http://dx.doi.org/10.14400/JDC.2015.13.12.193

네트워크의 보안성 강화를 위한 표준 정보보호 기술 분석

김봉한
청주대학교 컴퓨터정보공학과

Analysis of Standard Security Technology for Security of the Network

Bong-Han Kim
Dept. of Computer & Information Engineering, CheongJu University

요 약 인터넷 어플리케이션에서 다양한 정보보호 서비스를 제공할 수 있는 정보보호 솔루션의 개발이 시급하다. 이러한 정보보호 솔루션 개발을 위해서, 국제 표준 정보보호 기술에 대한 분석이 필수적으로 필요하다. 본 논문에서는 ISO/IEC JTC1 SC27, ITU-T SG-17, IETF Security Area 등 국제 표준화기구의 정보보호 기술 현황과 국제 표준으로 등록된 정보보호 기술을 분석하였다. 이 중에서 인터넷에 관련된 정보보호 기술을 중점적으로 개발하고 있는 IETF Security Area의 18개 워킹 그룹을 중심으로, 어플리케이션 브리징, DNS 기반 인증, HTTP 인증, IP 보안, 자바스크립트 보안, 차세대 인증, 보안사고 관리, 웹 인증 프로토콜, 보안 자동화, 전송 층 보안 등 최신 표준 정보보호 기술의 핵심내용을 분석하였다.

주제어 : 정보보호, 표준기술, 표준화, ISO/IEC JCT1 SC27, ITU-T, IETF, RFC

Abstract The development of the security solutions that can provide a variety of security services is needed urgently. For development of the security solutions, analysis of international standard security technology is the key. In this paper, international organizations' standardization(ISO/IEC JTC1 SC27, ITU-T SG-17, IETF Security Area, etc.) and the current trend of the standard security technology are mainly analyzed. The core of the latest security technology(Application Bridging, DNS-based Authentication, HTTP Authentication, IP Security, Javascript Security, Authentication Technology Next Generation, Managed Incident, Web Authorization Protocol, Security Automation, Transport Layer Security, etc.) is analyzed focusing on 18 working groups of the IETF.

Key Words : Security, Standard Technology, Standard, ISO/IEC JCT1 SC27, ITU-T, IETF, RFC

1. 서론

다양한 인터넷 접속 환경, 인터넷 사용 인구의 증가 그리고 사물에 의한 인터넷 접속 요구로 인해 TCP/IP 프로토콜은 IT 및 통신 분야의 핵심 기술로 등장하였다. 이러한 기술은 기존의 통신 장치 및 어플리케이션 뿐만 아니라 스마트 모바일 장치, 모바일 어플리케이션 등 관련 시장을 급격하게 성장시켰다. 그러나 이러한 성장과 같이,

* 이 논문은 2014-2015학년도 청주대학교 산업과학연구소가 지원한 학술연구조성비(특별연구과제)에 의해 연구되었음

Received 23 October 2015, Revised 28 November 2015
Accepted 20 December 2015
Corresponding Author: Bong-Han Kim
(Dept. of Computer & Information Engineering, CheongJu University)
Email: bhkim@cju.ac.kr

ISSN: 1738-1916

프라이버시 유출, 시스템 파괴, 바이러스 배포 등 악의적인 사용자에 의한 해킹의 피해도 늘어나고 있는 실정이다. 이러한 불법적인 공격 및 사용을 방지하고 대비하기 위해서는 국제적으로 통용될 수 있는 표준 정보보호 기술이 필요하게 되었다. 따라서 국내외의 많은 전문가들은 ISO/IEC JTC1 SC27, ITU-T SG17, IETF Security 영역 등과 같은 국제 표준화 기구를 통해, 다양한 최신 정보보호 기술을 개발하고 이를 국제 표준으로 등록하고 있으며, 이러한 표준화 문서들의 정보보호 기술을 시스템 및 네트워크, 어플리케이션에 적용하여 다양한 정보보호 솔루션을 개발하고 발전시키고 있다.

본 논문에서는 대표적인 국제 표준화 기구인 ISO/IEC JTC1 SC27, ITU-T SG17, IETF Security Area의 표준화에서 진행하고 있는 정보보호 기술의 동향을 분석하고 그 중에서 인터넷에 관련된 정보보호 기술을 중점적으로 개발하고 있는 IETF Security Area의 워킹 그룹을 중심으로 최신 표준 정보보호 기술의 내용을 분석하고자 한다.

2. ISO/IEC와 ITU-T의 정보보호

본 장에서는 대표적인 국제 정보보호 표준화 기구인 ISO/IEC JTC1 SC27, ITU-T SG17의 정보보호 기술의 표준화 진행 현황을 분석한다.

2.1 ISO/IEC JTC1 SC27

ISO/IEC JTC1 SC27은 ISO와 IEC가 공동으로 설립한 JTC1의 27번째 위원회이며, 암호화 기술의 국제표준을 담당하던 SC20(Cryptographic Techniques)의 표준화 기능을 확대하여 만들어졌다. 1989년 JTC1 총회에서 설립이 결정되어 1990년 4월 스웨덴에서의 창립총회를 통하여 조직, 범위 등이 갖추어졌다[1,2,3].

ISO/IEC JTC1 SC27은 2005년도까지는 3개의 워킹그룹이었으나, 2006년부터 5개의 워킹그룹으로 재구성 되었다. 매년 2회의 WG회의와 1회의 총회를 개최하고 있으며, 의장국인 독일을 포함하여 50개의 정 회원국과 20개의 옵서버 회원국이 활동하고 있다. 2016년 4월에 미국 플로리다 탬파에서 회의가 개최될 예정이다[4,5,6,11].

o WG1(정보보호 관리 시스템): ISMS(Information Security Management System) 이슈들에 대한 가이드라인 표준과 이를 기반으로 하는 서비스 적용 표준들을 개발하고 있다.

o WG2(암호 및 보안 메커니즘): 보안서비스 구현을 위해 적용되는 보안기술과 암호알고리즘에 대한 표준들을 개발하고 있다.

o WG3(보안평가기준): IT 보안성 보증 및 평가에 관한 표준들을 개발하고 있으며, 공통평가기준의 범위를 확장하여 인적, 관리적 부분을 평가하기 위한 표준들을 개발하고 있다.

o WG4(보안제어 및 서비스): 정보보호 시스템들의 접근제어 및 권한 관리를 위한 네트워크 보안과 사이버보안 등의 표준들을 개발하고 있다.

o WG5(아이덴티티 관리 및 프라이버시 보호 기술): ITU-T SG17과 협력하여, ID 관리 기술 및 네트워크 환경에서의 프라이버스 보호 기술들에 대한 표준들을 개발하고 있다.

<Table 1>에서는 ISO/IEC JTC1 SC27에서 개발이 완료된 정보보호 기술과 현재 개발 중인 정보보호 기술들의 수를 ISO 프로젝트 단계별 숫자코드로 표시하였다.

〈Table 1〉 Number of Published standards & Standards under development

STAGE	SUB-STAGE						
	00	20	60	90 Decision			
				92	93	98	99
00 Preliminary							
10 Proposal							25
20 Preparatory	2		1				1
30 Committee		3	18				
40 Enquiry		15	3				1
50 Approval	1		1				
60 Publication	4		89				
90 Review		8	1	23	28		
95 Withdrawal							
00: Registration, 20: Start of main action, 60: Completion of main action, 92: Repeat an earlier phase 93: Repeat current phase, 98: Abandon, 99: Proceed							

2.2 ITU-T SG17

ITU(International Telecommunication Union)는 1865년 5월에 UN 산하에 신설된 국제전기통신연합 기구로 전파규칙, 주파수 할당 등의 이슈를 다루고 있는 전파통신, 정보통신기술, 운용 및 요금 등의 이슈를 다루고 있는 정보통신, 개발도상국의 통신망 현대화를 위한 정책, 기

술적 지원 등을 다루고 있는 정보통신개발 부문으로 크게 3가지 부분으로 구분된다. 정보보호 표준화는 ITU-T 산하 10개의 연구그룹(SG: Study Group)중에서 SG 17에서 전담하고 있다. SG 17 연구그룹(Study Party)은 <Table 2>과 같이 5개의 작업반(WP1: 기초 보안, WP2: 네트워크와 정보 보안, WP3: 아이덴티티 관리와 클라우드 컴퓨팅 보안, WP4: 응용보안, WP1: 형식언어)과 12개의 연구과제로 구성되어 있다[7,9,10].

〈Table 2〉 Structure of ITU-T SG17

Study Party	Question	Title
WP1	Q1	Telecommunication/ICT security coordination
	Q2	Security architecture and framework
	Q3	Telecommunication information security management
WP2	Q4	Cybersecurity
	Q5	Countering spam by technical means
WP3	Q8	Cloud computing security
	Q10	Identity management architecture and mechanisms
WP4	Q6	Security aspects of ubiquitous telecommunication services
	Q7	Secure application services
	Q9	Telebiometrics
WP5	Q11	Generic technologies to support secure applications
	Q12	Formal languages for telecommunication software and testing

정보통신/ICT 조정(Q.1)은 ITU-T 내에 전체적인 보안 요약물, 전략, 비전, 계획 등을 연구하고 있으며, 정보보호 표준화 정보공유를 위한 워크숍 및 타 표준화 기구들과의 협력 체계 구축을 위한 작업들을 담당하고 있다. 보안구조 및 프레임워크(Q.2)는 보안시스템의 구조, 모델, 개념, 전반적인 서비스 시나리오 등을 연구하고 있으며, 개발도상국들을 위한 네트워크 기반인프라 구축을 위한 보안 가이드라인 표준을 개발하고 있다. 정보통신 정보보호관리(Q.3)는 정보통신 시스템을 위한 보안관리 표준들을 개발하고 있으며, ISO/IEC JTC1/SC27/WG1 그룹과 협력하여 ISMS, 개인정보보호 관리표준들을 개발하고 있다[8].

〈Table 3〉 Recommendations of ITU-T SG17

Series	Title	Recommendations Number
E	General provisions concerning Administrations	E.104, E.115
	International network management	E.409
F	The international telex service	F.85/F.421
	Message handling services	F.400/X.400, F.401, F.410, F.415, F.420, F.421/F.85, F.423, F.435, F.440, F.471, F.472
	Directory services	F.500, F.510, F.511, F.515
X	Open Systems Interconnection	X.200, X.207, X.210-219, X.220, X.222-229, X.233-237 bis, X.245-249, X.255-257, X.260, X.263, X.264, X.273, X.274, X.281-284, X.287, X.292
	Message Handling Systems	X.400/F.400, X.402, X.404, X.408, X.411-413, X.419-421, X.435, X.440, X.445, X.446, X.460, X.462, X.467, X.481-488
	Directory	X.500, X.501, X.509, X.511, X.518-521, X.525, X.530n
	OSI networking and system aspects	X.610, X.612-614, X.622, X.623, X.625, X.630, X.633, X.634, X.637-639, X.641, X.642, X.650, X.660, X.662, X.665-672, X.674, X.675, X.680-683, X.690-696
	Security	X.800, X.802, X.803, X.805, X.810-816, X.830-835, X.841-843
	OSI applications	X.851-853, X.860-863, X.880-882, X.891-893
	Open distributed processing	X.901-904, X.906, X.910, X.911, X.920, X.930, X.931, X.950, X.952, X.960
	Information and network security	X.1031-1037, X.1051, X.1052, X.1054-1057, X.1080.1-1084, X.1086, X.1088-1092
	Secure applications and services	X.1111-1114, X.1121-1125, X.1141-1144, X.1151-1159, X.1161-1164, X.1171, X.1191-1198
	Cyberspace security	X.1205-1211, X.1231, X.1240-1247, X.1250-1255, X.1275
	Secure applications and services	X.1303, X.1303 bis, X.1311-1314, X.1341
	Cybersecurity information exchange	X.1500, X.1500.1, X.1520, X.1521, X.1524-1526, X.1528-1528.4, X.1541, X.1544, X.1546, X.1570, X.1580-1582
	Cloud computing security	X.1601, X.1631
Z	Formal description techniques	Z.100-111, Z.119-121, Z.150, Z.151, Z.161-170
	Programming languages	Z.200
	Quality	Z.400, Z.450
	Middleware	Z.600, Z.601

사이버보안(Q.4)은 인터넷 및 네트워크 시스템 등에 발생할 수 있는 침해사고대응방법, 보안솔루션, 사이버보

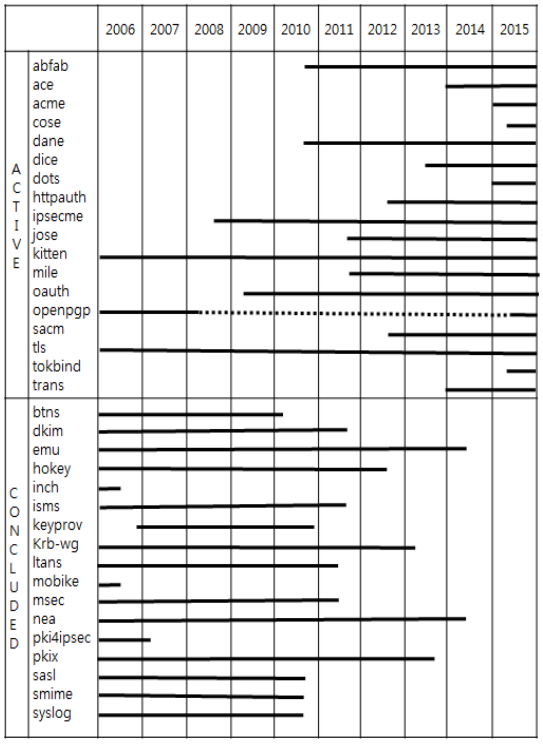
안 취약점들에 대한 해결방법 및 정보공유 방법 등을 개발하고 있다. 기술적인 방법에 의한 스팸대응(Q.5)은 한국과 중국을 중심으로 스팸대응을 위한 표준화를 연구하고 있으며, 크게 e-mail에 의한 스팸과 IP 멀티미디어 서비스에 의한 스팸, 단문서비스(SMS) 스팸을 분리하여 표준들을 개발하고 있다. 유비쿼터스 통신서비스 보안(Q.6)은 통신서비스 관점에서 IPTV 보안, USN 보안, 모바일 보안, 멀티캐스트 보안 표준을 개발하고 있다. 안전한 응용서비스 보안(Q.7)은 P2P 보안, 웹서비스 보안, 응용프로토콜 보안, TTP(Trusted Third Party)기반 인증 기술들을 중점적으로 다루고 있다. 클라우드 컴퓨팅 보안(Q.8)은 클라우드 기반의 정보통신 서비스 환경을 위한 보안요구사항 및 프레임워크, 정보통신 영역에서의 클라우드 컴퓨팅을 위한 보안 가이드라인, 가상네트워크를 위한 안전한 서비스 플랫폼 프레임워크 표준을 개발하고 있다[8].

텔레-바이오인식(Q.9)는 네트워크 환경에서 바이오정보를 응용하기 위한 표준초안들을 개발하고 있다. 특히, 전자상거래, e-헬스, CCTV 환경에서 프라이버시 보호 방법, 스마트폰에서 바이오정보를 탐재하기 위한 응용기술 및 바이오 하드웨어 보안 모듈에 대한 표준들을 개발하고 있다. 아이덴티티 관리 및 메커니즘(Q.10)은 아이덴티티에 대한 관리 기술과 이들을 기반으로 하는 인증 및 서비스, 네트워크 계층과 서비스 계층에서의 단일 인증 기술, 이기종 IDM 서비스에서의 상호운용성 확보 방법, 클라우드 컴퓨팅에서의 아이덴티티 관리 요구사항 정의에 대한 표준들을 개발하고 있다. 응용서비스 지원을 위한 일반적인 기술(Q.11)은 안전한 응용서비스들을 지원하기 위한 디렉터리 서비스, PKI, PMI, ASN.1, OID 기술들에 대한 표준을 개발하고 있다. 정보통신 소프트웨어 및 시험 형식 언어(Q.12)는 정보통신 시스템 설계 및 시험을 위해 사용되는 다양한 형식 언어에 대한 표준을 개발하고 있다. ITU-T SG 17은 <Table 3>와 같이, 다양한 정보보호 표준 기술에 대한 국제표준 권고안을 개발하고 있다[12].

3. IETF 정보보호

1986년에 신설된 IETF(Internet Engineering Task Force)는 인터넷 서비스의 품질을 보장하고 보다 향상된 인터넷 환경을 개발하기 위해 실무자들을 중심으로 구현 관점에서 사실표준화를 추진하고 있는 국제표준화 기구이다[1,13].

IETF는 어플리케이션과 실시간(Applications and Real-Time), 일반(Genera), 인터넷(Internet), 운영과 관리(Operations and Management), 라우팅(Routing), 정보보호(Security), 전송 (Transport)과 같이, 8개의 활동영역으로 구성되어 표준화가 개발되고 있다. 이중에서, 인터넷을 기반으로 하는 정보보호 기술은 정보보호 영역에서 담당하고 있으며, 2015년 현재 18개 워킹 그룹이 활동하고 있다. 정보보호 영역에서 다루고 있는 정보보호 분야는 웹 어플리케이션 정보보호, 웹 인증, 권한부여, 암호화, IP 정보보호 관리, DNS 기반 인증, 객체서명, 전송계층 정보보호, 토큰, 인터페이스, 전자메일 정보보호, 정보보호 자동화 및 모니터링, 공증 등의 인터넷과 관련된 정보보호 기술들을 개발하고 있다. [Fig. 1]은 지난 10년간의 IETF 정보보호 영역에서 구성된 워킹 그룹들의 변천과정을 보여주고 있다[14].



[Fig. 1] History of Active and Concluded Working Groups

4. 표준 정보보호 기술

본 장에서는 IETF 정보보호 영역의 워킹 그룹에서 개발하고 있는 정보보호 기술을 분석한다.

4.1 어플리케이션 브리징

abfab(Application Bridging for Federated Access Beyond web)는 다중 도메인에서 운영 주체에 대한 중복 등록을 방지하고 관리적 오버 헤드를 줄이고 개인 정보보호와 관련된 우려 사항과 일부 지역에서 규제 및 법적 요구사항을 해결하면서 사용성을 향상시킬 수 있는 기법을 개발하고 있다. 이 그룹에서는 인스턴스 IMAP, XMPP, SSH 및 NFS 등과 같이, HTML/HTTP를 기반으로 하지 않는 인터넷 프로토콜을 통해 사용되는 연합 ID 메커니즘을 기술하고 있다. 기존의 EAP(Extensible Authentication Protocol), AAA(Authentication, Authorization, Account)와 SAML(Security Assertion Markup Language)을 결합시킬 수 있는 방법을 설계하고 있다. abfab의 주요 정보보호 기술은 EAP를 위한 GSS-API 메커니즘이다. 이것은 EAP 메커니즘을 사용할 때, GSS-API(Generic Security Service Application Program Interface)를 구현하는 피어에 의해 사용되도록 프로토콜, 절차 및 협약 등을 정의한 기술이다. abfab는 <Table 4>와 같이, 3개의 정보보호 기술이 RFC로 등록되어 있다[15].

〈Table 4〉 RFCs in abfab

RFC	TITLE
RFC 7055	A GSS-API Mechanism for the Extensible Authentication Protocol
RFC 7056	Name Attributes for the GSS-API Extensible Authentication Protocol (EAP) Mechanism
RFC 7057	pdate to the Extensible Authentication Protocol (EAP) Applicability Statement for Application Bridging for Federated Access Beyond Web (ABFAB)

4.2 DNS 기반 인증

dane(DNS-based Authentication of Named Entities)은 인터넷 애플리케이션이 DNS에서 사용할 정보를 이용하여 암호화된 보안 통신을 수립할 수 있도록 하는 메커니즘과 기술들을 개발하고 있다. 도메인 이름에 키 정보를 결합하고 결합된 DNSSEC를 보호함으로서 어플리케이션은 서비스에 대한 인증키를 쉽게 발견할 수 있다. 이 그룹은 프로토콜 내에 dane과 dane과 같은 기능을 통합할 수 있는 방법을 개발하고 있으며 서비스의 위치를 표현하는 SRV를 사용하는 프로토콜에서도 dane를 사용할 것이다. 또한 SMTP, SMIME, OPENPGP, IPSEC, IMAP, POP에서도 dane를 사용할 것이다. dane은 현재까지 6개의 정보보호 기술이 RFC로 등록되어 있다. <Table 5>에서는 최근 2년간의 목록을 표시하였다[16].

〈Table 5〉 RFCs in dane

RFC	TITLE
RFC 7218	Adding Acronyms to Simplify Conversations about DNS-Based Authentication of Named Entities (DANE)
RFC 7671	The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance
RFC 7672	SMTP Security via Opportunistic DNS-Based Authentication of Named Entities(DANE) Transport Layer Security(TLS)
RFC 7673	Using DNS-Based Authentication of Named Entities (DANE) TLSA Records with SRV Records

4.3 HTTP 인증

현재의 HTTP 인증 메커니즘은 평문으로 인증서를 전달하거나 약한 알고리즘을 사용하고 있어 보안에 취약하다. 따라서 TLS에 의존하지 않고 HTTP 인증을 대체하거나 보강할 수 있는 메커니즘의 개발이 시급하다. httpauth(Hypertext Transfer Protocol Authentication)은 디지털 서명 기반의 HOBA(HTTP Origin-Bound Authentication)기술, HTTP 인증 메커니즘과 함께 이용할 수 있는 HTTP 다이제스트 인증 방식, Base64로를 사용하여 인코딩된 사용자 ID와 패스워드와 같은 인증서를 전송하는 HTTP 인증 기법을 개발하고 있다. httpauth은 <Table 6>와 같이, 3개의 정보보호 기술이 RFC로 등록되어 있다[17].

〈Table 6〉 RFCs in httpauth

RFC	TITLE
RFC 7486	HTTP Origin-Bound Authentication (HOBA)
RFC 7616	HTTP Digest Access Authentication Errata
RFC 7617	The 'Basic' HTTP Authentication Scheme Use Cases and Requirements for DNS-Based Authentication of Named Entities (DANE)

4.4 IP 보안

IP 보안은 IKEv1(RFC 2409), IKEv2(RFC 7296), IPsec

보안구조(RFC 4301)를 포함하고 있다. 또한 IP 보안은 VPN 게이트웨이, VPN 원격 액세스 클라이언트에서 널리 사용되고 있으며 호스트 대 호스트, 호스트 대 네트워크, 네트워크 대 네트워크 보안을 위한 기반구조로 사용되고 있다. ipsecme(IP Security Maintenance and Extensions) 그룹은 2005년에 종료된 IPsec 워킹 그룹의 작업을 계속해서 진행하고 있다.

ipsecme은 IPsec 표준 기술을 유지관리하고 IPsec에 대한 설명, 문제점 개선, 확장과 IKEv2에 대한 기술을 개발하고 있다. ipsecme은 현재까지 20개의 정보보호 기술이 RFC로 등록되어 있다. <Table 7>에서는 최근 1년간의 목록을 표시하였다[18].

〈Table 7〉 RFCs in ipsecme

RFC	TITLE
RFC 7427	Signature Authentication in the Internet Key Exchange Version 2(IKEv2)
RFC 7619	The NULL Authentication Method in the Internet Key Exchange Protocol Version 2(IKEv2)
RFC 7634	ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol(IKE) and IPsec

4.5 자바스크립트 보안

JSON(JavaScript Object Notation)은 RFC 4627에 기술된 구조화된 데이터의 직렬화를 위한 텍스트 형식이다. JSON 형식은 네트워크 연결을 통해 구조화된 데이터를 직렬화하고 전송하는데 사용된다. IETF 및 다른 표준화 기구의 프로토콜에서도 JSON의 사용이 증가하고 있으며, 암호화, 디지털 서명, MAC 알고리즘을 사용하여 JSON 형식으로 전달한다.

〈Table 8〉 RFCs in jose

RFC	TITLE
RFC 7515	JSON Web Signature(JWS)
RFC 7516	JSON Web Encryption(JWE)
RFC 7517	JSON Web Key(JWK)
RFC 7518	JSON Web Algorithms(JWA)
RFC 7520	Examples of Protecting Content Using JSON Object Signing and Encryption(JOSE)
RFC 7638	JSON Web Key(JWK) Thumbprint

jose(Javascript Object Signing and Encryption)은 잘 알려진 메시지 보안의 기본 요소에 기반을 두고(예; CMS) 에서 정보보호기술을 개발하고 있으며, 무결성 보호(서명, MAC) 및 암호화를 위한 메커니즘뿐만 아니라 JSON을 사용하는 프로토콜에 대한 보안 서비스의 호환성을 지원하는 키와 알고리즘 식별자의 형식을 표준화한다. jose은 현재까지 7개의 정보보호 기술이 RFC로 등록되어 있다. <Table 8>에서는 최근 1년간의 목록을 표시하였다[19].

4.6 차세대 인증

kitten(Common Authentication Technology Next Generation)은 GSS-API와 Kerberos 인증 시스템, 특정 GSS-API 보안 메커니즘을 개발하고 SASL(Simple Authentication and Security Layer)과 관련된 지침을 제공한다. 이 그룹은, GSS-API에 대한 확장 및 갱신, 인증서 관리에 대한 특정 항목, 재생 캐시 방지, 오류 보고, 분산된 수신자를 지원하기 위한 기법을 개발하고 있으며, Kerberos 프로토콜, 국제화에 관련된 항목, 새로운 초기 인증 유형, 권한 부여 프레임 워크 및 데이터, 재생 캐시 방지, 강화된 암호화, 제3자 인증을 이용한 호환성 및 ID 관리를 위한 기술을 개발하고 있다. kitten은 현재까지 16개의 정보보호 기술이 RFC로 등록되어 있다. <Table 9>에서는 최근 4년간의 목록을 표시하였다[20].

〈Table 9〉 RFCs in kitten

RFC	TITLE
RFC 6595	A Simple Authentication and Security Layer (SASL) and GSS-API Mechanism for the Security Assertion Markup Language (SAML)
RFC 6616	A Simple Authentication and Security Layer (SASL) and Generic Security Service Application Program Interface(GSS-API) Mechanism for OpenID
RFC 6680	Generic Security Service Application Programming Interface(GSS-API) Naming Extensions Errata
RFC 7546	Structure of the Generic Security Service(GSS) Negotiation Loop
RFC 7628	A Set of Simple Authentication and Security Layer (SASL) Mechanisms for OAuth

4.7 보안사고 관리

보안사고(잘못된 시스템 구성, IT 사고, 시스템 손상, 사회 공학적 피싱 공격, 서비스 거부 공격 등)는 IT 기반 구조에서 예기치 못하게 발생할 수 있다. 사고가 감지, 또는 의심되는 경우, 공동 분석, 정보 배포, 통합된 운영 대응과 같은 공동 작업이 요구된다. 따라서 보안사고 또는

위협과 관련된 손상의 지표를 함께 공유함으로서, 사전에 보안 사고를 방어할 있다.

mile(Managed Incident Lightweight Exchange)은 컴퓨터 및 네트워크 보안사고 관리를 지원하는 표준을 개발한다. 이 그룹은 IODEF(Incident Object Description Exchange Format와 RID(Real-time Inter-network Defense) 기술을 개발하고 있다. IODEF는 컴퓨터 및 네트워크 보안 사고를 나타내는 정보 프레임워크를 정의한다. 관련 기술은 RFC 5070, RFC 5091, RFC 6484에 기술되어 있다. RID는 컴퓨터 및 네트워크 보안 사고의 공유를 원활하게 하도록 프로토콜을 정의한다. 관련 기술은 RFC 6545, RFC 6546에 기술되어 있다. mile은 현재까지 6개의 정보보호 기술이 RFC로 등록되어 있다. <Table 10>에서는 최근 2년간의 목록을 표시하였다[21].

〈Table 10〉 RFCs in mile

RFC	TITLE
RFC 7203	An Incident Object Description Exchange Format (IODEF) Extension for Structured Cybersecurity Information
RFC 7495	Enumeration Reference Format for the Incident Object Description Exchange Format(IODEF)

4.7 웹 인증 프로토콜

웹 인증 프로토콜은 사용자가 인증서나 ID를 노출하지 않고 제3의 웹사이트나 어플리케이션이 사용자의 보호된 자원에 대한 접근을 허가하도록 하는 프로토콜이다. 예를 들어, 웹 인증 프로토콜을 지원하는 사진 공유 사이트는 제3의 사진 출력 사이트가 사용자의 계정에 대한 완전한 제어권을 획득하지 않거나 사진 공유 사이트의 인증서를 출력 사이트와 공유하지 않더라도 사용자의 사진을 출력하도록 허가할 수 있다. 웹 인증 프로토콜은 인증 서버를 발견하도록 클라이언트를 허용하는 방법, 자원 소유자의 동의를 이용하여 인증 서버에서 인증 토큰을 획득하기 위한 프로토콜, 자원에 접근하기 위해 보호된 자원에게 인증 토큰을 제시하기 위한 프로토콜, 보안 및 프라이버시에서 데이터 공유를 포함한다.

oauth(Web Authorization Protocol)는 보호 자원에 접근하기 위해서 인증 토큰을 제시하는 보안 체계를 개발하였다. 이것은 기존의 ID 관리 솔루션과 연동하는 MAC 접근 인증 및 SAML이 유지되는 작업뿐만 아니라 베어러 토큰의 발행에도 사용된다. oauth는 현재까지 13개의 정보보호 기술이 RFC로 등록되어 있다. <Table 11>에서는 최근 2년간의 목록을 표시하였다[22].

〈Table 11〉 RFCs in oauth

RFC	TITLE
RFC 7519	JSON Web Token(JWT)
RFC 7521	Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants
RFC 7522	Security Assertion Markup Language(SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants
RFC 7523	JSON Web Token(JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants
RFC 7591	OAuth 2.0 Dynamic Client Registration Protocol
RFC 7592	OAuth 2.0 Dynamic Client Registration Management Protocol
RFC 7636	roof Key for Code Exchange by OAuth Public Clients
RFC 7662	OAuth 2.0 Token Introspection

4.8 보안 자동화

규모가 큰 조직에서 정보와 시스템을 안전하게 저장하고 처리하고 전송하는 것은 매우 어려운 작업이다. 따라서 많은 보안 실무자는 이와 같은 일을 수동으로 처리하는데 많은 시간을 허비한다. 시스템 보안 구성을 수집하고 검증하고 업데이트하는 표준화된 프로토콜들은 이러한 과정을 자동화시킨다.

sacm(Security Automation and Continuous Monitoring)은 종단 상태를 평가할 수 있는 표준, 종단 상태를 평가하는데 관련된 콘텐츠의 저장소와 상호작용을 위한 표준을 정의한다. 또한 이 그룹은 SACM 구조, 종단 데이터 상태에 대한 정보 모델, 데이터 수집 및 분석을 위한 구성과 정책 정보를 검색하기 위한 프로토콜 및 데이터 형식, 실제 종단 상태를 수집하기 위한 프로토콜 및 데이터 형식에 대한 기술을 개발하고 있다. sacm은 1개의 정보보호 기술이 RFC 7632 'Endpoint Security Posture Assessment: Enterprise Use Cases'로 등록되어 있다[23].

4.9 전송 층 보안

tls(Transport Layer Security)는 전송 층의 보안 프로토콜을 표준화하기 위해 1996년에 개설되었으며, SSL 3.0(RFC 6101)을 기초하여, 프로토콜과 암호 집합의 확장뿐만 아니라 TLS 프로토콜 v1.0(RFC 2246), v1.1(RFC

4346), v1.2 (RFC 5346) 그리고 DTLS(Datagram TLS) v1.0(RFC 4347), v1.2(RFC 5346)를 개발하였다.

이 그룹의 주요 목표는 수동 및 능동 공격자가 관찰할 수 있는 데이터의 양을 줄이기 위해 많은 핸드셰이크 프로토콜을 암호화할 수 있는 모드와 주로 HTTP 기반의 어플리케이션을 지원하며, 핸드셰이크 지연시간을 줄일 수 있는 모드를 개발하고 있다. 또한 CBC 블록 암호 모드에서 알려진 약점을 해결하고 RC4를 대체할 수 있는 레코드 페이로드 보호 암호화 메커니즘과 알고리즘을 업데이트한다. tls는 현재까지 36개의 정보보호 기술이 RFC로 등록되어 있다. <Table 12>에서는 2005년에 등록된 목록을 표시하였다[24].

〈Table 12〉 RFCs in tls

RFC	TITLE
RFC 7465	Prohibiting RC4 Cipher Suites
RFC 7507	TLS Fallback Signaling Cipher Suite Value(SCSV) for Preventing Protocol Downgrade Attacks
RFC 7568	Deprecating Secure Sockets Layer Version 3.0
RFC 7627	Transport Layer Security(TLS) Session Hash and Extended Master Secret Extension
RFC 7685	A Transport Layer Security(TLS) ClientHello Padding Extension

4.10 기타

인증과 권한부여(ace: Authentication & Authorization for Constrained Environments)는 제한적인 환경에서 URI에 의해 식별된 자원들과 리소스 서버에 호스트된 자원들에게 허가된 접근(Get, Put, Post, Delete)이 가능하도록 인증과 허가를 위한 표준화된 솔루션을 생산할 수 있는 기술을 제공하며, 2개의 인터넷 드래프트가 개발 중에 있다.

자동화된 인증서 관리(acme: Automated Certificate Management Environment)는 일반적으로 인터넷 응용 프로그램(웹서버)을 위한 인증서 발행에는 인증기관을 통해 많은 수동적인 신원 확인 단계가 필요하다. 따라서 이 그룹에서는 식별자 제어 검증, 인증서 발급, 인증서 갱신 및 해지를 포함한 자동화된 X.509 인증서 관리를 위해 협약을 제공하며, 1개의 인터넷 드래프트가 개발 중에 있다.

CBOR 객체 서명과 암호화(cose: CBOR Object Signing and Encryption)는 CBOR(Concise Binary Object Representation) 기반 객체 서명 및 암호화 형식을 개발한다. CBOR은 JSON 데이터 모델의 확장 버전으로 구조화된 데이터의 직렬화에 대한 간략한 바이너리 형식이다. 1개의 인터넷 드래프트가 개발 중에 있다.

데이터그램 전송 층 보안(dice: DTLS In Constrained Environments)은 제한된 장치(메모리, 알고리즘 선택) 및 제한된 네트워크(PDU 크기, 패킷 손실)등과 같은 제한된 환경에서 DTLS(Datagram Transport Layer Security) 전송 계층 보안을 사용하기 위한 DTLS 프로파일 정의, DTLS 핸드셰이크, DTLS 레코드 기술을 제공하며, 1개의 인터넷 드래프트가 개발 중에 있다.

DDoS 신호 탐지((dots: DDoS Open Threat Signaling)는 DDoS 공격 탐지, 분류, 추적 및 차단과 관련된 요소들 사이에서 요청과 데이터를 다루는 원격측정 및 위협에 관련된 DDoS의 실시간 신호에 접근할 수 있는 기술을 제공하며, 2개의 인터넷 드래프트가 개발 중에 있다.

NSF는 원치 않는 네트워크 활동을 검출하거나 차단하기 위해, 통신 네트워크의 무결성, 기밀성, 가용성을 보장하기 위해 사용되는 기술이다. i2nsf(Interface to Network Security Functions)는 물리적 NSF와 가상적 NSF의 제어와 모니터링을 위한 소프트웨어 인터페이스 및 데이터 모델 집합을 개발 중에 있으며 아직 인터넷 드래프트가 없다.

전자메일 보안(openpgp: Open Specification for Pretty Good Privacy)은 객체 암호화, 객체 서명 및 ID 인증을 다루는 인터넷 표준이다. OpenPGP는 1997년 9월 개설되었다가 2008년 3월에 종료되었다. 그리고 2015년 6월에 다시 개설되었다. 이 그룹은 전자 우편이나 다른 전송 프로토콜을 통해 MIME 프레임워크를 제공하거나 PGP의 알고리즘과 형식에 대한 IETF 표준을 개발하고 있다.

웹 어플리케이션이 보호된 자원에 접근하기 위해서, 웹 서비스는 다양한 보안 토큰(HTTP 쿠키, OAuth 토큰 등)을 생성한다. 토큰 바인딩(tokbind: Token Binding)은 클라이언트와의 비밀성을 유지하기 위해 암호적인 바인딩 보안 토큰을 사용하여 공격을 방어를 할 수 있다. 현재, 3개의 인터넷 드래프트가 개발 중에 있다.

많은 인터넷 프로토콜(SMTPS, IPsec, DNSSEC, OpenPGP, HTTPS)은 식별자와 공개키 간에 매핑을 요구한다. 공증(trans: Public Notary Transparency)은

TLS를 통한 HTTP에 대한 실험적인 RFC 6962의 표준을 개발하고 그 규격이 개발된 후에 구현, 배포, 사용 등에 관해 설명하고 있다. 3개의 인터넷 드래프트가 개발 중에 있다.

5. 결론

유선 플랫폼 및 모바일 플랫폼을 통한 인터넷 접속 환경의 다양성과 인터넷 서비스에 대한 많은 요구사항으로 인해 서버 및 클라이언트 간에 전송되는 데이터의 양은 증가하고 있다 또한 이러한 통신 기반을 이용하는 많은 인터넷 사용자들로 인해 전송되는 데이터의 위협 사례도 증가하고 있다. 이러한 데이터의 위협으로부터, 기밀성, 무결성, 인증, 액세스 제어 등 다양한 정보보호 서비스를 제공하기 위한 정보보호 솔루션 개발이 시급한 실정이다. 따라서 이러한 정보보호 솔루션 개발을 위해서 국제적으로 인정되는 정보보호 기술의 분석은 필수적으로 요구된다.

본 논문에서는 ISO/IEC JTC1 SC27, ITU-T SG-17, IETF Security Area 등 국제 표준화기구를 중심으로 정보보호 기술의 현황과 국제 표준으로 등록된 정보보호 기술을 분석하였다. 이 중에서 인터넷에 관련된 정보보호 기술을 중점적으로 개발하고 있는 IETF의 18개 워킹 그룹을 중심으로, 어플리케이션 브리징, DNS 기반 인증, HTTP 인증, IP 보안, 자바스크립트 보안, 차세대 인증, 보안사고 관리, 웹 인증 프로토콜, 보안 자동화, 전송 층 보안 등 최신 표준 정보보호 기술의 핵심내용을 분석하였다.

ACKNOWLEDGMENTS

This work was supported by the research grant of Cheongju University in 2014-2015.

REFERENCES

[1] Heung-Ryong Oh, Jeong Sik Park, Byoung-Moon Chin, Heung-Youl Youm, "Security International Standardization Status and Driven Systems Analysis", Review of KIISC, Korea Institute of Infomation Security and Cryptology, Vol.21 No.2, pp. 7-18, 2011

[2] Yong-Nyuo Shin, HakIl Kim, Myung-Geun Chun, "Personal Information Protection Reference Architecture and International Standardization Trend", Review of KIISC, Korea Institute of Infomation Security and Cryptology, Vol.21 No.5, pp. 12-20, 2011

[3] Kyeong Hee Oh, Jungduk Kim, Heung-Youl Youm, "A Trend on Security International Standardization", Review of KIISC, Korea Institute of Infomation Security and Cryptology, Vol.23 No.3, pp. 5-13, 2013

[4] Heung-Youl Youm, "An Analysis on Personal Information Protection International Standards", Review of KIISC, Korea Institute of Infomation Security and Cryptology, Vol.25 No.4, pp. 6-10, 2015

[5] Younghun Jeong, Jeonghwan Song, "A Trend on lightweight cryptography International Standardization in ISO/IEC JTC 1/SC 27 WG2", Review of KIISC, Korea Institute of Infomation Security and Cryptology, Vol.25 No.4, pp. 11-17, 2015

[6] Hyun-Sun Kang, "An Analysis of Information Security Management System and Certification Standard for Information Security", Journal of Security Engineering, JSE, Vol.11 No.6, pp. 455-468, 2014

[7] HeungYoul Youm, Heung-Ryong Oh, "A Trend on Security Technology and International Standardization(ITU-T SG17)", Review of KIISC, Korea Institute of Infomation Security and Cryptology, Vol.24 No.4, pp. 7-14, 2014

[8] Heung-Ryong Oh, Young-Hwa Kim, Heung-Youl Youm, "A Trend on ITU-T SG17(Security) International Standardization", OSIA Standards & Technology Review, Vol.27 No.2, pp. 8-20, 2014

[9] Jungduk Kim, "A Trend on Security Management International Standardization", Review of KIISC, Korea Institute of Infomation Security and Cryptology, Vol.21 No.2, pp. 19-22, 2011

[10] Heung Ryong Oh, Sungpil Yu, Youngwha Kim, "A trend on information security standardization in ITU-T SG17", Proceedings of the Winter Conference, KICS, Vol.2015 No.1, 2015
[11] ISO/IEC JTC1 SC27, http://www.iso.org/iso/iso_technical_committee?commid=45306
[12] ITU-T, http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx
[13] IETF, http://www.ietf.org/
[14] IETF Security Area, http://datatracker.ietf.org/wg/#sec
[15] abfab, http://datatracker.ietf.org/wg/abfab/docume nts .
[16] dane, http://datatracker.ietf.org/wg/dane/documen ts
[17] httpauth, http://datatracker.ietf.org/wg/httpauth/documents
[18] ipsecme, http://datatracker.ietf.org/wg/ipsecme/documents
[19] jose, http://datatracker.ietf.org/wg/jose/documents
[20] kitten, http://datatracker.ietf.org/wg/kitten/docume nts
[21] mile, http://datatracker.ietf.org/wg/mile/documents
[22] oauth, http://datatracker.ietf.org/wg/oauth/docume nts
[23] sacm, http://datatracker.ietf.org/wg/sacm/documen ts
[24] tls, http://datatracker.ietf.org/wg/tls/documents/

김 봉 한(Bong-Han, Kim)

- 1994년 2월 : 청주대학교 전자계산학과(공학사)
- 1996년 2월 : 한남대학교 전자계산공학과(공학석사)
- 2000년 2월 : 한남대학교 컴퓨터공학과(공학박사)
- 2001년 3월 ~ 현재 : 청주대학교 컴퓨터정보공학과 교수

- 관심분야 : 네트워크보안, 가상현실, 모바일 소프트웨어
- E-Mail : bhkim@cju.ac.kr