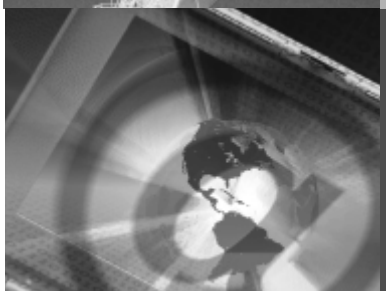


인터넷 정보보호 표준 동향

김학범
한국정보보호센터 기술표준팀장
TTA/TC10 시스템보안 연구반 의장

1. 서론

인터넷의 발전은 21세기 e-business 시대로의 새로운 전환을 가져왔고, 인터넷의 효율적인 활용이 모든 분야와 조직에서 경쟁력을 좌우하고 있어, 인터넷의 특성인 개방화 및 분산화된 환경에서 각종 전자거래, 전자문서, 전자우편 등에 이용되는 정보와 인터넷에 접속된 시스템과 LAN 등의 네트워크 보호를 위한 각종 보안기술과 표준화에 대한 중요성이 날로 부각되고 있다.

인터넷 정보보호기술에 대한 표준화도 인터넷의 급속한 발전과 전자상거래가 활발해짐에 따라 IETF(Internet Engineering Task Force)와 같은 민간단체에서 실용적인 사실표준(de facto standard) 활동이 더욱 활발히 추진되고 있다. 특히 IETF는 미국이 주도하는 민간단체로서 인터넷 표준의 개발 및 선정을 목적으로 정부기관, 업계, 학계 등 다양한 분야의 연구개발자들로 구성되어 개방적으로 국제적인 활동을 추진하고 있으며, 정보보호분야를 포함하여 세부기술 분야별로 워킹그룹을 결성하여 표준화활동을 수행하고 있다.

국내에서도 정보화추진과 더불어 다양한 정보통신망이 상호연동되고 정보보호서비스가 구축되어감에 따라 정보보호기술 표준화에 대한 필요성이 급증하였고 핵심기술과 응용기술분야에 대한 표준화를 추진하고 있다.

본 고에서는 인터넷의 발전과 더불어 개방적이고 분산된 환경에서 더욱 중요성이 부각되고 있는 인터넷보안 관련 국내외 표준화동향을 소개한다.

2. IETF 정보보호 표준화

IETF는 인터넷에 대한 프로토콜 공학과 개발수단을 제공하고자 1986년 1월에 출범한 단체이다. IETF는 인터넷구조와 운용에 관련된 망 설계자, 운영자, 벤더 및 연구자들로 구성되어 있다. IETF의 실제적인 기술적 활동은 다양한 분야(Area)의 워킹그룹(Working Groups) 활동을 통해 이루어지고 있으며, 대부분의 작업은 메일링 리스트를 구성하여 이메일을 통해 이루어지며 1년에 3회 회의가 개최된다.

현재 IETF는 인터넷의 각종 응용을 연구하는 응용(Applications) 분야, 인터넷 표준화절차 및 정책 등을 연구하는 일반(General) 분야, 인터넷(Internet) 분야, 운용관리(Operations and Management) 분야, 대규모 망에서 확장성을

지원하기 위해 기존 라우팅 프로토콜의 진화 및 새로운 라우팅 프로토콜을 개발하는 라우팅(Routing) 분야, 인터넷 정보보호 관련 사항을 연구하는 정보보호(Security) 분야, 인터넷상에서 오디오/비디오 등 여러 미디어를 사용하는 응용서비스 제공을 위한 전송 프로토콜 규격 작업 등을 담당하는 전송(Transport) 분야, 인터넷 상의 사용자 서비스를 포괄하는 사용자 서비스(User Services) 분야의 [표 1]과 같은 총 8개 분야로 구성되어 있다.

각 워킹그룹별 연구내용은 다음과 같다.

- An Open Specification for Pretty Good Privacy(openpgp)

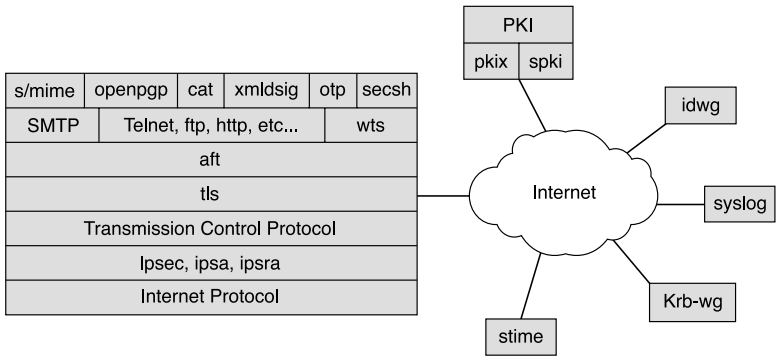
openpgp 워킹그룹의 목적은 MIME 프레임워크의 제공 뿐만 아니라 알고리즘과 PGP가 처리하는 객체들의 포맷에 대한 표준을 제공하는 것이다.

openpgp 워킹그룹에는 현재 OpenPGP Message Format이라는 RFC 2440이 있다. RFC 2440은 OpenPGP 포맷에 기반한 상호운용성있는 응용을 개발하기 위해 필요한 정보로써 암호화, 복호화, 서명과 키관리 기능을 제공하기 위해 OpenPGP에서 사용되는 메시지-교환 패킷에 대한 정보를 제공하고 있다.

[표 1] IETF의 분야별 워킹그룹

분야	워킹그룹
응용	Application Configuration Access Protocol(acap) 등 24개
일반	Process for Organization of Internet Standards ONg(poisson)
인터넷	AToM MIB(atommib) 등 14개
운용관리	ADSL MIB(adslmib) 등 21개
라우팅	Border Gateway Multicast Protocol(bgmp) 등 18개
정보보호	IP Security Protocol(ipsec) 등 20개
전송	Audio/Video Transport(avt) 등 25개
사용자 서비스	FYI Updates(fyiup) 등 4개

정보보호 분야는 openpgp, aft, cat, ipsp, ipsec, sacred, ipsra, idwg, kink, krb-wg, otp, pkix, smime, stime, secsh, syslog, spki, tls, wts, xmldsig의 총 20개의 워킹그룹으로 구성된다. 정보보호분야의 워킹그룹을 인터넷의 계층구조에서 표현해 보면 다음 (그림 1)과 같다.



(그림 1) IETF 정보보호 표준화 워킹그룹의 계층구조 표현

● Authenticated Firewall Traversal(aft)

aft 워킹그룹의 목적은 침입차단시스템에 대해 응용계층에서의 프로토콜을 규정하는 것이다. 침입차단시스템의 인증에 대한 일반적인 구조와 함께 TCP와 UDP 응용을 모두 지원하는 프로토콜을 규정한다. 또한 상호운용성을 위한 기본 인증방법도 제안하고 있다.

현재 aft 워킹그룹에는 3개의 RFC가 있다. RFC 1928에서는 TCP와 UDP 도메인에서 침입차단시스템을 안전하게 사용하기 위해 클라이언트-서버 응용을 위한 프레임워크를 제공하기 위해 설계된 SOCKS Protocol V5에 대해 설명하고 있다. RFC 1929와 1961에서는 이러한 프로토콜로써 SOCKS V5를 위한 Username/Password 인증을 기술하며, SOCKS V5 GSS-API 인증 프로토콜에 대한 명세를 제공하고 무결성, 인증과 선택적인 비밀성의 제공을 위해 GSS-API에 기반한 인캡슐레이션을 정의한다.

● Common Authentication Technology(cat)

cat 워킹그룹의 목적은 다양한 프로토콜 호출자에게 호출자를 정보보호 메커니즘의 구체적인 명세에서 격리시키는 방식으로 분산 정보보호서비스(인증, 무결성, 비밀성, 권한허가)를 제공하는 것이다.

cat 워킹그룹은 공통의 서비스 인터페이스로서 GSS-API를 정의했다. GSS-API는 연결지향 환경에서 호출자로 하여금 채택되는 정보보호 메커니즘을 식별하는 토큰 포맷을 가지고 정보보호서비스를 제공하게 한다. 지금까지는 GSS-API에 관한 C언어 바인딩을 제공하고 현재 Java 바인딩을 정의하고 있다. 또한 권한허가 인터페이스가 앞으로 수행될 작업의 관련 분야가 될 것이다.

● IP Security Protocol(ipsec)

ipsec 워킹그룹은 클라이언트 IP 프로토콜을 보호하는 메커니즘을 개발하고 있다. 인증, 무결성, 접근통제, 비밀성의 조합들을 유연하게 지원하는 암호화 정보보호서비스를 제공하기 위해 네트워크 계층에서의 정보보호 프로토콜을 개발한다.

IP Authentication Header(AH)와 IP Encapsulating Payload(ESP)에 대한 프로토콜 포맷은 암호화 알고리즘과 독립적이다. 우선은 host-to-host 보안을 추구하고 다음으로 subnet-to-subnet과 host-to-subnet 위상을 추구할 예정이다.

또한 ipsec 워킹그룹에서는 네트워크 계층에서의 키관리 요구사항을 지원하기 위한 프로토콜과 암호화기술이 개발될 것이다. IKMP(Internet Key Management Protocol)가 하위계층의 정보보호 프로토콜에 독립적인 응용계층 프로토콜로써 명시될것이며 ISAKMP/Oakley에 기반을 둘 것이다.

ipsec 워킹그룹이 개발하는 문서는 구조(Architecture), ESP 프로토콜, AH 프로토콜, 암호 알고리즘, 인증 알고리즘, 키 관리, DOI(Domain of Interpretation)의 7가지로 구성되어 있다.

최근 ipsec 워킹그룹에서는 주로 고속 네트워크를 위한 IPSEC 개선에 대한 내용들이 논의되고 있다. 주요 구성내용은 sequence number spare exhaustion, 암호화 성능, 무결성(및 인증) 성능에 관한 내용으로 Sequence Number Extension은 매우 빠른 속도(10 기가비트)일 경우에, 32비트 sequence spare는 몇 분내에 작은 패킷에 의해 확장가능하며, AES와 새로운 모델의 사용은 많은 양의 트래픽을 어느 정도는 감내하지만 더 큰 sequence spare가 적절하다. 두번째로 암호화 성능(Encryption Performance)에 있어서는 AES가 Triple-DES보다는 속도가 빠르지만, CBC 모드는 병렬 및 파이프라인된 구현의 기회를 감소시킨다는 의견이 제시되었다.

16바이트 블록 AES를 위한 counter는 128비

트이어야 하며, 각 SA 상에서의 각 패킷을 위한 다른 값을 허용해야 하는데, 처음의 32비트는 패킷내의 AES 카운터로서, IPv6 Jumbogram 만큼으로, 필요로 하는 것보다는 더 크며, 다음 48비트는 패킷 카운터로서 확장된 ESP Sequence Number를 사용한다. 또한 다음 16비트는 각 SA에 대해 유일하며, 카운터 셋을 유지하는 SKEYID로부터 확장된 secret value를 포함한다. 최상위의 32비트는 패킷에 대한 초기 벡터 값(Initial Vector)이다.

마지막으로 무결성 성능(Integrity Performance)에 대하여는 암호는 빠르지만, 무결성 및 인증을 위한 계산속도가 현재 bottleneck이 되고 있으며(즉, HMAC(MD5 or SHA-1)이 느림), 암호와 무결성을 혼합하는 모드가 좋은 선택이 될 수 있을 것으로 보이지만 몇가지는 ESP 및 신택스와 불일치가 발생할 수 있으며, 작은 패킷에 대해서 심각한 패널티가 부과되며, 국제적인 property의 문제점이 발생할 가능성이 있다는 의견이 제시되었다.

● IP Security Policy(ipsp)

통신경로상에서 보안 게이트웨이와 라우터 필터같은 개체에게 정책제한을 가할 필요가 있는 관리적인 개체가 있을 수 있다. 또한 보안 연결의 양단간이나 그들 각자의 관리개체가 엔드 호스트와 통신의 경로상에서 보안 게이트웨이와 라우터같은 정책시행 지점에 대한 접근통제 정보를 안전하게 발견하고 협상할 필요가 있다.

이러한 문제점에 대해서 워킹그룹은 다음과 같은 작업을 수행한다.

- IP 보안정책들을 지원하기 위해 저장소 독립적인 정보모델과 저장소에 특정한 데이터 모델 규정
- 확장가능한 정책명세 언어(policy specification language)를 개발하고 채택
- 현재 존재하는 정책분배 프로토콜을 사용하여 IPSec 정책제공에 대한 지침제공
- 정책 서버의 발견, 정보보호정책의 분배와 협상, intra/inter 도메인 환경에서 정책충돌을 해결하는 정책교환 프로토콜과 협상 프로토콜의 개발 및 채택

ipsp 워킹그룹의 작업 아이템들은 인터넷 프로토콜을 위한 정보보호구조(RFC 2401)와 IKE (RFC 2409)에 호환성이 있는 표준들을 산출할 것이며, ipsec 워킹그룹에 의한 표준들을 보충하게 된다.

최근 회의에서 ipsp 워킹그룹에서는 다음과 같은 내용들이 토의의제로 다루어졌다. 먼저 Roadmap 문서에 대해서는 ipsp 워킹그룹에서 다루는 문서들의 용도 및 일정을 담고 있다. 요구사항, 데이터 모델, 구조, 정책언어, 규정, 정책교환과 협상 프로토콜을 다룬 문서들은 표준 트랙을 밟을 것이라는 점이 강조되었다. 여러 문서 가운데서도 특히, requirement 문서와 architecture 문서에 대한 코멘트가 우선 필요한 것으로 발표되었다.

두 번째로 Requirement 문서에 대해서는 몇 가지 사항이 논의되었다. 먼저 정책모델은 IPSec 정책의 모든 구문을 정의하며, 언어나 프로토콜 등 세부사항들과는 독립적이어야 한다. IPSP 언어는 외부로 보이는 정책을 위한 것으로, 정책들이 내부적으로 어떻게 표현되는가는 WG의 관심사항이 아니다. 정책발견을 위해 프로토콜이 사용되나, 이는 노드들이 상호 어떻게 정책정보를 주고 받는지에만 관련된다. SA 변수조정은 정책발견후 취해지며, SA에 어떤 변수를 사용할지를 결정하는데, 그 계산은 충분히 효율적이어서 실용적이라야만 한다. 변수가 선택되고 나면, compliance 체크를 수행한다. 이후 몇 가지 Q/A가 진행되었다.

세번째로 IPSec 정책모델 갱신문서에 대해서는 정책, 필터, 동작, 제안/변형 클래스 등에서 많은 변화가 있었다.

네번째로 IPSP 구성모델 프레임워크 피드백(feedback)에 대해서는 PCIM, QPIM 및 IPsec

구성정보 모델간의 차이점이 발표되었다. 모델들간의 차이점은 네 가지 카테고리로 나누어 볼 수 있다. layering 관점면에서 차이, condition 관련 차이, group 관련 차이, 정책 role면에서의 차이로 나누어 생각할 수 있다. 이어서 각 카테고리별 세부 차이점이 발표되었다.

● IP Security Remote Access(ipsra)

ipsra 워킹그룹은 원격접속에 관한 연구를 수행하며 다음과 같은 목적을 가지고 있다.

- 원격접속 구조를 정의하고, 원격접속에 참여하는 실체들과 그들 사이의 관계 정의
- IKE를 운영하는 IPSec 장치에 기존 인증 메커니즘(legacy authentication mechanism)을 이용하여 사용자 인증을 수행하는 표준 메커니즘 정의
- 사용자 구성정보 및 사용자 접근통제 정보를 사용자의 사설 네트워크로부터 지역 IPSec이 구현된 곳까지 전달하는 표준 메커니즘을 정의

ipsra 워킹그룹은 ipsec 워킹그룹, mobilip 워킹그룹과 협조하여 표준화활동을 추진한다.

최근 회의에서는 다음과 같은 내용들을 다루었다. 첫번째로 Requirement draft 내용(draft-ietf-ipsra-reqmts-02.txt 문서)의 갱신사항 보고 및 이슈가 토의되었는데 바이트 카운트가 요구사항에서 제거된 이유에 대한 질문과 답변후, WG 임무에 대한 토의로 이어졌으며, 원격접속 형태에 대한 사람들의 의견이 엇갈렸다.

두 번째로 사용자 인증 메커니즘(getcert 문서와 PIC 문서)과 관련하여 사용자 인증을 다룬 PIC와 getcert 문서에 대해서는 아직도 아무런 합의를 보지 못한 상태로 이들에 대한 토의와 합의모색점이 주요 관심사가 되었다. 먼저, getcert draft 00 버전이 발표되었다. SCEP 프로토콜은 불안하므로 사용되지 말아야 한다는 주장에 getcert 제안에서는 SCEP 프로토콜의 안전한 부분만을 사용하고 있다. PIC 01 문서는 00에서 많은점이 변경되었는데 Xauth 프로토콜 대신에 EAP 프로토콜을 사용하며 새로운 ISAKMP 교환유형을 사용하여 왕복메시지 교환을 생략한다.

마지막으로 configuration 문서에 대해 WG에서 기술적인 토의를 완료하고 표준안으로 승격되기 위해 현재 WG last call중에 있다. 원래 IPSec WG 문서였으나 원격접속시 호스트 네트워크 변수설정을 다루는 문제로 이 WG에서 진행되어왔으며 이 문서는 DHCP 프로토콜을 사용한 virtual presence 제공방안으로 이제 WG에서의 논의를 마무리할 예정이다.

● Intrusion Detection Exchange Format(idwg)

idwg 워킹그룹의 목적은 침입탐지와 대응시스템, 이것들과 상호작용이 필요한 관리시스템에게 이익이 될 수 있는 정보들을 공유하기 위한 데이터 포맷과 교환절차들을 정의하는 것이다.

idwg 워킹그룹은 침입탐지 시스템간의 통신을 위한 기능적 요구사항, 침입탐지 시스템과 관리시스템간의 통신을 위한 요구사항, 이러한 요구사항에 대한 이론적 근거와 요구사항을 만족하는 데이터 포맷을 기술하는 공통언어 스펙, 침입탐지 시스템간의 통신을 위해 가장 잘 사용되어지는 현재의 프로토콜과 데이터 포맷을 연관시키는 방법 등에 관한 연구를 수행하고 표준을 제정한다.

침입탐지시스템은 정보보호시스템의 한 종류로써 컴퓨터시스템의 비정상적인 사용과 오용, 남용 등을 탐지하여 관리자에게 경고메시지를 보내주고 침입을 막는 시스템이다. 인터넷의 확장에 따라서 네트워크를 통한 침입의 가능성이 증가되고, 이에 따라 시스템이나 네트워크 침입을 탐지하고 대처할 능력이 있는 기술이 필요하게 되었다. 침입탐지시스템은 침입차단시스템만으로는 침입으로부터 안전하지 않기 때문에 침입시도에 관한 정보나 외부로부터의 사용정

보를 기록으로 남기려는 의도하에 계속 개발되어 왔다. 침입탐지시스템은 일단 침입차단시스템을 통과한 패킷일지라도 행위를 감시해 침입여부를 판단해 주기 때문에 시스템의 보안정도를 더욱 높일 수 있다.

침입탐지시스템의 상업적 중요성이 증가하고 여러 가지 제품들이 나오면서 하나의 사건에 대해서도 여러 가지 다른 양상으로 다른 시스템에 적용되었다. 따라서 다양한 침입탐지시스템들이 공격에 관한 자료를 공유하는 것이 바람직하다. 이를 위해서는 침입탐지시스템들 사이의 필요한 정보를 공유하기 위한 교환절차와 데이터 포맷을 정의해야 한다.

이러한 일련의 작업들을 수행하기 위해 IETF 내에 IDWG(Intrusion Detection Exchange Format Working Group)가 1998년 12월에 조직되었다. IDWG는 침입탐지시스템에 대한 요구사항 기술과 공통언어 정의, 그리고 침입탐지시스템에서의 통신 프로토콜과 데이터 포맷 등을 표준화하기 위해 노력하고 있다. IDWG는 또한 침입탐지시스템에 대한 표준화를 위해서 IETF의 다른 작업그룹들과도 함께 노력하고 있다.

현재 IDWG에서 발표된 RFC는 없으며, 다음과 같은 다섯 개의 Internet-Draft가 발표되었다.

- Intrusion Detection Message Exchange Requirements
- Intrusion Detection Exchange Format Data Model
- Intrusion Alert Protocol
- Intrusion Detection Message Exchange Format - Extensible Markup Language (XML) Document Type Definition
- Intrusion Detection Message Exchange Format - Comparison of SMI and XML Implementation

● One Time Password Authentication(otp)

사용자가 시스템에 로그인하기 위해 동일한 패스워드를 매번 사용하는 기존 패스워드 인증 시스템은 네트워크상에서 재사용 공격에 대한 위협에 취약하다. 이러한 문제점을 해결하기 위해 Bellcore의 S/Key을 토대로 패스워드를 매번 바꾸어 사용할 수 있는 일회용 패스워드 기술에 대한 표준화작업을 수행하고 있다.

● Public-Key Infrastructure(X.509)(pkix)

pkix 워킹그룹은 X.509에 기반한 공개키 기반구조를 지원하기 위해 필요한 표준개발을 목적으로 설립되었다.

X.509 V3 인증서와 V2 인증서 폐지목록, 인증서 생성과 관리를 위한 메시지들을 정의하는 인증서 관리 프로토콜, 인증서 폐지목록을 요청하지 않고도 인증서의 현재상태를 결정하는데 유용한 프로토콜인 OCSP(Online Certificate Status Protocol), X.509 인증서의 생성을 위해 인증기관에 인증서요청을 전송하기 위해 사용되는 인증서요청 메시지 포맷(CRMF : Certificate Request Message Format) 등이 RFC로 승인되었다.

pkix 워킹그룹은 PKI 관리에 통합적인 프로토콜과 PKI 사용과 밀접히 관련을 가지는 프로토콜의 개발에 착수하고 있다. 인증서 폐지방법의 대안에 관한 작업이 이루어지고 있으며 인증서 명명형태와 부인방지 문맥(context)에 사용되기 위해 설계된 인증서인 "qualified certificates"에 대해 확장사용(extension usage)을 정의하고 있으며, 시점확인과 데이터 인증에 관한 프로토콜도 작업중이다.

X.509 속성(attribute) 인증서 프로파일 작업이 수행될 것이고 공개키 인증서와 속성 인증서 사이의 차이점을 수용하기 위해 현재의 인증서 관리 표준에 확장을 가져올 것이다.

인증서 및 CRL 규격, 운영 프로토콜, 관리 프로토콜, 인증서 정책, 타임스탬프 프로토콜, 데이터 검증 프로토콜 등으로 구성된 주요 프로토콜을 제시한다.

- 인증서 및 CRL 규격: 인증서는 기본 필드

에 여러 선택 필 드들로 구성된 매우 복잡한 데이터 구조이다. 인증서 활용의 융통성을 부여하기 위하여 광범위한 선택 필드를 포함하고 있다. 인증서 규격은 X.509 버전 3 인증서 규격을 사용하고 있고, CRL 규격은 X.509 버전 2 CRL 규격을 사용하고 있다. 인증서의 규격 뿐만 아니라 인증서에서 요구되는 다양한 암호 알고리즘에 대한 OID(Object Identifier)를 정의하고 있다.

- 운영 프로토콜: 운영 프로토콜은 인증서와 CRL을, 인증서를 사용하는 시스템으로 전달하기 위하여 사용된다. LDAP(Light-weight Directory Access Protocol), HTTP, FTP, X.500 프로토콜에 기반을 둔 다양한 수단을 이용한다.
- 관리 프로토콜: 관리 프로토콜은 PKI 사용자와 관리 개체들간의 온라인 상호동작을 위하여 사용된다. 관리 프로토콜은 인증서를 발급받기 위하여 인증기관과 클라이언트간에 이용되거나, 상호인증을 위하여 인증기관과 인증기관 사이에 이용된다. 관리 프로토콜은 사용자의 등록정보와 인증서 취소요구 정보를 포함할 수 있다. 인증서 관리 프로토콜은 보내지는 메시지의 형태와 메시지 전송을 주관하는 프로토콜로 구성된다.
- 인증서 정책(Ceritificate Policy): 인증서 정책은 특정의 공개키 인증서를 적당한 가격을 갖는 전자거래를 위한 인증서로 적용할 수 있는지를 나타내는 이름이 있는 법칙들의 집합이다. 인증 실행규칙은 인증기관이 공개키 인증서를 발급할 때 사용한 규칙을 나타낸다. 인증서 정책과 인증서 실행규칙은 물리적 및 개인보안, 주체 신분확인 요구사항, 인증서 취소정책 등의 과정을 포함한다. 인증서는 보안정책에 관한 일반적인 사항을 규정하며, 주로 일반 메일을 위한 인증서 정책과 전자거래를 위한 인증서 정책으로 구분된다. 따라서 인증서 정책은 허용가능한 거래금액에 따라 달라질 수 있다. 그러나 인증서 실행규칙은 인증정책을 구체적으로 구현하기 위한 다양한 세부적인 절차를 규정하고 있다.
- 타임스템핑, 데이터 검증 및 인증서비스(DVCP: Data Validation and Certification Protocol): 타임스템프 서비스는 타임스템프 기관이 메시지가 특정시간 이전에 존재했음의 증거를 제공하기 위하여 메시지를 서명한다. 서명한다는 의미는 메시지를 자신의 개인키로 암호화한 서명문을 구하는 과정을 의미한다. 타임스템프 서비스는 사용자가 특정시간 이후에 개인 키의 누설로 인해 의문이 되는 거래정보가 생성되었음을 주장할 수 없게 하기위한 부인방지 서비스를 제공한다. 또한 시간 데이터 기관(TDA: Temporal Data Authority)은 시간 데이터 토큰을 생성하는 제삼의 기관이다. 시간 데이터 토큰은 특정의 메시지와 특정의 사건을 연관함으로서, 타임 스템프 토큰에 포함된 시간에 대한 보조적인 증거를 제시한다. 메시지와 연관되는 시간 데이터는 토큰의 전진 데이팅을 방지하기 위하여 충분히 예측 불가능해야 한다. 그러나 위원회는 이의 필요성에 대한 명확한 지원을 얻지 못해 Internet-Draft는 폐기되었다. 데이터 검증 및 인증 서버는 제출된 데이터의 정확성을 검증하는 믿을 수 있는 제삼자이다. TSP 서비스는 메시지를 분석하지 않고 대신 메시지에 신뢰성이 있는 시간을 나타내고, 데이터 해쉬된 결과 스트링만을 서명함으로서, 주어진 시간내 특정의 비트 스트링이 존재했음을 존재했다는 것만을 검증하는 반면, DVCS에 의하여 제공되는 서비스는 데이터의 소유를 직접 서버가 확인하고, 실제 서명문의 수학적 정확성을 검증하며, 인증경로의 유효성 역시 검증한다. DCVS는 두 가지 방법으로 부인방지 서비스를 제공한다. 서명문이나 인증서가 주어진 시간에 유효한다는 증거를 제공한다. 이 토큰은 인증

서의 유효성이 경과되고, 인증서 취소정보가 CRL에 더 이상 존재하지 않은 후에도 사용될 수 있다.

● S/MIME Mail Security(smime)

smime 워킹그룹은 전자우편의 보안문제를 해결하기 위한 워킹그룹으로서 MIME 데이터에 암호학적 서명과 암호화 서비스를 추가하는 프로토콜을 기술한 S/MIME Version 3 메시지 스펙, Diffie-Hellman 키 협상방식을 사용할 경우 small-subgroup 공격을 방지하기 위한 방법, CMS(Cryptographic Message Syntax), S/MIME을 위한 선택적인 보안서비스 확장과 인증서처리에 관한 RFC를 제정하였다.

전자우편의 보안문제를 해결하기 위해 1997년에 정식 WG으로 출범한 SMIME WG은 MIME 데이터에 암호학적 서명과 암호화 서비스를 추가하는 프로토콜을 기술한 S/MIME Version 3 메시지 스펙, Diffie-Hellman 키 협상방식을 사용할 경우 small-subgroup 공격을 방지하기 위한 방법, CMS(Cryptographic Message Syntax), S/MIME을 위한 선택적인 보안서비스 확장과 인증서처리에 관한 RFC를 제정하였다.

최근 회의에서는 CMS, Diffie-Hellman, CERT and ESS 구성요소에 대한 상호운용성 매트릭스를 개발한 내용(www.imc.org/ietf-smime/interop-matrix.html 참조)과 S/MIME 상호운용성 시험내역이 소개되었다. 아래 [표 2] 참조.

● Secure Network Time Protocol(stime)

인증된 원천으로부터 안전하게 시간을 얻는 방법이 정보보호와 부인방지를 위한 주요 요소가 되고 있다.

시간을 분배하는 현재의 방법은 공개키 기반구조나 암호학적 방법을 사용하지 않고 있기 때문에 외부의 공격과 변형에 취약하다. 이러한 취약점을 극복하기 위해 공개키 기반구조를 사용하여 시간분배를 안전하게 하며 위험을 감소시킬 수 있다.

stime 워킹그룹은 현재의 Network Time Protocol(NTP)에 대한 수정을 통해 인터넷에 대해서 인증된 시간의 분배를 지원하기 위해 필요한 메시지 포맷과 프로토콜을 정의한다.

[표 2] SMIME 표준 적합성 시험

참조문서	시험내역(통과/제품수)	세부시험 내역
RFC 2630	49/96	Signed Data - 24/25 Envelopted data - 11/25 Digested data - 0/4 Encrypted Data - 0/4 Authenticated Data - 0/16 Rest of Document 15/25
RFC 2631	0/13	
RFC 2632	16/21	
RFC 2633	17/61	
RFC 2634	27/81	Triple Wrap - 3/5 Signed Receipts - 19/41 Security Labels - 5/11 Equivalent Labels - 0/12 Mail list - 0/12

● Secure Shell(secsh)

telnet 혹은 rlogin 등은 보안측면에서 매우 취약한 응용시스템으로 강력한 보안서비스를 요구하고 있다. 이에 따라 SSH, Secure-Telnet, SSL-telnet 등과 같이 telnet 세션 전체를 암호화하여 동작하는 프로토콜이 제안되어 사용되고 있다.

secsh 워킹그룹에서는 SSH가 암호해독과 프로토콜 공격에 대해 강력한 보안을 제공하고, 글로벌한 키 관리와 인증서 기반구조 없이도 작동되며, 현존하는 인증서 기반구조를 사용할 수 있고, 채택과 사용이 쉽고, 사용자로부터 수동의 상호작용을 최소로 하거나 없도록 하며, 구현의 용이성 보증에 대해 연구하고 있다.

● Simple Public Key Infrastructure(spki)

spki 워킹그룹은 쉽고, 간단하고, 확장가능한 인증서 구조와 운영절차를 만드는 작업을 하고 있다. spki 워킹그룹에서는 키 인증서 형식, 서명형식 및 키 획득 프로토콜 등에 관한 표준개발 작업이 진행중이며 이러한 키 인증서 형식과 관련 프로토콜은 이해, 구현 그리고 사용이 간단해야 한다.

현재 제정된 RFC에서는 SPKI의 요구사항과 SPKI 인증서 및 인증서 폐지목록에 관한 이론을 제시하고 있다.

● Transport Layer Security(tls)

tls 워킹그룹은 일반적인 목적의 보안과 키 관리 메커니즘보다는 전송계층에서의 보안특성을 제공하는데 초점을 맞추고 있으며, 전송계층에서 인증, 무결성, 프라이버시를 구현하기 위한 방법을 제공하기 위한 방법을 제공하다.

현재까지 제정된 RFC에서는 TLS V1.0과 Kerberos에 기반한 인증을 지원하기 위해 TLS 프로토콜에 새로운 cipher suites를 제안하였다. 또한 현재의 TCP 연결에서 TLS를 개시하기 위해 HTTP/1.1에서 Upgrade 메커니즘을 사용하는 방법, HTTP 연결을 안전하게 하기위해 TLS를 사용하는 방법 등도 포함되어 있다.

● Web Transaction Security(wts)

wts 워킹그룹에서는 HTTP를 이용하는 웹 트랜잭션에 정보보호서비스를 제공하기 위한 요구사항과 명세를 개발하는 것을 목표로 하고 있으며 HTTP에 정보보호기능을 추가한 S-HTTP(Secure HTTP)를 근간으로 작업하고 있다. S-HTTP는 트랜잭션 비밀성과 무결성, 발신처 부인방지 등의 서비스를 제공한다. S-HTTP는 각 트랜잭션에 대해 협상을 지원하여 키 관리 메커니즘, 정보보호정책, 암호 알고리즘의 선택에 있어 유연성을 강조한다.

현재까지 제정된 RFC에서는 HTTP에 정보보호서비스를 제공하기 위한 비밀성, 무결성, 사용자 인증, 서버/서비스 인증 요구사항을 명시하고 있고, S-HTTP 협상 매개변수에 대한 문법을 기술하고 있다.

● XML Digital Signatures(xmldsig)

xmldsig 워킹그룹의 활동의 핵심범위는 데이터 모델, 문법, 암호학적 서명을 XML 자원에 바인드하기 위한 처리 등을 규정하는 것이다. 이를 위해 XML-DSig가 메타데이터와 객체모델 기술개발의 구성요소가 되도록 하는 데이터 모델 정의, 확장가능한 규범 프레임워크의 정의, XML 서명에 대한 문법과 처리절차 등에 초점을 맞출 것이다.

xmldsig 워킹그룹의 요구사항은 다음과 같다.

- 확장성이 높은 단순한 XML 서명문법을 정의
- 응용으로 하여금 분리된 서명블록에 대한 처리 뿐 아니라, XML과 non-XML로 이루어진 복합적인 문서의 생성과 처리

• XML-DSig는 다른 XML 기술과 함께 통합되어질 수 있어야 함.

● Security Issues in Network Event Logging (syslog)

syslog 워킹그룹에서는 기존의 Syslog 메커니즘의 보안 및 무결성 문제점에 대하여 문서화와 이에 대한 내용을 취급하는 것을 목적으로 한다. 이러한 작업을 위하여 기존의 프로토콜에 대한 문서화와 함께 보안문제를 취급하기 위한 표준을 개발한다. 또한 Syslog 프로토콜을 안전하게 하기위한 방법도 작업한다.

● Kerberos WG(krb-wg)

몇 년간에 걸쳐 Kerberos는 실질적으로 모든 운영체제에 이식되었으며, 상호운용성에 대한 문제가 제기되었다. krb-wg 워킹그룹에서는 불분명한 규정때문에 발생했던 과거의 상호운용성 문제가 다시 발생하지 않도록 Kerberos 규정(RFC 1510)을 분명하게 하고 확장할 것이다. 또한 상호운용성과 보안을 개선하는데 필요한 확장된 기능을 제안할 것이다.

● Kerberized Internet Negotiation of Keys(kink)

KINK 워킹그룹은 IKE의 대안으로서, IPsec 보안조직을 위한 집중형 키 관리(RFC 2401)를 촉진하기 위한 standards track 프로토콜을 만들기 위해 조직됐다. KINK 워킹그룹의 목표는 능률적이고 빠르며, 관리하기 쉬운 암호화 사운드 프로토콜(sound protocol)의 생산에 있다. 이 프로토콜은 공개 키 처리(operation)를 요구하지 않으며, 현재의 커버로스 구조(infrastructure)에 호환된다. 이 워킹그룹은 IPsec(RFC 2401)나 Kerberos(RFC 1510)의 변경을 요구하지 않는다. 그리고 Kerberos 구조에 기반한 중앙집중형 IPsec 키 관리 메커니즘을 개발한다.

● Securely Available Credentials(sacred)

SACRED 워킹그룹의 목표는 신뢰성 확보와 관련된 개인정보(공개 키/개인 키 쌍, 인증서, 인증서 체인, 신뢰정보, 루트 인증기관 정보...)의 안전한 export/import를 위한 메커니즘 개발과, 신임장(credential) 서버로부터의 전송, peer 장비간의 전송 등이 포함된다. 특히, SACRED 워킹그룹은 IPSRA의 요구사항의 해결을 위해 선택된 프로토콜을 수행한다.

3. 국내표준화 동향

국내에서는 '97년부터 한국정보보호센터를 중심으로 표준화를 추진하였으며, 우리나라 독자적인 정보보호기술 표준을 개발하기 위하여 국가 사회에 우선적으로 필요한 전자서명 알고리즘 표준(KCDSA), 해쉬 알고리즘 표준(HAS-160) 및 128비트 블록암호알고리즘(SEED)을 개발하였으며, 이중 SEED는 관련 전문가와 공동으로 전담반을 구성하여 ISO/IEC JTC 1에 국제표준화 작업중이다. 또한 침입차단시스템 선정지침과 컴퓨터 바이러스 방지지침, 전자서명 인증서 프로파일 등을 개발하였다.

또한 2000년 6월 국내에서도 인터넷 보안기술 표준화추진을 위하여 정보통신부가 앞장서서 인터넷 보안기술을 포함하는 인터넷 텔레포니, 인터넷 정보가전 등 정보통신분야의 11개 전략분야의 선정 및 정책적인 지원으로, 민간중심의 포럼을 출범시킴으로서 사실표준에 대한 국제적 동향과 국내에 적합한 표준제정을 위한 기반을 마련하였다.

2000년 6월 창립된 인터넷보안기술포럼(ISTF : Internet Security Technology Forum)은 현재 52개의 업체 및 기관들이 참여하고 있으며 다음과 같은 목적으로 활동하고 있다.

• 인터넷 보안기술 관련 국내표준 개발

• 인터넷 보안 관련 제품 상호운용성 항목 발

[표 3] 정보보호 관련 주요 TTA 단체표준 목록

표준번호	제목	제정년도
TTA.KO-12.0001	전자서명 알고리즘 표준(KCDSA)	1998. 8
TTA.IS-10118	해쉬 알고리즘 표준(HAS-160)	1998. 8
TTA.KO-12.0002	정보보호기술 전문용어 표준	1998. 11
TTA.KO-12.0003	침입차단시스템 선정지침	1999. 9
TTA.KO-12.0004	128비트 블록 암호알고리즘 표준(SEED)	1999. 9
TTA.KO-12.0005	암호학적 확인함수를 이용한 실체인증 기술표준	1999. 9
TTA.KO-12.0006	대칭형 암호화 기법을 이용한 실체인증 기술표준	1999. 9
TTA.KO-12.0007	공공시스템 보안을 위한 위험분석 표준 - 위험분석 방법론 모델	2000. 3
TTA.KO-12.0008	공공기관 정보시스템 구축 준비단계의 보안지침서	2000. 3
TTA.KO-12.0009	공공시스템 보안을 위한 위험분석 표준 - 위험분석 방법론 모델	2000. 3
TTA.KO-12.0010	컴퓨터 바이러스 방지지침	2000. 7
TTAS.IT-X.509/R2	디렉토리시스템 인증 프레임워크	2000. 7
TTAS.KO-12.0001/R1	부가형 전자서명 방식 표준 - 제2부 : 인증서 기반 전자서명 알고리즘	2000. 12
TTAS.KO-12.0011	해쉬함수 표준 - 제2부 : 해쉬함수 알고리즘표준(HAS-160)	2000. 12
TTAS.KO-12.0012	전자서명 인증서 프로파일 표준	2000. 12

굴 및 상호운용성 시험의 지원활동

- 인터넷 보안기술 관련 최신 기술정보의 수집, 분석, 보급 및 활용촉진
- 인터넷 보안기술 관련 세미나, 워크숍 등 행사개최
- 인터넷 보안기술 관련 국제표준화 회의, 국제포럼 등에의 참여지원 등의 사업을 추진하고 있다.

인터넷보안기술포럼의 표준 활동은 분과위원회를 중심으로 운영되며 현재 국내외적으로 가장 이슈가 되고 있는 주제들을 선정, 기술별로 구분하여 우선 네트워크 분과, PKI 분과, 무선 분과등 3개 분과로 구성하였으며, 이후 각 분야의 표준소요 제기시 해당분과를 증설하여 대처할 계획이다.

분과 활동계획을 살펴보면, 네트워크 분과에서는 우선 가상사설망(VPN) 보안 표준화에 관한 활동을 수행하게 된다. 인터넷을 이용하는 VPN 서비스의 핵심은 완벽한 보안환경을 제공하는 데 있으며, 현재 국제적으로 표준화가 추진되고 있는 터널링 기술은 IETF의 IPSec으로서 이의 분석을 통해 국내에 적합한 VPN 보안 표준을 개발하며, VPN 보안 제품간 상호운용성 시험에 관한 연구를 위해 IPSec Developers Forum과 VPNC(Virtual Private Network Consortium) 등의 활동동향도 파악하게 된다. 이미 VPN 보안기술 표준(안)과 침입차단 및 침입탐지시스템에 대한 로그 표준(안)을 개발하여 의견수렴중에 있다.

PKI 분과에서는 IETF의 PKIX X.509에 기반한 PKI 국제표준화 동향파악을 통해, 국내의 공인 인증기관 PKI 체계에 적합한 인증서 및 인증서 폐지목록 프로파일 표준을 개발하였고, 공개키 기반구조 구성요소간의 트랜잭션, 인증서 유효성 검증절차 등 다양한 기술적·정책적 표준화에 대처할 예정이다. 또한 표준개발을 통해 국내외 PKI 솔루션간의 상호운용성 확보방안에 관한 연구도 수행한다.

무선 분과에서는 무선 인터넷 프로토콜과 무선 인터넷 보안에 관한 국제표준화 동향파악을 위해 사실상의 표준인 WAP 분석과 보안 프로토콜인 WTLS 동향분석을 실시하여 국제 표준화활동에 적극 대응할 예정이다.

4. 결론

전세계적으로 인터넷의 활성화와 함께, 인터넷의 효율적 활용이 모든 분야와 조직에서 경쟁력을 좌우하는 세상에 살게 되었다. 인터넷의 특성인 개방화되고 분산화된 환경에서, 이용되는 각종 정보에 대한 보호와 인터넷에 접속된 시스템과 네트워크를 보호하는 기술 그리고 이를 경제적이고 효율적으로 사용하기 위한 표준화에 대한 중요성이 날로 부각되고 있다.

선진국들은 보유하고 있는 정보보호 핵심기술의 표준화와 적용제품 개발로 국제시장 점유를 확대하는 추세에 있으므로, 우리도 독자적으로 경쟁력 있는 표준을 개발하고 관련제품을 보급하여 국제화에 대비해야한다. 특히 인터넷과 전자상거래 등 시급한 분야에 대한 국제표준을 연계하여 국내실정에 적합한 표준의 우선적 개발로 관련 국내산업을 육성해야 한다.

또한 표준은 제정도 중요하지만 정부와 각 기관, 사업체 등에서 우선적으로 표준이 적용된 제품을 널리 활용될 수 있도록 하는 제도적인 뒷받침도 매우 중요하므로, 이를 위한 지속적인 노력도 병행되어야 한다.

국내 정보보호 표준화활동은 한국정보보호센터를 중심으로 관련기관, 단체, 산업체, 학계 등과의 유기적인 협조와, 한국정보통신기술협회(TTA)/정보보호기술위원회와 인터넷보안기술포럼을 통해 이루어지고 있으며, 이러한 표준화 활동은 국제환경에 부응하면서 국내에 적합한 실용적이고 경쟁력있는 표준을 제정·보급하여, 궁극적으로 국내 정보보호산업의 활성화와 국제 경쟁력제고에 일익이 될 것이라 기대한다.

컴포넌트 소프트웨어 부문 한·일 공동개발 사업추진

첨단 컴포넌트 소프트웨어(SW) 기술개발을 위한 한일 공동사업이 추진된다. 소프트웨어 벤처기업인 크래빅스(대표 한복동 http://www.crebix.co.kr)는 일본의 컴포넌트SW 전문업체인 매트릭스시스템스(대표 오오쓰카)와 패턴기반 개발방법론(PBD)에 따른 컴포넌트 기술의 공동개발 및 제품공급에 합의했다고 밝혔다. 이에 따라 양사는 3월 14일 여의도 63빌딩에서 사업 제휴식을 갖고 컴포넌트SW의 공동개발 및 기술공유와 개발된 제품에 대해 상호 독점 공급한다는 내용의 기본 계약을 체결했다. 이번 한일 공동사업에는 크래빅스를 비롯해 시스네트정보·대한정보서비스·둘리정보통신 등 국내 10여 개 소프트웨어 업체가 공동 참가하며 일본측도 매트릭스시스템스 등 10여개 컴포넌트 개발 전문업체들이 「PASCAL」이란 이름의 공동 컨소시엄을 구성, 컴포넌트 표준제정과 제품개발을 추진하기로 했다. 이에 따라 크래빅스는 국내 컨소시엄 참가업체들과 함께 독자적인 컴포넌트SW를 개발, 매트릭스시스템스를 통해 일본에 공급하고 한일 공동개발 제품의 제3국 수출도 추진할 계획이다. 또한 일본 매트릭스시스템스가 개발한 「피니언」 제품과 미국 CA사의 컴포넌트 자동화 개발도구인 「쿨 플렉스」도 국내에 공급한다. 특히 크래빅스 등 국내 참가업체들은 컴포넌트SW 기술단체인 한국소프트웨어컴포넌트컨소시엄(KCSC·회장 오길록)과의 협력을 통해 국내 컴포넌트 표준제정 및 제품개발에도 적극 동참할 계획이다. 크래빅스 한복동 사장은 『이번 소프트웨어 컴포넌트 분야의 한일 공동사업은 양국의 컴포넌트SW 전문업체가 공동으로 구성한 컨소시엄간의 협력이라는 사실과 재사용에 따른 SW의 생산적인 개발이 보다 구체화됐다는 점에서 큰 의미를 지닌다』고 강조했다.