通信情報保護學會誌
第3卷 第4號, 1993. 12

인터네트 보안 관련 연구 개발 현황

홍주영* · 임채호**

1. 개 요

Internet은 미국방부의 네트워크 프로토콜인 TCP/IP(Transmission Control Protocol/Internet Protocol)를 사용하는 네트워크들의 집합체이다. ARPANET부터 시작하여 MILNET, NSFNET 등 미국의 거대 네트워크에서 부터 전세계 여러 국가에서 구축된 TCP/IP 네트워크들이 있으며 지금까지 주로 학술 및 연구 개발 용의 네트워크였으나 현재는 미국을 중심으로 해서 상용의 네트워크까지 출현할 정도로 급격한 발전을 하고 있으며 이러한 추세는 미국의 통신 정책 주도로 오래 동안 지속되리라 예측할 수 있다. 한편, 인터네트의 발전에 따라 네트워크 프로토콜 및 관련 연구 개발이 활발히 진행되고 있다. IAN(Internet Architecture Board) 산하의 IETF(Internet Engineering Task Force)에서 여러 워킹 그룹들이 활동하고 있으며 여기서 개발한 각종 제안서들은 IAB 인준을 거쳐 인터네트 표준으로 고시된다.

그런데 예로부터 인터네트에는 각종 보안 침해 사건들을 경험하게 되었다[2]. 이는 BSD UNIX 내에 TCP/IP 프로콜이 기본으로 제공되기 시작하면서 대부분의 R&D 기관들이 실제로 이기종간에 가장 손쉽게 연결할 수 있는 방법으로 이를 채택하였고, 자유로운 정보의 교환을 목적으로 네트워크를 운영하기 때문이었다. 그러나 대형의 보안 사고들은 심각한 문제가 되어 이를 위한 보안 대책 수립이 시급히 요구되었으며 보안 사고의 확산을 예방하기 위한 보안 센터를 설치하고 각종 보안 관련 문서들을 배포하고 있다. 특히 IETF 산하의 SAAG(Security Area Advisory Group)에 여러 보안 워킹 그룹들이 형성되어 보안 정책 및 가이드라인을 발간하거나 각종 보안 프로토콜들을 개발하는 등 활발한 연구 개발 활동을 선도하고 있다[1] [10].

본고는 인터네트에서의 보안 관련 연구 개발활동을 소개함으로써 국내의 학술 연구망 중심으로 정착되고 있는 인터네트에서의 보안 기술을 정립하는데 도움이 되고자 한다.

2. IETF SAAG(Security Area Advisory Group) 현황

IETF는 인터네트를 위해 IAB 산하에서 각종 기술 지원 및 연구 개발을 담당하는 기구로 인터네트에서 요구되는 새로운 프로토콜, 서비스 등을 개발하는 많은 워킹 그룹들로 이루어져 있고 유사한 기능들을 담당하는 워킹 그룹들을 모아 분야(Area)별로 운영된다. 그 분야들은 다음과 같다.

• Applications : 전자 우편 서비스의 확장, 네트워트 데이타베이스, 네트워크 뉴스 프로토콜, 네트워크 팩스, 네트워크 프린팅, 가상 터미널 프로토콜 등

* 한국전자통신연구소
** 대전실업전문대학

• Internet Sevvices : 접속 지향 IP, 동적 호스트 구성, ATM 상의 IP, AppleTalk IP, FDDI IP, 라우터 요구 사항 등

• Network Management : 각종 망관리용 MIB, 어카운팅, 모니터링 등

• OSI Integration : 디렉토리, MHS, OSI네트워크 운영, ODA 등

• Operational Requirement : 벤치 마크, 통계, 라우팅 이용, 사용자 접속 등

• Routing : 각종 라우팅 방법

• Security : IP 시큐리티 옵션, 인증 기술, 보안 전자 우편, 망관리 보안 등

• Transport Service : 오디오, 비디오, 분산 화일 시스템, 도메인 네임, Service Location Protocol, Trusted NFS 등

• User Service : 디렉토리 서비스, FTP 아카이브, 인터네트 School 네트워크, 네트워크 운영 도구, 네트워크 정보 서비스 등

국내 인터네트 학술 전산망인 KREONet, HANA, KREN에서도 Internet IETF의 활동을 분석하고 이의 기술을 개발하기 위해 대응되는 워킹 그룹들을 조직하였으며 시급히 기술력이 요구되는 부분들을 우선적으로 시작하였는데 참여 인원이 적어 아직 안정된 활동이 진행되고 있지는 않다. 국내 학술 전산망들간에 정책 조정과 공동의 기술력 향상을 위한 ANC(Academic Network Council) 산하에 SG-INET(Special Group Internet)에서는 표 1과 같은 워킹 그룹들을 조직하고 있다.

3. 보안 워킹 그룹

3.1. Internet Security Policy/Guideline 그룹 (spwg & ssphwg)

SPWG(Security Policy Working Group)는 Internet Security Policy의 제안을 위한 그룹으로 기술적인 논의는 물론 관리적인 문제에도 관심을 갖는다. Internet는 단 하나의 기관이 운영하는 네트워크가 아니므로 특정한 보안 정책의 수립과 적용보다는 각각의 기관과 전체적인 네트워크의 보안성있는 운영이 중요하게 여겨지고 있다. 그러나 어떤 형태로든 가이드를 제시하는 것이 전체 네트워크 관련 사용자들에게 유용할 것이다.

이 그룹이 Guidelines for the Secure Operation of the Internet[RFC1281]에서 제공한 가이드라인은 네트워크 운영자, 관리자, 그리고 업체에게 좋은 보안 정책을 세우기 위한 기본을 다음과 같이 정의하고 있다[6].

• 사용자는 개개인이 보안 정책을 이해하고 따라야 할 책임이 있다. 사용자들의 행위는 개별적으로 기록된다.

• 사용자는 자신의 데이타 보호를 위해 보안 메카니즘과 절차를 사용할 책임이 있다.

• 시스템 서비스 제공자는 보안을 유지할 책임이 있다. 또한 보안 정책과 이에 대한 변경 사항을 사용자에게 알릴 책임이 있다.

• 업체와 시스템 개발자는 적절한 보안 제어 기능을 제공할 책임이 있다.

표1. 국내 SG-INET 워킹 그룹 현황

Mailing List 명칭	관련 작업
road	Routing, Addressing, OSI operation, NSAP Address
hangul	한글 e-mail, news, 기타 통신 환경에 적용
netoper	망운영, Ticket, 통계 등
security	Security Area, PEM, CAT 등
nis	Network Information, Directory 등의 사용자 서비스
protocol	IP, PPP, High Speed Protocol
pccom	BBS, PC Communcation 등
naming	X.400, RFC 822, X.500 등

• 사용자, 업체, 시스템 제공자들은 보안을 위해 상호 협조해야 한다.

• Internet 보안 프로토콜의 개발은 지속적으로 이루어지고 기타 여러 Internet에서의 개발은 보안에 관한 사항을 설계시 중요한 부분으로 고려해야 한다.

이와 함께 SSPHWG(Site Security Policy Handbook Working Group)은 Site Security Handbook (RFC1244)에서 Internet site마다 각자의 특성에 맞는 정책의 개발과 보안 사고 발생시 사후 처리 절차 등에 관해 많은 조언을 하고 있다. 기본적인 방식은 저렴한 비용으로 자산을 보호할 수 있는 대응책을 수립, 적용하면서 취약점이 발견되는 대로 개선해 가는 것이다. 핸드북의 구성은 다음과 같다[5].

☐ section 1 : 개요
☐ section 2 : site의 공식적인 보안 정책의 수립
컴퓨터 자원의 허가된 액세스의 정의, 내부/외부자의 액세스 정책 위반시 조치 사항, 내부자의 외부 site 액세스 정책 위반시 조치 사항, 비허가된 행위로 간주될때의 조치 사항 등을 정의
☐ section 3 : 보안 문제 해결을 위한 절차의 수립
시스템 보안 감사, 사용자 계정 관리 절차, 패스워드 관리 절차, 구성 관리 절차
☐ section 4 : 보안 사고의 처리
site관리자, 시스템 관리자, site 보안 전문가, response team 등의 책임과 권한의 명시와 침입 행위의 유형들의 정의 등
☐ section 5 : 보안 사고 이후의 처리 절차
발견된 취약점 제거, 정책과 절차의 개선.

♣ 관련된 메일링 리스트

Security Policy(SPWG) : spwg@nri.reston.va.us
Site Security Policy Handbook (SSPHWG) : *ssphwg* @cert.sei.cmu.edu

3.2. Privacy Enhanced Mail(PEM)

PEM은 Internet Mail protocol(RFC822)을 사용하여 전송되는 E-mail에 다음과 같은 보안 서비스를 제공 한다[8].

• Integrity
• Data-origin authenticity
• Confidentiality(선택 사항)

PEM은 메세지의 암호화에는 대칭적 암호 기법(DES)을 키 분배 방식에서는 비대칭적 암호기법(RSA)을 권고한다. 비대칭적 키 분배 방식은 안전하게 키를 공유할 방법이 없는 Internet의 환경적 특성(광범위한 규모와 관리의 비균일성 등)에 적절하다. PEM이 채택한 표준 양식은 CCITT X.509 (Directory Authentication Framework) 권고안을 따르는 profile이다.

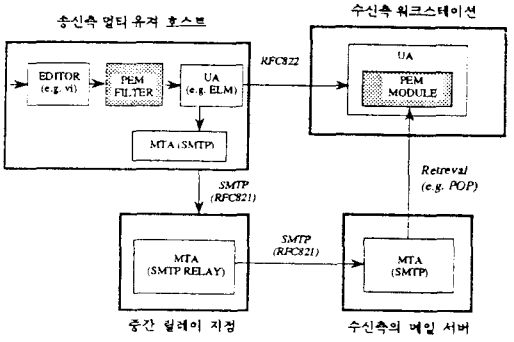


그림 1. PEM의 환경

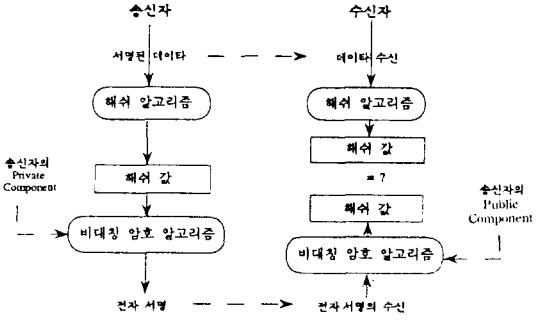


그림 1. 전자 서명 발생 및 검증

세가지 보안 서비스를 구현하기 위해 PEM protocol은 다음의 4가지의 절차를 통한다.

1. Message Digest가 계산된다.
2. 송신자의 private key를 이용하여 Message Digest가 암호화되며 이것은 송신자를 식별하기 위한 정보임과 동시에 메세지에 대한 digital signature로서 제공된다.

3. Confidentiality를 제공하는 경우, random DES를 생성시켜 이를 이용하여 메세지를 암호화한다.
4. 메세지가 암호화되면 DES key는 수신자의 public key로 암호화한 후 메세지에 포함시켜 전송한다.

그림 1은 PEM의 환경이며 그림 2는 전자 서명을 생성하고 검증하는 과정을 도시한 것이다. PEM의 가장 중요한 부분은 송수신자들간의 public key를 어떻게 인증(certificate)할 것인가에 있다. 이러한 문제를 위해 Internet Society에서는 PEM을 위한 public key certification hierachy를 구성 문제를 논의하고 있다. 이는 authority를 부여해주는 certificate의 global 시스템의 역할을 하게 된다.

PEM을 정의한 4가지 시리즈로 된 문서들은 다음과 같다.

1. REM1421 : Privacy Enhancement for Internet Electronics Mail :
   Part I :Message Encryption and Authentication Procedures
   메세지 처리 절차를 기술
2. RFC1422 : Privacy Enhancement for Internet Electronics Mail :
   Part II : Certificate-Based Key Management
   PEM이 채택한 public-key certification system을 정의
3. RFC1423 : Privacy Enhancement for Internet Electronics Mail :
   Part III : Algorithms, Modes, and Identifiers
   PEM에 사용되는 여러 알고리즘들의 정의와 식별자들을 기술
4. RFC1424 : Privacy Enhancement for Internet Electronics Mail :
   Part IV : Key Certification and Related Services
   사용자 등록과 Certification Revocation List(CRL) 배포등의 관습과 메세지 형식들을 정의

위 네가지 문서중 처음 세가지는 RFCs 1113-1115로 이미 발표된 것이다. 모든 문서들은 많은 개정을 거쳤으며 '93년 2월에 Proposed Standard로서 발표되었다. 구현 사례로는 미국 TIS사의 TISPEM과 EC 후원의 PASSWORD 프로젝트의 결과로 영국과 독일등의 UCL, Cambridge version, INRIA, CMD, 그리고 스웨덴의 COST 등이 있다[7]. 현재 PEM의 연구는 최근 채택된 MIME(Multipurpose Internet Mail Extension, RFC 1341)와 함께 사용되기 위한 확장 작업이 진행되고 있다. 이는 보안 전자 우편과 멀티미디어 전자 우편 기능들을 결합시키기 위한 것이다[8]. 관련된 문서는 〈draft-ietf-pem-mine-03.txt〉MIME-PEM Interation이 93년 10월 개정되어 나와 있다.

♣ 관련된 메일링 리스트

- 일반적인 의견 교류 : pem-dev@tis.com
- PEM관련 메일 수신 : pem-dev-request@tis.com
- Archive : pem-dev-request@tis.com

3.3. IPSO and CIPSO

네트워크상의 정보의 흐름을 제어하는 가장 강력한 수단 중에 하나가 데이타의 비밀 등급과 사용자 및 site의 비밀 취급인가 수준을 나타내는 레이블링 방식을 사용하는 것이다. 1991년 11월에 최종 확정된 IPSO(Internet Protocol Security Option, RFC1108)는 미국내의 보안 분야에서만 통용되도록 설계된 프로토콜이다. 현재 두가지 옵션을 제공하고 있다.

- DoD Basic Security Option(BSO, option type =130) : Unclassified, Confidential, Secret 혹은 Top Secret의 4가지 classification과 관련 DoD Authority 플래그로써 IP 데이타그램이 레이블되며 이를 통하여 액세스 제어가 이루어진다.
- DoD Extended Security Option(ESO, option type=133) : Security category나 release marking과 같은 부가 정보들을 처리할 수 있도록 한다.

두 옵션의 고정 필드들은 Defense Information system Agency(DISA)에서 관리한다.

CIPSO(Common IPSO)는 미국의 보안 분야가 아닌 다른 정부 기관들과 민간 기업을 대상으로 하는 IPSO이다. BSO와 ESO의 고정된 종류의 보안 등급과 권한, 적은 종류의 ESO 형식 코드들로는 다양하고 방대한 사용자 계층의 요구를 충족시킬 수가 없었다[4].

CIPSO의 구조는 그림 3과 같이 크게 Header와 Tag부분으로 나누어진다. 헤더는 다시 옵션의 유형을 알리는 식별자와 DOI(Domain of Interpretation)로 구성된다. 이 DOI는 보안 어트리뷰트 정보들을 담고 있는 Tag 부분을 옳바로 해석하기 위한 것으로 이 DOI 필드가 같은 경우 같은 보안 정책을 갖고 있으며 보안 어트리뷰트들을 동일하게 해석하게 된다. 즉, DOI는 보안 도메인 식별자로 사용되며 동일한 보안 도메인내에서만 Tag 정보는 의미가 있는 것이다.

CIPSO 프로토콜을 사용하는 기관은 IANA(Internet Assigned Numbers Authority)로부터 Labeling Number(혹은 Domain Of Interpretation Identifier : DOI)를 제공 받는다. 한 시스템은 여러 보안 도메인의 구성원이 될 수 있다. 십여개의 회사들이 CIPSO를 성공적으로 구현하고 상호 연동성의 테스트도 수행했다고 한다. 또한 NIST에서 작업중인 새로운 NIST GOSIP security label과의 연관성에 대한 검토도 진행되고 있다.

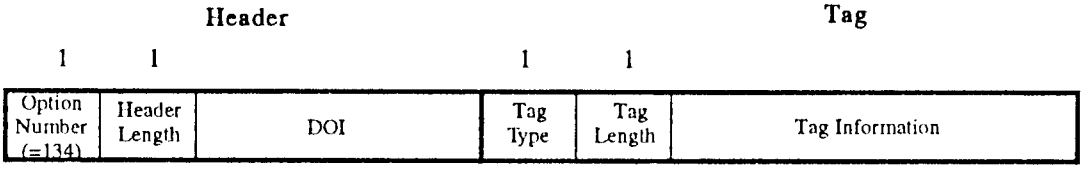


그림 3. CIPSO 구조

CIPSO는 IETF와 TSIG가 협력하여 개발하고 있으며 원래 Commercial IPSO라 하였으나 그 목적에 좀더 부합되는 현재의 명칭, Common IPSO로 변경되었다. 1993년 3월 9일 버젼의 CIPSO가 Draft Standard로 나와 있으며 추후 Standard로 발표될 예정으로 있다.

♣ 관련된 메일링 리스트

cipso@wdll.wdll.loral.com

3.4. Common Authentication Technology Working Group(CAT)

어떤 호스트의 사용자의 신분을 다른 호스트로 하여금 인증케 하는 아이디어를 이용한 인증 메카니즘의 예로 비밀 키 방식을 이용하는 MIT의 Kerberos와 X.509 공개 키 방식을 사용하는 DEC의 DASS(Distributed Authentication Security Service)가 있다[3].

CAT 그룹에서는 이들이 사용하는 암호 키방식은 상이하나 제공하는 서비스가 같다는 점에서 응용 프로그램들이 어떤 인증 방식하에서도 동작될 수 있도록 하는 공통의 인터페이스를 제공하기 위한 작업을 하고 있다. GSS-API(General Security Services Application Program Interface)가 그것이다.

GSS-API base specification, GSS-API C 언어 bindings, 그리고 Kerberos Version 5문서가 Proposed Standards로써 검토 중에 있다.

♣ 관련된 메일링 리스트

- 일반적인 의견 교류 : cat-ietf@mit.edu
- CAT 관련 메일 수신 : cat-ietf-request@mit.edu
- Archive : ~/cat-ietf/archive@bitsy.mit.edu

3.5. Secure SNMP(SNMPSEC)

SNMP(Simple Network Management Protocol)는 네트워크상에 장비들을 제어하기 위한 프로토콜이다. Management station이 생성한 질의(get 혹은 set)를 agent가 MIB(Management Information Base)를 참조하여 응답하게 된다. 이때 불법적인 get/set 질의를 방지하기 위해 secure SNMP는 security "wrapper"를 제공한다[9]. Wrapper는 허가된 management station 만이 질의를 보내고 허가된 agent만이 응답할 수 있도록 한다.

♣ 관련된 메일링 리스트

snmp-sec-dev@tis.com

4. 결 론

이상으로 인터네트에서의 보안 관련 연구 개발 현황들을 요약하여 살펴보았다. 인터네트는 국제 표준기구인 ISO에서 개발한 OSI 보다도 현실적인 이기종간의 접속을 보장하고 있으므로 지속적인 네트워크 확대가 이루어지고 있으며 국내에서도 이의 확대가 급속적으로 이루어지고 있는 상태이다. 그리고 인터네트에서의 여러 보안 사고의 경험으로 인터네트의 자체적인 보안 관련 프로토콜들의 개발이 IETF/SAAG 산하 그룹에서 이루어지고 있는데 국내 인터네트 확장을 고려할때 국내 기술에 의한 이러한 기술력 습득과 개발이 매우 시급한 실정이라고 본다. 특히 ISO/OSI 보다 연구 개발 환경에 있어 우수하다고 보는데 이는 인터네트가 R&D 환경에서 개발되었고 각종 관련 정보 및 소스코드들이 많이 개방되어 있기 때문이다. 만약 국내에서 IETF/SAAG 관련한 연구 개발을 시도하고자 한다면 인터네트를 통해 각종 회의 내용과 표준 문서들을 즉각적으로 입수할 수 있으며 또한 관련한 기관의 시제품, 알고리즘등의 소스를 가져다 자신의 연구 개발에 응용할 수 있는 것이다. 이러한 의미는 또한 국내에서도 관련한 연구 개발 그룹간에 서로의 정보를 네트워크를 통해 교환함으로써 전체의 연구 개발 성취도를 높일 수 있음과 동시에 네트워크에서의 보안 사고를 방지하는 방법론들을 모색할 수 있음을 뜻한다.

여기에서 소개한 PEM, CAT, IPSO, Security Policy WG 등 모두가 국내에서도 중요한 기술이라고 보며 학술적인 연구면에서도 우수한 환경을 제공할뿐 아니라 인터네트의 세계적인 확장 추세와 국내에서의 도입 추세를 볼 때 이 분야의 연구 노력이 활성화되길 바란다.

참고 문헌

[1] 임채호, IETF Security Area 활동 현황, WG-SECURITY : 0002, 1992.7.

[2] Peter J.Denning, Computers Under Attack, Intruders, Worms, and Viruses, Addsion-Wesley, 1990.

[3] Charles Kaufman, DASS(Distributed Authentication Security Seruice), Internet Draft, December 1992.

[4] IETF CIPSO Working Group, Common IP Security Option, Version 2.3, March 1993.

[5] RFC1244, Sits Security Handbook

[6] RFC1281, Guidelines for Secure Operation of Internet.

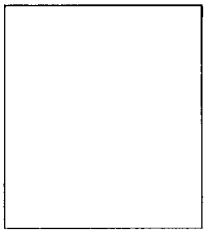
[7] PEM WG Meeting Minutes, July 1993.

[8] Stephen T.Kent, Internet Privacy Enhanced Mail, CACM Vol.36, No.8, August 1993.

[9] Stephen T.Kent, An Overview of Internet Privacy Enhanced Mail, INET '93, June 1993.

[10] Steve Crocker, Overview of Internet Security Development, INET '93, June 1993.

□ 著者紹介



임 채 호(정회원)

1985년 홍익대학교 전산학과 졸업(학사)
1989년 건국대학교 전산학과 졸업(석사)
1991년~현재 홍익대학교 전산학과 박사과정중
1985년~1992년 한국과학기술연구원 시스템공학 연구소 교육연구망 그룹 선임연구원
1991년 University of Maryland 전산계산과 방문연구원
1992년~현재 대전실전 전자계산과 교수
관심 분야 : TCP/IP, OSI, Network Security
사진은 학회지 제1권 제2호 ('91.8) 101page 참조

홍 주 영(정회원)

1990년 홍익대학교 전산학과 졸업(학사)
1990년~현재 한국전자통신연구소 연구원
관심 분야 : Computer Security, Network Security