IETF OPENPGP WG의 표준화 동향 분석

박희운
한국정보보호진흥원 기술표준팀

The Analysis of Standardization in IETF OPENPGP WG

Hee-Un Park
Korea Information Security Agency

요 약

정보통신의 급속한 발전은 유무선 네트워크 및 컴퓨팅 환경에 대한 다양한 서비스를 제공하고 있다. 이중 가장 전자우편 서비스와 관련하여 현실적인 보안 취약성을 보완하기 위한 여러 가지 보안 서비스가 개발되고 제공되고 있다. 따라서 본 논문에서는 대표적인 전자우편 서비스인 PGP, PGP/MIME, OpenPGP에 대한 표준화에 대해 분석하고, 전자우편 서비스를 국내에 적용하기 위한 가이드라인을 제시하고자 한다.

1. 서론

전 세계적으로 유·무선 네트워크 및 컴퓨팅 환경의 발전으로 인해 인터넷과 관련된 다양한 서비스들이 제공되고 있다. 이중 많은 비중을 차지하고 있는 분야로 전자우편 서비스를 들 수 있다. 전자우편은 메시지 전송시 평문으로 전송이 되며, 전송과정에서 많은 노드들을 통과하게 된다. 이로 인하여 메시지의 노출과 변조, 전송 부인 등 다양한 공격으로부터 안전성과 신뢰성을 보장받지 못하는 것이 현실이다. 이와 같은 문제점을 해결하기 위해서는 대칭키 암호화 기법 등을 통해 메시지의 기밀성을 보장하고, 디지털 서명 서비스 등 공개키 암호화 기법을 통해 개체 인증과 메시지 인증을 제공해야 한다.

현재 이러한 전자우편의 안전성과 신뢰성을 제공하기 위한 방안으로 PGP와 S/MIME 등이 사용되고 있다. PGP는 91년에 Phil Zimmermann에 의해 제안된 방식으로 현재까지 버전 8.x가 개발되어 있다. PGP는 사용 알고리즘의 특허 문제로 인해 상용 버전과 국제 버전으로 구분된다. 국제 버전은 Windows 및 MAC 기반의 8.x 버전까지 발표되어 북미 지역 이외의 국가에서 비 상업용 freeware로 사용할 수 있고, 상용 버전은 북미 지역에 한하여 미국의 Network Associates. Inc에서 구매 가능하다.

이와는 별도로 기존의 MIME 서비스에 PGP를 적용하여 기밀성과 인증성을 제공하는 방식으로 PGP/MIME이 있으며, Qualcomm사의 Eudora 등 몇몇 업체들에 의해 제공되고 있다. 그러나, PGP/MIME은 RSA를 사용하기 때문에 특허 문제로 인해 표준화 작업은 이루어지지 못 하고 있는 상황이다.

현재 PGP의 국제표준화를 위해서 IETF의

OpenPGP 워킹그룹이 활동하고 있으며, 표준화를 위해 사용하는 알고리즘은 특허와 관련하여 문제가 없는 것으로 선택하고 있다. 따라서, 적용되는 알고리즘에 약간은 차이가 있으나, 제공하는 정보보호기능들은 PGP, PGP/MIME, OpenPGP가 모두 동일하다.

2. 표준화 동향

2.1 적용 기술 현황

PGP를 특징짓는 것 중에 하나가 인증기관을 각각의 PGP 사용자에게로 분산시키고, Web of Trust라는 개념으로 공개키 인증을 구현하였다는 것이다. 즉, PGP의 사용자들 모두가 다른 사용자의 공개키에 전자서명을 생성함으로써 각자 인증기관의 역할을 수행하고, 인증 주체들은 공개키의 신원에 대해 신뢰도 점수를 제공함으로서 신뢰도에 따른 공개키 사용이 가능하도록 하였다. 이는 X.509가 안전성 측면에서는 신뢰할 만하나, 구현상 어려움으로 인해 통일된 인증 체계를 구축하기가 어려운 상황에 따른 것으로, PGP 7.x부터 X.509 인증서 사용이 가능해 졌다.

OpenPGP에서 사용되는 알고리즘은 크게 공개키 알고리즘, 대칭키 알고리즘, 해쉬 알고리즘, 압축 알고리즘 등이 있다. OpenPGP에서 사용하는 알고리즘 및 인증서 형식을 OpenPGP Message Format, "draft-ietf-openpgp-rfc2440bis-09.txt"에 기초하여 나열하면 [표 1]와 같다.

[표 1] OpenPGP 사용 암호알고리즘

표준 / 분야	OpenPGP		
인증서 형식	• PGP 인증서		
대칭키 알고리즘	• Triple-DES • Blowfish • Twofish	• IDEA • SAFER-SK128	• CAST • AES
공개키 알고리즘	• Elgamal • Elliptic curve	• DSA • ECDSA	• RSA • Diffie-Hellman
해쉬 알고리즘	• SHA1 • SHA(256/384/512)	• MD5	• RIPEMD160
압축 알고리즘	• ZIP	• ZLIB	• BZIP2

PGP는 메시지 전송에 앞서 ZIP 등을 이용하여 평문을 압축하여 대칭키 암호화를 수행한다. 이는 더욱 안전한 암호문 생성 역할을 수행할 수 있게 한다. 또한 비밀키를 사용하려 할 경우 한 번의 패스프레이즈 입력 과정을 거치고, 다음 입력시기 까지 비밀키를 반복해서 사용 가능하게 하였다. 이를 통해 PGP는 안전성과 함께 기능상의 편리성도 함께 추구함을 알 수 있다.

2.2 표준 문서 현황

현재 PGP와 관련하여 IETF의 Security Area에서 운영 중인 "openpgp" 워킹그룹은 PGP 사용에 필요한 오브젝트의 형식, 암호알고리즘, 전자우편 등을 통해 전송되는 메시지 및 MIME 프레임워크의 표준을 제공할 목적으로 활동하고있다.

주요 활동 방향은 메시지 형식의 표준을 정의하고, MIME 등과의 호환을 고려한 작업이 이루어지고 있다. 아직까지는 PGP 고유 인증 방식인 Web of trust 이외에 인터넷 표준인 X.509를 동시에 지원하는 방식에 대해서는 문서가 발표되지

않고 있으나 조만간에 고려될 것으로 예상된다. PGP와 관련되어 발표된 문서의 현황은 [표 2]과 같다.

[표 2] OpenPGP WG 문서 현황

문서번호	제 목	작성자	작성일
RFC3156	MIME Security with OpenPGP	M. Elkins, D. Del Torto, R. Levien, T. Roessler	Aug. 2001
RFC2440	OpenPGP Message Format	J. Callas, L. Donnerhacke, H. Finney, R. Thayer	Nov. 1998
draft ietf openpgp rfc2440bis -09.txt	OpenPGP Message Format	J. Callas, L. Donnerhacke, H. Finney, R. Thayer	Oct. 2003

RFC의 내용을 간단히 살펴보도록 한다. MIME Security with OpenPGP (RFC3156)에서는 OpenPGP 메시지 형식이 RFC1847에 기술되어 있는 MIME에 어떠한 방법으로 기밀성과 인증성을 제공하는 지에 대해서 기술하고 있다. OpenPGP Message Format (RFC2440)은 기밀성, 키 관리, 인증, 전자서명을 제공하는 응용 프로그램을 개발하는 데에 필수적인 모든 메시지 형식을 정의하고 있다. RFC2440 개정판에 해당되는 draft-ietf-openpgp-rfc2440bis -09.txt에서는 PGP Message Exchange Format(RFC1991)에서 기술된 PGP에서의 기밀성, 전자서명 등의 기능을 제공하는 방법과 사용하는 알고리즘에 대한 설명이 추가되어 있다.

이전 문서들에서는 RIPE DB갱신과 관련된 디지털 서명 인증 및 TLS 프로토콜이 OpenPGP에서 사용되는 인증서, 알고리즘, 신뢰모델을 지원할 수 있도록 확장하는 방법들이 설명되었었으나, 사용 환경의 변화 및 문서 개정 등으로 인해 별도의 표준 문서로는 남아 있지 않다.

2.3 IETF OpenPGP 표준화 이슈

금번 59차 IETF 표준화 회의가 2월 29일부터 3월 4일에 걸쳐 서울에서 개최되었으며, 의장인 Derek Atkins의 주관하에 OpenPGP 2440bis와 관련된 몇몇 이슈들과 차기 Agenda가 논의되었다. 금번 회의에서는 특히 "End-of-Line Whitespace Canonicalization"에 대해 여러 의견들이 나왔으나, 결과는 얻지 못하고 담당자에게 재검토를 요청하기로 하였다. 그 밖에 논의된 사항을 [표 3]에서 정리하였다.

[표3] 제59차 IETF OpenPGP 주요 이슈

문서번호 및 제목	일련번호	검토타입	이슈 내용
문서번호:draft-ietf-openpgp-rfc2440bis-09.txt 제목:OpenPGP Message Format	1	문서편집	User IDs가 Non-Textual함
	2	일반	Shamir's Discrete Log Hash 함수에 대한 신규 알고리즘을 포함하기위한 의견 조율이 없었음
	3	문서편집	Comment에 대한 길이와 양식이 정의되어 있지 않음
	4	기술	DSA 서명 알고리즘에 해쉬 함수를 적용할 경우 계산상 문제가 발생될 수 있음
	5	기술	IDEA V3와 V4를 동시에 사용할 경우 충돌이 발생될 수 있음
	6	기술	3rd party signatures in a one-pass signed message : 2440bis-09에서는 언급되지 않았으나, 기술적 필요성으로 인해 논의하기로 함
	7	문서편집	Primary key signature는 Subkey backward signature로 통일하기로 함
	8	일반	메시지 바디에서 UTF-8 Text에 관한 내용이 정확히 언급않됨
	9	기술	Elgamal 서명 삭제 요망 : 위조 및 도청 가능한 ID의 사용으로 인해 구현시 문제 발생 가능
	10	일반	4.2.2.4에서 언급된 유효 인코딩 길이는 5 byte로 하기로 함
	11	문서편집	Cleartext signature는 Cleartext로 통일하기로 함
	12	일반	5.13과 5.14에서 Hash 값을 어떻게 받는지 설명이 모호함
	13	일반	5.5.3에서 비밀키 패킷 형식에 대해 명확한 설명이 필요함

OpenPGP 활동과 관련된 추후 일정으로, 2440bis와 multiple sig draft를 각각 2004년 5월과 8월에 IESG에 넘기기로 했으며, RFC2440bis와 PGP/MIME간의 상호운용성 시험을 2004년 8월부터 하고 Advance 2449bis to Draft는 2005년

2월까지 정리하기로 하였다.

3. 결론

현재, 상업용 PGP의 판매권은 미국의 "Network Associates"사에서 가지고 있으며 PGP를 응용한 Desktop firewall과 VPN Client 제품 등이 제공되고 있다. PGP/MIME의 경우에는 몇 개의 업체에서 이를 수용하는 제품을 제공하고 있고, OpenPGP를 지원하는 제품은 아직 발표된 것이 없다.

PGP사용자는 freeware인 국제 버전을 중심으로 꾸준히 증가하여 국제적인 호응을 얻고 있으며, X.509가 도입되면 전자상거래 및 전자정부와 같은 분야에서도 충분히 사용 가능하리라 판단된다.

국내에서는 포럼을 중심으로 전자우편 보안프로토콜인 S/MIME v3를 표준화 중에 있어 그 사용이 증가할 것으로 예상되는 가운데, PGP를 개발하여 상용화하는 경우는 없이 일부의 단체 및 그룹에서 국제 버전을 활용하고 있는 정도이다. 따라서, S/MIME 표준화가 어느 정도 자리를 잡은 다음에 OpenPGP에 표준화 검토 논의가 진행되리라 판단된다.

[참고문헌]

[1] IETF, Security Area, OpenPGP Working Group.

[2] J. Callas, L. Donnerhacke and H. Finney, "OpenPGP Message Format," IETF Network WG, draft-ietf-openpgp-rfc2440bis-09.txt, October, 2003.

[3] J. Callas, L. Donnerhacke, Hal Finney and R. Thayer, "OpenPGP Message Format," IETF Network WG, rfc2440.txt, Nnovember, 1998.

[4] M. Elkins, D. Del Torto, R. Levien and T Roessler, "MIME Security with OpenPGP IETF Network WG, rfc3156.txt, August 2001.

[5] KISA, "IETF 정보보호 표준화 동향 분석에 관한 연구," 10, 2002.