM)
 종신회원

한양대학교 전자공학과 학사 졸업
 한양대학교 대학원 전자공학과 석사 졸업
 한양대학교 대학원 전자공학과 박사 졸업

1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
 1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
 2011년 1월~12월 : 한국정보보호학회 회장(역), 명예회장(현)
 2009년~현재 : ITU-T SG17 부의장
 2009년~현재 : ITU-T SG17 WP2/WP3 의장
 2012년 6월~2015년 5월 : 정보보호포럼 의장
 2016년 5월~현재 : 개인정보보호포럼 의장
 <관심분야> 인터넷 보안, USN 보안, IPTV 보안, 홈네트워킹 보안, 암호 프로토콜

<저자소개>



오 홍 룡 (Heung-Ryong Oh)
 종신회원

2002년 2월 : 순천향대학교 전자공학과 졸업
 2004년 2월 : 순천향대학교 정보보호학과 석사
 2007년 6월 : 순천향대학교 정보보호학과 박사 수료

2004년 2월~현재 : 한국정보통신기술협회 표준화본부 책임연구원
 2005년 3월~현재 : ITU-T SG17 국내 분과위원회 간사(역) 및 위원
 2009년 2월~현재 : ITU-T SG17 Q.2 Associate Rapporteur
 <관심분야> 보안프로토콜, 정보보호표준