情 報 保 護 學 會 誌
第21卷 第2號, 2011. 4

IETF 국산 암호기술의 국제표준화 동향

윤 석 웅*

요 약

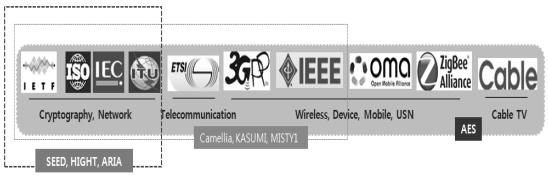
암호기술은 IT기반 다양한 응용서비스에서 정보의 안전한 처리를 위한 프리미티브 기술로써, 다양한 보안제품에 적용되어 활용되고 있다. 다양한 보안제품에 암호기술이 활용되기 위해서는 제품간 호환성을 보장해 줄 수 있는 표준화가 반드시 필요하며, 주로 외국의 주요 장비 제조업체들을 중심으로 표준화가 이루어져 오고 있다. 최근 국내에서도 공공・행정기관 인터넷전화 장비에 국산 암호기술 적용여부가 이슈가 되어 국산 암호기술의 국제표준화에 대한 중요성도 날로 커지고 있다. 본 논문에서는 국제 표준화단체인 IETF에서 추진되고 있는 국산 암호기술의 국제표준화 동향에 대해 살펴본다.

Ⅰ. 개 요

암호기술은 정보보호기술의 기반이 되는 기술로써 국방, 통신, 금융, 보건 등 정보의 안정성이 중요시되는 산업분야에서 정보의 저장・관리 및 송신 단계별로 기밀성 및 무결성, 사용자 인증 등을 위해 사용되고 있다. 최근에는 모바일 환경에 적합한 경량의 저전력 특성을 가지는 암호기술에 대한 연구 및 표준화도 활발히 진행되고 있다.

이러한 암호기술이 산업에 활용되기 위해서는 암호기술을 탑재한 제품의 호환성이 필수조건이라고 할 수 있으며, 호환성을 위해서 [그림 1]과 같이 다양한 국제표준화 기구에서 표준화가 진행되고 있다.

우리나라도 공공・행정기관 인터넷전화 서비스를 제공하면서 통화내용의 보호를 위해 국산 암호알고리즘인 ARIA만을 적용하려고 하였으나, 미국에서 WTO 무역기술장벽협정(Technical Barriers to Trade Agreement) [1] 을 이슈삼아 외교・안보부처에만 제한적으로 적용



〔그림 1〕 암호 알고리즘 표준화 현황

> *Article 2*
>
> 2.2 Members shall ensure that technical regulations are not prepared, adopted or applied with a view to or with the effect of creating unnecessary obstacles to international trade
>
> 2.5 Whenever a technical regulation is prepared, adopted or applied for one of the legitimate objectives explicitly mentioned in paragraph 2, and is in accordance with relevant international standards, it shall be rebuttably presumed not to create an unnecessary obstacle to international trade.

〔그림 2〕 WTO/TBT 조항

되고 있다. 이를 계기로 국제표준화의 중요성이 커지게 되었고, 현재는 한국인터넷진흥원(KISA) 및 국가보안기술연구소(NSRI)를 중심으로 국산 암호알고리즘의 표준화가 활발하게 추진 중에 있다.

본 논문에서는 각국에서 추진하고 있는 암호기술 표준화 동향 및 IETF(Internet Engineering Task Force)에서 추진 중인 국산 암호기술 표준화 동향을 살펴본다.

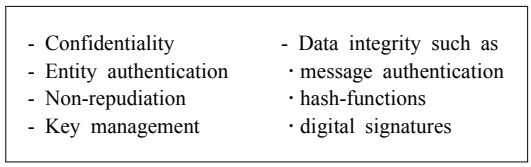
Ⅱ. 암호기술 국제표준화 현황

2.1. ISO/IEC JTC 1

국제 표준화 기구인 ISO/IEC JTC 1(Joint Technical

* 한국인터넷진흥원 인터넷침해대응센터 연구개발팀 (seokung@kisa.or.kr)

Committee 1: Information technology)에서는 SC27 (IT Security techniques) 분과위원회 내 WG2 (Working Group 2) 작업반에서 암호 기술에 대한 표준화가 이루어지고 있으며, WG2의 표준 제정 범위는 [그림 3]과 같다 [2].



〔그림 3〕 WG2 표준 제정 범위

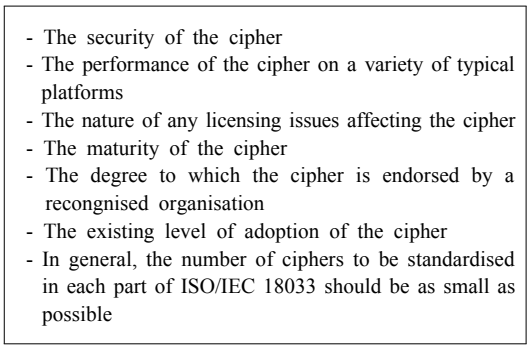
ISO/IEC는 2005년 제정된 18033-1를 통해 [그림 4]와 같은 7개의 암호 알고리즘 평가 기준 [2] 을 제시하고 있다. 이러한 평가기준에 따라 우리나라에서는 2005년도에 SEED가 표준으로 채택되었으며, 2011년에 HIGHT가 표준으로 채택되었다. ISO/IEC에서 채택한 블록 암호 알고리즘 현황은 다음과 같다.

■ 64-bit block ciphers: TDEA, MISTY1, HIGHT, CAST-128
■ 128-bit block ciphers: AES, CAMELLIA, SEED

2.2. IETF

IETF에서는 RFC3565(Encryption and Security Requirements)를 통해 보안이 필요한 서비스를 다음과 같이 정의하고 있다 [3].

■ Authentication service: A security service that verifies an identity claimed by or for an entity, be it a process, computer system, or person
■ Data confidentiality service: A security service that protects data against unauthorized disclosure to unauthorized individuals or processes
■ Data integrity service: A security service that protects against unauthorized changes to data, including both intentional change and accidental change, by ensuring that changes to data are detectable



〔그림 4〕 암호 알고리즘 평가 기준

암호기술 표준화는 보안 그룹(Security Area) 내 WG을 중심으로 이루어지고 있으며, 다양한 보안프로토콜에서 ISO/IEC, NIST(National Institute of Standards and Technology) 등에서 표준화된 암호기술의 적용 방법에 대한 표준화가 이루어지고 있다. 보안 그룹 내 WG에서 추진하고 있는 표준화 범위는 [표 1]과 같다. 최근에는 보안과 관련된 WG 뿐만 아니라 IT 기반 응용서비스와 관련된 WG에서 표준화를 진행하면서 동시에 보안을 고려하고 있는 추세이다. 또한 블록암호 알고리즘을 적용하기 위해 반드시 필요한 운영모드도 기존의 ECB(Electronic Code Book), CBC(Cipher Block Chaining), OFB(Output FeedBack), CFB(Cipher FeedBack)에서 실시간 환경으로의 변화에 따라 점차 CTR (Counter) [4], CCM(Counter with CBC-MAC) [5], GCM(Galois/Counter Mode) [6] 의 활용이 늘어나는 추세이다.

한편 제 78차 IETF 미팅(2010년 7월)에서는 IETF 보안 그룹 의장인 Tim Polk와 Sean Tuner에 의해 "Cipher Suite Proliferation"이 제안되었으며, 향후 암호와 관련된 표준 개발에 대한 방향성이 논의되었다. 그간 암호알고리즘 자체는 참조표준(Informational)으로 제정한 반면에 다양한 응용서비스에서의 암호 알고리즘은 특별한 기준이 없어 WG의 성향에 따라서 권고표준(Standard Track) 또는 참조표준으로 제각각 제정되었다. 그러나 향후에는 다음 두 가지를 경우를 제외하고는 참조표준(Informational)으로 진행할 예정이다.

■ WG에서 채택되어 올라오는 경우
(If the I-D came from a WG)
■ 국제적으로 널리 활용되는 알고리즘이거나, 구현

해야 할 필요성이 있는 경우
(If the cipher suite has broad international support and there's a need and implementation(s))

[표 1] IETF 보안 그룹 내 WG현황

WG	표준화 범위
abfab	IMAP, XMPP 등에서 사용되는 신원확인 메커니즘 표준화
dane	DNS 보안을 위한 공개키 기반의 인증 메커니즘 표준화
dkim	전자서명을 통한 도메인의 유효성 검증 표준화
emu	EAP 메소드 관련 키 관리, 인증 관련 표준화
hokey	핸드오프 과정에서 키의 재사용, 전달 등과 관련 절차 표준화
ipsecme	IPSec 프로토콜의 개선 및 키 관리 프로토콜인 IKE 표준화
isms	SNMP 프로토콜을 위한 통합 보안 모델 표준화
kitten	GSS-API의 확장 및 SASL의 사용과 관련된 가이드라인 표준화
krb-wg	Kerberos의 확장과 관련된 표준화
ltans	장기 전자서명의 요구사항, 데이터 구조 및 프로토콜 표준화
msec	인터넷상의 그룹 통신에서 사용되는 멀티캐스트 보안기술 표준화
nea	네트워크 엔드포인트 평가를 위한 정책, 요구사항 등 표준화
pkix	ITU-T X.509기반 PKI 적용과 관련된 표준화
tls	TLS 프로토콜 개선과 관련된 표준화

Ⅲ. IETF 국산 암호기술의 국제표준화 동향

본 장에서는 IETF에서 제정한 대표적인 보안 프로토콜인 TLS [7], IPSec [8], SRTP [9], DTLS [10] 에서 국산암호기술인 SEED, ARIA의 국제표준화 추진 동향에 대해 살펴본다.

3.1. TLS (Transport Layer Security)

TLS는 TCP상에서 클라이언트/서버 응용프로그램 간 통신과정에서 인증, 암호화를 통한 데이터의 기밀성을 유지시켜 주는 보안프로토콜이며, 2008년도에 최종적으로 TLS v1.2가 표준화 되었다. 공공·행정기관 인터넷전화에서도 TLS v1.2를 사용할 것을 권고하고 있으나 아직까지는 이 버전을 지원하는 라이브러리가 개발되고 있지 않으며, 개발된다 하더라도 실제 사용까지는 상당기간이 필요할 것으로 보여 당분간은 TLS v1.0이 사용될 것으로 예상된다. TLS에 적용되어 있는 암호기술 목록을 살펴보면 [표 2]와 같다.

〔표 2〕 TLS Cipher Suite

구분	목록	운영모드
암호 알고리즘	RC2	CBC
	IDEA	CBC
	DES, TDES	CBC
	AES 128/192/256	CBC, GCM
	CAMELLIA 128/192/256	CBC
	SEED	**CBC**
	ARIA 128/192/256 (진행중)	**CBC, GCM**
메시지 인증	SHA-1/256/384	-
	MD5	-

3.2. IPSec (IP Securiy)

IPSec은 네트워크 계층의 보안 프로토콜로써, 송신자의 인증을 허용하는 인증 헤더(AH: Authentication Header)와 인증 및 데이터 암호화를 함께 지원하는 ESP(Encapsulating Security Payload) 등 두 가지 보안 서비스를 제공하며 VPN(Virtual Private Network) 등에서 널리 활용된다.

〔표 3〕 IPSec Transform Identifiers

구분	목록
AH	MD5
	SHA-1/256/384/512
	RIPEMD
	RSA
	AES-XCBC-MAC
	AES/128/192/256-GMAC
ESP	DES/TDES
	RC4, RC5
	IDEA
	CASE
	BLOWFISH
	AES-CBC/CTR/CCM/GCM
	SEED-CBC, SEED-CTR/CCM/GCM(진행중)
	CAMELLIA-CBC

IPSec의 경우 IPSec연산에 사용되는 키를 교환할 수 있는 프로토콜인 IKE프로토콜[11] 과 함께 사용되며, 2004년도에 표준화가 완료된 IKEv2가 널리 쓰이고 있다. IKEv2프로토콜은 IKEv1에 비해 키교환 과정이 간소화 되어 모바일 환경에도 적용이 가능할 것으로 예상된다. 올해 2월에 보안 그룹 내 IPSECME WG에서 추진하고 있던 RFC 6071(IPSec and IKE Document Roadmap)이 표준화가 완료되면서 IPSec과 IKE 버전별로 필요한 암호 알고리즘 수준을 정리하였다[12]. IPSec에 적용되어 있는 암호 기술 목록은 [표 3]과 같다.

3.3. SRTP (Secure Real-time Transport Protocol)

SRTP는 인터넷전화 서비스 등에서 실시간으로 전송되는 음성 및 영상 데이터를 암·복호화하는데 사용되는 프로토콜이며, 공공·행정기관 인터넷전화 서비스에서 이슈가 된 보안프로토콜이다. SRTP에서의 SEED 사용표준은 2010년에 완료되었으며, ARIA는 2010년부터 표준화가 추진 중에 있다.

최근에는 암호키길이의 증가추세에 따라 AES를 중심으로 192/256 bits를 병행해서 사용할 수 있는 표준화가 진행 중에 있으며, SRTP에 적용되어 있는 암호기술 목록은 [표 4]와 같다.

〔표 4〕 SRTP Crypto Suites

구분	목록	운영모드
암호 알고리즘	AES 128, AES192/256(진행중)	CTR
		CCM, GCM(진행중)
	SEED	**CTR, CCM, GCM**
	ARIA (진행중)	**CTR, CCM, GCM (진행중)**

3.4. DTLS (Datagram Transport Layer Security)

DTLS는 UDP상에서 TLS와 같이 클라이언트/서버 응용프로그램 간 통신과정에서 인증, 암호화를 통한 데이터의 기밀성을 유지시켜 주는 보안프로토콜이다. DTLS는 핸드쉐이크시 패킷 손신을 처리하기 위해 재전송 타이머를 사용하며, 단편화 문제를 해결하기 위해 UDP 데이터그램의 크기를 1500바이트 이내로 제한하고 있다. 또한 서비스 거부공격을 방지하기 위해 응답 메시지 내 쿠키를 포함시킨 것을 제외하고는 TLS와 동일한 절차 및 식별자를 갖는다.

국내 인터넷전화 제공 환경을 살펴보면 대부분 UDP 기반이기 때문에 2010년 5월에 표준화가 완료된 RFC 5764(DTLS Extention to Establish Keys for SRTP)는 중요한 의미를 갖는다고 할 수 있겠다[13]. 그간 인터넷전화 통화내용을 보호하기 위한 TLS를 지원하기 위해서는 장비를 변경해야 하는 부담이 있었는데 DTLS-SRTP 표준화가 완료되면서 바로 적용할 수 있는 기반이 마련되었다. DTLS-SRTP 표준에는 현재 AES만이 적용되어 있으므로, SEED 및 ARIA의 표준화가 시급할 것으로 생각되며, 현재 적용되어 있는 암호 기술 목록은 [표 5]와 같다.

〔표 5〕 DTLS-SRTP Protection Profiles

구분	목록	운영모드
암호 알고리즘	AES 128	CTR
메시지 인증	HMAC-SHA1	-

Ⅳ. 결 론

다양한 산업이 IT와 접목하면서 빠른 속도로 발전해 나가고 있는 현대의 정보사회에서는 정보보호의 중요성이 날로 커지고 있다. 이러한 정보보호의 핵심이 되는 기술이 바로 암호기술이라고 할 수 있다. 암호기술은 정보의 생산과 유통에 이르는 전 단계에서 적용될 수 있으며, 암호기술의 통일된 사용을 위해서는 국제표준화 역시 반드시 추진이 필요하다.

그간 우리나라는 2005년 ISO에서 SEED 알고리즘을 효시로 2011년 HIGHT 표준화를 완료되었다. 또한 IETF에서는 2005년부터 SEED알고리즘을 여러 보안 프로토콜에 적용하는 표준을 표준화시켜오고 있으며, ARIA역시 IETF에서 표준화 활동을 시작하고 있다. 작년부터 ITU-T에서도 역시 국산 암호기술을 적용하는 국제표준화가 진행 중에 있다.

그러나 IETF 경우를 살펴보면 새로운 보안 프로토콜의 표준화를 추진하거나, 기존 프로토콜을 업데이트하는 표준화를 추진 중에 있을 때 미국의 암호기술은 기본적으로 포함시키고 있는 반면에 다른 나라의 암호 기

술은 고려하지 않고 있다. 따라서 국내의 암호기술을 표준화 하는데 WG의 관심도 부족할 뿐만 아니라 추진과정에서도 어려움이 많이 따르는 게 현실이다. 또한 표준화를 산업에 적용시키는 데도 처음부터 적용하지 못하기 때문에 사장되어 버리는 경우도 발생할 우려가 있다.

앞으로도 암호 기술의 활용은 더 늘어날 것이다. 따라서 IETF 보안그룹에서 추진하고 있는 표준화 동향을 세심히 파악하고, 표준화 초기부터 국산 암호기술을 활용할 수 있도록 제안함으로써 표준화하는 노력도 줄이고 표준의 활용도도 극대화 시키는 전략이 필요하다.

참고문헌

[1] WTO/TBT, www.wto.org

[2] 한국인터넷진흥원, “정보보호기반기술 국제 표준화 동향 및 전망”, 2010.

[3] ISO/IEC 18033-1:2005/Amd 1:2011, “Information technology-- Security techniques--Encryption algorithm-- Part 1: General”.

[4] Dworkin, M., “Recommendation for Block Cipher Modes of Operation -- Methods and Techniques”, NIST Special Publication 800-38A, December 2001,

[5] Whiting, D., Housley, R., and N. Ferguson, "Counter with CBC-MAC (CCM)", RFC 3610, September 2003.

[6] Dworkin, M., "NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", U.S. National Institute of Standards and Technology.

[7] T. Dierks, E. Rescorla, "The Transport Layer Security(TLS) Protocol Version 1.2", RFC 5246, 2008.

[8] S. Kent, "IP Encapsulating Security Payload (ESP)", RFC 4303, 2005.

[9] M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman, "The Secure Real-time Transport Protocol(SRTP)", RFC 3711, 2004.

[10] E. Rescorla, N. Modadugu, "Datagram Transport Layer Security", RFC 4347, 2006.

[11] C.kaufman, "Internet Key Exchange (IKEv2) Protocol", RFC 4306, 2005.

[12] S. Frankel, S.Krishnan, "IPSec and IKE Document Roadmap", RFC 6071, 2011.

[13] D. McGrew, E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)", RFC 5764, 2010.

〈著者紹介〉

윤 석 웅 (Yoon Seokung)

1998년 2월 : 인하대학교 자동화공학과 학사
2003년 2월 : 인하대학교 전자계산공학과 석사
2003년 1월~2006년 8월 : 삼성전자 무선사업부 선임연구원
2006년 8월~현재 : 한국인터넷진흥원 인터넷침해대응센터 연구개발팀 책임연구원
2007~현재 : TTA PG503, 국내 SG17 분과위원회 위원
2009~현재 : ITU-T Q.5/17 부의장
관심분야 : VoIP, 암호, 정보보호