전자상거래와 보안†

서울대학교 윤호빈 · 김서진 · 박근수*
전북대학교 박경수

1. 서 론

최근에 인터넷의 급속한 확산에 따라, 인터넷을 상거래에 이용하는 전자상거래가 활발하게 이루어지고 있다. 그리고 인터넷의 영향력이 날로 증대되고, 인터넷 사용자 수가 점점 많아지면서 전자상거래는 향후 일반적인 거래형태로 정착될 전망이다. 이러한 전자상거래를 안전하게 실현하기 위해서는 보안기술이 필수이며, 따라서 보안의 중요성이 점점 크게 부각되고 있다.

인터넷의 확산과 더불어 해킹사고도 매년 꾸준히 증가하는 추세에 있다. 한국정보보호센터의 통계에 따르면 국내에서 접수된 해킹사고는 97년 64건, 98년 158건, 99년 572건이며, 2000년 1월에만 117건이다. 이런 추세로 보아 2000년에는 모두 1000건 이상의 해킹사고가 있을 것으로 전망되고 있다[1].

본고에서는 2장에서 현재 사용되고 있는 해킹의 유형들을 살펴보고, 3장에서는 이러한 해킹에 대비할 수 있는 시스템 보안 기법을 설명한다. 4장에서는 보안의 기초가 되는 암호학에 대해 간단히 설명하고, 5장에서 전자상거래와 보안의 관계를 살펴본 후 6장에서 결론을 맺도록 하겠다

2. 해킹의 방법

99년의 해킹사고 유형을 공격 대상에 따라 분석해 보면 대학(ac.kr) 262건, 기업(co.kr) 248건, 비영리 기관(or.kr) 22건, 연구소(re.kr) 11건, 기타 29건 이다. 국내, 국제간의 피해관계를 살펴보면, 국내에서 국내로 공격한 경우 48건, 국내에서 국외로 24건, 국외에서 국내로 91건, 국외에서 국내를 거쳐 다시 국외의 컴퓨터를 공격한 경우는 183건이다. 이를 분석해 보면 공격대상은 주로 대학과 기업에 해커들의 공격이 집중되고 있으며, 국내, 국제간의 피해관계는 국외→국내→국외의 경로를 거치는 해킹이 가장 많은데, 이는 국외의 해커들이 국내의 보안이 취약한 컴퓨터들을 자신들의 위치를 감추기 위한 수단으로 사용하고 있다는 것을 의미한다[1].

사용된 해킹 기법을 살펴보면, 서비스 거부 공격 16건, SW 보안오류 이용 3건, Email 관련 공격 20건, 버퍼 오버플로 214건, 취약점 정보 수집 272건, 구성, 설정 오류로 인한 공격 2건, 사회공학을 이용한 공격 4건, 악성 프로그램 이용 58건, 사용자 도용 68건 등이다[1]. 이 중 몇 가지 공격에 대하여 살펴보면 다음과 같다.

서비스 거부(DoS, Denial of Service)공격은 이전부터 있었으나, 지난 2000년 2월에 일어난 공격은 분산 서비스 거부(Distributed DoS)공격이라는 점에서 주목할 만하다. 서비스 거부 공격이 이루어지는 과정은 다음과 같다. 해커는 우선 수백, 수천 개의 보안이 허술한 컴퓨터를 미리 공격하여 서비스 거부 공격을 할 수 있는 프로그램을 미리 심어 놓는다 그리고, 이 프로그램들을 특정시간이 되면 동시에 하나의 컴퓨터를 공격하

† 이 논문은 2000년도 두뇌한국21사업에 의하여 지원되었음.
* 종신회원

도록 설정해 둔다. 그러면 공격대상이 되는 컴퓨터는 단시간에 몰려오는 엄청난 데이터를 감당하지 못하고 다운되게 된다[2, 4].

Email 관련 공격에는 스팸메일(Spam Mail)과 메일폭탄(Mail Bomb)이 있다. 스팸메일은 주로 광고의 용도로 사용되는 불특정 다수에게 보내는 소모성 메일이고, 메일폭탄은 특정 사람 또는 특정 시스템에 보내는 과도한 양의 메일을 말한다. 두 가지 모두 받는 이의 디스크를 다 써버리게 하기도 하고, 단기간에 서버가 처리하지 못할 정도의 메일이 와서 서버가 다운되기도 한다. 초기에는 메일폭탄이 스팸메일을 보내는 사람을 응징하기 위한 도구로 사용되기도 했다고 한다.

시스템의 취약점에 대한 정보를 수집하여 공격하는 방법은 매우 다양하다. MSCAN (Multi SCAN)은 그 중에서 가장 널리 쓰이는 방법중의 하나인데, 지정된 도메인에서 알려진 모든 취약점을 찾는 도구이다. MSCAN은 statd, nfs, cgi-bin programs, X, POP3, IMAP, domain name service, finger 등에서 이미 잘 알려진 취약점들을 찾는다. MSCAN 자체가 공격도구는 아니지만, 해커는 MSCAN을 이용해서 얻어진 정보를 다음 공격에 사용할 수 있다. 따라서 MSCAN의 흔적이 보이면 주의해야 한다. MSCAN은 외부 네트워크 상에서 보이는 호스트만을 탐색할 수 있으므로, 방화벽(Firewall)이 잘 설치된 곳에서는 무용지물이 된다. 근본적인 방지를 위해서는 취약점이 있을 법한 프로그램의 최신의 패치를 설치하는 것과 꾸준한 시스템의 모니터링이 필요하다[5].

사용자의 권한을 도용하는 방법에는 여러 가지가 있는데, 그 중에 스니핑(Sniffing)과 Crack이 있다. 스니핑은 한 호스트에서 그 주위를 지나는 패킷들을 엿보는 방법인데, 인터넷의 패킷 라우팅 구조의 약점을 이용한 것이다. 패킷 라우팅시 일반적으로 자신에게 오지 않는 패킷은 받지 않는데, 스니퍼(Sniffing을 하는 도구)는 자신을 경유해 가는 모든 패킷들을 다 엿듣는다. 이렇게 하기 위해서는 네트워크 디바이스의 상태 flag가 promisc로 되어 있어야 한다. 만약 자신의 네트워크 device의 상태가 promisc로 되어 있으면, root권한으로 실행되고 있는 프로세스 중에서 수상한 것이 있는지 의심해 보아야 한다(주로 a.out, in.telnetd, in.uucpd 등으로 위장되곤 한다). 스니핑의 주된 목적은 네트워크를 통해 전달되는 패스워드를 알아내기 위한 것이므로 패스워드를 전달할 때 암호화를 하는 Secure shell, Kerberos 등을 이용하면 안전하다[4].

Crack은 유닉스 시스템의 암호를 추적하는 프로그램이다. 유닉스의 패스워드는 DES를 따르므로 암호화된 패스워드에서 바로 원래의 패스워드를 얻기는 힘들다. 따라서 Crack은 있을 법한 패스워드를 추측해서 이를 DES로 암호화한 후 저장된 패스워드(/etc/passwd)와 비교를 하는 방법을 쓰고 있다[3].

IP spoofing은 패킷의 출발지 주소를 위조하는 것이다. 그래서 패킷이 공격자의 실제 출발지가 아닌 다른 곳에서 출발한 것처럼 보이도록 하는 것이다. 위조된 주소는 일반적으로 수신자의 컴퓨터가 신뢰하는 주소이므로, 패킷이 수신자에게 아무 문제없이 받아들여지게 되며, 때로는 이 방법으로 방화벽이 설치된 곳의 컴퓨터를 공격하기도 한다. IP spoofing의 한 예로, 공격자는 공격대상 컴퓨터(A)와 공격대상 컴퓨터가 신뢰하는 컴퓨터(B)가 있는 경우, 그들 사이의 연결을 낚아챌 수 있다. 우선 공격자는 B에게 과도한 양의 패킷을 보내어 B의 네트워크 기능을 잠시 상실하게 만든다 그리고 위조된 패킷을 A에게 보내어 A와 대화를 시도한다. A가 이에 대한 응답을 B에게 하면 공격자는 중간에서 그 패킷을 가로챈다. 이렇게 되면 A는 공격자와 대화를 하게 되는 것이고, 이러는 동안 B는 무슨 일이 일어나는지 알지 못하게 된다.

3. 시스템 보안

앞에서 설명한 해킹에 대비할 수 있는 보안기법에는 여러 가지가 있다. 여기서는 방화벽, COPS, Satan, Kerberos 등에 대하여 간단히 살펴보겠다.

방화벽(Firewall)은 내부 네트워크와 외부 네트워크 사이에 있는 컴퓨터를 가리키는 것인데, 방화벽은 이 사이에서 어떤 정보를 내보내고 들여올 건지 여과하는 역할을 한다. 스크리닝 라우터(Screening router)는 외부 네트워크와 내부 네트워크를 물리적으로 구분하고 둘을 연결하는 것이며, 응용 게이트웨이(Application Gateway)

는 내부와 외부가 물리적으로 구분되지 않으면서 게이트웨이 안의 proxy를 통해 연결하는 것이다. 스크리닝 라우터에는 Draw Bridge, Karlbridge 등이 있고, 응용 게이트웨이에는 TCP wrapper, TIS firewall toolkit 등이 있다[4].

COPS는 Sun Microsystems에서 개발된 프로그램으로, 시스템 내부에 존재하는 취약성을 검사한다. COPS가 주로 하는 일은 시스템 파일, directory, device의 소유자와 권한, 패스워드 파일과 그룹파일 형식상의 취약점, 보안성이 없는 anonymous ftp에 대한 검사 등이다. COPS의 가장 큰 단점은 네트워크 보안은 전혀 검사하지 못한다는 것이다. 유닉스 시스템은 바로 네트워크 컴퓨터라는 개념에 비추었을 때, 어떤 한 시스템의 보안 점검을 COPS만으로 한다는 것은 부족한 감이 있다. 따라서 다른 툴들과 같이 사용하여, 시스템의 보안을 강화하여야 할 것이다[3].

Satan(Security Administrator Tool for Analyzing Network)은 네트워크의 결함을 찾는 도구이다. 주어진 도메인에 대해서 현재까지 알려진 거의 모든 네트워크의 결함들을 찾아주고, 그에 대한 예방책까지 알려주는 툴이다. 원래 해킹에 대한 예방의 목적으로 만들어졌지만, 오히려 해커들에 의해 원거리 공격(remote attack)의 한 방법으로 애용되기도 한다[4].

Kerberos는 지난 10년간 Unix에서 사용된 역사가 깊은 프로그램으로, 안전하지 않은 네트워크 상에서 사용자를 인증하는 시스템이다. 네트워크 상에서 패스워드를 직접 전달하게 되면, Sniffing 등의 공격에 대하여 안전하지 못하다. 따라서 패스워드를 암호화해서 전달하고 있다. Kerberos는 Windows2000에서 기본 보안도구로 채택되어 있다[4].

언제 어떤 유형의 해킹이 이루어질지 모르므로 시스템을 항상 로깅(logging)하는 것이 중요하다. Syslog, firewall, router 등의 log를 정기적으로 검사하여서 의심이 나는 곳으로부터의 접속이 있었는지를 확인해야 한다. 이 파일들은 수정이 가능하면 무용지물이 되므로 가능하면 수정이 불가능한 매체에 저장되는 것이 좋다.

4. 암호학

암호학은 암호기술과 암호해독의 두 분야로 구성된다. 암호기술은 키를 사용하여 평문을 암호문으로 바꾸는 암호 알고리즘과 키를 사용하여 암호문을 평문으로 바꾸는 복호 알고리즘을 개발하는 분야이고, 암호해독은 키를 모르는 상태에서 암호문에서 평문을 얻어내려는 노력을 일컫는다.

암호시스템의 기본적인 설정은 정보를 주고받는 송신자와 수신자, 그리고 이 정보를 얻어내려는 적, 즉 암호해독자로 구성된다. 송신자가 보내고자 하는 정보를 평문이라 하고 이것을 암호화한 것을 암호문이라 한다. 송신자는 키를 이용하여 평문을 암호문으로 만들고, 안전하지 않은 통신망을 통해 이 암호문을 전송한다. 수신자는 키를 이용해 암호문을 복호화하여 평문을 얻는다. 암호시스템은 평문의 집합, 키의 집합, 암호문의 집합, 암호 알고리즘, 복호 알고리즘, 이 다섯 가지 구성요소로 이루어진다.

암호시스템의 고전적인 예로 Caesar 암호시스템이 있다. Caesar 암호시스템은 키가 3인 shift cipher를 말한다. 암호화 과정에서는 평문에 나타난 알파벳 문자 각각을 알파벳 순서상에서 세 번째 뒤에 있는 문자로 대치시킨다. 즉 평문에 'C'라는 문자가 있다면 이 'C'를 알파벳상에서 세 번째 뒤에 있는 'F'로 대치시킨다. 따라서 평문이 'CAESAR'일 경우 암호문은 'FCHVDU'가 된다. 복호화 과정은 암호화의 과정과 반대로, 암호문에 있는 문자들을 알파벳 상에서 그 문자보다 세 번째 앞에 있는 문자로 대치시키면 된다.

암호시스템은 크게 비밀키 암호시스템과 공개키 암호시스템으로 나눌 수 있다 먼저 비밀키 암호시스템이란 암호화와 복호화에 같은 키를 사용하는 암호시스템으로 위에서 설명한 Caesar 암호시스템이 비밀키 암호시스템에 속한다. 이러한 비밀키 암호시스템의 문제점은 송신자와 수신자가 같은 키를 미리 가지고 있어야 하기 때문에 키를 수신자에게 안전하게 전달하는 방법을 마련해야 하는 것이다. 따라서 인터넷에서 독립적으로 사용되기는 어렵다. 현재 사용되는 비밀키 암호시스템의 예로는 DES[6], IDEA[7], Blowfish[8] 등이 있다. DES는 1977년 미국 국립표준연구소가 공개한 비밀키 암호시스템으로 64-bit 평문과 56-bit 키를 가지고 64-bit 암호문을 만드

는 암호시스템이다. 이 시스템의 장점은 permutation, substitution(S box), exclusive or 등의 연산을 사용하기 때문에 속도가 매우 빠르다는 점이다[6].

공개키 암호시스템은 1976년에 제안된 새로운 개념으로 공개키 암호시스템을 기반으로 현대 암호학의 발전이 이루어졌다 해도 과언이 아니다. 공개키 암호시스템은 비밀키 암호시스템과 달리 암호와 복호에 서로 다른 키를 사용한다. 즉 암호화할 때는 공개키를 사용하고 복호화할 때는 비밀키를 사용한다. 예를 들어 갑과 을이 서로 통신을 행한다고 할 때, 갑은 을의 공개키를 이용하여 평문을 암호화한 뒤 을에게 전송한다. 이 암호문은 을의 비밀키를 이용해서만 복호화가 가능하므로 오직 을만이 암호문으로부터 평문을 얻을 수 있다. 따라서 같은 키를 미리 공유하지 않고도 암호문을 주고 받을 수 있다. 이 시스템의 단점은 비밀키 암호시스템에 비해 속도가 느리다는 점이지만 키를 안전하게 전달해야 하는 문제가 없기 때문에 인터넷 환경에서 사용 가능하다는 장점을 갖는다. 공개키 암호시스템의 예로는 RSA[9], ElGamal[10], Elliptic curve[11]를 이용한 암호시스템 등이 있다. RSA는 1978년에 Rivest, Shamir, Adleman이 제안한 공개키 암호시스템으로 512-bit 평문과 512-bit 키로 같은 길이의 암호문을 만든다. RSA 암호시스템의 장점은 정수론에 기반하고 있어서 안전도가 높다는 점이며 현재 미국에서 2000년 9월까지 특허 등록되어 있다[9].

암호시스템 외에 중요한 암호 기법들로는 전자서명, 해쉬 함수(message digest), 키 분배(key distribution), 비밀 공유(secret sharing), zero-knowledge proof 등이 있다. 이 중 전자서명은 전자 문서에 덧붙여지는 암호화된 코드를 말하며 지금까지 발표된 전자서명 방법 중 대표적인 것들로는 NIST의 표준인 DSS[12]와 NTT에서 개발한 Esign[13], 그리고 Schnorr[14]가 제안한 방법 등이 있다.

이제 암호기술을 인터넷 응용에 적용한 예를 살펴보자. 먼저 전자우편 시스템의 보안상 취약점을 보완하고 인터넷과 같은 개방된 네트워크 환경 하에서 전자우편 시스템을 이용해 개인 정보 및 비밀 정보를 안전하게 상대방에게 전송하기 위해 개발된 도구들 중 PEM(Privacy Enhanced Mail)[15], PGP(Pretty Good Privacy)[16], S/MIME(Secure/Multipurpose Internet Mail Extension) 등이 있다. PEM과 PGP는 보내고자 하는 내용을 암호화해서 보내는 방식으로 기밀성, 인증, 무결성, 부인방지 등의 기능을 지원한다. 하지만 PEM의 경우 구현이 복잡하다는 단점을 가지고 있고, PGP의 경우는 기존의 전자우편과 통합이 어렵다는 단점이 있다[13,14]. 한편 S/MIME는 위에서 설명한 PEM과 PGP의 단점을 극복하고자 RSA Data Security 사에서 개발한 프로토콜로 인터넷 전자우편 형식인 MIME에 암호화와 전자서명을 추가하였다. S/MIME는 현재 MS Outlook, Netscape Communicator, 퀄컴 Eudora 등에서 사용되고 있다.

다음으로 Web 통신 보안 측면을 살펴보자. WWW 응용에 직접 관련된 보안 프로토콜의 대표적인 예는 S-HTTP와 SSL[17]이 있다. S-HTTP는 응용계층의 HTTP에 보안 기능을 추가한 표준 프로토콜인데 S-HTTP보다 다음에 설명할 SSL이 더 널리 쓰이고 있다. SSL은 원래 Netscape에서 처음으로 제안한 보안 프로토콜로서 자사의 웹 어플리케이션에 처음으로 구현함으로써 현재 웹 보안의 대명사로 알려져 있다. SSL은 인터넷의 TCP/IP 구조상에서 트랜스포트 계층과 응용 계층 사이에 위치하여 네트워크 상에서 전송되는 패킷들을 암호화한다. SSL은 암호화, 전자 서명, 키 교환 등 기본적인 보안 기능을 투명하게 제공하며, Microsoft에서도 채택하여 사용하는 등 현재 널리 쓰이고 있다[17]. 하지만 미국의 암호 수출 제한 정책으로 인해 충분한 보안성을 보장하지 못한다는 약점을 가지고 있다.

5. 전자상거래와 보안

전자상거래는 인터넷과 같은 개방형 네트워크를 이용하여 상품이나 서비스를 매매하는 것으로, 다시 말하면 비즈니스 과정에 관련되는 주체의 정보시스템이 네트워크에 연결되어 거래 과정을 모두 네트워크 상에서 전자적으로 행하는 것이라고 말할 수 있다

전자상거래의 국내외 규모를 살펴보면 세계 시

장의 경우 1999년에는 670억불이었고 2003년에는 1조 700억불로 성장할 것으로 예측하고 있다. 한편 국내의 경우도 1998년에 500억원에서 1999년에는 1,500억원의 규모로 성장했고, 2005년에는 2조 600억원에 달할 것으로 예측되고 있다.

이처럼 급속도로 성장해 가는 전자상거래의 국내외 동향을 잠시 살펴보자. 먼저 미국의 경우 인터넷 무관세 지대를 추진하고 있으며 CommerceNet을 통한 표준화를 주도하고 있다. 한편 민간 기업으로서도 Oracle-HP-Cybercash와 IBM 등이 전자상거래에 참여하고 있다. 그리고 일본의 경우는 정부 주도로 ECOM이 설립되었으며 민간주도로는 Smart Islands Consortium 등이 구성되어 있고, 유럽은 EU가 공동으로 전자상거래에 대응하고 있다.

한편 국내에서는 1998년에 정보통신부에서 전자서명법을 발표하였고, 1999년에는 산업자원부에서 전자상거래 기본법을 발표하였다. 그리고 공공 부분으로 한국전산원에서 국가·공공기관 정보화 사업을 추진중이고, 한국정보보호센터(KISA)에서 정보보호기술 관리와 연구를 하고 있으며 한국통신정보보호학회가 설립되어 있다.

전자상거래에서 비용을 지불하는 방법은 신용카드를 이용하는 방법과 현금을 이용하는 방법이 있다. 이 중 신용카드를 이용하는 방법은 현재 인터넷에서 많이 사용되고 있으며 NetBill, NetCheque, SET 등이 이에 속한다. 현금 시스템의 경우는 전자 현금을 이용하는 Ecash, NetCash 등과 전자 지갑을 이용하는 Mondex 등이 있다. 이 중 인터넷상에서 신용카드 지불을 위한 프로토콜 SET을 좀더 살펴보자. SET은 Master Card, Visa International이 주도하여 개발한 프로토콜로, 인증과 키 교환을 위해 1024비트 키의 RSA를 사용하고 일반적인 SET 메시지에는 DES를 사용한다. 또한 SET은 프로토콜에 맞는 엄격한 데이터 타입을 요구한다[18].

이제까지 설명한 전자상거래가 사이버 공간에서 이루어지는 모든 경제활동을 거래관점에서 바라본 것이라면, 이러한 경제활동을 사업의 관점에서 바라본 것을 인터넷 사업이라고 칭한다. 인터넷 사업을 크게 네 가지로 분류하면 다음과 같다[19].

먼저 인터넷 인프라 사업이 있다. 인프라 사업은 인터넷 비즈니스의 필수요건인 인터넷 프로토콜 기반 네트워크인 하부구조, 즉 인터넷 접속 관련 제품과 서비스를 제공하는 사업을 말한다. 고속통신망을 제공하는 통신사업, 통신장비 제공, 컴퓨터 제조, 방화벽 등의 보안장비를 제공하는 것들이 인프라 사업에 속한다.

두 번째로 인터넷 응용 사업이 있다. 응용사업은 인터넷 인프라를 통하여 온라인 경제활동이 기술적으로 실행 가능하도록 해주는 소프트웨어를 개발하고 관련 서비스를 제공하는 사업을 말한다. 여기에는 Netscape, MS Explorer 등의 응용 소프트웨어와, 검색 엔진, 데이터베이스, 보안 소프트웨어 등이 속한다

세 번째로 인터넷 중개 사업이 있다. 중개 사업은 인터넷을 통한 구매자와 판매자의 거래를 촉진시킴으로써 인터넷시장의 효율성을 향상시키는 사업이다. Yahoo 등의 포탈서비스와 E*Trade 등의 금융 서비스, AOD, VOD, 전자책 등의 컨텐츠 사업, 그리고 경매나 eBay 등의 중개사업이 여기에 속한다.

마지막으로, 인터넷 상거래 사업이 있다. 인터넷 상거래의 범주에 드는 것들로는 Amazon 등의 소매업, Dell 등의 직접 판매업, 쇼핑몰 사업 등이 있다.

위에서 보는 바와 같이 인터넷 사업의 모든 부분에서 보안은 매우 중요한 역할을 한다. 보안 장비와 보안 소프트웨어는 전자상거래를 가능케 하는 기본적인 도구들이고, 금융서비스, 컨텐츠 사업 등 중요한 가치가 오고가는 인터넷 사업에서 보안기술은 필수 불가결한 요소가 된다.

6. 결 론

해킹은 오래 전부터 있어왔지만, 전자상거래의 활성화와 더불어 더욱 그 수가 늘어나고 있다. 특히 국외에서 국내를 경유하여 다시 국외로 가는 해킹이 많은 것을 보면 보안이 취약한 국내 컴퓨터가 국외의 해커에 의해 이용당하는 것을 알 수 있다. 따라서 국가적인 차원의 컴퓨터 시스템 보안 대책이 필요하다

기존의 방법과 툴을 이용한 교과서적인 해킹은 그 대응방법도 대부분 알려져 있어서 방어가 가능하다. 하지만 서비스 거부 공격 같은 알고서도 막지 못하는 공격도 있을 뿐더러, 기존에 알려지

지 않은 새로운 해킹방법도 계속 나타나고 있으므로 언제 있을지 모르는 새로운 해킹에 항상 대비하기 위해서는 지속적인 보안관리 및 점검이 필요할 것이다.

인터넷 응용에서 공개키 암호시스템과 비밀키 암호시스템이 둘 다 사용되고 있다. 공개키 암호시스템은 인터넷 상에서 키를 주고받거나 또는 중요한 데이터를 보내는데 사용되고, 비밀키 암호시스템은 많은 양의 자료를 암호화하여 보내는데 사용된다. 암호를 깨기 위한 노력도 계속되고 있는 만큼, 안전성 유지를 위해서는 암호학에 대한 깊은 연구가 계속 필요하다.

전자상거래의 규모는 급속도로 커지고 있으며, 전 세계가 이 전자상거래의 흐름에 뒤지지 않기 위해 총력을 다하고 있다. 인터넷 사업을 4가지 유형으로 나눌 수 있으며, 보안은 4가지 유형의 어느 단계에서도 빠질 수 없는 중요한 요소로 자리잡고 있다. 전자상거래와 보안을 잘 접목시키는 것이 인터넷 중심의 지식기반사회에서 경쟁력을 높이는 중요한 과제임을 명심해야 한다.

참고문헌

[1] 한국정보보호센터, "http://www.kisa.or.kr/K_trend/KisaNews/200003/정현철.htm"

[2] Crypto-Gram newsletter, CounterPane, "http://www.counterpane.com/crypto-gram-0002.html"

[3] William Stalling, Internet Security Handbook. IDG Books Worldwide, 1996

[4] Garfinkel and Spafford, Practical UNIX & Internet Security 2nd Edition, O'Reilly, 1996

[5] The U.S. Department of Energy Computer Incident Advisory Capability Bulletin I-073: MultiScan Tool "http://www.sgi.ethz.ch/secadv/msg0040.html"

[6] M.E. Smid and D. K. Branstad. The data encryption standard: past and future. In Contemporary Cryptology, The Science of Information Integrity. 1992.

[7] X. Lai and J. Massey, A proposal for a New Block Encryption Standard, Advances in Cryptology-EUROCRYPT '90, 19991.

[8] B. Schneier, The Blowfish Encryption Algorithm, Dr. Dobb's Journal, 1994.

[9] R.L. Rivest and A. Shamir, How to Expose an Eavesdropper, Communications of the ACM, 1984.

[10] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 1985.

[11] N. Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation, 1987.

[12] Proposed Federal Information Processing Standard for Digital Signature Standard. Federal Register, Aug 1991.

[13] T. Okamoto, A Fast Signature Scheme Based on Congruential Polynomial Operations, IEEE Transactions on Information Theory, 1990.

[14] C.P. Schnorr. Efficient Signature Generation for Smart Cards. Advances in Cryptology-EUROCRYPT '88, 1988.

[15] J. Linn, Privacy Enhancement for Internet Electonic Mail: Part I -Message Encipherment and Authentication Procedures, RFC 989.

[16] 'PGP'. Simson Garfinkel, O'Reilly & Associates. Inc, 1995.

[17] Introducing SSL and Certificates using SSLeay, "http://www.camb.opengroup.org/RI/www/prism/wwwj/"

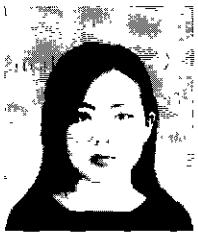
[18] 전자상거래 보안 기술, 이만영 · 김지홍 · 류재철 · 송유진 · 엄흥렬 · 이임영 저.

[19] "http://www.internetindicators.com/facts.html"

윤 호 빈

1999 서울대학교 컴퓨터공학과 학사
1999~현재 서울대학교 컴퓨터공학부 석사과정
관심분야 전자서명, 전자상거래
E-mail:hbyoon@theory.snu.ac.kr

김 서 진

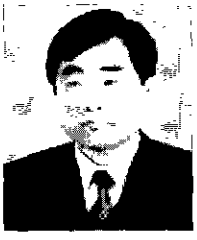


1999 서울대학교 컴퓨터공학과 학사
1999~현재 서울대학교 컴퓨터공학부 석사과정
관심분야 전자상거래, 전자화폐, 전자서명
E-mail:sjkim@theory.snu.ac.kr

박 근 수

1983 서울대학교 컴퓨터공학과 학사
1985 서울대학교 컴퓨터공학과 석사
1991 미국 Columbia 대학교 전산학 박사
1991.11~1993.8 영국 런던대학교 King's College 조교수
1995.7~1995.8 호주 Curtin 대학교 방문연구원
1993.8~현재 서울대학교 컴퓨터공학과 부교수
관심분야 컴퓨터 이론, 병렬 계산, 암호학
E-mail:kpark@theory.snu.ac.kr

박 경 수



1982 전북대학교 경영학과 학사
1984 전북대학교 대학원 경영학석사
1990 전북대학교 대학원 경영학박사
1993.8~1994.8 미국 University of Nebraska-Lincoln 객원교수
1991.3~현재 전북대학교 경영학부 부교수
관심분야 수리계획법, 정보기술의 전략적활용, 전자상거래
E-mail:parks@moak.chonbuk.ac.kr

• 2000년 하계 컴퓨터통신 워크숍 •

- 일 자 : 2000년 8월 24 ~ 25일
- 장 소 : 상록리조트(천안)
- 주 체 : 정보통신연구회
- 문 의 처 : 연세대학교 전자공학과 이재용 교수
  Tel. 02-361-2873 E-mail:jyl@nasla.yonsei.ac.kr