情 報 保 護 學 會 誌
第21卷 第2號, 2011. 4

ITU-T 응용서비스 보안 및 서비스 지향 구조(SOA) 국제표준화 동향

임 형 진*, 서 대 희**, 나 재 훈***

요 약

국제표준화기구 ITU-T에서는 연구그룹(Study Group)17이 정보통신 응용보안에 관한 표준화를 리드하는 연구그룹으로, 산하 4개의 연구과제(Question)를 구성하여 정보보호 국제표준을 개발하고 있다. 이 연구과제들 중 Q.7(의장, 나재훈, ETRI)에서는 안전한 응용 서비스라는 범주로 안전한 응용 프로토콜, 웹서비스 보안, P2P(Peer-to-Peer) 보안 등 정보통신 환경의 응용서비스 보호에 적용될 수 있는 국제표준들의 개발을 담당하고 있다. Q.8(의장, Liang Wei, CATR)에서는 서비스 지향 구조라는 범주로 SOA(Service Oriented Architecture) 기술 및 통신 보안에 관련된 국제표준들의 개발을 담당하고 있다. 현재 Q.7에서는 총 7건의 국제표준을 제정하였으며, 총 6건의 표준초안들이 개발중에 있다. Q.8의 경우는 현재 총 3건의 표준초안들이 개발중에 있다. 본 논문에서는 해당 연구과제들의 표준화 현황과 향후 추진 방향을 제시한다.

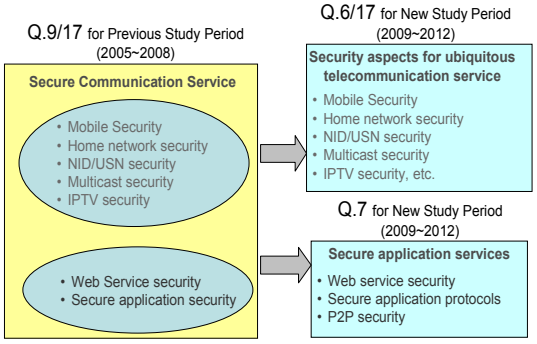
Ⅰ. 서 론

최근 정보통신분야 기술의 발전을 체감하는 현상으로 스마트 열풍과 함께 나타나는 기술들과 서비스들의 융합으로부터 사회·문화적 파급효과를 들 수 있을 것이다. 지속적인 정보통신 인프라의 기술적 발전과 함께 다양한 서비스가 제공되고 있으며, 여기에서 정보보호 기술은 안전한 서비스 제공이라는 측면에서 매우 중요한 역할을 하게 된다.

ITU-T SG17에서는 정보통신 보안에 관련된 표준을 선도하는 그룹으로 특히 Q.7과 Q.8은 정보통신 서비스 관점의 정보보호 기술표준들을 개발하고 있다. 본 기고문에서는 이번 연구회기('09~'12)중에 Q.7과 Q.8에서 개발한 국제표준들과 개발중에 있는 표준초안들에 대해 소개하고, 향후 추진 방향 및 전망을 제시하고자 한다.

Ⅱ. ITU-T SG17 연구과제 7의 표준화 현황

2009년 신규 연구회기의 시작과 함께 Q.7은 안전한 응용서비스라는 주제로 [그림1]과 같이 안전한 응용 프로토콜, 웹서비스 보안, P2P보안이라는 분야로 국제표준들을 개발하고 있다. Q.7의 연구분야는 지난 연구회기(2005-2008)동안 Q.9(안전한 통신 서비스)의 세부 개발 주제였으나 이번 연구회기(2009-2012)의 단독 연구과제로 분할하여 관련 표준들을 개발하고 있다[1][2].



〔그림 1〕 신규 연구회기(2009~2012) 구조조정

3.1 안전한 응용 프로토콜

본 절은 안전한 응용 프로토콜 분야의 표준 제정 현

* 금융보안연구원 정보보안본부 (hjlim@fsa.or.kr)
** 한국전자통신연구원 지식정보보안본부 (dhseo@etri.re.kr)
*** 한국전자통신연구원 지식정보보안본부 (jhnah@etri.re.kr)

〔표 1〕 ITU-T SG17 Q.7 국제표준 현황(총 8건), 개정(총 2건) 및 표준초안 현황(총 4건)

No	국제표준번호	제정시기	국제표준명(제목)	제안국가	국내표준
1	X.1141	2006-06	Security Assertion Markup Language (SAML 2.0)	캐나다	TTAS.IT-X1141_1~6
2	X.1142	2006-06	eXtensible Access Control Markup Language(XACML 2.0)	캐나다	TTAS.OT-10.0040/R1
3	X.1143	2007-11	Security architecture for message security in mobile web services	한국 (이재승)	TTAE.IT-X1143
4	X.1151	2007-11	Guideline on secure password-based authentication protocol with key exchange	한국 (염흥열)	X
5	X.1152	2008-05	Secure end-to-end data communication techniques using trusted third party services	일본	추진중(2010-1483)
6	X.1153	2011-01	The management for an one time password based authentication service	한국 (심희원, 김근옥, 임형진)	TTAK.KO-12.0128
7	X.1161	2008-05	Framework for secure peer-to-peer communications	일본	TTAE.IT-X1161
8	X.1162	2008-05	Security architecture and operations for peer-to-peer network	한국 (나재훈)	TTAE.IT-X1162
9	Amendment of X.1141	2011-09	Security Assertion Markup Language (SAML 2.0)-Amendment 1	캐나다	X
10	Amendment of X.1142	2011-09	eXtensible Access Control Markup Language (XACML 2.0)-Amendment 1	캐나다	X
11	X.sap-4	2011-09	The general framework of combined authentication on multiple identify service provider environment	일본, 한국 (임형진)	X
12	X.sap-5	2011-09	Guideline on anonymous authentication for e-commerce service	한국 (이석준)	X
13	X.p2p-3	2011-09	Security requirements and mechanism of peer-to-peer based telecommunication network	중국	X
14	X.websec-4	2011-09	Security framework for enhanced web based telecommunication services	한국 (서대희)	X

황과 연구과제 계획 및 추진 현황을 기술한다. [표 1]에서는 ITU-T SG17 Q.7에서 추진되는 국제표준 개발 현황을 나타내고 있다.

3.1.1 표준 제정 현황

안전한 응용 프로토콜 분야는 정보통신 환경에서 안전한 통신 환경 보장과 다양한 응용서비스 등에 접목 가능한 부분들을 표준화하고 있다. 지난 회기에서 Q.9는 키 교환이 가능하고 안전한 패스워드 기반의 인증프로토콜 가이드라인(X.1151)[6]과 신뢰된 제3기관(TTP : Trusted Third Party) 서비스를 이용한 안전한 종단간 데이터통신 기술(X.1152)[7] 총 2건의 국제표준을 제정하였다.

X.1151 국제표준의 주요내용은 기억하기가 편하고 별도의 인프라(PKI 등) 환경이 요구되지 않는 패스워드 기반의 인증 프로토콜에 대한 가이드라인을 제시하기 위한 표준이다. 즉, 패스워드 기반의 프로토콜이 가지고 있는 문제점, 운영절차, 특징들을 분석하여, 안전성 확보를 위해 요구되는 요구사항들을 선별하였고, 사용자가 프로토콜 설계 시, 안전성에 따라 패스워드 기반의 인증프로토콜을 선택할 수 있는 기준을 정의하고 있다. 또한, 기존에 연구되어 발표된 다양한 패스워드 기반의 인증프로토콜들과 안전성 비교 및 평가기준을 정의하고 있다[6]. X.1152 국제표준의 주요내용은 온라인에서 TTP 서비스를 이용하여 안전하게 종단간 데이터통신이 가능하기 위한 기본 인터페이스, 상호연동 방법, 보안고려사항 등을 정의하고 있다. 또한, 기본 모델은 2개의 객체 간에 TTP 서비스를 이용하고 있으나, 이를 다수의 객체로 확장하여 이용할 수 있는 방법을 정의하고 있으

며, 이들에 대한 서비스 시나리오 및 기존에 개발된 TTP 서비스 관련 국제표준들과의 비교를 통한 차별성을 정의하고 있다[7]. X.1153 국제표준의 주요내용은 OTP(One Time Password) 기반의 인증 서비스를 위한 관리 프레임워크를 제시하는 표준이다. 해당 프레임워크는 OTP 기반의 인증서비스 모델을 정의하고 관리 요소들을 정의하고 있다[8].

3.1.2 표준안 개발 계획 및 현황

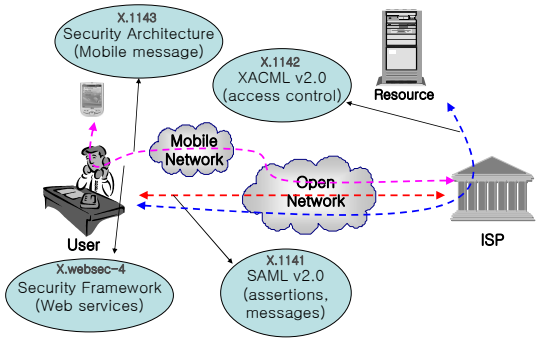
다음은 안전안 응용 프로토콜과 관련된 표준개발 범주를 나타내고 있다.

- 응용서비스의 위협을 정의하고 이를 위한 기술적 대응안 개발
- 안전한 통신서비스를 위한 PKI 응용 프로토콜, 종단간 전송 프로토콜, 키 교환 프로토콜, 패스워드 인증/권한 프로토콜 등 안전한 응용 프로토콜의 연구 및 권고
- 안전하고 안정적인 통신 네트워크와 안전한 통신서비스를 지원하고 보안성을 향상하기 위한 보안 기술 및 보안 정책 표준화
- 안전한 응용 서비스들 간의 상호 연결성 구현을 위한 표준화
- 안전한 응용 서비스를 지원하기 위한 보안 메커니즘에 대한 표준화
- OASIS, OMA등 관련 표준 그룹과 협력
- X.1151 및 X.1152와 같은 기존 표준안의 관리
- 안전한 응용 프로토콜 영역에서 새로운 표준 초안의 발굴 및 개발
- 안전한 응용프로토콜들을 위한 ITU-T 표준안 제정

2009년부터 지난해 말까지 신규 회기동안 안전한 응용프로토콜 분야에서는 총 3건의 표준초안 작업이 진행되고 있다. 먼저 표준초안 X.sap-4[11]는 멀티팩터 인증방식과 같은 결합인증(combined authentication) 서비스를 제공하는 서비스제공자들을 위한 프레임워크를 개발하고 있다. 이 프레임워크는 서비스 제공자들에 의한 결합인증 처리시 전체적인 인증 보증 수준을 유지하기 위해 구성요소들 간의 메시지와 보안 요구사항, 기본동작, 구성모델들을 포함하고 있다. 표준초안 X.sap-5[12]는 전자지불 환경을 위한 참조 모델과 익명 인증 가이드라인을 개발 하고 있으며, 프라이버시 보호 기술을 위한 익명인증 기술을 고려하고 있다. 이 표준초안은 프라이버시 보호 기능을 제공하는 전자지불 서비스 환경을 위한 보안 요구사항과 프라이버시 위협을 정의하고 있다. 또한 전자지불 서비스 환경의 익명 인증을 위한 참조 모델과 보안 요구사항을 만족하는 보안 기능을 개발하고 있다.

3.2 웹서비스 보안

본 절은 웹서비스 보안 분야의 표준 제정 현황과 연구과제 계획 및 추진 현황을 기술한다.



〔그림 2〕 SG17 Q.7 - 웹서비스 보안

3.2.1 표준 제정 현황

웹서비스 보안 분야는 지난회기 중인 2005년 7월, OASIS에서 개발한 XML 기반의 보안 표준들을 ITU-T 차원으로 확대하여 국제표준으로 도입 및 개발하자는 캐나다의 제안으로 시작되었다. 현재 웹서비스 보안과 관련된 국제표준으로는 보안주장마크업언어(SAMLv2.0, X.1141[3]), 확장성 접근제어마크업언어 (XACMLv2.0, X.1142[4])와 한국에서 제안한 모바일 웹서비스에서의 메시지 보호를 위한 보안구조(X.1143[5]) 총 3건이 개발되었다. 다음의 [그림 2]는 Q.7에서 개발한 웹서비스 보안 표준들간에 관계를 나타내고 있다.

X.1141 국제표준의 주요내용은 보안 정보를 교환하기 위한 XML 기반의 프레임워크를 정의하는 표준이다. 즉, 통신 주체들(사용자, 컴퓨터, ISP 등) 간에 요구되는 보안주장(인증, 권한부여, 속성 등)들을 XML 언어로 표현하기 위한 방법과 주체들 간에 교환되는 메시지 형식 및 프로토콜을 XML 언어로 정의하고 있다. SAMLv2.0 구성은 주장 및 프로토콜, 메타데이터, 바인

딩, 프로파일, 인증문맥, 적합 요구사항, 스키마, 보안 및 프라이버시 고려사항 등으로 구성된다[3]. X.1142 국제표준의 주요내용은 통신 주체들 간에 요구되는 접근제어 정책들을 XML 언어로 표현하기 위한 방법을 정의하고 있다. 즉, 임의의 어떤 자원에 접근하고자 하는 개체들에게 일정한 권한을 부여하는 정책과 이들 정책을 평가하는 규칙, 이를 XML로 표현하는 방법들을 정의하고 있다. XACMLv2.0 구성은 코어, 계층구조의 RBAC 프로파일, 다중자원 프로파일, XACMS을 위한 SAMLv2.0, XML 전자서명 프로파일, 계층구조의 자원 프로파일, 프라이버시 정책 프로파일, 데이터 타입 및 기능 정의, 식별자 정의, 컴바인 알고리즘, 스키마, 보안 고려사항, 활용사례 등으로 구성된다[4]. X.1143 국제표준의 주요 내용은 모바일 웹서비스에서 메시지 보호를 위한 보안구조와 다양한 서비스 시나리오를 정의하고 있다. 즉, SOAP 메시지가 방화벽에서 필터링이 되고 있지 않기 때문에 메시지를 필터링할 수 있는 메커니즘을 보안구조로 단일화하였고, 이를 지원하기 위한 보안정책 메커니즘, 모바일 웹서비스 응용과 다른 응용간에 상호연동이 가능한 메커니즘을 정의하고 있다. 또한 보안구조에 따른 활용사례와 다른 표준화 기구(Parlay X, MWSSG, OMA)에서 개발된 표준들 간에 비교 사항을 정의하고 있다[5].

3.2.2 표준안 개발 계획 및 현황

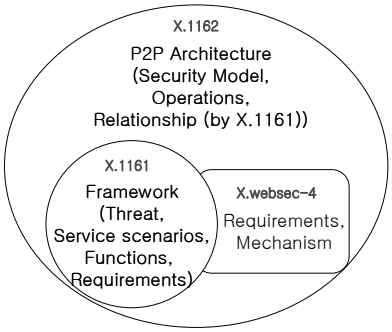
다음은 웹서비스 보안에 관련된 Q.7에서의 연구범주를 나타내고 있다.

- 안전한 인증과 접근제어, 싱글 사인온 등을 포함하는 웹 서비스 보안 기술의 연구
- 정보통신 서비스 시나리오, 네트워크, 시스템 및 관련 응용을 위한 웹서비스 보안의 활용사례를 개발하고, 통신망 구조안에서의 안전한 웹서비스들을 권고 및 연구
- 공격으로부터 웹서비스 기반 정보통신 시스템을 보호하기 위한 최적의 방법에 대한 가이드 개발
- X.1141, X.1142 및 X.1143과 같은 제정된 표준에 대한 유지 및 관리
- 웹서비스 보안 분야에서의 새로운 표준 초안 발굴
- Liberty Alliance, OASIS, OMA, W3C 등 다른 표준화 그룹과 웹서비스 보안에 관한 협력
- 웹서비스 보안을 위한 새로운 ITU-T 표준 제정

지난해 말까지 신규 연구회기 동안 웹서비스 보안 분야에서는 표준초안 X.websec-4[14]가 개발 중에 있다. 이 표준 초안은 확장된 웹 기반 통신서비스를 위한 보안 프레임워크를 제안하고 있으며 보안 위협, 보안 요구사항을 기술하고 있다. 또한 보안 요구사항을 만족할 수 있는 보안 기술과 기능을 포함한다.

3.3 P2P 보안

본 절은 P2P 보안 분야의 표준 제정 현황과 연구과제 계획 및 추진 현황을 기술한다.



〔그림 3〕 SG17 Q.7 - P2P보안

3.3.1 표준 제정 현황

P2P 보안 분야는 불법적인 콘텐츠 배포 및 악의적인 목적 등의 이유로 사람들에게 잘못된 기술로 오해받는 시절이 있었지만, 현대사회에서는 P2P 통신을 기반으로 다양한 서비스들이 응용되고 있어, 해당 기술을 배제하기 보다는 보안 부분을 강화한 P2P 통신 기술 개발과 표준화의 중요성이 부각되고 있다. 지난 회기 Q.9에서 2005년 10월 한국과 일본의 제안으로 표준화가 시작되었으며, 안전한 P2P 통신을 위한 프레임워크(X.1161), P2P 네트워크를 위한 보안구조 및 운영방법(X.1162) 총 2건이 제정되었다[9][10]. 다음의 [그림3]은 현재 Q.7에서 개발하는 P2P 보안 표준들 간에 관계를 나타낸다.

X.1161 국제표준의 주요내용은 다양한 P2P 통신에서 공통적인 특징들과 기본적인 서비스 시나리오를 기반으로 보안 위협과 보안 요구사항들을 정의하였으며, 이들의 보안요구사항을 충족하기 위한 보안 기능들을 정의하고 있다[9]. X.1162 국제표준의 주요내용은 다양

한 P2P 통신을 고려한 공통된 보안구조 및 모델을 정의하고 있으며, 이 모델을 근거로 P2P 통신의 운영방법, X.1161에서 정의하고 있는 보안요구사항과의 관계 정의 및 보안기능들과의 관계를 정의하고 있다. 또한, 부록으로 다양한 P2P 통신 모델들을 정의하고 있다[10].

3.3.2 표준 개발 계획 및 현황

Q.7에서의 P2P 표준 개발 분야는 다음과 같다.

- P2P 서비스에 대한 위협과 이에 대한 대응 기술의 연구
- P2P를 위한 다양한 서비스 프로토콜에 대한 연구
- P2P 서비스들을 위한 보안 정책들과 기술에 대한 표준화
- P2P 서비스들을 지원하기 위한 보안 메커니즘들의 표준화
- IETF 등의 관련 표준화 그룹들과의 협력
- X.1161 및 X.1162 등 기존 표준들의 관리 및 유지
- P2P 서비스 보안 영역에서의 신규 표준 아이템 발굴
- P2P 서비스 보안을 위한 ITU-T 표준 제정

지난해 말까지 신규 연구회기 동안 P2P 보안 분야에서는 표준초안 X.p2p-3[13]가 개발 중에 있다. 이 표준은 P2P 기반의 통신 환경에서의 보안 요구사항을 분석하고 있으며 P2P 기반의 통신망 구조와 서비스 시나리오를 위한 보안 기술 프레임워크를 개발하고 있다. 또한 이 표준 초안에서는 네트워크와 서비스 보호를 보장하기 위한 세부적인 보안 메커니즘을 개발하고 있다.

Ⅲ. ITU-T SG17 연구과제 8의 표준화 현황

3.1 연구범위

Q.8의 연구범위는 SOA 코어 기술의 보안과 통신망에서의 SOA 보안으로 분류되며 다음과 같다.

- SOA 코어 기술들의 보안;
  - SOA 기술에서 관련 위협 평가 및 기술 진화에 대한 보안 보증을 위한 메커니즘 개발
  - ITU-T 관점에서 SOA 코어 기술 보호를 위한 연구
  - ITU-T 관점에서 SOA 보안 프레임워크 및 구조 연구
  - SOA 기반 서비스의 보안 기술 개발
  - SOA 기술과 연관된 위협과 분석의 필요성에 대한 기술적 접근 방법론 연구
  - SOA 보안에 관련된 ISO/IEC JTC 1/SC 27, IETF, OASIS, W3C, 3GPP, 3GPP2, OMA, ETSI/TISPAN, TM Forum 및 다른 표준 그룹들과의 협력
  - SOA 보안 개발을 위해 다른 ITU 연구그룹들 지원
- 통신망에서의 SOA 보안
  - 보안 요구사항, 위협 분석, 상호운용성 등 안전한 SOA 서비스 보안을 위한 프레임워크 정의
  - 사이버 공간에서 SOA 기술의 보호를 위해 ISP(Internet service provider), 망사업자 등 관련 주체들의 역할에 대한 연구
  - 분산 SOA 구현에서 보안성 확보와 관련 정책, 서비스 공유를 위한 기술 개발

특히, SOA 보안에 관련된 표준 개발을 위해 ITU-T SG2(운영 관리)의 Q.3(서비스 정의 및 운영 관리) 및 Q.5(네트워크 및 서비스 유지/관리)와 SG16(멀티미디어)의 Q.13(멀티미디어 응용 플랫폼 및 IPTV 종단 시스템)과의 협력을 추진하고 있다.

3.2 개발 표준 개발 현황

클라우드 컴퓨팅 서비스는 지능형 전력망인 스마트 그리드 서비스와 더불어 핵심 요소 기술로 보안 기술이 필수적으로 요구되는 가운데 2009년 9월 스위스 제네바에서 ITU-T SG17 회의가 개최되었으며, 이 회의에서 가장 중요한 논의 의제는 클라우드 컴퓨팅 보안, 스마트 그리드 보안, e-health 보안 등 새로운 보안 주제에 대한 국제 표준화 추진 방향에 관련된 내용이었다. 특히, 연구 방법, 연구시기, 연구 범위 등에 대하여 어떻게 표준화를 수행할 것인지에 대한 논의가 결정되어 SG17의 역할과 추진 방향을 결정하기 위한 전문가 그룹(CG, corresponding group)을 결성하고 텔레 컨퍼런스를 통해 SG17 Q.6에서 스마트 그리드, Q.7에서 e-health 보안, Q.8에서 클라우드 컴퓨팅 보안을 추진하고 각 주제에 대해 전문가 그룹 활동의 적극적인 참여를 권유하고 기고서 제출 격려에 합의하였다. [표 2]에서는 ITU-T SG17 Q.8에서 추진중인 표준화 현황을 나타내고 있다.

현재 Q.8에서는 클라우드 컴퓨팅과 관련된 보안 모

〔표 2〕 ITU-T SG17 Q.8 표준초안 현황(총 3건)

No	국제표준번호	제정시기	국제표준명(제목)	제안국가	국내표준
1	X.ccsec[15]	2012-03	Security guideline for cloud computing in telecommunication area	중국	X
2	X.srfctse[16]	2012-03	Security requirements and framework of cloud based telecommunication service environment	중국	X
3	X.fsspvn[17]	2012-09	Framework of the service platform for virtual network	중국	X

델 및 프레임워크에 대한 표준화가 진행 중에 있다. 클라우드 컴퓨팅의 경우 2010년 2월 ITU-T TSAG (Telecommunication Standardization Advisory Group) 회의를 통하여 클라우드 컴퓨팅에 대한 포커스 (Focus Group) 그룹을 신설하였다. 신설된 그룹은 기존의 ITU-T SG 활동과는 차별화된 형태로 ITU-T의 기술적 이슈를 분석하고 표준화가 가능한 아이템들을 도출하기 위한 선행 연구를 수행하도록 하였다.

ITU-T 클라우드 컴퓨팅 포커스 그룹은 의장으로 Vladimir Belenkovich(러시아), 부의장에 Jamil Chawki (프랑스), 이강찬(한국), Mingdong Li(중국), Monique Morrow(미국), Koji Nakao(일본)으로 구성되었으며, 주요 의제는 다음과 같다.

- 클라우드 컴퓨팅 정의와 분류체계
- 통신과 ICT(Information & Communication Technology) 관점에서 클라우드 컴퓨팅을 지원하기 위한 활용사례(use case)와 참조모델(reference model) 개발
- 클라우드 컴퓨팅의 통신과 ICT 관점에서의 비전과 가치 정립
- 통신과 ICT 입장에서 클라우드 컴퓨팅을 통한 이점
- 클라우드 컴퓨팅 에너지와 그린하우스 관점에서의 갭 분석
- 통신과 ICT의 네트워킹 요구사항 기능과 클라우드 컴퓨팅 서비스/응용(유·무선) 지원을 위한 기능 분석
- 통신과 ICT가 클라우드 컴퓨팅 표준화를 지원하기 위한 ITU-T 표준들 간의 이해격차 분석 (클라우드 컴퓨팅 표준화 분석 포함)
- 클라우드 컴퓨팅 관련 ITU-T 권고 개발을 위한 로드맵 개발

Q.8에서는 클라우드 컴퓨팅 포커스 그룹과 연계하여 보안과 연계된 가이드라인 및 프레임워크에 대한 표준이 진행 중에 있으며, 이는 다음과 같다.

- 클라우드 컴퓨팅 보안

- Telecommunication 영역의 클라우드 컴퓨팅에 대한 보안 가이드라인 제안
- 클라우드 기반 통신 서비스 제공자에 의해 서비스가 요청 될 경우 사용자 로그인 과정의 서로 다른 매커니즘이나 표준 형태를 분산된 클라우드 기반 통신의 최종 개체에 적용시키기 위한 연구
- 클라우드 기반 통신 서비스 기반 구조의 보안에 대한 등장 배경과 CTSE(Cloud based-Telecommunication Service Environment)의 보안 매커니즘 개발 및 참조에 대한 내용을 기술
- Complex NAT 기반의 보안 서비스 플랫폼의 프레임워크와 새로운 연구 제안
- X.ccsec를 위한 서비스 기반구조에 대한 제안

Ⅳ. 결론 및 향후 전망

본 논문에서는 ITU-T SG17 Q.7과 Q.8에서 신규회기(2009~2012)동안 추진되어온 표준화 현황을 살펴보았다. Q.7의 경우 안전한 응용서비스 보호를 위한 표준 개발을 주도하고 있다. 특히, 2010년 ITU-T SG17 Q.7 정기회의에서 제시되었던 '응용보안 분야에서 필요한 표준 아이템'[18]에서 제시되었던 바와 같이 다양한 ICT기술에서 아직까지 다루어지지 않고 있는 표준 이슈들이 존재하고 있다. 이러한 측면을 고려하여 ICT기술의 개발 동향과 타 연구그룹의 표준화 동향에 맞추어 향후 표준화 아이템이 도출될 수 있어야 할 것이다.

Q.8의 경우 최근 클라우드 컴퓨팅 보안에 대한 표준 초안이 개발되고 있으며, 이에 대한 국내의 대응 활동도 필요한 시점이다. SG17 Q.8과는 별도로 2010년 4월 ITU-T SG13(미래네트워크) Q.23(클라우드 컴퓨팅 표준작업반)이 신설되어 국내의 ITU-T에서의 클라우드

컴퓨팅에 대한 전략적이고 적극적인 대응이 필요하다. 특히, 보안 기술에 대한 세부적인 기술적 명세를 위하여 ITU-T SG13 Q.23 및 기타 관련 표준 연구과제에서 개발하는 세부 명세를 참조 하는 등의 병행 전략이 당분간 필요할 것으로 사료된다.

참고문헌

[1] 오흥룡, 나재훈, 염흥열, 김대경, “ITU-T SG17 Q.9 (안전한 통신 서비스) 국제표준화 동향 및 향후 전망”, 정보보호학회지, 제18권 4호, 2008.

[2] 오흥룡, 염흥열, “안전한 통신 서비스 표준화 동향 및 향후 전망”, 정보보호학회지, 제17권 1호, 2007.

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

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

[5] ITU-T Recommendation X.1143, "Security Architecture for Message Security in Mobile Web Services", ITU-T SG17, November 2007.

[6] ITU-T Recommendation X.1151, "Guideline on secure password-based authentication protocol with key exchange", ITU-T SG17, November 2007.

[7] ITU-T Recommendation X.1152, "Secure end-to-end data communication techniques using Trusted Third Party services", May 2008.

[8] ITU-T Recommendation X.1153, "The management framework for One Time Password based authentication service", January 2011.

[9] ITU-T Recommendation X.1161, "Framework for secure peer-to-peer communications", May 2008.

[10] ITU-T Recommendation X.1162, "Security architecture and operations for peer-to-peer network", May 2008.

[11] Tadashi Kaji, and Hyungjin Lim, "The revised draft text of X.sap-4: The general framework of combined authentication on multiple identity service provider environment", ITU-T SG17, TD 1328, Dec. 2010.

[12] SokJoon Lee, "Draft Recommendation X.sap-5, Guideline of Anonymous Authentication for e-Commerce Service", ITU-T SG17, TD1094, Jul. 2010.

[13] Minpeng Qi, Lijun Liu, Zhaoji Lin, and Hongwei Luo, "The draft Recommendation for X. p2p-3: Security requirements and mechanisms of P2P-based telecommunication network", ITU-T SG17, TD1418, Dec. 2010.

[14] Daehee Seo, "Draft text on X.websec-4: Security framework for enhanced web based telecommunication services", ITU-T SG17, TD1303, Dec. 2010.

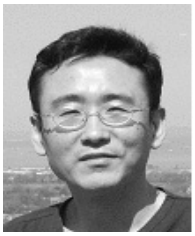
[15] Huirong Tian, Liang Wei, and Shitong Wang, "Draft text of X.ccsec : Security guideline for cloud computing in telecommunication area", ITU-T SG17, TD1349, Dec. 2010.

[16] Shitong Wang, and Huirong Tian, "Draft text of X.srfctse : Security Requirements and Framework of Cloud Based Telecommunication Service Environment", ITU-T SG17, TD1361, Dec. 2010.

[17] Jun Shen, Min Huang, Yuchen Wang, and Huirong Tian, "Draft text of X.fsspvn : Framework of the Secure Service Platform for Virtual Network", ITU-T SG17, TD1363, Dec. 2010.

[18] Jaehoon Nah, Yutaka Miyake, and Tadashi Kaji, "Document for discussing missing parts of standardization in application security area", ITU-T SG17, TD0726, Apr. 2010.

〈著者紹介〉



임 형 진 (Hyung-Jin Lim)
정회원
1998년 2월 : 한림대학교 컴퓨터공학과 졸업 (학사)
2006년 8월 : 성균관대학교 컴퓨터공학과 졸업 (석사, 박사)
2007년 10월~현재 : 금융보안연구원 책임연구원
2008년 10월~2010년 12월: ITU-T X.1153 에디터
2009년~현재: 방송통신위원회 위촉 IT 국제표준전문가
2009년 1월~현재: ITU-T SG17 국내 분과위원회 위원
2010년 2월~현재: ITU-T X.sap-4 에디터
<관심분야> 신뢰 플랫폼 응용 서비스, 응용 서비스 보안/관리, 금융정보보호

서 대 희 (Dae-Hee Seo)
정회원
2003년 2월 : 순천향대학교 전산학과 졸업(석사)
2006년 2월: 순천향대학교 대학원 전산학과 졸업(박사)
2007년: Howard University Post-Doc.
2007년 5월~2007년 12월: 한국정보 보호진흥원
2008년 7월~2009년 9월: 이화여자 대학교 컴퓨터공학과 연구교수
2009년10월~현재: 한국전자통신연구원 선임연구원
2009년~현재: ITU-T X.websec-4 에디터
2009년 1월~현재: ITU-T SG17 국내 분과위원회 위원
<관심분야> 네트워크 보안, 소형 디바이스 보안, 오버레이 네트워크, 공격자 추적

나 재 훈 (Jae-Hoon Nah)
정회원
1985년 2월 : 중앙대학교 컴퓨터공학과 졸업
1987년 2월: 중앙대학교 컴퓨터공학과 석사
2005년 2월: 한국외국어대학교 전자 정보공학과 박사
1987년2월~현재: 한국전자통신 연구원 책임연구원
2003년~현재: 방송통신위원회 위촉 IT 국제표준전문가
2005년10월~현재:ITU-T SG17 에디터
2008년12월~현재: ITU-T SG17 Q.7 래포처
2009년2월~현재: ITU-T SG17 국내 분과위원회 부의장
<관심분야> 네트워크 보안, IPv6/MIPv6 보안, P2P 보안, 스마트TV 보안, 웹서비스 보안