□ 기술해설 □

인터네트 보안

성균관대학교 정 진 욱*
대전실업전문대학 임 채 호**

목 차

1. 서 론

인터네트(Internet)는 세계 최대의 네트워크로서 세계 최초의 네트워크구조인 미국방성 망구조에 의해 개발된 이기종간의 연결방법인 TCP/IP(Transmission Control Protocol/Internet Protocol)을 통신 프로토콜로서 사용한다. 여러 기종에서 손쉽게 이식하여 상호 연결이 용이하므로 꾸준하게 발전해온 인터네트는 개방형시스템상호접속(OSI, Open System Interconnection)이 정착되기 전까지는 국제적인 현실표준으로서 지속적으로 발전되리라고 예측되고 있으며, 이의 표준화, 정책등은 IAB(Internet Activity Board)에서 조정하고 있다.

한편 인터네트에서는 초기 R&D 환경에서 출발하였으므로 연구소나 대학 등이 주된 가입기관이였고, 네트워크의 개방과 접속의 용이성으로 누구나 네트워크에 접속하기 쉬웠고, 네트워크 관련 정보나 프로그램 소스 등이 개방되어 있어 크고 작은 보안 사고들을 겪어왔다. 대표적인 보안 사고의 예를 보자면.

- 서독 해커 간첩 사건(Cukoo's Egg)
  미국의 한 연구소 시스템관리자가 1년 반에 걸친 추적 끝에 밝혀진 이 사건은 이 연구원의 저서 뻐꾸기알(Cuckoo's Egg)이라는 책에서 밝히고 있는 것 처럼 인터네트에 접속된 주요 군사기관의 호스트에 침입하여 SDI, 미사일 개발 정보등을 불법적으로 빼내 구 쏘련의 KGB 에 팔아넘긴 유명한 사건이다.
- 인터네트 Worm 사건(Internet Worm)
  코넬대학의 한 대학원생이 만든 통신망을 통해 스스로 전파되는 바이러스 프로그램인 Worm 에 의해 7,000 여대의 Berkeley UNIX 버전의 컴퓨터가 하루밤에 고장, 정지된 사건이다.

그 밖에도 국제적으로 해커가 침입하여 시스템의 하드디스크를 모두 지우는 행위 등은 자주 보고되는 사건이며, 이는 국내에서도 보고된 사례가 꽤 있는 편이다. 시스템에 침입하는 침입자

* 종신회원
** 정회원

(해커라는 용어는 엄밀히 말해 좋은 일을 하는 사람이라고 보며, 침입자와는 구별되어야 한다)는 업체가 제작하여 판매할때 시스템이 가진 보안구멍(Security Hole)을 찾아 침입하여 관리자 권한을 획득한 후 피해를 주는 것이다. 인터네트에 가입된 국내의 기관이라면 누구나 침입을 받은 경험이 있을 정도이며, 단지 침해 증상을 관리자나 사용자가 모를 따름인데, 실제로 패스워드 화일이 없어지든가 하드디스크의 정보가 지워진다든가, 사용자의 계정과 패스워드가 모두 침입자에게 넘겨진다든가, 침입자가 만든 뒷문 프로그램(Backdoor Program) 으로 인해 항상 관리자의 권한을 쉽게 넘겨준다든가 하는 일이 수시로 발생하는 것이다. 이러한 심각한 문제를 현재에도 또 앞으로도 가지고 있는 것이 국내의 인터네트의 문제이며, 특히 국내에서는 아직 초보적인 수준이지만 조금 관리자의 관심이 높아지면서 침입자의 방법이나, 행위도 교묘해지고 있는 실정이다.

본고에서는 인터네트에서의 보안문제를 크게 2가지로 나눠 해외 인터네트에서의 보안을 구조적, 공학적으로 해결하려는 표준 연구개발분야들을 살펴보고 다음 현실적인 보안사고들을 예방하고 막아보려는 접근 방식을 살펴보기로 한다. 그리고 국내인터네트에서의 현재 추진하고 있는 현황을 간략하게 언급하기로 한다.

2. 인터네트에서의 보안 연구개발 현황

2.1 IETF SAAG

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 : 전자우편 서비스의 확장, 네트워크 데이타베이스, 네트워크 뉴스 프로토콜, 네트워크 팩스, 네트워크 프린팅, 가상 터미널 프로토콜 등
- Internet : 접속지향IP, 동적 호스트 구성, ATM상의 IP, AppleTalk IP, FDDI IP, 라우터 요구사항
- Network Management : 각종 망관리용 MIB, 어카운팅, 모니터링 등
- OSI Integration : 디렉토리, MHS, OSI 네트워크 운영, ODA 등
- Operational Requirement : 벤치마크, 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, 분산화일시스템, 도메인네임, Service Location Protocol, Trusted NFS 등
- User Service : 디렉토리 서비스, FTP 아카이브, 인터네트 School 네트워크, 네트워크 운영도구, 네트워크 정보 서비스 등

2.2 보안정책 그룹(SPWG/SSPWG)

SPWG(Security Policy Working Group)는 Internet Security Policy의 제안을 위한 그룹으로 기술적인 논의는 물론 관리적인 문제에도 관심을 갖는다. Internet은 단 하나의 기관이 운영하는 네트워크가 아니므로 특정한 보안 정책의 수립과 적용보다는 각각의 기관과 전체적인 네트워크의 보안성 있는 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[4]에서 제공한 가이드라인은 네트워크 운영자, 관리자, 그리고 업체에게 좋은 보안 정책을 세우기 위한 기본을 다음과 같이 정의하고 있다.

- 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 유지 할

책임이 있다. 또한 보안 정책과 이에 대한 변경사항을 사용자에게 알릴 책임이 있다.

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

이와함께 SSPHWG(Site Security Policy Handbook Working Group)은 Site Security Handbook[3]에서 Internet site마다 각자의 특성에 맞는 정책의 개발과 보안 사고 발생시 사후 처리 절차 등에 관해 많은 조언을 하고 있다. 기본적인 접근방식은 저렴한 비용으로 자산을 보호할 수 있는 대응책을 수립, 적용하면서 취약점이 발견되는 대로 개선해가는 것이다. 핸드북의 구성은 다음과 같다.

- section 1 : 개요
- section 2 : Site의 공식적인 보안 정책의 수립
- section 3 : 보안 문제 해결을 위한 절차의 수립
- section 4 : 보안 사고의 처리
- section 5 : 보안 사고 이후의 처리 절차

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

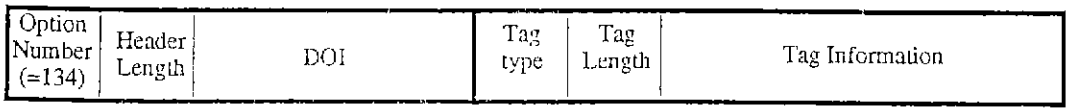
2.3 IP 보안옵션 그룹(IPSO/CIPSO)

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

- DoD Basic Security Option(BSO) : Unclassified, Confidential, Secret, Top Secret의 4가지 classification과 관련 DoD Authority 플래그로써 IP 데이타그램이 레이블이 되며 이를 통하여 엑세스 제어가 이루어진다.
- DoD Extended Security Option(ESO) : 보안 카테고리나 release marking과 같은 부가정보들을 처리할 수 있도록 한다.

두 옵션의 고정 필드들은 Defense International 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 수 없었다. CIPSO 프로토콜을 사용하는 기관은 IANA(Internet Assigned Numbers Authority)로부터 Labeling Number(혹은 Domain of Interpretation Identifier DOI)를 제공받는다. 같은 보안 정책과 보안 요소들의 의미를 동일하게 해석하는 같은 보안 영역의 시스템들은 동일한 DOI를 사용한다. 한 시스템은 여러 보안 영역의 구성원이 될 수 있다. 십여개의 회사들이 CIPSO를 성공적으로 구현하고 상호 연동성의 테스트도 수행했다고 한다. 또한 NIST에서 작



DOI : Domain of Interpretation Identifier, Labeling Number IANA(Internet Assigned Numbers Authority)로부터 할당 받음.

Tag : Security Attribute들을 담고 있다.

그림 1 CIPSO의 구조

업중인 새로운 NIST GOSIP security label과의 연관성에 대한 검토도 진행되고 있다. CIPSO는 IETF와 TSIG가 협력하여 개발하고 있으며 원래 Commercial IPSO라 하였으나 그 목적에 좀더 부합되는 현재의 명칭, Common IPSO로 변경되었다. 1993년 3월 버전의 CIPSO가 Draft Standard로 나와 있으며 추후 Standard로 발표될 예정으로 있다. 그림 1에서 CIPSO의 구조를 보여주고 있다.

- 전자우편그룹
  cipso@wdl1.wdl1.loral.com

2.4 보안 전자우편 그룹(PEM)

PEM은 Internet mail protocol(RFC 822)을 사용하여 전송되는 전자우편 메세지에 1) Integrity, 2) 메세지 발신자 인증(Message Origin Authentication), 3) 기밀성(Confidentiality, 선택사양) 을 제공한다. PEM은 메세지의 암호화에는 대칭적 암호기법(DES)을 키 분배 방식에서는 비대칭적 암호기법(RSA)을 권고한다. 비대칭적 키 분배 방식은 안전하게 키를 공유할 방법이 없는 인터네트의 환경적 특성(광범위한 규모와 관리의 비균일성 등)에 적절하다. PEM이 채택한 표준방식은 CCITT X.509(Directory Authentication Framework) 권고안을 따르는 profile이다. 세가지 보안 서비스를 구현하기 위해 PEM 프로토콜은 다음의 4가지 절차를 통한다.

- Message Digest가 계산된다.
- 송신자의 private key를 이용하여 Message Digest가 암호화되며 이것은 송신자를 식별하기 위한 정보임과 동시에 메세지에 대한 디지탈서명으로 제공된다.
- 기밀성를 제공하는 경우, random DES를 생성시켜 이를 이용하여 메세지를 암호화한다.
- 메세지가 암호화되면 DES 키는 수신자의 공개키로 암호화 한후 메세지에 포함시켜 전송한다.

PEM의 가장 중요한 부분은 송수신자간의 공개키를 어떻게 보증(certificate)할 것인가에 있다. 이러한 문제를 위해 Internet Society에서는 PEM을 위한 공개키 certification hierarchy를 설립중에 있다.이는 authority를 부여해주는 certificate의 global 시스템의 역할을 하게 된다. PEM을 정의한 4가지 시리즈로 된 문서들은 다음과 같다.

- RFC 1421 : Privacy Enhancement for Internet Electronics Mail :
  Part I : Message Encryption and Authentication Procedures, 메세지 처리 절차를 기술
- RFC 1422 : Privacy Enhancement for Internet Electronics Mail :
  Part II : Certificate-Based Key Management, PEM이 채택한 public-key certification system을 정의
- RFC 1423 : Privacy Enhancement for Internet Electronics Mail :
  Part III : Algorithms, Models, and Identifiers, PEM에 사용되는 여러 알고리즘들의 정의와 식별자들을 기술
- RFC 1424 : Privacy Enhancement for Internet Electronics Mail :
  Part IV : Key Certification and Related Services, 사용자 등록과 Certification Revocation List(CRL) 배포 등의 관습과 메세지 형식들을 정의

위 네가지 문서 중 처음 세가지는 RFCs 1113-1115로 이미 발표된 것이다. 모든 문서들은 많은 개정을 거쳤으며 '93년 2월에 Proposed Stan-

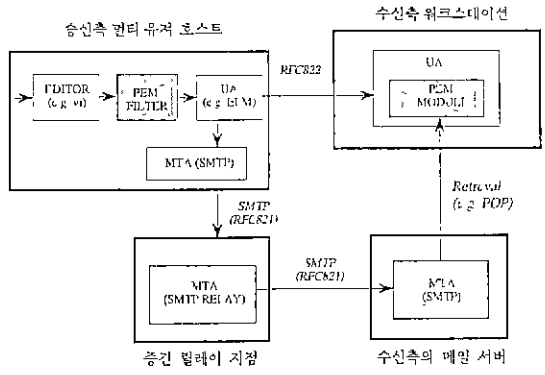


그림 2 PEM Filter 형식의 구현 모델

dard로써 발표되었다. 현재 구현 사례로는 TIS-PEM 등이 있으며 여러 구현들이 EC PASSPORT 프로젝트 작업의 결과로 영국과 독일에서 사용될 것이다. PEM의 모델을 그림 2에서 보여주고 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

2.5 인증 그룹(CAT)

어떤 호스트의 사용자의 신분을 다른 호스트로하여 그 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. CAT 그룹에서는 이들이 사용하는 암호 키방식은 상이하나 제공하는 서비스가 같다는 점에서 응용프로그램들이 어떤 인증 방식하에서도 동작할 수 있도록 하는 공통의 인터페이스를 제공하기 위한 작업을 하고 있다. GSS-API(General Security Servides Application Program Interface)가 그것이다. GSS-API base specification, GSS-API C 언어 bindings, 그리고 Kerberos Version 5 문서가 Proposed Standards로써 검토중에 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

2.6 보안 망관리 그룹(sec-snmp)

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 방지하기위해 secure SNMP는 security "wrapper"를 제공한다. Wrapper는 허가된 management station만이 질의를 보내고 허가된 agent만이 응답할 수 있도록 한다. 이를 위해 secure SNMP는 message digest를 사용하는 대칭적 키 암호를 사용한다. 사용된 함수는 MD5(RFC1321)이다. Confidentiality가 선택 사항으로 제공되어질 수 있으며 이때 DES를 이용하여 질의/응답이 암호화된다. Secure SNMP에 대한 명세서는 Proposed Standard로 발표될 예정이다.

- 관련된 메일링 리스트 :
  - snmp-sec-dev@tis.com

2.7 기타

TSIG(Trusted Systems Interoperability Group)은 컴퓨터업체, SI업체, 사용자, 정부기관들이 모여,

- 안전시스템끼리의 상호연동에 대한 분야를 개발하고,
- 상호연동 사양을 개발하며,
- TSIG 사양에 따라 상호연동을 전시하는

그룹으로서, 1) CIPSO 를 개발하였으며, 2) B1 수준의 보안 NFS 프로토콜, 3) TREES(Trusted Realm Environment Exchange Sevice)라는 분산시스템 환경에서의 인증방법을 개발하였으며 94년초부터 시범을 계획하고 있다.

3. 인터네트 운영상의 보안대책

3.1 보안 침해 모델

침입자는 시스템에 침입한 후 불법적으로 관리자 권한을 취득하고 "rm-rf/" 명령어 하나로써 시스템의 모든 정보를 없에버릴 수가 있으며 실제로 그러한 사건이 종종 발생 되곤 하는 것이다. 이러한 시스템 침입을 예방하기 위한 노력들이 이루어지고 있는데, 인터네트에 접속된 UNIX 시스템등의 호스트, 게이트웨이 등에서의 보안 위험 요소들을 분석하여 적절한 예방(Prevention), 감시(Monitoring, Discovering a Break-in)

등의 기능을 수행하는 연구개발이 많이 진행되고 있으며, 또한 보안이 요구되는 어느 도메인의 네트워크를 외부의 인터네트로부터의 위험으로부터 격리(Isolation)하려는 방법으로서 방화벽(Firewall) 구축 방식들도 최근에 시도되고 있다. 이러한 방법들의 접근을 다음 그림 3과 같이 설명할 수 있으며 이의 요약을 표 1에서 설명하고 있다.

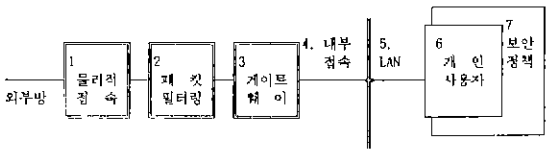


그림 3 인터네트에서의 보안모델

표 1 보안모델 각 계층의 설명

7	보안문제의 정의화 적절한 보안정책 정의
6	보안정책에 의한 사용자 교육
5	내부 LAN에서의 보호
4	내부 LAN 세그먼트의 분리
3	외부로 부터 들어오는 트래픽을 게이트웨이에서 보안
2	외부로 부터 들어오는 트래픽을 리우터에서 필터링
1	모뎀이나, 실제 물리적인 이터페이스에서의 보안

3.2 대표적인 보안 도구

여기에서는 국내에서도 관련 연구개발이 약간 진전되고 있으나 우선 해외 인터네트에서 널리 쓰이고 있는 보안 도구들을 중심으로 요약하여 표 2에 설명하고 있다.

3.3 방화벽(Firewall) 시스템 방법

방화벽시스템(Firewall System)은 인터네트에

표 2 인터네트 보안도구 요약표

분 야	제 품 명	설 명
인 증	npasswd	패스워드관리 정책을 강제화 가능, 길이, 특정패턴 등
	passwd+	추측하기 쉬운 패스워드의 상용을 방지
	shadow	Shadow Passwd, 패스워드 화일의 패스워드를 일반사용자가 없도록 함
	passwd.2.1	기존의 기능에 aging, expire 기능이 추가
	crack	패스워드 화일에서 사용자 패스워드를 알아내는 도구
	kerberos	LAN 환경에서의 주요 정보를 암호화 통신, 인증하는 방법
시스템 점검 예방	miro	보안요소의 정의 및 체크
	COPS	시스템의 권한 모드의 체크, 보안구멍 체크 기능
	Tripwire	UNIX 화일시스템의 Integrity 를 체크하는 도구
	Swatch	syslog 도구등과 같이 시스템의 감시 도구
네트워크	tcp_wrapper	TCP/IP의 응용서비스에 대해 접근제어, 인증, log, 함정기능 제공
	SOCKS	TCP_Wrapper 와 유사한 기능을 하며, 접근제어, log등이 제공됨
	TCPDUMP	Ethernet 상의 트래픽 dump, Traffic Tapping 가능
	nfswatch	NFS 트래픽 모니터링 도구

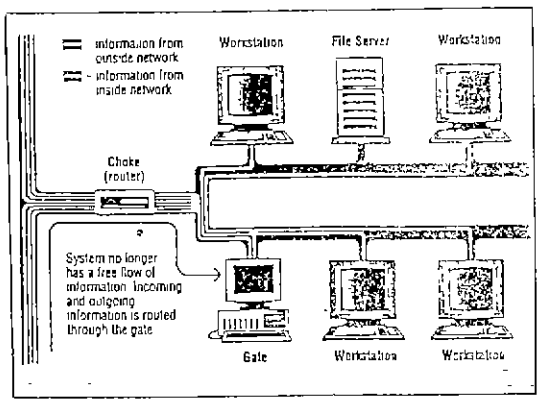


그림 4 Firewall 시스템 모델

접속한 가입기관의 내부도메인 네트워크를 보호하기위한 방법으로, 이는 외부네트워크와 접속하는 게이트웨이 시스템을 단지 하나만 두고 그 시스템에서 인증을 받아야만 내부로, 외부로의 접근을 허용하는 시스템으로서, 그림 2에서 보이는 모델에서의 기본적인 조건은 다음과 같다.

- Choke는 외부에서 들어오는 패킷의 목적지 호스트가 게이트웨이가 아니면 접속을 거부한다.
- 게이트웨이 시스템은 내부와 외부네트워크 패스, 2개의 네트워크 인터페이스를 가진 시스템이다.
- 내부네트워크의 호스트이름, 어드레스, 라우팅정보는 외부로 발행하지 않음으로서 외부에서 내부의 어느 호스트라도 직접 접근하지 못한다.
- 내부 호스트로 접근하려는 외부의 사용자는 게이트웨이 시스템에 계정이 있어야하며, 인증을 받아야만 내부 시스템에 접근할 수 있다.
- 게이트웨이 시스템은 Dynamic Routing을 실행하지 않으며, Static 라우팅만이 제공된다.
- 게이트웨이 시스템은 일반 사용자계정을 가지고 있지 않으며, 단지 root, 그리고 외부에서 내부 도메인으로 접근이 허용된 사용자계정만이 있다.
- 게이트웨이 시스템은 해커의 표적이 되는 시스템 유틸리티들을 삭제하고, Trojan Horse, Backoor의 표적이 되지않도록 권한 조정과 보안환경을 극대화한 시스템이다.

이러한 Firewall 시스템은 최근 활발하게 연구개발되고 있는 현실적인 보안대책의 하나로서 위의 기본적인 개념하에 다음 표 3과 같은 여러가지 공개, 상용의 제품들이 발표되고 있으며, 앞장의 TCP_WRAPPER 도 게이트웨이 시스템에 적용할 수 있는 Firewall 시스템의 일종이라고 볼 수 있다.

표 3 발표된 Firewall 시스템 모델

제 품 명	개 발 자	공/상	
InterLock	ANS CO+RE Systems, Inc.	상용	TELNET, FTP, SMTP Gateway, X-Window, NNTP 응용 접근제어, Logging, 사용자인증, 트래픽 암호화등
Eagle Network Security Management System	Eagle Network Security	상용	시스템 인증, Monitoring & Tracing, Real Time Event Reporting, Audit Log, 사용자 인증 등
Internet Firewall Toolkit	Trusted Information Systems	공개	FTP, TELNET, rlogin, NNTP Proxy 서비스, SMTP Gateway, 사용자 인증, TCP 접근제어
Texas TAMU	Texas TAMU Univ	공개	라우터 필터링, 스크린
Karlbridge	Ohaio Univ.	공개	PC-Based 라우터 필터링 키트
Cisco's ??	CISCO, Inc.	상용	CISCO 라우터의 액세스 리스트를 통한 필터링

3.4 보안사고응답센터

현재 국내에서 보안 침해 사례가 빈번하게 발생하고 있음에도 불구하고 적절하게 이에 대응하지 못하고 있는 까닭은 전문적인 보안관련 전담기능을 하는 곳이 없어서 이기도 하다. 이러한 기능을 해외에서의 여러 보안센터들을 파악함으로서 국내에서의 보안센터가 어떠한 기능을 담당해야할지를 도출하는 계기로 삼아야할 것이다. 주로 미국에서의 인터네트보안센터를 분석하고자 하는데, 보안 침해 사고를 통하여 이에 대한 체계적인 대응책을 마련하고자 세워진 보안 응답 센터이므로 국내에서도 이의 운영 모델을 잘 파악한다면 도움이 되리라고 여겨진다. 그리고 보안센터 이외에서 제공하는 보안관련 정보를 획득하는 것을 위해 해외에서의 보안 전자우편 그룹을 소개 분석하기로 한다.

3.4.1 CERT/CC

1988년에 발생한 Internet Worm 사건은 미국 인터네트의 보안 취약점을 드러낸 중요한 사건으로서 기록되었다. 이 사건 이후 곧장 미국방성 첨단 프로젝트 관리국에서 체계적인 인터네트 보안전담기구를 결성하기로 하였으며 Computer Emergency Response Team/Coordination Center (CERT/CC)를 카네기멜룬대학내 소프트웨어 엔지니어링연구소 산하에 조직을 만들었다. CERT/CC는 어떤 보안침해 사고가 접수되면 전문가들을 동원하여 문제를 해결하고 인터네트 전체에 해결책을 전파하는 역할을 담당한다. 즉 CERT는 보안침해, 시스템보안문제점을 사용자뿐만 아니라 제조업체들을 위해 해결하는 역할을 수행한는 것이다. 이를 위해 CERT가 하는 업무는,

- 보안문제 해결책 지도 전자우편그룹 운영 : cert-advisory@cert.sei.cmu.edu
- 보안문제 해결책 지도 Netnews 그룹운영 : comp.security.announce←cert-advisory와 같은 내용
- 24시간 보안 접수 및 상담 전화 운영 :
- 보안관련 프로그램개발 전자우편그룹의 운영 : cert-tools@cert.sei.cmu.edu
- Anonymous FTP를 통한 보안관련정보의 배포 : cert.sei.cmu.edu

3.4.2 DDN SCC

DDN Security Coordinaton Center는 DDN 사용자를 위하여 운영되는 보안센터로서 CERT/CC와 유사한 기능을 담당하고 있으며, 보안문제를 해결하고자 하는 센터이다. 그리고 DDN에서는 보안문제를 위한 전자게시판을 운영하고 있다. nic.ddn.mil에 액세스하며 SCC 디렉토리내의 DDN-SECURITY-yy-mm.TXT(yy : 년도, mm : 게시판번호)를 Anonymous FTP로 정보를 가져올 수 있다.

3.4.3 NIST CSRC

NIST Computer Security Resources and Response Center(CSRC)는 NIST가 주로 미정부기관들을 위한 컴퓨터, 정보처리기계들을 담당하므로 보안문제에 관한 센터를 발족한 것이다. 특히 virus 대책에 관한 가이라인 문서를 개발한 바 있으며 csrc.ncsl.nist.gov 에서 보안관련 정보를 Anonymous FTP를 이용하여 가져올 수 있다.

3.4.4 DOE CIAC

미국 에너지성에서 운영하는 Computer Incident Advisory Capability (CIAC)는 주로 미에너지성 산하기관을 위해 발족되었으며 Lawrence Livemore National Lab.(LLNL)의 4명의 컴퓨터 전문가들이 이를 위해 종사하고 있다. 보안문제 접수는 ciac@tiger.llnl.gov를 이용하면 된다.

3.4.5 NASA CNSRT

NASA Ames 연구센터에서 운영하는 Computer Network Security Response Team(CNSRT)는 CERT/CC의 Local Version으로서 주로 NASA기관과 연구소내 사용자들을 위한 보안센터이다. cnsrt@ames.arc.nasa.gov로 접촉하면된다.

3.4.6 보안 전자우편그룹

위에서 열거한 보안센터에서 운영하는 전자우편그룹이 아닌 기타 보안관련 전자우편그룹들이 있다. 이것은 순수 보안관련한 정보교환 전자우편그룹도 있지만, UNIX, 혹은 TCP, SUN System 등 다양한 주제로 보안문제를 다루는 경우도 있기 때문에 특히 여기에서는 밀접한 관련이 있는 경우를 다루고자 한다.

- SUN Customer Warning System(CWS)
  CWS는 1990 cert-tools 전자우편그룹으로 발표하였으며, 주로 SUN 제품의 보안문제를 접수받아 해결하고, patch를 배포한다. security-alert@sun.com으로 운영하고 있다.
- Zardoz
  Neil Gorsuch가 운영하는 제한된 UNIX보안그룹으로서 보안사고의 문제가 널리 알려지기 전에 미리 문제를 분석 배포하게 된다. 상세한 보안정보를 다루므로 가입하기가 까다로운 편인데 가입하기 위해서는 security-request@cpd.com으로 신청하면 Internet WHOIS 등을 통해 확인하고 가입이 허락된다. 즉 시스템관리자를 대상으로 하고 있다.
- RISKS
  RISKS Digest는 컴퓨터의 보안과 프라이버시 등에 대해 토론하는 ACM Committee의 기능으로서 risks-request@csl.sri.com으로 가입하고 comp.risks USENET 그룹도 있다.
- TCP-IP
  TCP-IP프로토콜 개발자 및 관리자등을 위한 전자우편그룹으로서 보안문제도 다루고 있다.
  tcp-ip-request@nic.ddn.mil로 신청하며 comp.protocols.tcp-ip USENET그룹도 존재한다.
- SUN-SPOTS, SUN-NETS, SUN-MANAGERS
  SUN Micro사의 제품을 사용하는 사용자, 시스템관리자들의 전자우편그룹으로서 가입신청은 다음과 같다.
  sun-spots-request@rice.edu
  sun-nets-request@umiacs.umd.edu
  sun-managers-request@eecs.nwu.edu

3.5 보안사고의 대응

3.5.1 기본 대처 상황

현재 침입을 당하고 있는것을 알았을 때, 혹은 침입의 흔적을 발견했을때 어떻게 해야 할지 보통 시스템 관리자는 당황하게 된다. 이럴 경우를 대비하여 사실 미리 이 경우의 절차를 정책으로 세워두는 것이 필요한 것은 당연하다. 아뭏든 이 경우 어떻게 할 것인지 보기로 한다. 먼저 다음을 염두에 두고 사태에 대처하는 것이 중요하다.

1) 그 침입자를 포착하여 잡을수는 있을까?
2) 시스템의 손상을 어떻게 복구 할것인지?

그리고 주의해야 할 점으로서 1) 당황하지 말고, 2) 정말 침해당한 것인지 의심해보는데, 시스템 관리자나 프로그래머의 실수일 가능성이 있기 때문이며, 3) 실제 화일이 손상을 입었나? 많은 경우 침입자는 그렇지 않은 경우가 많으며, 4) 증거물을 획득하고 보관할 필요성을 체크하며, 5) 가능한 빨리 복구하여 정상화해야 하는가?, 6) 화일의 변경유무를 다시 확인할 필요성이 있는가?, 7) 내부나 외부 사람이 이일을 알아도 되는가?, 8) 다시 발생가능한 일인가?, 9) 문서화 작업, 10) 즉시 log를 만들어야 하는데, 연필로 써도 좋고, 하드카피나, script(1) 명령을 이용할 수도 있을 것이다.

3.5.2 침입자의 발견

침입자를 발견하기 위해서는 다음과 같은 여러가지 형태를 알아야 한다.

1) 관리자가 침입자의 활동을 직접 모니터링할 수도 있으며,
2) security hole, /etc/passwd 등의 시스템 화일이 변경된것을 확인하거나,
3) 다른 지역의 관리자로부터의 통지를 받아 알 수도 있다.

관리자가 이를 알기 위해서는 시스템의 비정상적인 활동이나, 현상을 파악하는 것인데, 예를 들어 다음과 같은 것들이다.

1) 한 사용자가 둘이상 로그인하고 있다
2) 일반 사용자가 컴파일러, 디버거를 사용한다
3) 네트워크에 로드를 걸고 이상한 프로그램을

실행한다
4) 한 사용자가 많은 외부 접속을 시도하고 있다
5) 일반 모뎀 사용자가 아닌데 모뎀으로 로그인하고 있다
6) 관리자가 아닌데 관리자로 명령어를 사용한다
7) 휴가이거나 근무시간이 아닌데 사용한다

3.5.3 해커 발견후 조치

침입자를 발견한 후 관리자의 초치는 상황을 보며 판단하는 것이 좋은데, 다음은 일반적으로 취할 수 있는 방법들을 열거한 것이다.

1) 무시한다?
2) 대화한다, talk(1),write(1) 등으로 적절하게 추적할 시간을 벌며 침입자의 의도도 파악하려는 방법이다.
3) 접속을 추적한다 : 침입자를 실제 잡으려는 시도인데, 네트워크로 접속한 경우에는 대화하며 역추적할 충분한 시간을 벌어야 한다. 물리적 단말기일 경우 즉시 단말실에서 확인한다.
4) 접속을 끊는다, process, 네트워크 연결을 끊거나, 전원을 중단한다.

여기에서 네트워크를 통해 들어온 침입자를 역추적하기 위해 finger, rwho, netstat 등의 명령을 통해 알아보는데, 상대 시스템의 정보를 알아낸후 상대 시스템 관리자의 협조를 요청한다.

충분한 대비를 한 다음 침입자를 몰아내야 하는데 가장 간단한 방법은 전원을 꺼버리거나, 아니면, 그 침입자의 패스워드를 바꾸고 침입자의 프로세스를 죽인다(kill!). 만약 관리자에게 들킨것을 침입자가 먼저 알아낸다면 관리자나 시스템에 큰 손상을 먼저 가할 수도 있는 것이다.

3.5.4 침입자의 침입방법 분석

이를 위해서는 UNIX의 log 화일을 분석해야 하는데, 주로 1) 비정상적인 시간대의 login 과, 2) Failed Login 이 많은 경우, 3) 의심스러운 su 명령, 4) 낯설은 시스템으로부터의 login 등을 우선 체크한다. 하지만 교묘한 침입자는 대부분 이러한 시스템 log 화일이나, 자신의 사용흔적을 지워 보통의 정상상태로 만들어 두는 예가 많다. 이것이 어려울 경우 아예 log 화일 전체를 없애버리기도 한다.

3.5.5 침입자의 시스템 불법 정리

침입자를 몰아내고 여러분석을 마친 후 침입자가 만들어둔 여러가지 불법작업들을 정리해야 하는데, 먼저 새로운 계정을 만든 경우에는 /etc/passwd 화일을 원래대로 복구해야한다. 특히 UID 가 0인 경우, passwd가 없는 경우 등을 검사한다. 그리고 침입자들이 만들어둔 불법 바이러스 프로그램 등을 없애기 위해 SUID, SGID 프로그램 등을 색출하고 화일과 디렉토리 등의 권한 모드의 변경 유무 체크, backup과 비교 Integrity 체크를 시도한다. 특히 다음과 같은 시스템 화일의 조작이 있는지 필히 검사한다.

/.rhosts
/.forward
/etc/hosts.equiv
/etc/netgroups
/etc/exports
/usr/spool/cron/crontabs

그리고 감추어진 화일과 디렉토리들을 찾기 위해 /etc/fsck 를 이용하거나, /usr/bin/cat -v 등을 이용한다. 또한 침입자가 지우지 못하고 혹은 실수로 남겨둔 주인없는 화일을 찾기 위해서는 다음 명령을 사용한다.

```
# find / -nouser -o -nogroup -print
```

4. 국내에서의 관련 활동

국내 학술연구전산망은 연구전산망(KREONet)을 비롯하여 HANA, KREN 등이 있으며, 서로의 정책적인 결정사항들을 국내에서 조정하기 위해 ANC(Academic Network Council, 의장 : 전길남)이 조직되었고 기술적인 문제의 조정이나 상호 기술력 향상을 위해 SG-INET(의장 : 박현제)가 ANC의 보조로 조직되어있다.이는 인터네트의 IAB(Internet Activity Board) 산하의 보조로서 존재하는 IRTF(Internet Research Task Force)나 IETF(Internet Engineering Task

Force)와 유사한 체계를 갖추기 위해서 이다. 그리고 국내 학술연구전산망이 그 규모가 확대됨에 따라 SG-NET에서는 IETF에서의 연구개발과 기술을 습득하기 위한국내에서의 구체적인 작업 그룹들이 요구되었고, 라우팅 관련기술, 네트워크 정보관련기술, 한글 관련기술, PC통신 관련기술, 네트워크 관리기술, 네트워크 보안기술 등 시급하게 필요한 부분을 묶어 관련 연구자들을 집약, 기술개발 노력을 하기에 이르렀다. 보안관련 작업그룹은 1992년 7월30일 15여 인원들이 참석한 가운데 첫 회의를 가지고 다음과 같은활동 목표들을 세웠다.

- IETF SAAG에서의 연구개발 습득 및 국내 기술 개발
- 국내 보안침해 모니터링 및 자문
- 보안지침서 등의 발간

초기에 작업그룹에서 활동하는 회원들은 주로 각 가입기관의 네트워크관리자들이 중심이 되어 자발적인 참여에 의해 운영되고 있었으나, 회원들의 잦은 교체와 각자의 업무부담으로 인해 적극적인 활동은 이루어지지 않고 있으며, 최근까지 5회에 걸쳐 회의와 세미나가 있었다.[11] '93년도의 사업목표는 (1) 국내인터네트 관리자를 위한 보안 지침서의 개발 및 배포, (2) 보안센터 체제의 구축, (3) IETF SAAG현황 및 분석 보고 등으로서 그 성과는 아직 미지수라고 볼 수 있겠다. 먼저 (1)의 경우 부록 A와 같은 목차를 잠정결정하고 자발적인 회원들을 중심으로 진행하고 있으며, (2)의 경우 최근 SERI에서 구체적인 프레임워크를 연구한 바 있다. 그리고 (3)의 경우에는 인터네트에서 개최되는 IETF Conference의 지속적인 참가 및 메일링 리스트의 등록을 통한 최근 정보의 수집 등이 요구되는데 SAAG의 4개의 주된 작업들을 구체적으로 담당을 맡길 필요성이 대두되고 있다고 본다. 본 그룹의 가입과 관련자료의 획득 등의 문의를 위한 메일링 리스트는 다음과 같다.

- security-request.security@garam.kreonet.re.kr
- chlim@garam.kreonet.re.kr, hjy@etrivax.etri.re.kr

지금까지는 자발적인 회원들의 참여에 의해서만 활동이 이루어져 왔으므로 구체적인 결과물과 성과를 얻는데는 미흡한 면이 있었으며 앞으로는 다음과 같은 부분에 초점을 맞추어 진행하고자 한다.

- 프로젝트의 추진 : 관련기관의 협조를 받아 국내 학술연구전산망에서 시급하다고 판단되는 관련기술을 프로젝트화하여 인력과 효율성을 높힌다.
- 시스템 보안 전문가의 흡수 : 보안문제를 기술적으로 자문할 수 있는 전문가 그룹으로 흡수하여 활성화된 작업그룹을 운영한다.
- SAAG 산하의 그룹과 대응되는 소그룹의활성화 : SPHWG, PEM, CAT, IPSO 등 IETF SAAG의 그룹 각각의 기술들을 습득하고 자체 개발하는 소 그룹을 조직한다.
- 관련 지침서 및 기술문서의 배포 : 국내에서 요구되는 지침서나 관련 문서들을 개발하거나 필요하다면 인터네트의 중요한 문서들을 번역 발간한다.

5. 결 론

이상으로 인터네트에서의 보안관련 연구개발 현황으로서 인터네트의 현재 운영상 발생하는 문제점에대한 것과 IETF/SAAG에서의 보안관련 프로토콜 및 서비스 개발이라는 두가지 관점에서 살펴보았으며,그리고 국내 보안그룹에서의 활동 현황도 살펴보았다. 인터네트의 전세계적으로나 국내에서의 발전 및확대추세에 미루어 보았을 때, 아직 국내에서는 관련 기술이 아직 미흡한 점이 많으며 또한 국내에서도학술연구전산망에서 보안침해 사고가 많이 발생하고 있으나 그에 대한 대책이 미비한 실정임을 볼 때이에 대한 관심과 연구개발 투자가 시급하게 요청되고 있는 것이다. 그리고 아직은 국내 보안그룹의 활동이 미비한 실정인데 이는 각 기관의 자발적인 관심자들의 지원에만 의존하고 있으며, 또한 ANC나 SG-INET등이 공식적인 조직이 아닌 자발적인 협조 조직일 뿐이라는 면에도 기인한다고 본다. 그러므로 본 보안그룹에 대한 지원이 관련 기관 등을 통해 이루어진다면 국내의 네트워크관리자 및 보안관리자들이함께 조직된 그룹으로서 협조

하는 활동적인 그룹이 되리라고 본다.

참고문헌

[1] Robert B. Reinhardt, An Architectural Overview of UNIX Network Security, Oct.8, 1992.

[2] David A Curry, UNIX System Security: A Guide for Users and System Administrators, Addision-Wesley, 1992.

[3] Garfinkel & Spafford. Practical UNIX Security, O'Reilly & Associate, Inc.,1992.

[4] Clifford Stoll, "Stalking the Wily Hacker", Communications of the ACM , May 1988.

[5] Daniel C. Lynch, Marshall T. Rose, Internet SystemHandbook, Addison-Wesley, 1993.

[6] RFC1244, Site Security Handbook.

[7] RFC1281, Guidelines for Secure Operation of the Internet.

[8] Steve Crocker, Ocerview of Internet Security Development, INET '93, June 1993.

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

[10] Richard D. Pethia, Kenneth R. Van Wyk, Computer Emergancy Response-An International Problem, CERT/CC SEI CMU, 1990.

[11] Russell L. Brand, Coping with the Threat of Computer Security Incidents A Primer from Prevention through recovery, CERT, 1990.

[12] W.R. Cheswick, "An Evening with Berferd, In Which a Cracker Is Lured, Endured, and Studied", Proceedings of the Winter USENIX Conference, 1992.

[13] Eugene H. Spafford, "The Internet Worm Program: An Analysis", Purdue Technical Report CSD-TR-823, Nov. 1988

[14] S.M. Bellovin, "There Be Dragons", Third UNIX Security Symposiyum. 1992.

[15] Alessandro Berni, Paolo Franchi, Joy Marino, "Experience of Internet Security in Italy," Third UNIX Security Symposium, 1992.

[16] L. J. Hoffman, "Rogue Programs: Virus, Worms and Trojan Horses, Van Nostrand Reinhold, 1990.

[17] Bill Cheswick, "The Design of a Secure Internet Gateway", AT & T Bell Lab. 1991.

[18] Herve Schauer & Christopre Wolfhugel. An Internet GateKeeper, UNIX Security Symposium III. Sept. 1992.

[19] Marcus J. Ranum, A Network Firewall, Digital Equipment Corp., 1992.

[20] Wietse Venema, TCP WRAPPER:Network Monitoring, Access Control and Booby Traps, UNIX Security Symposium III, Sept. 1992.

[21] ANS CO%RE, Inc., InterLock-The Key to Network Security, May 1993.

[22] TSIG, Trusted Realm Environment Exchange Serveice.

[23] TSIG, Trusted Systems Interoperability Group: FAQ with Answers, Jan. 1944.

[24] TIS, Internet Firewalls Frequently Asked Questions, March 1994.

[25] Raptor Systems Inc., Eagle Network Security Management System : User's Guide V 2.2.

[26] TIS, TIS Internet Firewall Toolkit-An Overview,User's Overview, 1993.

[27] 임채호, WG-SECURITY : 0001, 국내시큐리티 WG계획, 1992.7.

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

[29] 시스템공학연구소, Workstation Security Guide Summary, 1993.

[30] 임채호, UNIX 시스템 보안가이드, 통신정보보호학회지, 1권2호, 1991. 8.

[31] 임채호, 한상철, 변옥환, 연구전산망 보안 가이드, 동계컴퓨터통신워크샵논문집.

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

[33] 임채호, 한상철, 변옥환, "연구전산망 보안 가이드", 동계컴퓨터통신 워크샵논문집, 1992.1.

[34] 임채호, 인터네트보안, KRNET '93, 7. 1993, KTRC.

[35] KUS, "WG-SECURITY : 0003,Discovering a Break in", 1992.7.

[36] 시스템공학연구소, "Workstation Security Guide Summary", 1993.

[37] 이필중, 정진욱, 박멍순, 이재용, "전산망의 안전대책 개요", 정보통신보호학회지, 1권2호, 3호, 1991.8.

[38] 서보환, 한상철, "연구전산망과 과학기술정보유통의 보안대책 연구", WISC '91, 1990 4.

[39] 한국전산원, 전산망 안전신뢰성 표준개요, 1993.4

정 진 욱

성균관대학교 전기공학과 졸업
서울대학교 계산통계학과(전산학 박사)
한국과학기술 연구소 연구원
한국과학기술 연구원 시스템공학연구소 데이타통신 실장
Maryland 대학교 객원교수
(현) 성균관대학교 정보공학과 교수

임 채 호

1986 홍익대학교 전산과 학사
1990 건국대학교 전산과 석사
1991 ~현재 홍익대학교 전산과 박사과정
1985 ~1992 시스템공학연구소 선임연구원
1992 ~현재 대전실업전문대학 전산과 교수
관심 분야 : 컴퓨터통신, 컴퓨터통신 보안, 운영체제보안, 분산시스템

제 21회 정기총회 및 추계학술대회

- 일 자 : 1994년도 10월 28일~29일
- 장 소 : 연세대학교
- 주 최 : 한국정보과학회
- 문 의 : 학회 사무국
  Tel : 02-588-9246
  Fax : 02-521-1352