정보보호와 기술의 활성화 방안

An Active Planning of the Information Security and Technology

장 우 권(Woo-Kwon Chang)*

목 차

초 록

지식경제가 기반이 되는 21세기에 인터넷의 개방성, 글로벌성, 접근용이성이 기술, 산업 그리고 문화의 새로운 융합과 발전을 구축하는 중심 축이 되고 있다. 그러나, 사이버공간에서 발생되고 있는 정보화의 역기능(인터넷을 이용한 각종범죄, 정보시스템 불법침입 및 파괴, 불건전정보의 유통, 개인의 프라이버시 침해, 개인정보의 오남용 등)들은 갈수록 빈번하고 지능화되고 있어 심각한 사회적 혼란과 국가의 전략적, 행정적, 경제적으로 막대한 손실은 물론 군사활동마저 마비시키고 있는 실정이다.

따라서 본 글에서는 사이버공간에서의 범죄행위를 예방하고 차단시킬 수 있는 정보보호와 기술 그리고 그 패러다임을 조사 분석하여 기술하고 정보보호기술과 산업현황을 국내외적으로 알아본 다음 정보보호기술의 측면에서 바람직한 활성화 방안을 제시한다.

키워드: 인터넷, 정보화 역기능, 정보보호, 정보보호기술, 정보보호산업

ABSTRACT

In the 21st Century of the Knowledge-based Economy Internet's Openness, Globality, and Ease to access is the central axis to construct the new melting down and the development of the technology, industry, and culture. However, it takes place the disordered ability in the information society. That is, to intrude personal privacy, unlawful actions, to circulate an illegal information, to encroach and to destroy information system, even to, to be in confusion society, national strategy, administration, economy, and military action.

As conclusion, first, in this article it looks into and analyzes the information security, technology, and paradigm to prevent and to stop up criminal actions in the cyberspace. Second, this author propose an active planning of the information security and technology.

* 전남대학교 문헌정보학과 강사
접수일자 2000년 12월 6일

1. 서 론

인간은 진정 만물의 영장일까, 수천 년 동안 내려온 영적인 신의 존재는 끝나는 것일까. 얼마전 미국을 비롯한 선진국 과학자들에 의한 『인간게놈지도』 완성발표는 우리의 넋을 혼돈 속에 빠져들게 하였다. 과학기술의 발전은 어디까지 갈 것인가. 하지만 세계곳곳에서 들려오는 자연재앙과 과학기술발전에 의한 사생활 침해 등은 우리를 슬프게 하고 있는 것이다.

흔히들 오늘날 사회를 지식정보화사회라고 한다. 모든 사회구성원 및 조직, 그리고 업무의 정보기술의존도가 심화되는 즉 고도로 발전된 정보기술활용을 극대화하여 지식정보경쟁력을 제고시키는 일련의 사이버 패러다임시대가 도래하고 있다.

얼마 전까지만 해도 "정보의 홍수", "정보의 바다", "정보의 보고"라는 막연한 추상적인 개념들이 전자상거래, 원격교육, 온라인행정서비스, 전자투표 등 정치, 경제, 사회, 문화의 모든 영역에서 실생활에 활용되고 있다. 이것은 시공을 초월해 모든 정보가 생산, 가공, 축적, 유통되는 새로운 패러다임의 인터넷이 출현한 결과이다.

인터넷의 개방성, 글로벌성, 접근용이성이 기술, 산업 그리고 문화의 새로운 융합과 발전을 구축하는 중심 축이 되고 있다.

따라서 21세기는 사이버공간의 확대, 선점이 곧 국가와 기업 그리고 개인의 생존경쟁력의 바로미터가 될 것이다.

그러나, 사이버공간에서 발생되고 있는 정보화의 역기능(인터넷을 이용한 각종 범죄, 정보시스템 불법침입 및 파괴, 불건전 정보의 유통, 개인의 프라이버시 침해, 개인정보의 오남용 등)들은 갈수록 빈발하고 지능화되고 있어 심각한 사회적 혼란과 국가의 전략적, 행정적, 경제적 막대한 손실은 물론 군사활동마저 마비시키고 있는 실정이다.

아무리 훌륭한 지식과 정보시스템이라 할지라도 심각한 범죄를 야기한다면 무슨 소용이 있겠는가.

따라서 본 논문에서는 이러한 사이버공간에서의 범죄행위를 예방하고 차단시킬 수 있는 정보보호와 기술 그리고 기업체나 도서관에서 응용되고 있는 그 패러다임을 조사 분석하여 기술하고 정보보호기술과 산업현황을 국내외적으로 알아본 다음, 정보보호기술의 측면에서 활성화 방안을 제시하고자 한다.

2. 정보사회의 역기능과 정보보호기술

2.1 정보사회와 역기능

일찍이 앨빈토플러(Alvin Toffler)는 그의 저서 『제3의 물결』에서 정보사회의 도래를 예견했으며, 이 시대의 부(富)의 원천을 "정보(information)"라고 하였다. 또한 미래학자 피터 드러커(Peter Drucker), 다니엘 벨(Daniel Bell) 등은 다가오는 사회는 과거와 단절된 새로운 『디지털혁명(Digital Revolution)』의 시대, 즉 지식(Knowledge)과 정보(information)가 경제와 사회발전을 결정하는 핵심 패러다임의 시대, 국가경쟁력의 원천이 되는 지식혁명의 시대가 될 것이라고 예측하였다.

실제로 인터넷의 출현으로 우리사회의 모든

분야에서 대변혁(大變革)이 이루어지고 있는 실정이다. 최근의 여러 통계에 의하면, 미국에서 5천만명의 사용자를 확보하는데 걸리는 시간을 조사했더니 〈표 1〉과 같이 걸렸다고 한다. 또한 인터넷 거래가 100일마다 2배가된다는 통계와 2000년 10월말 현재 국내 인터넷 이용자 수가 2000만 명에 이르렀다니 정보통신의 혁명적 발전에 의한 인터넷 세상이 되고 있는 것이다.

우리는 현재 자신의 컴퓨터 앞에 앉아 세계 곳곳의 문화를 관광할 수 있고, 신문과 TV를 보거나 시청할 수 있고(인터넷 신문과 방송), 서로의 안부를 물을 수 있으며(전자메일), 의식주나 전자제품, 영화와 연극, 그리고 스포츠 입장권을 주문할 수 있다.(전자상거래) 즉, 지식정보화에 의한 생활의 편리성이 진전될수록 외부침입(해킹과 바이러스 유포)과 내부상의 중요 기밀문서가 외부로 유출되는 등의 사생활 침해와 경제적 손실 등의 정보화의 역기능이 날로 증가되고 있어 심각한 사회문제가 되고 있다.

정보화의 역기능을 살펴보면, 첫째, 정보통신기술의 발달과 컴퓨터의 보급에 의한 음란·폭력물, 남을 해치는 허위사실 등의 불건전 정보의 유통이 다양하게 전개되고 있다.

둘째, 불특정 다수를 노리는 대규모 해킹과 웹기반 악성 바이러스 등의 신종바이러스 출현으로 인한 개인정보, 거래정보 등 자료의 유출, 변조, 삭제, 서버 및 네트워크 파괴 등으로 막대한 정신적, 경제적 손실을 주고 있다.

셋째, BBS, LAN 등의 사설통신망, E-mail에 의한 개인의 통신 프라이버시 침해와 인터넷상에서 개인신용정보 유출에 의한 개인정보의 오남용은 개인의 인격형성의 저해, 건전한 대인커뮤니케이션과 상거래 커뮤니케이션의 불신으로 사회와 경제생활을 위축시키고 있다.

넷째, 불특정 다수인들을 상대로한 인터넷사기와 도박, 스토킹(사이버), 매매춘 알선(원조교제)의 각종범죄가 늘어나고 있다. 다섯째, 인터넷 등 정보통신망을 통한 암호기술의 부정이용(예, 전자상거래)은 정보유통에 심각한 부작용을 일으킬 뿐만 아니라 국가안보와 공공질서를 저해하는 범죄행위에 이용되고 있다.

여섯째, 인터넷 홈뱅킹, 온라인 민원행정서비스, 도서관에서의 온라인 상호대차와 대출/반납시 타인명의의 ID나 패스워드(비밀번호와 기호) 도용, 송수신 신용카드정보, 개인 의료정보 등에 의한 정보의 유출 위험이 증가하여 전자거래의 안전성과 신뢰성이 저해되고 있다.

2.2 정보보호의 정의와 그 필요성

정보보호(Information Security)란 통신이나 컴퓨터 등에서 처리하는 정보를 제3자로

〈표 1〉 5천만명 사용자 확보기간

구 분	시간(기간)
전 화	25년
라디오	38년
TV	13년
케이블 TV	10년
인터넷	5년

불법적인 열람, 변환, 파괴로부터 보호하는 것이다. 즉, 사이버공간에서 일어나는 불법적인 해킹, 바이러스 유포, 기업과 개인정보의 유출과 파괴로부터 보호하는 것이다. 또한 위에서 언급한 정보와의 역기능을 순기능으로 바꾸는 것이라고 할 수 있다.

그렇다면 정보보호가 왜 필요한가. 인터넷이 가지고 있는 개방성, 글로벌성, 접근용이성 때문에 누가 언제, 어디에서든지 정치, 경제, 사회, 문화 등의 생활공간에서 편리한 혜택을 누리고 있지만, 역으로 모든 사람들에게 공개되어 있는 사이버공간이기 때문에 지역과 거리, 시간의 개념이 존재하지 않으며, 언제, 어디서, 누가, 어떤 경로를 통해서든 공격할 대상의 취약점이 발견되면 수초이내에 공격하여 상황을 종료해버린다는 것이다. 오랫동안 심혈을 기울여 아무리 좋은 정보를 구축해 놓았다할 지라도 시스템과 DB가 파괴되어 복구가 어렵고 무용지물이 되어버린다면, 어떻게 될 것인가를 상상해 보라. 지식정보의 유무형의 가치 및 의미를 상실하게 될 것임은 물론 이에 따른 정신적·물질적 피해보상은 어떻게 받을 것인가.

따라서, 안정된 지식정보사회를 구축하는데 필수적인 정보를 보호하지 않으면 안될 이유와 그 필요성이 여기에 있는 것이다. 뿐만 아니라 지식정보를 보호할 영역은 개인정보, 사생활보호, 기업정보, 주요 사회기반에 대한 정보, 그리고 국가기반에 대한 정보 등으로 확대되어야 하고, 정보보호기술산업을 활성화시키고 법률적, 제도적으로 적극적인 지원이 이루어져야 한다. 예를 들어, 1994년에 제정된 『공공기관의 이용 및 보호에 관한 법률』, 1998년 2월부터 운영되고 있는 『정보화촉진기본법』, 1999년 2월에 제정되고 동년 7월1일부터 시행되고 있는 『전자서명법』과 『전자거래기본법』, 2000년에 제정예정인 『암호이용촉진법』을 들 수 있다.

2.3 정보보호기반기술

암호화된 메시지로 정보의 안전성과 신뢰성을 보장하는 수단인 암호기술, 상점과 소비자는 서로간의 신분을 확인하거나 메시지의 변경이 없다는 메시지 무결성(integrity)을 인증(Authentication)하는 인증서비스기술, 분산환경하에서 데이터전송시 사용자가 요구하는 수준의 비밀성 보장과 무결성 지원을 위해 비보호(no-protection), 무결성, 비밀성(confidentiablity), 무결성 및 비밀성 등과 같은 파라미터를 갖는 QoP(Quality of Protection) 기능을 지원하는 CORBA(Common Object Request Broker Architecture)의 관리 및 제어에 의한 보안서비스 등의 접근통제기술, 그리고 네트워크 보안기술 등은 정보를 보호하는 기반기술이다.

① 암호기술과 응용서비스

암호기술은 인터넷을 이용한 사이버업무를 변환될 때 야기되는 여러 가지 문제를 해결해 주는 툴로써, 통신의 주체인 송신자와 수신자를 제외한 제3자로, 전송로상의 정보를 위조/변조 유출하려는 능동적인 도청자(active wiretapper) 또는 부정한 사용자(dishonest user)를 막기 위한 기술이다.

또한 전송된 정보의 송신자/수신자를 확실하게 보장하는 기술, 정보의 위변조를 판단하는 기술, 전자계약에서의 동시성문제, 계약시간을

확인해주는 시점확인(tine-stamp)문제, 전자상거래에서의 거래당사자들간에 형평성을 보장하는 공정성(fairness)문제, S/W 불법복제 방지문제, 지적재산권 보호문제 등은 암호기술을 해결할 문제이다. 이러한 암호기술은 현대사회에서 정보보호의 핵심인프라가 되고 있다.

암호기술에서 안전한 알고리즘은 존재하지 않은 것으로 알려져 있으나 암호알고리즘 설계자들은 최소한 첫째, 암호해독비용의 암호화된 가치초과와 둘째, 암호해독시간의 정보유효기간 초과의 두 가지 기준 중 하나 또는 전부를 만족케 해주는 안정성을 획득해야 한다.

암호방식은 크게 비밀키 암호, 공개키 암호, 디지털서명, 뉴 암호기술로 나눌 수 있다. 〈표 2〉은 각 암호방식에서 사용되고 있는 암호기술들이다.

또한 암호기술을 안전한 다자간 프로토콜(secure multi-party protocol)개념에서 분류하면 〈그림 1〉과 같이 서비스와 요소기술로 나눌 수 있다.

암호기술의 응용서비스는 〈그림 1〉의 공통기반기술에 의한 사용자인증기술, 전자서명기술, 대칭 키 공개 키 암호알고리즘 및 주어진 암호기술의 신뢰성 검증을 위한 전자상거래, 가상기업, 가상대학, 가상정부 등 다양한 분야에서 응용되고 있다.

② 인증서비스기술(전자상거래)

인증기술이란 네트워크환경에서 자신이 누구인지를 상대방 또는 제3자에게 증명하는 기술을 말하며 전자문서 형태로 서로의 신분을 증명할 수 있는 인증서(Certificate)를 사용한다.

인증서를 등록하고 발급 또는 조회하는 조직을 인증기관(CA: Certification Authority)이라고 한다. 이 인증서를 활용하는 분야는 대표적으로 전자상거래이며 인증서비스는 사용용도, 목적 및 신뢰 등에 따라 몇 개의 분류로 나누어 독창적인 서비스를 제공한다. 쓰이는 용도는 〈표 3〉과 같다.

• 전자상거래

총 가계 소비에서 전자상거래로 이루어지는 부분은 1999년 0.1%에서 2004년에는 2%로 증가할 것이며 2005년에는 인터넷사용자 수가 7억이 넘어설 것으로 전망하고 있다.

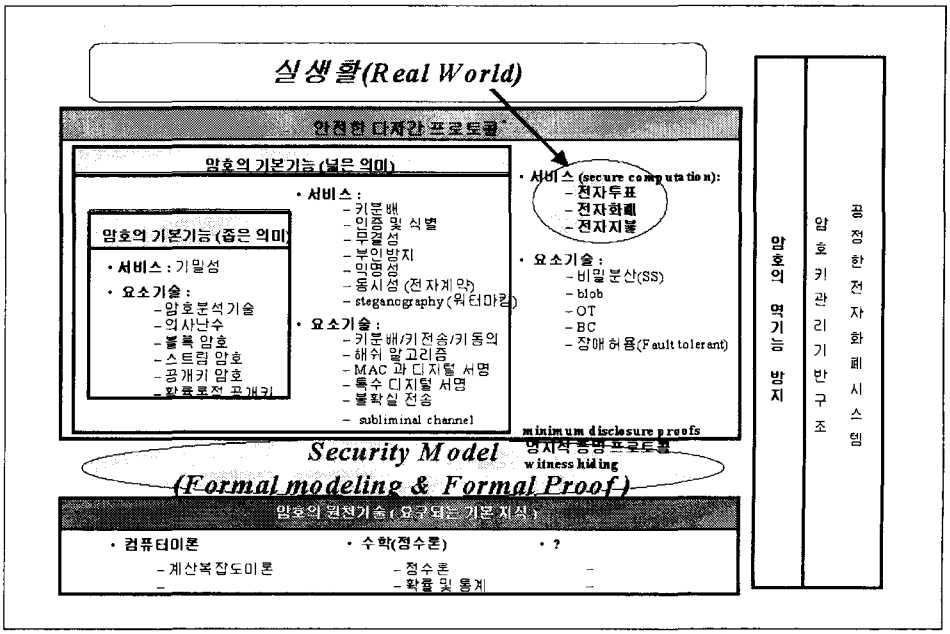
또한 최근에 가상공간에서 책을 주문하고 제공하는 인터넷 북샵(internet online bookshop)이 성황을 이루고 있는 실정이다. 출판업자와 도서판매업자간의 도서유통질서와 이윤창출 때문에 여러 가지 문제점(도서정가제 등)을 야기하고 있으나, 이처럼 빠르게 전개되고 있는 전자상거래의 안정성과 신뢰성을 위해서는 고객의 신용정보와 개인정보 그리고 실시간으로 이루어지는 결재정보 등이 인터넷상에서 보호되어야 한다.

여기에서 중요한 것은 상거래상에서 필수적인 신분증명을 어떻게 할 것 인가이다. 법률적으로는 이미 1997년 7월 1일에 『전자서명법』, 『전자거래법』등이 제정되어 시행되고 있다. 미국에서는 2000년 6월 14일 상·하 양원에서 압도적으로 /만장일치로 승인되어 동년 10월 1일부터 효력을 발휘하고 있다(http://news.cnet.com).

전자서명(Digital Signature)은 공개키 기반구조(PKI: Public Key Infrastructure)로 되어있다. 이것은 서로의 신뢰가 생성됨을 뜻하며, 서로간의 상호인증 (cross certificate)과 상호

〈표 2〉 암호방식의 유형(장우권 2000)

방식	유 형		내 용
비밀키암호	DES (Data Encryption Standard)		-. 미연방정보처리표준 46으로 채택된 대칭키 암호 알고리즘 -. 56비트 키를 사용 -. ISO의 표준(DEA-1)
	3중DES (Triple DES)		-. 안전성 증가로 현재 실용적인 암호분석 공격법은 없는 것으로 알려짐. -. 112비트 키를 사용 -. 키관리표준 ISO8732나 PEM에서 채택
	AES(Advanced Encryption Standard)		-. NIST에서 1998년 DES를 대신할 새로운 블록알 고리즘 표준으로서 제안 -. 2000년 8월에 최종 알고리즘이 채택될 예정
공개키암호	RSA		-. 이해 및 구현하기가 가장 용이한 알고리즘(가장 대중적) -. 큰 수의 인수분해의 어려움에서 안정성
	Rabin		-. 합성수 모듈러에 관하여 제곱근을 찾기 어렵다는 사실로부터 안정성 -. C = M(m+b)mdn(n=pq(p,q는 소수, 0≤b〈n에서 임의로 선택한 b를 공개, M의 크기는 n보다 작아야 함)
	ElGamal		-. 이산대수 계산의 어려움으로부터 안정성 x -. Y=G MP(y, g, p는 공개키, x는 비밀키)
	ECC		-. 유한체상의 타원곡선이 유한군을 가지며 그 위에서 이산대수 문제가 구성될 수 있음에 착안되어 제시된 암호알고리즘
디지털서명	디지털서명방식	DSS (Digital Signature Standard)	-. 미국의 NIST에서 1991년 8월 30일 발표한 디지 털서명안 -. 핵심알고리즘은 DSA -. 6개월 공개검토기간 중 검토자의 90% 정도가 문 제점 지적
		KCDSA	-. 1998년 한국정보통신기술협의회에서 표준으로 규정 -. 부가형 전자서명알고리즘 -. 공개검증키는 CA에서 인정하는 제3자 공개키검증 정보를 CA의 비밀키로 서명한 확인서를 배포함으로 써 공개검증키의 소유자를 보증
	특수디지털서명방식	부인방지서명	-. 서명자의 도움없이는 서명검증이 불가능
		의뢰부인방지서명	-. 오직 특정인만이 부인과정수행
		수신자지정서명	-. 지정된 수신자만이 서명
		은닉서명	-. 서명문의 sodydans을 확인하지 못한 상태에서 서명
		대리서명	-. 본인의 부재중 자신을 대신하여 제3자가 자신의 서 명을 수행
		그룹서명	-. 자신이 특정그룹의 서명자임을 제3자에게 증명할 수 있는 방식
		다중서명	-. 한 명이상의 서명자가 동일문서에 서명
뉴암호기술	양자암호 (quantum crytography)		-. 불확정성의 원리를 통신에 적용(광자나 전 자 이용) -. 비밀키를 필요치않은 암호시스템 실현가능 -. 광통신이 많이 이용
	워터마킹 (water marking)		-. 멀티미디어컨텐트의 불법복제를 막고, 데이터소유자의 저작권과 소유권을 효율적으로 보호하기 위한 도구로써, 데이터에 일정한 기밀정보를 숨겨서 부호화하는 과정으로 이러한 부호를 워터마크(water mark)라 한다.



(*자료: 정보보호뉴스, 1999.6, p.4)

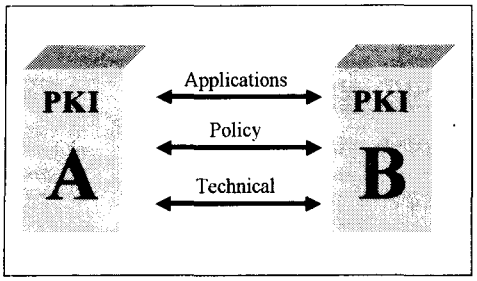
〈그림 1〉 암호기술의 분류

〈표 3〉 전자상거래 안정성과 인증서비스

인증서비스	발급대상	발급과정	용 도
Class1	개인	E-mail 주소 확인과정을 통한 온라인 발급	개인간 E-mail 교환
Class2	개인	전화로 신원확인 후 온라인 발급	일반상거래, 기업내, 기업간 E-mail 교환, 소프트웨어 검증, 회원제 온라인 서비스
Class3	개인	인증기관이나 인증기관의 인증으받은 등록기관에 직접가서 신원확인과정을 거친 후 발급	고가의 전자상거래, 전자계약문서, 인터넷뱅킹, 온라인청약, 기업 DB 접근, SSL, 소프트웨어 검증, 등록기관인증, 공공서비스
	기관	상동	상동
웹서버용인증서	웹서버	검증은 회사 또는 기관의 이름과 도메인 등록, 담당자 이름검사	SSL 보안

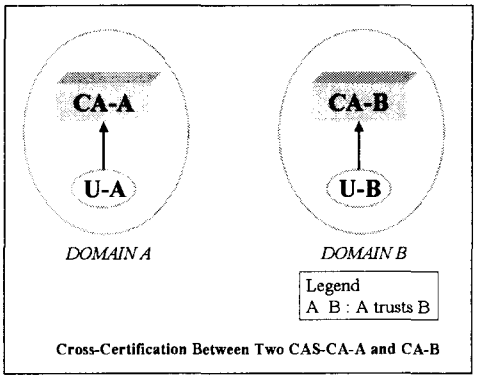
인정(cross recognition)에 의한 기술, 정책, 서비스가 갖추어진 인증서 교환이 이루어져야 한다.

〈그림 2〉는 어플리케이션/서비스, 정책 그리고 기술이 가장 이상적으로 상호연동을 구현할 수 있는 『상호연동체계』의 프레임워크이다. 〈그림 3〉은 두 개의 다른 영역의 인증기관(CA)이 서로 상호연동하는 것이고, 〈그림 4〉는 공신력이 있는 제3자기관과 연결된 인증기관들의 상호인정을 나타낸 것이다(http://www.kisa.or.kr).

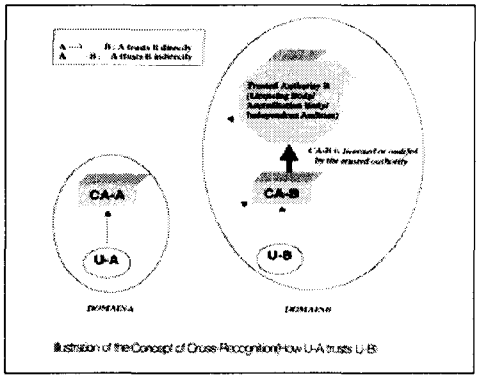


A Framework for Analysing PKI Inter-operability Schemes

〈그림 2〉 상호연동체계



〈그림 3〉 상호인증



〈그림 4〉 상호인정

※ 참고로, 〈그림 3, 4〉에서 사용된 "⇒"는 신뢰(Trust)의방향을 뜻한다. 이 교차인정(Cross Recognition)은, 사용자 U-A⇒ Trusted Authority ⇒ 인증기관 CA-B ⇒ 사용자 U-B. 그래서, 사용자 U-A⇒사용자 U-B. 이와마찬가지로, 사용자 U-B⇒Trusted Authority⇒인증기관 CA-A⇒사용자U-A. 그래서 사용자U-B⇒U-A. 종합적으로, 사용자U-A Cross-Recognizes U-B 라는 논리로 이해할 수 있겠다.

우리나라는 국가 최상위 인증기관으로서 전자서명인증관리센터가 1999년 7월 7일자로 설립되어 운영되고 있다. 〈그림 5〉는 동 센터업무를 전체적으로 조감하고, 국내의 전자서명인증관리체계를 나타내고 있다.

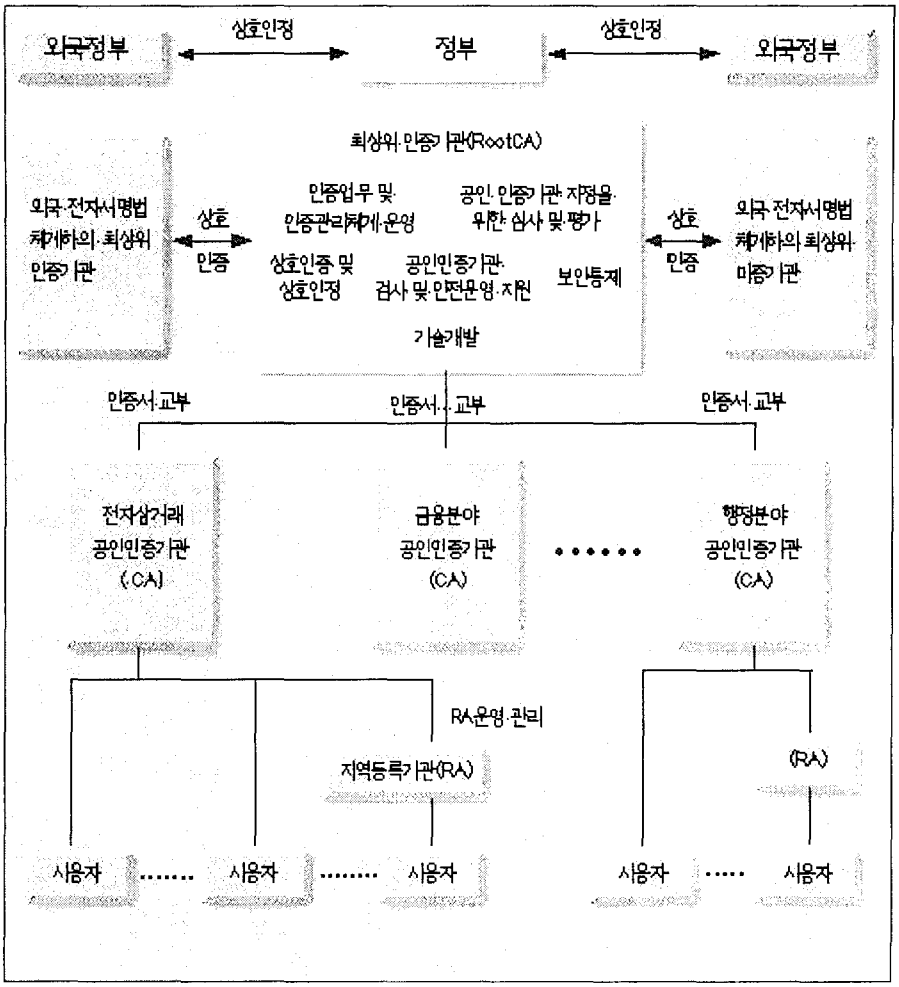
③ 접근통제기술

핵심기술로는 임의 접근통제, 강제적 접근통제, 역할기반접근통제가 있으며 국내외적으로 활발히 연구가 진행중이다.

2.3 시스템 및 네트워크 보호기술

1) 인터넷 관련보안

누구나 인터넷의 접근용이성에 의한 편리성을 추구한 나머지 외부로부터의 침입에 심각한 취약성을 노출시키고 있다는 사실을 등한시하고 있는 실정이다. 알고 보면 개인의 프라이버시를



(*자료: 정보보호뉴스, 1997.7, p.6)

〈그림 5〉 전자서명인증관리체계

보호할 수 있는 기능들이 웹브라우저의 대표적인 도구인 넷스케이프와 익스플로러에 내장되어 있다. 남을 탓하기 전에 자신의 정보는 자신이 보호한다는 기본적인 책임감을 가지고 있어야한다는 것이다.

여기에서는 웹을 항해할 때 외부로부터의 자신을 보호할 수 있는 기능들을 브라우저의 보안 취약성과 더불어 그 대책을 알아보고자 한다.

① 아이콘에 의한 암호화된 통신지원(보안지시자)

- 넷스케이프 네비게이터(Netscape Navigator)

4.0이상에 보안 기능들이 내장되어 있으며, 브라우저와 서버가 동시에 SSL 기능을 제공하면 HTTP 메시지는 암호화되어 전송한다. 이때 "http" 대신에 "https"를 사용한다. 보안여부

는 브라우저의 왼쪽아래에 있는 "보안아이콘"으로 알아볼 수 있다. 여기에서 파란색 아이콘은 보안채널로 연결되어 있다는 것이고 회색아이콘(부러진열쇠모양)은 보안이 되지 않았다는 것을 의미한다.

• 인터넷 익스플로러

4.0이상에는 하단의 상태표시줄(status line) 중앙에 열쇠아이콘이 나타난다. 또한 익스플로러에서는 클라이언트와 서버인증을 효과적으로 수행하기 위해 인터넷 사이트를 인터넷 영역, 로컬인트라넷 영역, 신뢰할 수 있는 사이트 영역, 제한된 사이트 영역이라는 4개의 영역으로 나누어 사용자가 보안수준을 각 영역별로 지정할 수 있도록 하였으며 이에 대한 정보는 상태표시줄 오름쪽에 나타나 있다.

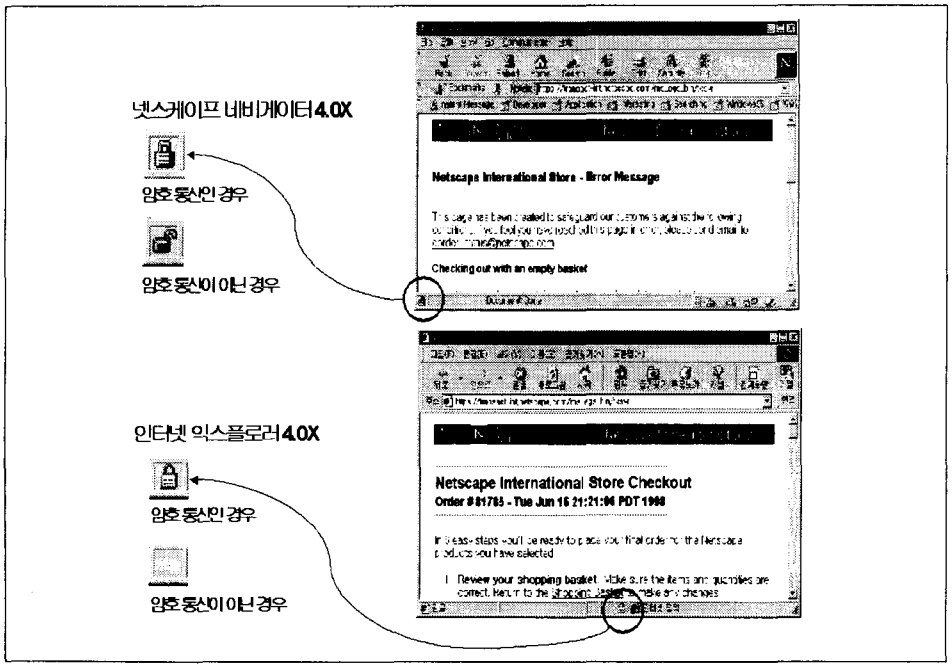
〈그림 6〉는 웹브라우저에 나타난 암호화된 통신지원(보안지시자 아이콘)을 나내고 있다.

• 접근제어모드

전송메시지가 ㉠ 40비트 RC4나 RC2로 암호화, ㉡ 56비트, 128비트지원 RC4로 암호화, ㉢ 56비트 지원 DES(CBC모드), ㉣ FIPS 140-1호환, 168비트 지원 삼중 DES 암호화는 더욱 안전한 모드로 한때 미국의 수출규제로 미국과 캐나다를 제외한 다른 나라에서는 지원할 수 없게 되어 있었으나 현재는 부분적으로 지원되고 있다.

② 전자우편(E-mail)

웹브라우저 사용자의 폭발적인 증가는 전자우편 때문이라고 해도 과언이 아닐 것이다. 이



〈그림 6〉 웹브라우저에 나타난 암호화된 통신지원(보안지시자 아이콘)

처럼 누구나 편리하게 사용할 수 있는 전자우편은 사용자정보(identity)를 사용자가 쉽게 바꿀 수 있다는 것에서 송신자의 이름과 주소의 위조를 용이하게 사용자를 가장한 공격의 수단으로 역이용될 수 있다.

따라서 현재는 전자우편 보안을 위해 S/MME이 사용되며, 40비트 RC2와 56비트 DES 암호화 알고리즘이 지원되어 이전보다 훨씬 안전한 전자우편을 송수신할 수 있다.

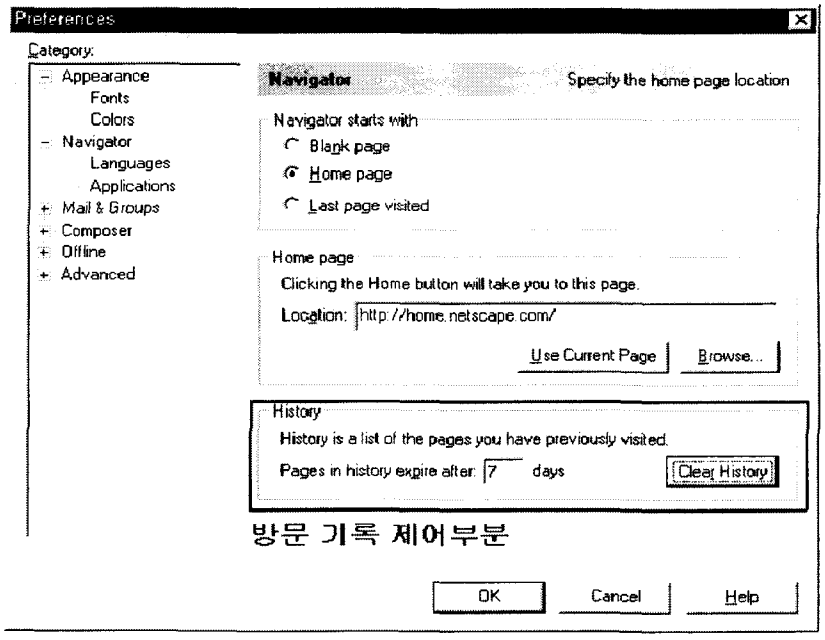
③ 방문링크 기록유지(History)와 헬퍼 프로그램서비스(Helper Application)

히스토리는 사용자가 방문한 사이트를 기록 저장 해두는 편리성이 있으나 공격자에 의한 사용자의 방문사이트에 대한 정보유출로 프라이버시를 침해 할 수 있다. 방문기록제어부분에서 웹페이지 목록 보관일수를 짧게 설정하는 것이 좋다.

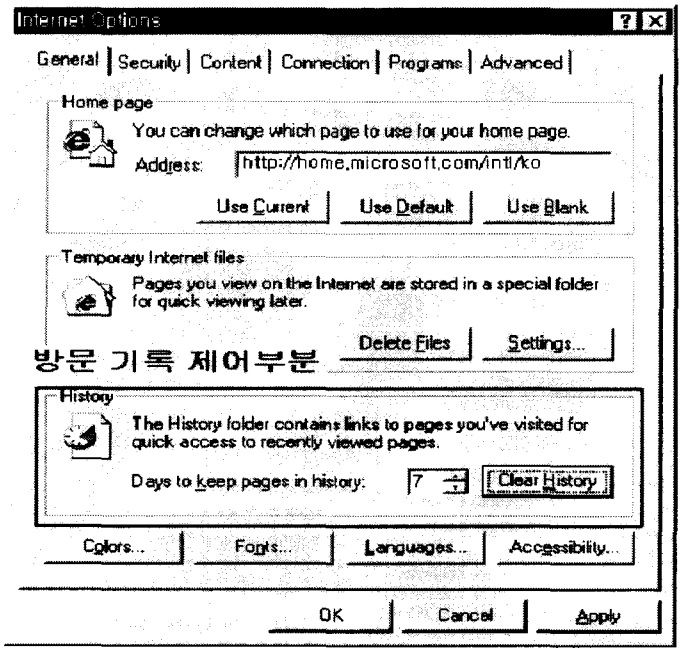
웹브라우저에서 새로운 파일 프로그램을 다운로드시 이를 처리해 줄 수 있는 처리프로그램을 지원해주는 헬퍼 프로그램의 출처나 사이트를 많은 사용자들이 사용하고 있는가에 대한 명성 등을 참고해야 한다. 〈그림 7〉은 넷스케이프 네비게이터와 인터넷익스플로러 방문링크 기록 제어부분을 나타내고 있다.

④ 쿠키(Cookie)

웹상에서 매우 다양한 정보를 사용자에게 제공해주는 것으로, 후에 다시 접근할 것을 대비하여 사용자의 컴퓨터에 저장되는 작은 크기의 파일이다. 주요기능에는 웹 검색엔진이나 웹 홈페이지를 사용자의 취향에 맞게 꾸며준다. 또한



〈그림 7-1〉 넷스케이프 네비게이터 4.0X



〈그림 7-2〉 인터넷익스플로러 4.0X

웹 컨테스트에 사용자를 한번만 참여할 수 있도록 하여주고 가상 쇼핑몰에서 사용자가 선택한 목록을 저장하여 제공한다.

하지만, 이러한 장점에도 불구하고 쿠키가 서버로 전송되어질 때 IP주소, 사용중인 브라우저, 운영체제와 같은 개인정보가 유출될 수 있다.

이와 같은 개인정보 유출을 방지하기 위해서는 첫째, 브라우저내의 쿠키설정옵션(편집→설정→고급→쿠키설정)을 변경하여 쿠키를 받을때마다 경고 메시지가 나타나도록 한다. 둘째, 주기적으로 쿠키가 저장되어있는 디렉토리를 이동하여 누적된 쿠키파일을 삭제한다. 셋째, 쿠키를 아예 받지 않도록 한다. 이 경우는 쿠키의 장점을 살리지 못해 의미가 없다. 넷째, 쿠키방지 소프트웨어를 사용한다.

다음 사이트에서 이에 대한 정보를 제공받을 수있다.

-. http://www.cookiecentral.com/files.htm

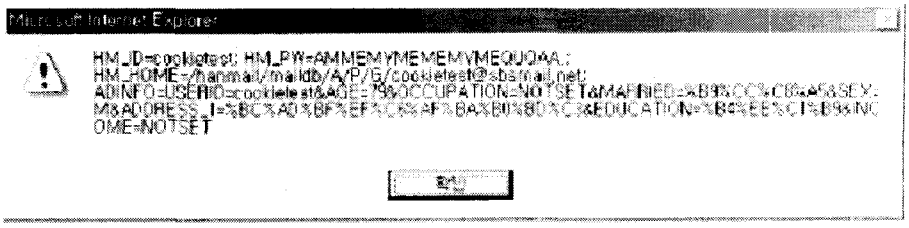
-. http://www.junkbusters.com/ht/en/ijbwin.html#zip

〈그림 8〉은 인터넷 익스플로러 4.X에 표시된 서버의 쿠키설정내용을 보여주고 있다.

⑤ 캐시(Cache)

캐시는 웹브라우저에서 한번 방문한 사이트를 다시 방문할 경우, 그 페이지를 다시 다운로드하지 않고 캐시에 저장되어 있는 내용을 보여줌으로써 시간을 절약할 수 있는 기능이다.

그러나, 공격자가 사용자의 관심사항 및 브라우징 습관을 파악할 수 있어, 자바를 사용하여



〈그림 8〉 인터넷 익스플로러 4.X에 표시된 서버의 쿠키설정내용.

악성코드를 캐시에 저장토록 한 후 코드를 실행하여 피해를 줄 수 있다.

따라서 캐시를 비우는 습관이 필요하다.

⑥ 프락시(Proxy)서버

외부 인터넷 서비스 환경으로부터 사용자 내부의 정보를 보호하기 위해서 인트라넷을 구축하는데, 이때 설정하는 것이 프락시서버이다.

그러나, 공격자에 의해 프락시 설정이 바꾸어진다면 사용자의 웹 탐색습관이나 비밀정보(패스워드)를 유출시킬 수 있다.

⑦ 자바애플릿 및 자바스크립트

웹의 동적인 다양한 서비스를 제공하는 것이 자바애플릿과 자바스크립트이다. 즉, 웹의 다양한 표현력과 높은 기능성을 나타낸 것으로 사용빈도가 높다.

그러나, 악의적으로 사용될 경우 사용자 시스템에 유해한 동작을 유보시킬 수 있다. 다음은 일반적인 침해사항으로서 사용자 시스템자원을 불법적으로 획득하는 비밀성(secrecy) 침해공격, 사용자시스템자원을 불법적으로 수정 또는 변경하는 무결성(integrity) 침해공격(예, 프로세스/쓰레드, 메모리 등), 사용자시스템자원을 과도하게 사용하여 사용자의 정상적인 사용을 방해하는 가용성(availability) 침해공격, 웹사용자에게 수많은 윈도우나 프레임을 생성시켜 사용상의 불편을 끼치거나 원하지 않은 음향을 지속적으로 발생시키고, 사용자에게 불쾌감을 유발시키는 경우가 있다.

⑧ 액티브 X(Active X)

실행에 아무런 제약을 두지 않으나 개발자의 전자서명이 추가된다. 그러나, 윈도우즈 95를 정지시키거나, 악성 액티브 X 컨트롤을 배포한 사건(CCC: Chaos Computer Com)의 예에서 보듯이 안전성을 보장하는데 한계가 있다는 것이다.

따라서 액티브 X를 잘 사용하지 않거나, 액티브 컨텐트 페이지에 대한 보안설정을 최상위(High Security)로 선택하여 액티브 X 컨트롤이 다운로드 될 때 경고메시지가 나타나도록 하여, 실행시 전자인증서를 주의 깊게 읽고, 이름, 발행자, 다운로드일시 등을 기록해 두는 것이 바람직한 방법이 될 것이다.

⑨ 사용자 ID와 패스워드

웹 상에서 운영되는 많은 웹 사이트가 필요한 정보를 주고받기 위해, 또는 상거래를 위해 회원이나 사용자들의 ID나 비밀번호가 필요하다.

〈표 4〉 비밀성 침해 공격

공격유형	자바애플릿	자바스크립트
특정 디렉토리 존재여부 확인	⊙	
특정파일 존재여부 확인	⊙	⊙
디렉토리 목록 획득		⊙
파일 데이터 획득		⊙
시스템정보 획득	⊙	

〈표 5〉 가용성 침해 공격

공격유형	자바 애플릿	자바스크립트
파일시스템의 가용공간소멸 *	⊙	
CPU 자원을 과도하게 소모	⊙	⊙
메모리자원을 과도하게 소모	⊙	⊙
*는 특정버젼(Netscape Communicator4.05)에만 해당		

〈표 6〉 사용상의 불편함 및 불쾌감 유발행위의 유형

공격유형	자바애플릿	자바스크립트
지속적인 윈도 및 프레임 생성	⊙	⊙
지속적인 음향발생	⊙	
재귀적 윈도생성으로 브라우저 사용방해	⊙	⊙
원치않는 사이트로의 이동	⊙	⊙

하지만, 사용자를 가장하여 공격할 시 사용자의 시스템용 로그인 계정과 패스워드가 도난당하여 프라이버시 침해와 막대한 경제적 손실을 초래할 수 있다.

따라서, 사용자는 웹사이트 등록시 내부시스템 로그인용 패스워드를 사용하여 여러 웹사이트에 동일한 비밀번호(패스워드)를 사용해서는 안된다.

⑩ 인증서(Certificate)

인터넷에서 사용자가 프로그램을 상대방이나 제3자에게 전송하거나 실행할 때, 원본여부를 확인할 때 사용한다.

넷스케이프 브라우저에서 인증서를 획득할 수 있으며 자신, 타인, 웹사이트, 인증서 서명자의 인증서 등으로 나누어 관리한다.

인터넷 익스플로러에서 인증서를 발급 받을 수 있으며 DER, Base 64로 인코딩된 X.509와 PKCS#7 인증서 형태로 저장 관리된다.

클라이언트/서명인증, 프로그램코드서명, 안전한 전자우편/타임스탬핑, MS 신뢰목록 서명/MS 타임스탬핑, IPsec 종단시스템, IPsec 종

단/IPsec 사용자에 대한 인증, 파일시스템 암호화, 윈도우 하드웨어 드라이버 검증, 윈도우 시스템 컴퍼넌트 검증 등으로 이용되고 있다.

⑪ 웹 브라우저 보안 옵션관리

넷스케이프 네비게이터 4.0이상과 인터넷익스플로러 4.0이상은 위에서 기술한 각 기능별로 보안옵션을 설정하여 관리할 수 있다.

⑫ 인터넷 웹브라우저 보안에 가장 많은 영향을 끼치고 있는 기구는 IETF의 WK(Working Group)과 ISO/IEC JTC1이다(장우권 2000, http://www.kisa.or.kr).

2) 시스템보호와 침입탐지시스템

인터넷의 응용기술발전으로 외부인에 의한 시스템 불법침입에 의한 사고가 국내외에서 동시다발적으로 빈번히 일어나고 있다. 이에 대한 적극적인 대처방법은 〈그림 9〉와 같은 시스템 보호기술개발이다. 특히, 침입탐지와 차단기술은 안전한 지식정보화 환경구축을 위한 핵심기술중의 하나이다.

(1) 침입탐지 기술

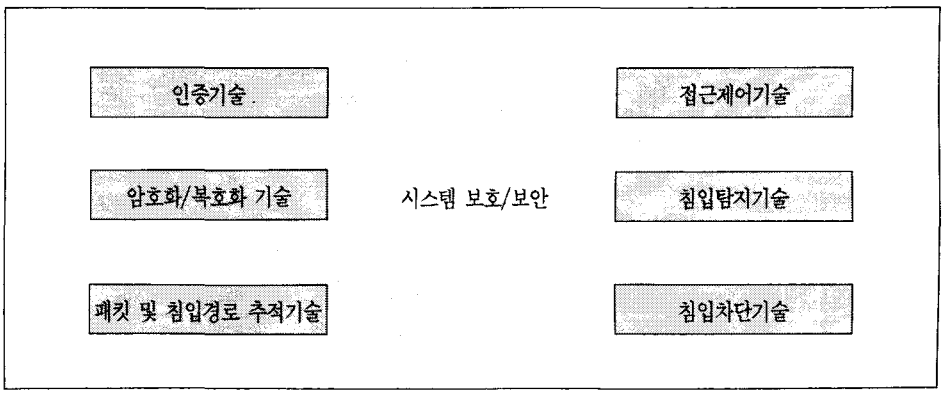
어떤 침입자가 컴퓨터시스템에 특정의 목적을 위해 불법적으로 접속하여 시스템을 사용하거나 오용, 남용하는 것을 탐지하고 그 문제점을 처리하는 기술이다.

① 침입탐지 기법

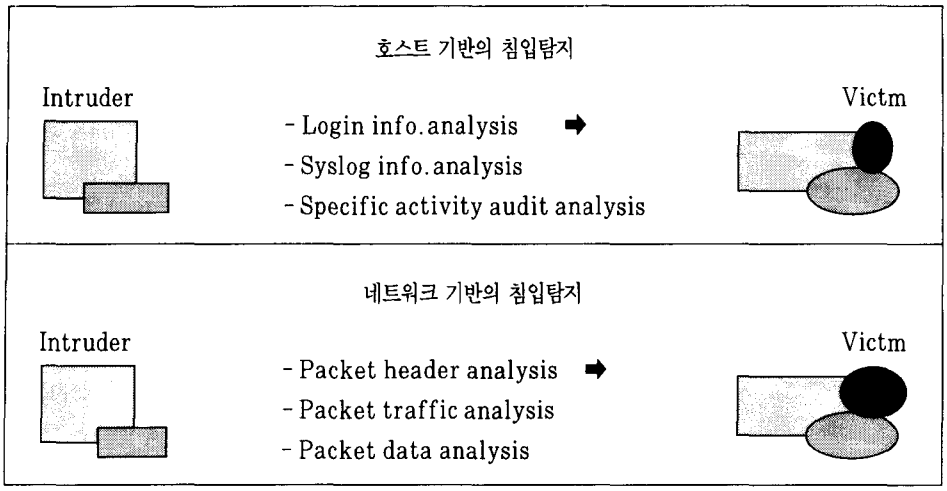
침입탐지 기법은 크게 데이터소스(source)를 기반으로 하는 분석방법과 침입탐지 모델을 기반으로 하는 기법으로 나눌 수 있다.

• 데이터소스를 기반으로 하는 분석방법에는 첫째, 시스템 로그정보와 특정행위에 대한 감사(audit)자료분석 등을 통한 자료를 침입탐지에 사용하는 호스트(Host Based)기반과 둘째, 네트워크의 패킷헤더 및 데이터를 분석하거나 패킷트래픽 량을 분석하여 침입을 탐지하는데 사용하는 네트워크 기반(Network Based)이 있다. 〈그림 10〉은 데이터소스기반의 분석방법이다(김병구, 정태명 2000).

• 침입탐지 모델을 기반으로 하는 분석방법



〈그림 9〉 시스템 보호/보안 관련기술



〈그림 10〉 데이터소스 기반의 분석방법

에는 첫째, 비정상적인 행위탐지(Anormaly Detection) 기법으로 통계적인 방법(Statistical Approach), 특징추출(Feature Selection), 예측가능한 패턴생성(Predictive Pattern Generation), 행위측정방식들의 집합(Anormaly Measures)과 신경망(Neural Network) 등이 있다. 둘째, 시스템의 알려진 취약점들을 이용하여 공격하는 행위들을 사전에 공격에 대한 특정정보를 가지고 있다가 탐지하는 오용 침입탐지(Misuse Detection) 기법으로, 조건부 확률(Conditional Probability), 전문가시스템(Expert System), 상태전이분석(State Transition Analysis), 키-스트로크 관찰(Keystroke Monitoring), 모델에 근거한 탐지(Model-based Detection), 패턴매칭(Pattern Matching) 등이 있다.

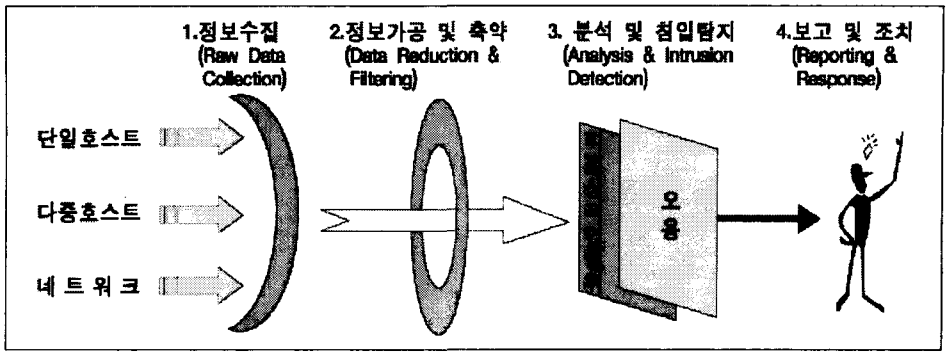
② 침입탐지 단계별 구성요소

침입탐지를 위한 데이터 수집에서 침입한 사실을 탐지하여 보고하고 조치하는 과정을 단계별로 나타내면 정보수집⇒정보가공 및 축적⇒분석 및 침입탐지⇒보고 및 조치 순서이다.〈그림 11〉 (http://www.kisa.or.kr)

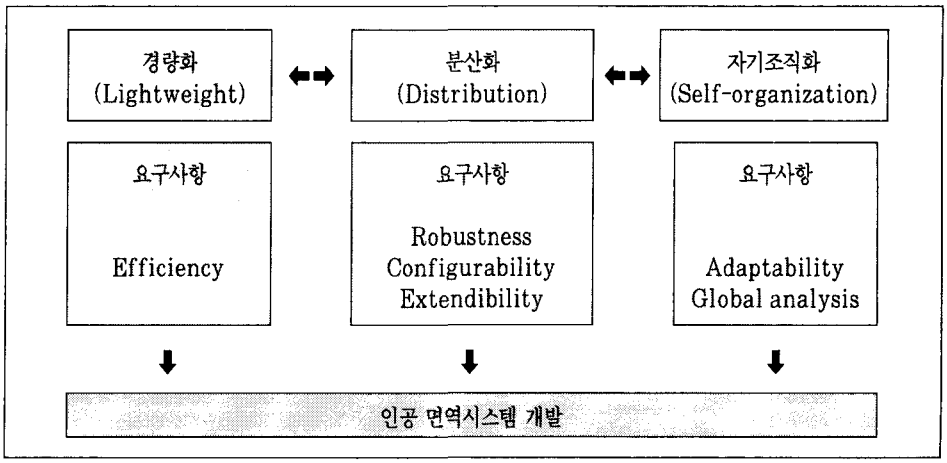
③ 침입탐지기술의 문제점과 해결방안

기존의 침입탐지기술로는 해커로부터 시스템을 보호하기 위해서는 방화벽(Firewall)만으로는 충분하지 못하며, 단일시스템 환경에 적용되어 대규모 네트워크 확정시 또는 다른 기존시스템들을 재 사용시 어려움이 따른다(예, 메시지 처리방식, 패킷스니퍼링, CRACK, send mail공격, NFS공격, IP Spoofing 등).

이러한 문제점을 해결하기 위해 첫째, 침입차단시스템과의 연동을 통한 접근제어, 둘째, TCP Wrapper과의 연동을 통한 서비스 접근제어, 셋째, 침입자를 역추적하기 위해 로그, 호출자, 판별, 모니터링과 같은 기술사용, 넷째, 공격형 정보보호기술로서 부정행위자 신분확인시스템, 다섯째, 방화벽이 감지하지 못하는



〈그림 11〉 침입차단 시스템의 기술적 구성요소



〈그림 12〉 인체 면역시스템의 도입과 기대효과

공격에 대해 인식할 수 있고 이전에 경험하지 못한 공격에 대해서도 이를 감지하여 퇴치할 수 있는 IDS시스템을 사용한다.

최근에는 새로운 공격유형에 탐지력을 높이는 수단으로 인체 면역 메카니즘을 적용한 인체 면역시스템을 적용하려는 연구를 계속하고 있다 (Warrender, Pearlmutter 1999).

④ 침입탐지기술의 응용분야

침입탐지기술은 전자상거래(실시간 경보, 서비스거부행위, 정보를 탈취하거나 파괴, 변조하는 행위 등), 금융기관(예금관련 DB감시, 고객정보유출방지, 웹서버 등 사내전산자원의 불법사용 여부 판단), 교육기관으로서 도서관(학술정보 DB감시, 연구자료와 수서/정리자료에 대한 불법적인 유출방지, 도서관 시스템에 대한 유해행위 방지, 대출/반납자료에 대한 파괴와 변조, 통지결과에 대한 적절한 대응), 관리대상의 정보가 대량화, 다양화되고 있는 대규모 인트라넷에서 응용, 수많은 정보침해유형(예, 바

이러스, 서비스거부공격 등)에 적절히 대응하여 안전한 사이버공간의 구축과 이용활성화에 응용되고 있다.

⑤ 침해사고방지와 탐지기술의 적용

〈그림 13〉은 침해사고방지와 탐지기술의 적용 예를 나타내고 있다.

3) 해킹현황과 보안대책

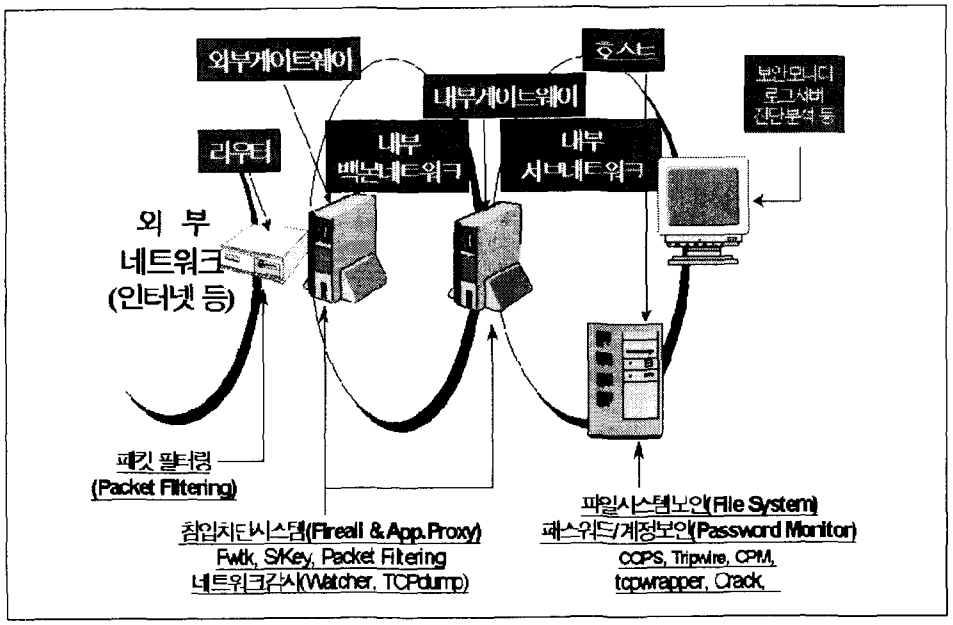
1980년대 컴퓨터보급이 확산되면서 1987년의 "카오스사건"(미국방성에 침입하여 기밀을 소련에 유출)과 1988년 "인터넷 웜사건"(네트워크에 연결된 수 천대의 컴퓨터를 일시정지) 이후 2000년대에 들어서는 국가안보를 위협하는 단계에 이르렀고, 특히 최근에 해킹기법은 더욱 복잡해지고 다양화되고 프로그램화되어 자동화되고 있으며 심지어 MS 윈도우 시스템을 다운시키는 등 피해사례가 속출하고 있다. 〈그림 14〉 참조.

정보통신부에 따르면, 국내의 해킹사고는 1997년에 64건에 불과하던 것이 '98년에 158건, 지난해 572건으로 늘어난 데 이어 올 들어 상반기(2000. 1-6월)에만 721건이 발생했다.〈그림 15〉 참조

이러한 현상은 〈그림 16〉와 같이 미국, 일본, 영국 등과 마찬가지로 전 세계적으로 크게 증가하고 있음을 알 수 있다.

1999년 기관별 해킹피해건수를 비교 분석한 결과 전체 572건중 대학이 262건(45.8%)으로 가장 많은 피해를 보았으며 그 다음에 일반기업 248건(43.4%)순이었다

또한 국내·국제간의 피해관계를 비교·분석해보면, 국내에서 국내로 해킹 시도 및 공격이

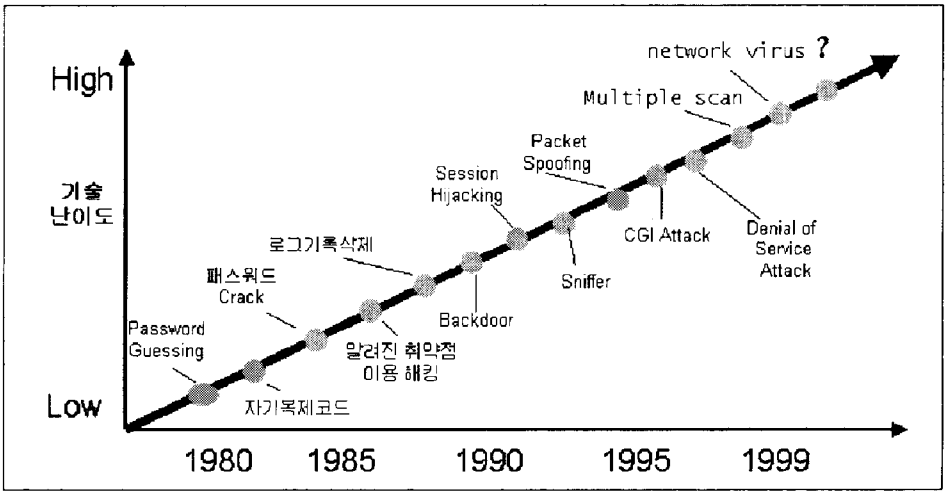


〈그림 13〉 침해사고방지와 탐지기술(http://www.kisa.or.kr)

48건(8.1%), 국내에서 국외로 24건(4.0%)인데 비하여 국외에서 국내로가 91건(15.3%), 국외에서 국내로 다시 국외로가 183건(30.7%)이 발생한 걸로 집계되었다.

인터넷상에서 운영되고 있는 시스템이라면 누군가 자신의 시스템자원을 훔쳐보고 있다는 사실을 명심해야하며, 특히 한국의 인터넷 보안상태가 심각하다는 외국전문가의 조사결과를 심사숙고하게 받아들여 이에 대한 대책을 하루빨리 세워나가야 한다.

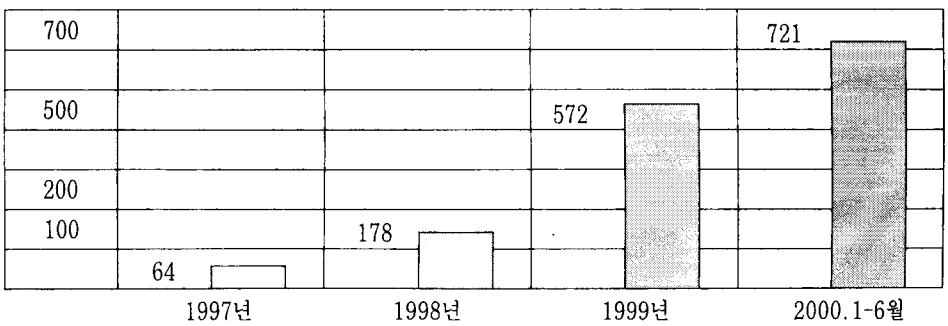
1999년에 해킹사고에 사용된 기법들을 비교·분석하면 취약점 정보수집에 272회, 버퍼오버플로우 취약점에 214회, 악성 프로그램에 58회, 사용자 도용에 68회, E-mail 관련공격에 20회, 서비스거부공격에 16회, 사회공학에 4회, S/W 보안오류이용에 3회, 구성·설정오



(*자료: http://www.kisa.or.kr)

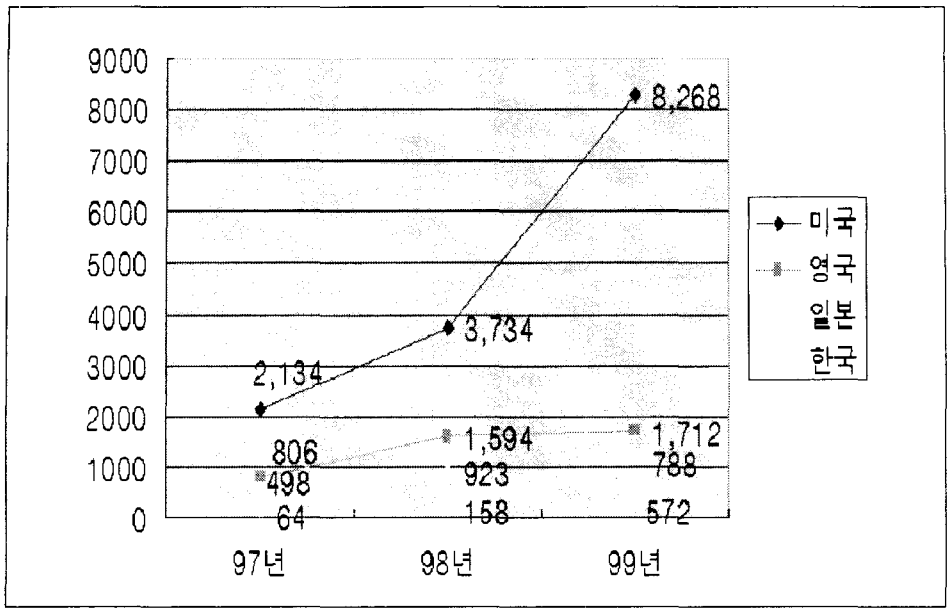
〈그림 14〉 연도별 해킹기법과 난이도분석

(단위 : 건)



(*자료: 정보통신발표, 매일경제, 2000.7.31(월), p.39)

〈그림 15〉 국내의 연도별 해킹건수



(*자료: http://www.kisa.or.kr)

〈그림 16〉 국외해킹사고 증가추이

〈표 6〉 국내 · 국제간의 해킹피해관계

경 로	건 수	비 율(%)
국내 → 국내	48	8.1
국내 → 국외	24	4.0
국외 → 국내	91	15.3
국외 → 국내 → 국외	183	30.7
N/A	250	41.9
계	596	100

류에 2회순으로 나타났다.

대표적인 피해사례를 살펴보면;

• 백오리피스(Back Orifice)를 이용한 주요 자료유출: 1999년 3월 KAIST "우리별 3호" 정보유출

• 홈페이지 해킹사고: 1999년 6월 H대학교 컴퓨터 공학과 홈페이지 변조(국외해커: "Chojin")

• 국외에서 국내시스템을 해킹한후 다시 국내기관을 공격: 에스파니아에서 국내 K대학 시스템을 해킹한 후 영국을 비롯한 캐나다, 대만, 미국 대학 및 기업들을 상대 186,547 사이트를 공격하여 취약정보 수립

• 분산서비스 공격사례 1: 2000년 2월7일 세계 적인 인터넷 포탈사이트인 "yahoo"가 공격당한 후 계속해서 Ebay, Amazone, CNN 등

주요사이트를 공격하여 수시간동안 관련사이트를 작동 불능상태로 빠뜨림.

• 분산서비스 공격사례 2: 2000년 7월 31일 정보통신부(www.mic.go.kr)의 발표에 의하면, 해커가 미국 버지니아주에 있는 인터넷 접속서비스업체(ISP)에 전화로 접속해 인터넷을 통해 강원도 강릉소재 한 PC방의 리눅스 서버를 해킹한 후, 이 PC방을 거점으로 대학30개, 기업200개, 공공기관 20개 등 국내 250여 곳 서버에 침입한 후 서버를 마비시켜 서비스를 불가능하게 만드는 사고가 발생.

이에 대한 보안 대책으로는 다음과 같다.

• 유닉스버퍼오버플로우 경우: 첫째, 보안패치를 적용한다. 둘째, 불필요한 프로그램을 정지시킨다. 셋째, 버퍼오버플로우차단 프로그램을 설치 운영한다.

• 윈도우즈 트로이 목마인 경우: 첫째, 통신망, 인터넷을 통한 파일다운로드 주의, 둘째, 출처가 불투명한 첨부파일 실행주의, 셋째, 최신백신 소프트웨어사용, 넷째, PC의 물리적 보안강화(예, ROMBIOS 패스워드), 다섯째, 네트워크 모니터링을 통한 침입감시(예, netstata 이용), 여섯째, 정품소프트웨어를 사용한다.

• 해킹보안기술: Firewall, 침입탐지시스템, 해킹취약점 분석, 진단 및 복구기술(예, 이동에이전트기술), 클라이언트-서버환경기반 보안관리기술, 역추적기술, 컴퓨터포렌식스(Computer Forensics: 법적 증거물), 인공지능기술, 면역기술, 신경망기술 등이 연관된 많은 기술개발이 이루어지고 있고 이에 대한 제품들이 출시되고 있다.

• 해킹 · 보안관련 검색엔진을 활용한다. 예를들면, 아스탈라비스타(http://www.Astalavista.box.sk)

4) 바이러스 현황과 대책

컴퓨터바이러스는 컴퓨터의 프로그램이나 실행 가능한 부분을 변형하여 고의로 제작 · 유포하여 피해를 주는 프로그램으로 그 감염속도가 생물학적 바이러스 질병처럼 매우 빨라 수시간/수일내에 인터넷을 통해 E-mail이나 인터넷을 통해 전 세계에 전파한다.

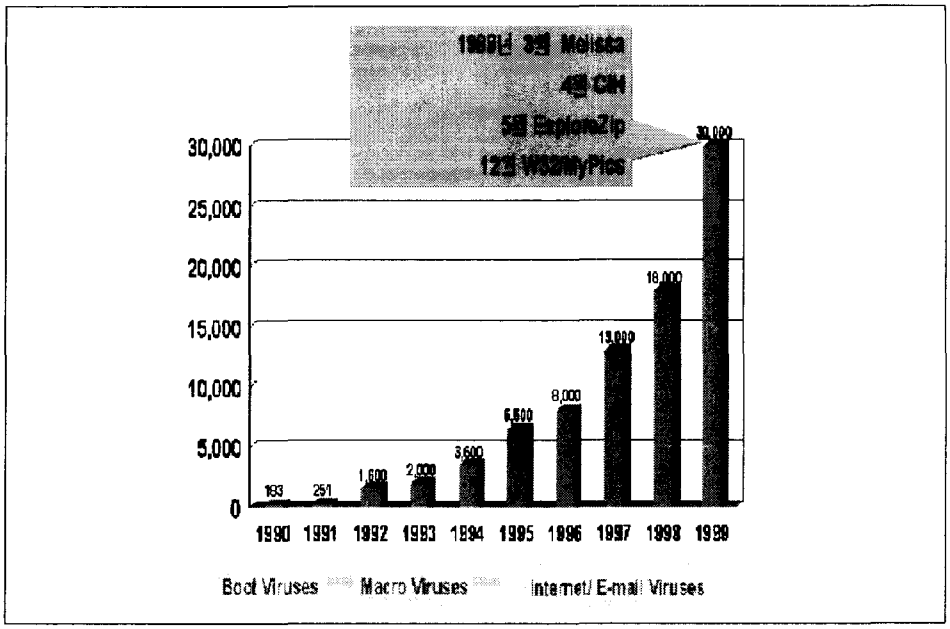
최근에는 "미켈란젤로", "멜리사바이러스", "ExploreZip", Win32-Worm, "love", "CIH바이러스" 등의 신종 및 변종 바이러스가 출현하여 바이러스 백신기술의 향상에도 불구하고 세계곳곳에서 많은 피해를 주고 있는 실정이다.

• 국외 컴퓨터바이러스 발생현황분석

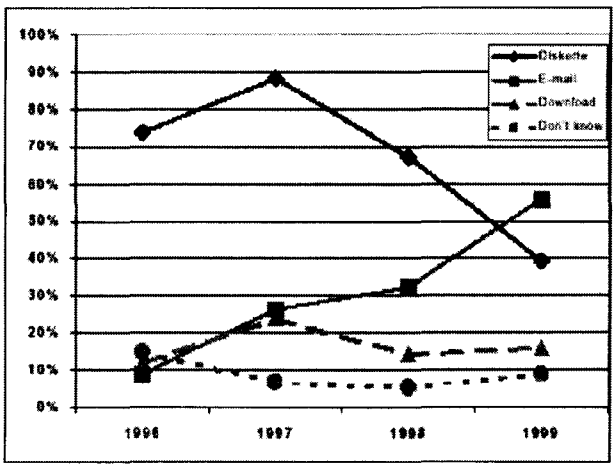
최근 미국의 ICSA(International Computer Security Agency)의 분석보고서에 따르면, 1997년부터 1999년 2월까지 26개월간 300여 개 조직에 806,614대 PC로부터 263,784개의 컴퓨터바이러스를 발견할 수 있었으며, 조사기간 중 한 달에 1,000대의 PC에서 평균 13개의 컴퓨터바이러스가 발견되어, 컴퓨터바이러스 전파속도가 매우 빠르게 진행되고 있음을 알 수 있다.

또한 컴퓨터바이러스 발생유형별로 보면 파일이나 부트 바이러스에서 매크로바이러스로 그리고 인터넷 E-mail를 이용한 바이러스로 전파경로가 이동되고있음을 보여주고 있다. 〈그림 17〉(장우권2000, 김재성2000, 안철수컴퓨터바이러스연구소)

또한 보고서에 나타난 감염경로를 비교분석하여 보면 299명의 응답자중 컴퓨터바이러스 감염매체로 E-mail에 의한 경우가 가장 많은 것으로 나타났다(매일첨부파일 〉 디스켓 〉 BBS, 통신 다운로드 〉 unknown 〉 웹(홈)페이지 사용 〉 공개용 프로그램 사용 〉 FTP, BBS, Host 다운로드 〉 복구, 서비스 〉 기타)(http://www.kisa.or.kr).



〈그림 17〉 유형별 년간 컴퓨터바이러스 발생추세 (http://www.kisa.or.kr)



〈그림 18〉 연도별 감염경로 변경추세

또한 일반기업의 PC사용자가 피해를 입은 유형을 복구소요 시간과 노력, 비용측면에서 분석하여 보면, 생산성 저하, 파손 및 삭제 등의 파일변조, 파일판독불능, 메시지 화면출력, 간섭현상, 화면 잠금, 파일저장 불능 순으로 나타났다. 〈그림 19〉. (WOI, http://www.wildlist.org)

• 국내 컴퓨터바이러스 발생현황분석(http://www.kisa.or.kr)

국내에서 발생한 컴퓨터바이러스는 다양한 종류와 양적인 증가(예, 매크로바이러스, 윈도우바이러스, 웜), 그리고 그 위험성이 날로 높아가고 있다〈그림 20〉.

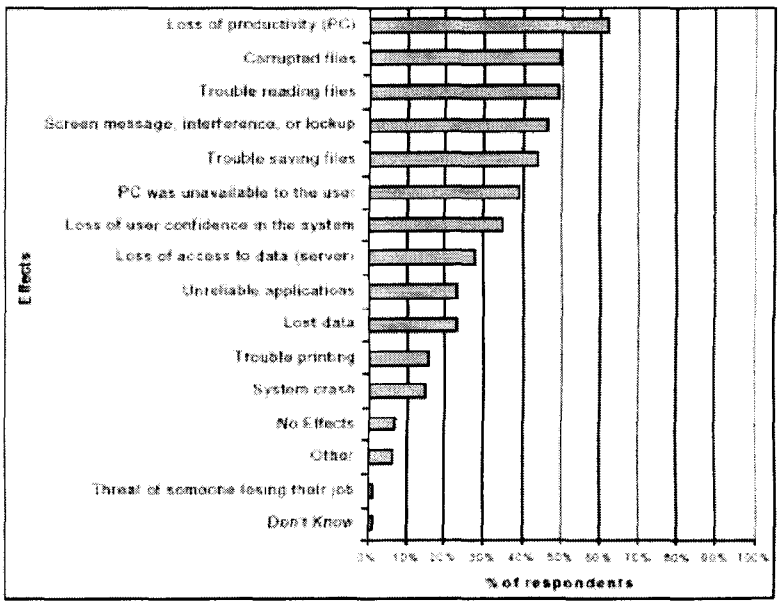
1999년 한해에 발생한 컴퓨터바이러스를 유형별로 분석하여 보면;

첫째, MS Word, Excel 등의 MS 오피스 대상의 공격형 매크로바이러스가 36%, 해킹기법을 이용한 트로이목마 등의 유포가 26%, 전자우편, IRC (Internet Relay Chat) 등의 전송 메커니즘 등을 이용한 네트워크상의 대규모적인 인터넷 ExploreZip, 웜(Worm)이 2%, 윈도우스크립트인 VBS(Visual Basic Script)를 이용한 신종 컴퓨터 바이러스가 2% 순으로 출현하였다.

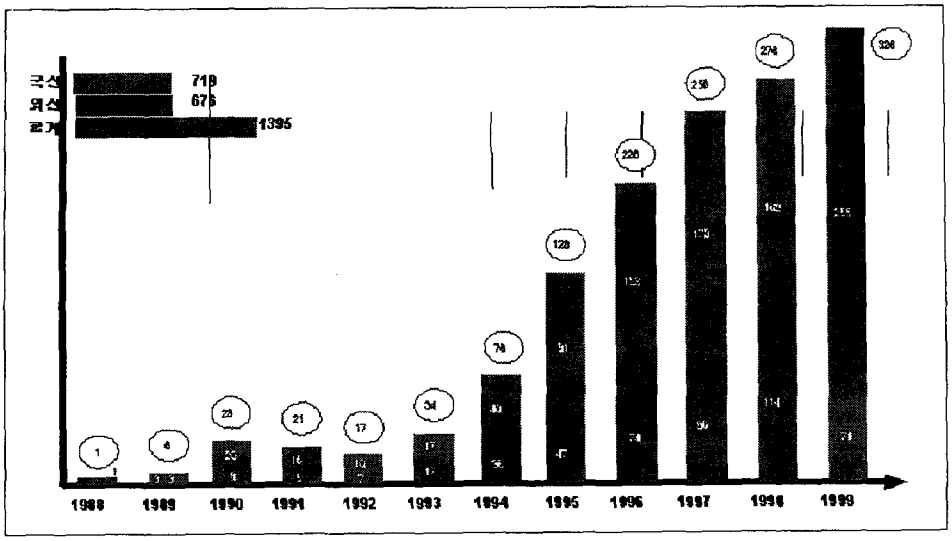
• 최근의 변종바이러스

가장 최근에 CIH바이러스 변종이 발견되었다; Win95/CIH.1042. 이것의 특징은 매달 4일 활동하고(원형은 매달26일 활동), 윈도우 95, 98에서만 작동하며 윈도우 NT2000에서는 작동하지 않는다.

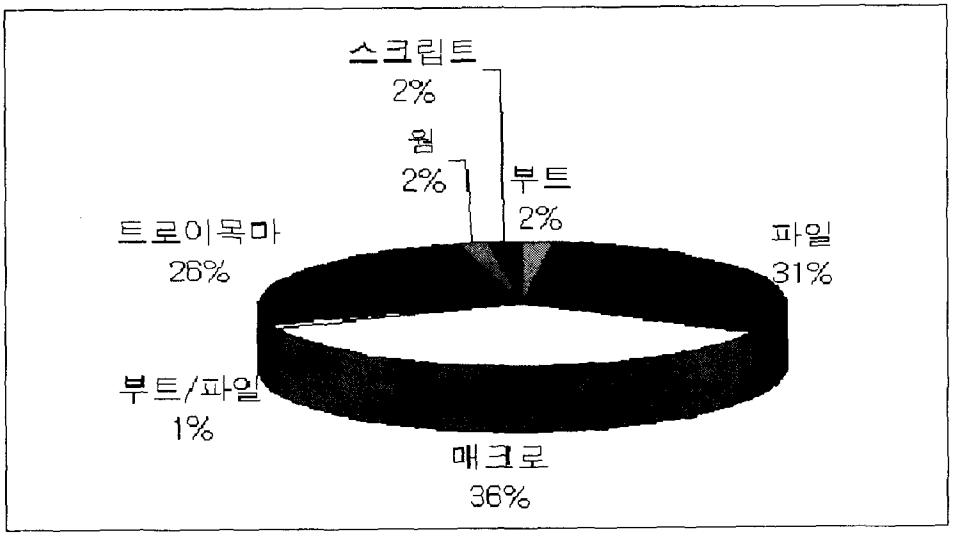
감염파일 내부에는 "Go away fuck up by NetCracker1"이라는 문자가 나타난다.



〈그림 19〉 피해유형 통계치 분석



〈그림 20〉 국내 컴퓨터바이러스 발생추세



〈그림 21〉 국내 출현한 컴퓨터바이러스 유형분석

이 바이러스는 하드디스크 정보를 삭제하고 플래시 메모리 기본입출력장치(BIOS)를 손상시켜 컴퓨터를 뷰팅 조차 안되게 만든다.

• 바이러스 침입방지 및 대책

제품인증, 침해사고처리, 신종악성 컴퓨터바이러스 정보공유와 시험분석, 바이러스 대응정도 DB구축, 바이러스 신고센터 운영과 정책수립등을 담당할 기관들을 살펴보면 다음과 같다.

■ 국외 컴퓨터바이러스 대응기구

- ICSA(International Computer Security Association) (http://www.icsa.net/services/consortia/ant-virus/)
- CIAC(Computer Incident Advisory Capablity)(http://ciac.llnl.gov/ciac/)
- FedCIRC(The Federal Computer Incident Response Capability) (http://www.fedcird.gov)
- Wildlist Organization International(http://www.wildlist.org)
- EICAR (European Institute for Computer Antivirus Research) (http://www.eicar.org)
- VTC(Virus Test Center) (http://agu-www.informatik.uni-hamburg.de/vtc)
- IPA(Information-technology Promotio Agency)(http://www.ipa.go.kr)

■ 국내 컴퓨터바이러스 대응현황

1995년 5월 한국정보보호센터 침해사고대응지원팀(CERTCC-KR)내에 컴퓨터바이러스 전담반이 구성되어 첫째, 국가적인 컴퓨터바이러스 종합대응체계 구축, 운영. 둘째, 컴퓨터바이러스 종합상황실 운영. 셋째, 선도적인 차세대 악성 컴퓨터바이러스 대응 기술연구개발. 넷째, 컴퓨터바이러스방지 관련, 법·제도 및 지침서 개발. 다섯째, 컴퓨터바이러스 대응기술교육 및 EORNRALS 홍보활동 등을 중심으로 운영되고 있다.

■ 컴퓨터바이러스 감염예방지침

일반 PC 사용자가 컴퓨터바이러스로부터 자신의 지식정보를 보호할 대책은 무엇인가. 즉, 예방지침을 제안하면 다음과 같다.

- 중요데이터의 장기적인 백업을 실시
- 신종 바이러스에 대비한 최신 백신 프로그램의 업데이트 사용
- 불법복제 소프트웨어 사용금지
- 인터넷 또는 PC통신공유자료 사용시 개발자가 확실한 프로그램 사용
- 백신 프로그램의 자동감시 기능을 이용한 수시 감염여부 점검.
- 한국정보보호센터 컴퓨터바이러스 전담반, 국내 백신업체 등 홈페이지를 통한 컴퓨터바이러스 관련정보 숙지
- 비상시를 대비하여 복구용 시동 디스켓 준비
- 정품 백신 프로그램을 사용한 주기적인 바이러스 점검

피해사례는 하드디스크 정보를 삭제하고 플래시 메모리 기본입출력장치(BIOS)를 손상시켜 컴퓨터를 뷰팅조차 안되게 만든다.

치료백신은 안철수 바이러스연구소의 웹사이트(http://www.ahulab.com)에서 내려받을 수 있고 온라인 백신 "MyV3"로도 치료할 수 있다.

5) 무선인터넷 보안기술

차를 타고 이동하거나, 식사도중, 대화도중, 무선인터넷(핸드폰)을 통해 필요한 정보를 손쉽게 획득할 수 있다. 무선 인터넷용 표준프로토콜은 WAP(Wireless Application Protocol)이

며 보안을 담당하고 있는 계층이 WTLS (Wireless Transport Layer Security)이다. WTLS는 WDP(Wireless Datagram Protocol)과 WTP(Wireless Transaction Protocol)사이에 위치하고 있으며, SSL을 기반으로 무선환경에 적합하도록 구성되어 있다.

이러한 WTLS 프로토콜은 두 가지 측면에서 단점을 가지고 있으며 그 해결책은 다음과 같다.

첫째, 무선단말기가 기존의 웹서버와 통신을 해야 할 경우, WAP gateway를 통과해야 하며, 이 Gateway 때문에 보안에 문제가 생길 수가 있다는 것이다. 만약 Gateway가 해킹을 당하거나 Gateway에 합법적인 접근이 가능한 시스템관리자가 악으로 데이터의 원본을 훔쳐보려고 할 경우에 문제가 생겨, 무선단말과 웹서버사이에 단대단 보안이 이루어지지 않는다는 것이다. 현재로서는 WAP Gateway가 무선 인터넷서비스 제공자에 종속되어 있는 한 별다른 해결방법이 없으나, Gateway가 기존의 웹서버와 통합된다면 단대단 보안문제는 점차 해결 될 것으로 전망된다.

둘째, 데이터에 대한 서명기능이 없어 부인방지가 제공되지 않는다는 것이다. 전자상거래서비스에서 부인방지가 실현되지 않으면 물건을 구입한 후 구입신청을 하지 않았다고 발뺌하는 등의 사기가 발생할 수 있다. 이러한 문제점을 해결하기 위해 응용계층상에서 WMLScript Cryto Library를 이용한다.

3. 정보보호기술산업의 패러다임과 활성화방안

3.1 국내외 정보보호기술과 산업의 패러다임

① 국외

세계는 바야흐로 '정보전쟁의 시대'가 도래하고 있다. 세계 각국은 자국의 국익을 위해정보보호기술 개발과 정보보호산업육성에 국가의 모든 역량을 결집시키고 있다. 즉 주요산업기반구조를 보호하기 위한 노력을 범 국가적인 차원에서 추진하고 있다는 것이다.

미국은 이를 위해 각계 의견을 수렴하여 2000년 1월 7일 "국가주요기반시설보호계획"을 발표하였다. 국가계획의 목표는 2000년 12월 31일까지 주요기반구조보호관련 초기운영능력을 확보하고, 2003년 5월까지 완벽한 운영능력을 확보하여 주요정보시스템에 대한 보호대책을 구축하는 것이다. 국가계획은 준비 및 예방, 탐지 및 대응, 튼튼한 기반구축의 3가지 목적을 가진 10개의 실행프로그램과 세부실행계획을 제시하였는데 그 세부계획을 살펴보면 다음과 같다.

- 주요기반구조 자산 및 공유된 상호의존성을 파악하고 취약점을 다룬다(프로그램 1).
- 공격 및 침입을 탐지한다(프로그램 2).
- 강력한 정보 및 법 집행능력을 개발하여 법률과 일관되도록 주요 정보시스템을 보호한다(프로그램 3).
- 공격에 대한 경고 및 정보를 시기 적절한 방식으로 공유한다(프로그램 4).
- 대응, 재구성 및 복구능력을 창출한다(프로그램 5).

- 프로그램 1-5를 지원하는 연구 및 개발을 촉진한다(프로그램 6).
- 적절한 수의 정보보안 전문가를 훈련시키고 고용한다(프로그램 7).
- 사이버 보안의 개선이 필요함을 인식시킨다(프로그램 8).
- 프로그램 1-8을 지원하는 법령과 정부예산을 지원한다(프로그램 9).
- 보호책의 모든 단계 및 구성요소에 있어서 미국 시민들의 시민적 자유, 프라이버시 및 사유 데이터 보호권을 충분히 보호할 수 있도록 한다(프로그램 10). (National Plan for Information System Protection Ver.1.0, Jan2000)

또한 암호 알고리즘 설계·분석, 키 관리 및 전자서명 인증기술, 각종 네트워크를 이용한 각종 서비스에 대한 네트워크 보안기술과 PC, 서버차원의 시스템보안기술, 네트워크를 이용한 각종 서비스에 대한 보안기술 및 행정, 보건, 교육, 금융서비스와 전자상거래, 전자지불보안과 같은 정보보호기술개발을 국가주도로 적극 추진하고 있다.

한편, 세계의 정보보호산업은 연평균 32%의 높은 성장률을 보이고 있으며, 2003년에는 시장규모가 100억달러에 이를 것으로 예상되며, 또한 암호알고리즘, IC카드 칩(chip)개발 기술과 무선인터넷 및 차세대 인터넷과 같이 첨단기술에 대한 의존도가 매우 높을 것으로 전망된다.

② 국내

국내의 정보보호산업의 발전패러다임을 시기별로 살펴보면;

첫째, 도입기('97.10). 정보제품을 외국에서 들여와 국내에 소개하는 수준이었으며 정보통신부가 1997년 9월에 "정보보호산업 발전대책"수립을 천명하였다.

둘째, 침체기('97.11~'98.8). 불행히도 한창 정보보호마인드가 확산될 시기에 IMF에 의한 투자가 위축되었고, 매출의 성장세가 크게 둔화되었다. 해킹과 바이러스 등에 의한 여러 산업망들이 피해를 당했음에도 이에 대한 예방과 치료대책을 소홀히 하였다.

그러나 이러한 어려운 상황에도 불구하고 일부정보보호산업업체들은 재정비를 하고 인력을 보강하는 계기가 되었다. 하지만 전반적으로 정보보호산업의 암흑기였다.

셋째, 회복기 ('98.9~'99.10). 이 시기에는 정보보호산업이 본격적으로 형성되었으며, 민간부문에서 신규 사업 모델 링이 도입되었다. 인터넷 해킹대책이 세워졌으며, 전자서명법, 전자거래법 등이 제정되어 시행되었고, 정보보호 인식의 척도인 "인증서"를 발급 받을 수 있는 인증기관이 설립되었고 전자상거래에 대한 마인드가 확산되었으며, e-business 패러다임이 정착되면서 IT에 대한 정보통신분야의 투자분위기도 형성되었다.

넷째, 도약기('99.11~). 정보화 패러다임의 중요한 성분으로 "정보보호"가 인식되었고, 전자상거래 시장이 활성화되었으며, 이는 인터넷 산업의 견실한 인프라가 갖추어지게 되었다.

정보보호산업제품은 크게 침입차단시스템(예, Firewall), 바이러스 백신, 시스템보안, PKI, 침입탐지시스템, 투자컨설팅, PC보안/메일보안 등으로 분류할 수 있다.

보고에 의하면 올해는 약1,000억원 정도의

시장규모가 형성될 것으로 예측하고 있다. 다른 산업에 비하여 액수가 적으나 기술개발 제품 출시 면에서, 다른 어떤 산업보다 빠른 신장 세를 보이고 있다고 할 것이다.

3.2 정보보호기술과 산업의 활성화방안

이제 정보보호기술과 산업은 누구도 부인하기 어려운 국가경쟁력의 핵심분야가 되고 있다. 정보통신망을 백본(backbone)으로 한 국가정보화 산업의 기반을 구축하기 위해서는 정보의 정책입안과 의지만 갖고 되는 것이 아니며, 전국민적 정보화 마인드에 대한 공감대가 형성되어야 한다.

따라서 정보보호산업 활성화 대책을 제시하면 다음과 같다.

첫째, 정부는 정보보호에 대한 확고한 정책을 수립하고 이를 실천할 수 있는 의지가 있어야 한다. 왜냐하면, 정보보호산업은 정보화와 비례하여 발전하는 산업이기 때문이다.

또한 이제 인터넷산업은 IT산업의 전체 패러다임을 형성하고 있으며 정보보호산업으로 발전하는 추세이다.

주지하는바와 같이, 미국의 클린턴 대통령이 PDD(Presidental Decision Directive63)에서 이제 "미국의 주요기반구조는 정보보호산업"임을 천명하였듯이, 정보화 촉진 그 자체로 정보보호산업이 발전할 수 있는 기반이 조성된 것이다.(http://www.ciao.ncr.gov/63factsheet.html)

둘째, 정보보호를 위한 전문인력을 양성해야 한다. 오랫동안 많은 인력과 기술이 투입되어 완성된 시스템자원과 DB가 남의 의해 피해를 당한다면 어떻게 될 것인가. '사후 약 방문격'이 될 것인가. 이를 보호하고 새로운 기술을 개발할 수 있는 모티브를 제공하기 위해서는 전문인력의 확보가 필수적이라 할 것이다. 왜냐하면 정보보호산업은 창조적인 아이디어가 필요한 지식 집약적 산업이기 때문이다.

이미 언급한 바와 같이 정보통신부가 최근에 발표한 보고(2000.7.31)에 의하면 국내서버 250여곳이 뚫리는 대형 해킹사고가 발생했으며, 대학, 기업, 공공기관을 막론하고 특히 대규모 인터넷데이터센터(IDC)까지 해킹 당한 것으로 밝혀졌다.

따라서 시스템 및 네트워크 기술에 기반을 둔 응용/서비스 분야의 제품 개발자와 위와 같은 해킹기법 등 공격기술에 대한 전문컨설팅을 할 수 있는 전문인력 양성이 필요하다. 이를 위해서는 대학 내에 관련학과를 설치 운영하거나, 정보통신센터의 교육관련 기능을 강화해야 하며, 정보보호교육센터를 설치할 필요가 있다. 또한 정보보호 교육과정에 대한 지속적인 연구가 이루어져야 한다.

셋째, 정보보호에 대한 공감대가 형성되어야 한다. 이제 정보는 개인의 것을 넘어서 사회, 국가, 세계의 소중한 지적자산이 되고 있다. 즉 지적자산을 보호해야 할 의무와 책임감이 누구에게나 있다는 정보보호 마인드가 형성되어 확산되어야 한다는 것이다. 이러한 정보보호 인식을 제고시킬 때 정보보호 제품에 대한 수요기반을 확대할 수 있다.

따라서 산업계, 학계, 정부는 정보보호인프라를 견실하게 구축해야 한다.

넷째, 연구개발을 통한 산업체의 기술개발을 지원해야 한다. 대학과 연구소에는 우수한 인력

과 정보자원이 확보되어 있다. 이에 기업체에서는 생산설비가 갖추어졌다. 정부와 기업체가 대학교와 연구소에 프로젝트를 주고 이를 수행할 때, 연구원들이 연구능력향상과 기초과학 발전에 기여를 함은 물론 솔루션을 제공받음으로써, 산업현장의 활성화와 우수한 제품을 생산할 수 있다. 그 결과, 국내 정보보호산업을 한층 더 발전시킬 것이고 우수업체와 제품이 해외 시장에 진출함으로써 얻을 수 있는 매출 수익과 보이지 않는 국가와 기업 및 도서관의 유·무형의 가치는 이루 말할 수 없을 것이다.

다섯째, 정보보호산업이 국제적 경쟁력을 가져야 한다. 정보보호산업은 개방된 네트워크를 통하여 정보를 공유하며 이를 바탕으로 새로운 부가가치서비스를 창출하는 산업이다. 글로벌 경제시대에 정보보호산업을 국제 경쟁력이 있는 산업으로 육성하기 위해서는 정보화 촉진에 대한 강력한 의지와 우수한 정보보호통신 인력과 과감한 투자로 시장을 리드해 가는 장단기적 성장전략이 필요하다.

4. 결 론

이제 우리는 누구도 부인할 수 없는 지식정보화 사회, 가상공간의 사회에 생활하고 있다. 인터넷의 출현은 우리의 문명사를 획기적인 변화의 물결로 만들어 버렸으며, 누구나 언제, 어느 곳, 어디에서든지 원하는 실생활의 정보와 의·식·주를 해결할 수 있는 장이 되고 있다.

그러나, 인간의 소유욕구가 충만한 나머지, 건전한 사이버문화가 사이버테러로 변질되어 세계 곳곳의 통신망을 통한 프라이버시 침해와 국가 기밀정보를 훔쳐갈 뿐만 아니라 아예 시스템 망을 파괴하는 무법천지의 장이 되고 있는 것이다.

이에 우리 나라를 비롯한 각국은 자국의 이익과 국민 사생활의 보호를 위해 여러 가지 대책을 수립하고 시행하고 있다(예, 법률제정과 시행, 기술개발). 위와 같은 사이버 공간의 위협으로부터 보호받을 수 있는 정보보호 기술과 산업이 활성화되고 있는 것이다.

따라서 사용자 개개인은 정보보호의 심각성을 깨우쳐, 자신의 재산은 자신이 보호하는 책임을 가져야 하며 해킹과 바이러스의 침입으로부터 보호받을 수 있는 기본적인 정보보호지식을 가져야 한다.

기업과 도서관 그리고 국가는 정보보호산업 육성에 아낌없는 투자를 해야하고, 전문인력을 양성하고 국제 경쟁력을 갖출 수 있도록 여러 가지 제도적 세제지원과 정책 수립으로 우수한 정보보호 기술이 개발될 수 있도록 적극적 지원이 이루어져야 한다.

우리가 명심해야 할 것은 "해킹과 바이러스는 국경이 없으며 수 시간 내에 우리의 모든 재산을 파괴시킨다"는 사실이다.

참 고 문 헌

강신각, 박정수. 2000. 월드와이드 웹(WWW) 보안기술. 정보처리, 7(2): 41-48.

김병구, 정태명. 2000. 침입탐지 기술의 현황과 전망. 정보과학회지, 18(1): 29-39.

김홍선. 2000. 국내·외 정보보호 산업현황. 정보처리, 7(2): 98-106.

매일경제. 2000.7.31

신홍식. 2000. 전자상거래 안전성과 인증서비스. 정보처리, 7(2): 107-113.

안철수컴퓨터바이러스연구소. 트렌드코리아. 웹사이트. http://www.ahulab.com

임재호, 김병천. 2000. 해킹피해 분석방법과 대응기술. 정보과학회지, 18(1): 40-52.

장우권, 박성우. 2000. 정보보호와 뉴패러다임에 관한 연구. 제7회 한국정보관리학회 학술대회. 2000년 8월 17-18일. [서울: 이화여자대학교]: 175-180.

정보통신부. http://www.mic.or.kr

정현철 외5인. 2000. 분산서비스 공격 등 최근 해킹기법과 대응방안. 정보처리, 7(2): 82-90.

한국정보보호센터. 정보보호뉴스 (1997.7, 1999.6)

한국정보보호센터 컴퓨터바이러스 전담반 종합상황실 홈페이지. http://www.certc.or.kr/cvirc/cvirc_2.htm

한국정보보호센터. 1999. "99 해킹 및 바이러스 대응 현황".

Advanced Encryption Standard(AES) Development Effort. http://csrc.nist.gov/encryption/aes/1999

http://news.cnet.com

http://www.cert.org/stats/cert_stats.html

http://ja.net/CERT/JANET-CERT/monthly_re ports.html

http://jpcert.or.jp./nl/

http://www.kisa.or.kr

National Plan for Information System Protection Ver 1.0, Jan.2000 http://www.ciao.ncr.gov

Protecting America's Critical Infrastructures, 1998.5. http://www.ciao.ncr.gov/63factsheet.html

The Netcraft Web Server Survey. http://netcraft.com/survey/2000.2

Warrender, C. S. Forrest and B. Pearlmutter. "Detecting Intrusions Using System Calls: Alternative Data Mpdels," Proceedings of 1999 IEEE Symposium on Security and Privacy (1999): 133-145.

WOI(The Wildlist Organization International) Web page. http://www.wildlist.org