情 報 保 護 學 會 誌
第 12 券 第 6 號, 2002. 12

국방 정보보호 기술 발전 동향

김 배 현*, 나 원 식*, 유 인 태**, 권 문 택***

요 약

정보화가 진전되면서 국방·통신·금융·전력 등 주요사회기반체계의 정보시스템에 대한 의존도가 심화되고 있고 이에 따라 해킹, 컴퓨터바이러스 등의 사이버테러가 국가 안보를 위협하는 새로운 위협요소로 대두되고 있다. 사이버테러가 대규모, 지능화, 첨단화의 양상으로 발전됨에 따라 정보전에 대한 대비책이 무엇보다 시급한 실정이다. 이러한 시대적 요구에 부응하기 위해서는 국가 차원에서의 국방 정보보호기술 체계를 구축하여야 하며 이를 위해 본 논문에서는 현재의 정보보호기술 동향과 앞으로의 발전 전망을 분석하여 향후 발전계획을 수립하는데 필요한 기초 자료를 제시하고자 한다.

Ⅰ. 서 론

사회 전반에 걸쳐 급속히 정보화가 진행이 되면서 정보화 선진국을 중심으로 이에 따른 정보화 역기능이 급격히 증가하고 있다. 따라서 각국은 국가 중요 정보보호기반구조의 완벽한 안전성을 확보하기 위한 체계적인 대책 마련이 필요하게 되었다. 미국의 경우 9.11 이후 본토의 안전을 지키기 위해 Homeland Security 계획을 세우고 이 계획에 따라 새롭게 등장하는 위협에 대한 기민한 대응체계를 구축하고 있다. 이 Homeland Security 계획에서 정보통신기반은 강력한 기반인 동시에 매우 취약하고 공격당하기 쉽다는 사실을 인식하고 사이버보안을 위한 예산을 대폭 확대 하고 있다. 따라서 전 세계적으로 정보전에 대한 관심이 고조되고 있으며 정보전 대응체계 마련이 그 어느 때 보다도 중요하게 부각되고 있다. 기민한 정보전 대응 체계를 구축하기 위해서는 체계적인 국방 정보보호 기술 개발정책을 수립하여 추진해야 한다. 따라서 본 논문은 국내외의 국방 정보보호 기술의 현황과 전망을 분석한다.

Ⅱ. 정보보호 기술 정의 및 분류

국방 정보보호 기술은 정보전 대응체계의 기반이 되는 분야로 의도적으로 또는 우연히 허가받지 않은 형태로 컴퓨터 및 통신망에 접속하여 정보를 누출, 전송, 수정, 파괴하는 등의 행위를 방지함으로써 유·무선통신이나 시스템, 생체 등 관련 정보를 안전하게 생성.유통.저장.소비.인식.관리하도록하여 안전한 정보사회 구현을 가능하도록 하는 정보통신의 핵심 기반기술이다.

1. 정보보호기술 분류

국방 정보보호기술은 크게 나누어 [표 1]과 같이 정보보호 기반기술, 시스템·네트워크 정보보호기술, 응용체계 보호기술의 3가지 기술로 분류된다.

2. 정보보호 기반기술

2.1 암호기술

암호기술은 인가된 사람만이 정보를 이용할 수 있도록 하고, 인가되지 않은 자에 대해서는 정보를 노출 시키거나 변경 가능하지 않도록 하는 기술이다. 암호화 기술을 구현하기 위한 방법으로 암/복호화 키가 동일한 대칭형 암호화(symmetric cryptography)와 암/복호화 키가 서로 다른 비대칭형 암호화

* 경희대학교 전자정보학부 멀티미디어정보통신 연구실 ({bhkim, wsna}@mic.khu.ac.kr)
** 경희대학교 전자정보학부 조교수 (itryoo@khu.ac.kr)
*** 경희대학교 산업정보대학원 교수 (kmt@khu.ac.kr)

(asymmetric cryptography)로 크게 구분할 수 있다.

〔표 1〕 정보보호기술 분류

분류	기술 분야	기술 내용
정보보호 기반기술	암호기술	암호 알고리즘 설계 및 분석 암호 키 관리 암호구현 등
	인증기술	공개키 기반구조 구축 생체인식 등
	정보보호 평가기술	정보보호 시스템 평가 기술
시스템 네트워크 보호기술	시스템 보호기술	보안 O·S, 보안 DBMS, 보안 IC카드 등
	네트워크 보호기술	유선망 정보보호, 침입탐지, VPN, Firewall 기술 무선망 정보보호
응용체계 보호기술	정보보호 응용기술	전자서명, 전자계약, 전자투표 등
	해킹 바이러스 대응기술	취약성분석, 침입대응 복구 불특정 바이러스 차단, 악성 이동코드 트랩 도어 관리

대칭키 암호화는 송·수신자 간에 미리 약속된 동일한 키를 가지고 있어여야 하기 때문에 키 분배의 어려움이 있지만 빠른 속도와 비교적 높은 안전성 및 키의 사이즈가 작다는 장점이 있다.

대칭키 암호화 알고리즘은 다시 데이터 처리 형식에 따라 블록 암호(Block Cipher) 알고리즘과 스트림 암호(Stream Cipher) 알고리즘으로 나누어진다. 블록 암호 방식은 평문을 정해진 사이즈의 블록 단위로 암·복호화를 수행하는 방식이 다. 우리에게 가장 널리 알려진 블록 암호 알고리즘은 1972년 미국 NIST(National Institute of Standards and Technology)에서 표준으로 정한 DES(Data Encryption Standard)이며 1990년대에 유럽의 Lai와 Massey가 제안한 IDEA(International Data Encryption Algorithm), AES(Advanced Encryption Standard), Skipjack, Kasumi, SEED 등이 있다. 스트림 암호 방식은 평문을 일련의 비트열로 취급하여 한 번에 1비트씩 또는 바이트 단위로 암호화시키는 알고리즘이다. 에러 전파 현상이 없으며 블록 암호 알고리즘에 비해 빠르고 용이하게 구현할 수 있다.

비 대칭키 암호는 공개키 암호 시스템으로도 불리며 대칭키 암호와는 달리 서로 다른 두 개의 키를 사용하여 하나는 개인의 비밀키로 하고 나머지 하나는 공개하여 모든 사람으로 하여금 사용할 수 있게 한 것이다. 공개키 암호는 대칭키 암호에 사용되는 키를 안전하게 공유할 수 있기 때문에 키 분배, 전자서명, 인증, 부인방지 등의 정보보호에서 중요한 역할을 담당하고 있다. 그러나 공개키 암호화 알고리즘은 비밀키 암호 알고리즘에 비해 속도가 매우 느리다. 우리에게 가장 널리 알려진 공개키 암호 알고리즘은 1977년 Rivest, Shamir 및 Adleman이 제안한 RSA(The Rivest-Shamir-Adleman)이며 ElGamal, Diffie-Hellman, XTR 등이 있다.

2.2 인증기술

공개키 암호 시스템 방식을 이용하여 네트워크 사용자들에게 암호기능과 서명기능을 제공할 수 있는 기반구조를 PKI(Public Key Infrastructure)라 한다. PKI의 구성요소는 인증기관, 등록기관, 디렉토리, 사용자이다.

인증기관은 공개키 기반구조를 구성하는 가장 핵심적인 객체로 그 역할 및 기능에 따라 계층적으로 구성된다. 인증기관은 PKI 구축의 루트 CA(Certification Authority)로의 역할을 수행하는 정책승인기관(PAA:Policy Approving Authority), 인증기관의 공개키를 인증하고 인증서, 인증서취소목록을 관리하는 정책인증기관(PCA:Policy Certification Authority), 사용자의 공개키 인증서를 발행, 취소를 하며, 사용자에게 자신의 공개키와 상위기관의 공개키를 전달하는 인증기관(CA:Certification Authority)을 포함한다. 등록기관은 인증기관과 사용자사이에 위치하며 인증기관을 대신하여 사용자의 신분과 소속을 확인하는 기능을 수행한다. 디렉토리는 인증서와 사용자 관련정보, 상호 인증서 쌍 및 인증서 취소목록 등을 저장 및 검색하는 장소로 응용에 따라 이를 위한 서버를 설치하거나 인증기관에서 관리한다. 사용자는 PKI를 사용하는 사람뿐만 아니라 사람이 이용하는 시스템 모두를 의미한다.

생체인식 기술은 생물학적 특성을 이용하여 개인을 확인하는 기술로서 신체의 일부분이거나 개개인의 행동 특성을 반영하기 때문에 도난, 분실, 대여, 복사가 되지 않기 때문에 안전한 정보보안을 위한 분야로 대두되고 있다. 생체인식의 종류로는 신체적 특성을 이용하는 방법과 행동학적 특성을 이용하는 방법이 있다. 신체적 특성을 이용하는 방법은 지문, 얼굴, 손의 형태, 홍채 및 망막, 정맥 패턴, 귀, 입

술 인식 등이 있다. 신체적 특성을 이용하는 방법은 서명, 음성, 걸음걸이, 키 스트로크 인식 등이 있다.

2.3 정보보호 평가기술

정보보호시스템 평가·인증을 시행하는 중요한 목적은 객관적이고 공정한 평가·인증을 통해 안전성과 신뢰성이 검증된 정보보호시스템 사용을 권장하기 위한 것이다. 정보보호시스템 평가기술은 평가 기준을 개발하는 기술과 보안기능 평가 기술, 취약성 평가 기술, 보안 신뢰도 평가 기술이 있다. 평가기술은 정보보호시스템 평가 시 필요한 보안 요구사항들에 대한 기준으로 단일 제품 또는 시스템, 네트워크 시스템 등에 대한 평가기준이 있다. 보안기능 평가 기술은 보안위협 요소로부터 정보를 보호하기 위한 비밀성, 인증, 접근통제, 무결성, 부인방지, 바이러스 방지 등 제품에 구현된 보안기능에 대해 평가하는 기술이다. 취약성 평가 기술은 평가 대상 제품이나 시스템에 대하여 보안상 취약점을 분석하여 평가하는 기술이다. 보안 신뢰도 평가 기술은 형상 관리 및 설계 분석, 개발 방법, 배포와 운영, 제품 사용 설명서, 시험 등에 대하여 보안기능을 보증해 줄 있는가를 평가하는 기술이다.

3. 시스템 · 네트워크 보호기술

3.1 시스템 보호기술

IC카드는 IC칩을 내장하고 있는 전자 카드로 개인 정보를 생성 및 저장, 복구하거나 정보시스템에 대한 사용자 인증 및 정보 자원에 대한 접근 통제 수단으로도 사용될 수 있기 때문에 다양한 정보통신 서비스, 전자 상거래, 교통 및 운수, 방송 및 통신 분야 등에 응용될 수 있다. IC카드는 카드와 카드 리더기사이의 인터페이스 방식에 따라, 접촉식과 비접촉식으로 분류된다.

보안 O·S는 컴퓨터 운영체제가 가지고 있는 보안상 결함을 보완하기 위해 기존의 운영체제 내에 보안기능을 통합시킨 보안 커널을 추가로 이식한 운영체제이다. 보안 운영체제의 기본 기능으로는 컴퓨터 사용자에 대한 식별 및 인증, 강제적인 접근 제어, 임의적 접근 제어, 재사용 방지, 침입탐지 등의 보안기능 요소를 갖추어야 한다.

보안 데이터베이스는 데이터베이스에서 요구되는 정보보호 서비스인 시스템 감사, 사용자인증, 정당한 사용자의 데이터 접근 통제 등을 제공한다. 특히, 대용량의 자료를 보관하는 데이터베이스 관리시스템에서는 논리적 일관성 유지를 위한 요구사항으로는 데이터 무결성 유지, 데이터 연산의 무결성 유지 등이 있으며, 다양한 데이터베이스 응용들을 위한 강력한 정보보호 요구사항으로는 접근제어, 정보흐름 제어, 혹은 추론제어의 3가지 방법이 주로 사용되고 있다.

3.2 네트워크 보호기술

VPN(Virtual Private Networks)이란 인터넷이나 네트워크 서비스 사업자의 PSTN, ISDN, ADSL과 같은 공중망을 자사의 WAN 백본 처럼 사용하는 네트워크이다.

VPN을 교환 방식에 따라 구분하면 IP 기반 VPN과 ATM 기반 VPN, 그리고 MPLS 기반의 VPN으로 구분할 수 있고, 구현 방법에 따라 구분하면 침입차단시스템 기반의 VPN, 라우터 기반의 VPN, Dedicated VPN 등으로 구분할 수 있다. 현재 IP 기반의 VPN이 주류를 이루고 있다. VPN을 구현하기위한 기반기술로서는 터널링 기술, 키 관리기술, VPN 관리기술이 필요하고 그 외에 인증 및 암호화 기술, 라우터, 침입차단시스템에서 사용되는 일부 보안기술도 필요하다.

침입차단시스템은 외부 네트워크에 연결된 내부 네트워크를 외부의 불법적인 사용자의 침입으로부터 안전하게 보호하기위한 정책 및 이를 지원하는 H/W 및 S/W를 총칭하는 것으로 두 네트워크 사이의 신뢰할 수 있는 경계를 정하기 위한 메커니즘이다. 그러나 내부의 인증된 사용자에 대해서는 한정된 제어만 가능하고, 외부 공격자에 대해서도 완벽하게 방어할 수 없다는 근본적인 취약점을 가지고 있다. 따라서 외부 네트워크에서 내부네트워크로의 진입을 1차적으로 방어해주는 기능만을 수행한다. 침입차단시스템은 H/W 및 S/W로 구성된다. H/W적인 측면에서 침입차단 시스템은 패킷 필터링 라우터, 베스천 호스트, 사용자 인증 시스템, 암호화 장비 등으로 나눌 수 있다.

침입탐지시스템(Intrusion Detection System)은 허가받지 않은 접근이나 해킹 시도를 감지하여 시스템 또는 망 관리자에게 통보해 주고, 필요한 대응을 취하도록 하는 시스템이다. 침입탐지시스템은 모니터링 대상에 따라 네트워크 기반 침입탐지시스템과 호스트 기반 침입탐지시스템으로 나눌 수 있다.

4. 응용체계 보호기술

4.1 응용 서비스 보호기술

전자서명은 실생활에서 사용되는 서명 기능을 전자문서에 대하여 똑같은 기능을 가질 수 있도록 구현한 알고리즘으로 기본적으로 공개키 알고리즘에 기반하고 있다. 기본적으로 전자서명의 안전성은 그 근본이 되는 공개키 암호의 안전성에서 기인하며 해시 함수를 사용하여 무결성 등의 기능도 함께 제공할 수 있다. 전자서명은 크게 두 가지 방법으로 나눌 수가 있는데 그중 하나는 일반적으로 사용되는 메시지 부가형으로 보내지는 메시지에 서명이 부가되어 따라가는 형태이고 다른 하나는 메시지 복원형으로 메시지에 대한 사전 정보 없이도 서명 값으로부터 메시지를 복원할 수 있는 방법이다.

4.2 해킹 · 바이러스 대응기술

악성 코드는 시스템의 무결성 및 가용성을 침해하기도 하지만, 트로이 목마 형태나 스파이웨어로 활동하는 경우도 있어 해킹의 위협과 개인 정보 유출의 위험을 안고 있다. 더구나, 정보 기술의 발전에 따라 전쟁 양상이 정보전으로 바뀌면서, 국가간의 정보 우위 확보를 위한 노력으로 바이러스나 악성 코드를 정보전 수행을 위한 핵심 기술로 인식하고 있다.

Ⅲ. 정보보호 기술 현황

1. 정보보호 기반기술

1.1 암호기술

선진각국은 암호알고리즘을 국가용은 정부가 주도하고, 민간용은 공모방식을 통해 국가표준으로 채택하여 보급하고 있다. 미국은 첨단의 기반기술을 확보하고 있으며 DES, RSA알고리즘이 암호화, 전자서명 인증분야에서 전 세계적으로 50%이상의 시장을 점유하고 있다. 불록암호의 경우 미국은 NIST가 1977년 국가 표준으로 채택한 DES가 전 세계적으로 사용되고 있고, 1998년에 DES의 표준 기한이 만료되므로 1997년 1월부터 2000년까지 4단계 공모를 통하여 2000년 10월에 AES 블록암호화 알고리즘으로 벨기에의 Rijndael알고리즘을 최종 선정하였다. 이 밖에도 미국 Cylink사의 요구로 Massey가 개발한 SAFER(Secure And Fast Encryption Routine), 1994년 미국 RSA 연구소의 Rivest가 개발한 RC5(Ron's Code 5), 미국 NSA에서 개발한 Skipjack등이 있다. 유럽에서는 1992년도에 128비트 암호 알고리즘인 IDEA를 개발하여 유럽표준으로 채택하여 국제통상 등의 업무에 활용하고 있다. 일본은 1996년에 MISTY를 개발하여 IMT-2000 표준으로 채택 중이다.

스트림 암호의 경우 현재까지는 표준화된 스트림 암호방식은 없고, 대부분의 경우에는 암호알고리즘 자체를 비밀로 취급하는 경향이 있다. 최근에 들어서 IMT-2000이나 블루투스 등에 사용되는 스트림 암호 알고리즘이 공개되고 있다. 공개키 암호화의 경우에도 아직까지 표준화된 알고리즘이 없으나, 1978년 개발된 RSA알고리즘이 사실 표준으로 범세계적으로 수용되고 있다. 미국은 국가안보를 이유로 512 bits 이상의 암호체계에 대해서는 수출을 금지하고 있다. 한편 소인수분해의 난해성에 기반을 둔 RSA에 비해 Certicom사의 타원곡선 암호화(ECC: Elliptic Curve Cryptograph)방식은 타원곡선 이산대수문제에 기반을 두고 있으며, 안전도 및 짧은 키 길이로 인해 빠른 계산 속도가 큰 장점을 가지고 있지 때문에, RSA를 중심으로 한 미국의 독주에 제동을 걸 수 있는 공개키 암호 방식으로 많은 연구와 개발이 이루어지고 있다

우리나라의 경우 현재 선진국과 기술 수준 격차는 3년에서 5년 정도를 보이고 있다. 국가용은 현재 ETRI 부설 국가보안기술연구소에서 개발 중 이며, 한국정보보호진흥원에서 1999년 2월에 개발한 128비트 블록 암호 알고리즘인 SEED가 1999년 TTA 표준으로 제정되었으며 인증서 기반 표준 전자서명 알고리즘인 KCDSA가 1997년 개발되었고 1998년 해시 함수인 HAS_160이 개발되었다. 최근에는 KCDSA를 ECC에 적용한 EC-KCDSA가 2001년 11월에 TTA 표준으로 제정되었다. 국내 공개키 연구실태는 2000년 세계 암호학세미나(CRYPTO 2000)에서 「땋임군 암호」 이론을 발표한 이래 'CRYPTO 2001'에서는 비가환군을 이용한 공개키 암호이론을 발표하였고, 이어, 2002 韓·日월드컵 대회시 국내 정보통신대학원 주관으로 공개키 암호를 이용한 월드컵 MVP를 선정하기 위한 인터넷투표시스템을 선보이는 등 공개키 암호분야의 강국으로 부상하고 있다.

1.2 인증기술

인증을 위해서는 공개키 알고리즘인 RSA를 이용한 서명 및 인증기법이 사실상 산업표준으로 널리 사용되고 있고, 미국은 1996년부터 연방정부 차원의 PKI 구축을 추진하여 각주별로 공인인증 기관을 지정하여 개별 전자서명 인증체계를 구축하였다. 최근에는 서로 다른 구조를 가진 자국뿐만 아니라 전 세계 PKI 시스템을 상호 연동을 하기위한 FBCA (Federal Bridge CA)를 설립하여 운영 중이다. 최근 각국은 PKI 방식을 이용한 디지털 서명이외에 다양한 전자서명기술을 수용하도록 전자서명의 개념을 확대하는 추세이다. 우리나라의 경우 1998년 2월부터 각계의 의견을 수렴하여 제정된 전자서명법안은 1999년 2월 5일 법률 제5792호로 공포되었고, 1999년 7월 1일부터 본격 시행되었다.

전자서명법에 의한 국내 PKI 인증체계는 정보통신부가 공인인증기관에 대한 정책·감독 기관으로서의 기능을 수행하고, 한국정보보호진흥원(KISA)이 최상위 인증기관 역할을 담당하고 있다. 현재 국내 공인인증기관은 모두 7곳이다.

1.3 정보보호 평가기술

선진 각국은 이미 자국에 적합한 평가기준을 마련하여 실시하고 있다. 그러나 국제공통평가기준인 CC가 2000년 12월 ISO 15408로 공인된 후, 각국은 CC 기반 평가 체제로 전환 되고 있는 중이다. 미국은 1983년 정보보호시스템 평가기준인 오렌지북을 발표하였으며 이를 기반으로 1985년 TCSEC (Trusted Computer System Evaluation Criterian), 1987년 TNI(Trusted Network Interpretation of TCSEC), 1991년 IDI(Trusted DBMS Interpretation of TCSEC) 등 정보보호시스템 평가기준을 제정하고 TPEP(Trusted Product Evaluation Program) 평가 프로그램에 의하여 정보보호시스템을 운영 체제, 네트워크 컴포넌트 등으로 분류하여 평가를 시행해 왔다. 미국의 평가기준인 TCSEC은 평가기준으로 C2, C1, B3, B2, B1, A1 등 6개의 등급 체제로 이루어져 있다. 1997년에 NSA와 NIST가 공동으로 CC에 대처하기 위해 NIAP(National Information Assurance Partnership)을 설립하였고 1998년 9월에는 CC 평가·인증스킴 발표로 NVLAP(National Voluntary Laboratory Accreditation Program)에 의한 민간 평가기관 심사 및 인정, 민간평가기관인 CCTL의 평가와 NIAP Validation Body에 의한 인증이 시작되었다.

영국은 1987년 정보보호시스템 평가기준인 Green Book을 발표하였으며, 1990년 독일, 프랑스, 네덜란드와 공동으로 유럽공통평가기준인 ITSEC(Information Technology Security Evaluation Criteria)을 개발하여 UK scheme에 의한 평가를 시행하고 있다. 그리고 CESG를 인증기관으로 하여 Logica UK Ltd, Admiral Management Services Ltd. 등 5개 민간 평가기관(CLEF)에서 통신, 데이터베이스 네트워킹 등으로 정보보호시스템을 분류하여 평가를 수행하고 있다. ITSEC은 보안기능 요구사항과 보증 요구사항으로 구성되어 있고, E1~E6의 6개 등급 체계로 이루어져 있다.

국내에서의 평가기술은 아직 부분적으로 추진 중이며, CC도 도입 준비중에 있다. 한국정보보호진흥원에서 정보화촉진기본법에 따라 1998년 2월 정보통신망 침입차단시스템 평가기준 및 평가지침서를 제정 및 고시하였고 2000년에는 침입탐지시스템 평가기준을 제정하고 고시하여 침입차단시스템 및 침입탐지시스템에 대한 평가를 시행해 오고 있다. 또한 2000년 8월 5일에는 정보통신부 고시 제2002-40호-'정보보호시스템 공동 평가 기준'과 정보통신부 고시 제2002-41호-'정보보호 시스템 평가·인증 지침이 고시되었다. 그리고 CC 수용을 위해 스마트카드, PKI시스템, VPN 및 침입차단·탐지시스템에 대한 PP(Protection Profile) 개발을 추진 중에 있다.

우리나라의 평가인증체계를 보면, 인증기관은 국가정보원, 평가기관은 한국정보보호진흥원으로 되어 있다.

우리나라의 생체인식 기술은 지문인식, 홍채인식 등을 중심으로 생체인식을 활용한 인증기술을 일부 확보하고 있으며, 향후 생명공학기술로의 전이를 목표로 연구개발을 시작한 단계이며, 업체 중 독자적인 알고리즘이나 기술을 보유하고 있는 업체는 소수에 국한되어 있는 실정이다. 국내 업체들은 지문인식시스템, 음성인식 시스템, 그 외에 혈관, 홍채 및 얼굴인식시스템 등의 상품을 내놓고 있으며 음성과 지문인식 시스템이 시장을 당분간 주도할 것으로 예상된다.

2. 시스템 · 네트워크 보호기술

2.1 시스템 보호 기술

IC 카드의 경우 일반적으로 8비트 마이크로 프로세서를 주로 사용되고 있으며 최근에는 16-bit 및 32-bit CPU를 개발하고 있다. 또한 최근에는 Co-processor가 내장되어 있지 않아도 공개키 암호 시스템을 스마트카드에 구현할 수 있도록 ECC (Eliptic Curve Cryptosystem)가 등장하여 RSA의 대체 알고리즘으로서 점점 각광을 많이 받아가고 있다. 스마트카드의 응용분야 중에서 공중전화 카드용, 교통 카드와 독일, 스페인, 싱가폴 등 세계 10여 개국에서 사용 중인 전자지갑용 카드가 성공한 분야이다. 유럽은 현재 단일 통화인 EURO 통화에 맞게끔 소프트웨어를 수정하고 스펙도 바뀌고 있다. 우리나라의 경우 버스카드로 일부 도입되어 사용되고 있으며 국내의 IC카드 핵심기술부문은 선진국에 비해 뒤떨어져있다. 2002년 1월에 국내 공인 인증기관간의 스마트 카드의 상호연동성을 확보하고 PKI 관련 정보를 사용하는 모든 스마트카드간의 호환성을 제공하기위해 "PKI 관련 스마트 카드 기술규격"을 개발하였다.

보안 O · S에 대한 연구는 미국을 중심으로 이루어지고 있으며, 최근 리눅스 시스템의 보급에 따라 우리나라를 포함한 세계 각국에서 리눅스 시스템 커널에 자체적으로 보안 기능을 통합하는 작업들을 수행하고 있다. 특히, 미국을 비롯한 유럽 각국에서는 운영체제 자체에 대한 평가 기준을 마련하여 일정한 평가 등급 이상의 시스템을 요구하고 있다. 이미 TCSEC에 의해 60여개 제품, ITSEC에 의해 30여개 제품이 평가를 받았다. 미국의 경우 국가정보기반구조 구축과 국방용으로 정부기관과 군사기관들이 사용하기 위해 정부 차원에서 기술개발을 진행중이며, NSA(National Security Agency) 주도하에 1995년부터 보안 O · S를 개발하고 있으며 이미 마련된 TCSEC에 따라 B3 등급 이상을 공공기관에서 사용하도록 하고 있으며, 기업 정보시스템은 B2이하의 등급을 개발하여 사용토록 하고 있다. 우리나라의 경우 선진국과 3년에서 6년 정도 격차를 보이며, 연구 초기단계에 있다. 리눅스 시스템 보급이 활성화된 1999년 말경부터 활발해졌으나, 여전히 몇 개 업체와 학계에서만 관심을 가지고 진행하고 있다.

보안 데이터베이스의 경우 DBMS 자체에 대한 보안에 대해서는 ORACLE사의 보안 기능이 뛰어나고, O · S와의 연동을 통해 보안을 제공하는 MS SQL-Server도 접근제어 부분에서 우수함을 나타내고 있다. 그러나 위의 두 시스템은 DBMS 자체에 대한 보안기능 제공인 반면 Sybase Enterprise Portal Security Framework는 시스템간의 연동면에 비중을 둔 보안 시스템으로 앞으로 나아가야 할 DBMS 보안 방안으로 여겨지고 있다.

2.2 네트워크 보호기술

VPN은 최근 업계에서 IPsec 적용을 위한 독립적인 H/W를 구현한 VPN 전용 장비를 제공하고 있으며, 침입차단시스템, 침입탐지시스템, 라우터 등과 통합된 형태의 제품을 내놓고 있기도 하다. 또한 기가비트 이더넷 환경에서 적용 가능한 제품을 선보이고 IPsec처리를 위한 전용 칩을 생산하여 판매하고 있다. 우리나라는 몇 개 선발 업계에서 IPsec을 적용한 VPN 장비를 개발하여 출시하고 있으며, 세계적인 수준의 장비로 발전하고 있다. 특히, IPsec에 적용하는 암호 알고리즘 등을 국내 표준 알고리즘으로 대체하여 제공함으로서 독자적인 보안 솔루션을 제공하고 있다. 국내 업체들은 침입차단시스템과과 VPN을 결합시킨 제품, VPN과 라우터기능을 결합한 시스템 그리고 VPN 전용시스템 개발에 주력하고 있다.

침입차단시스템은 미국이 역시 세계최고의 기술을 보유하고 있으며, 기가비트의 속도를 지원하고 Proxy 침입차단시스템의 결점인 속도저하를 보완하기 위해 Adaptive proxy나 Stateful Inspection 등의 기법을 사용하고 있다. 국내 업체들도 기가급 침입차단시스템을 출시하고 있다.

미국 등 선진국은 20여 년 전부터 침입탐지시스템에 대한 연구를 수행하여 광범위한 연구개발 결과를 보유하고 있다. 미국은 DARPA/ITO의 침입탐지 프로젝트, SRI International, UCSB(University of California, Santa Barbara), COAST(Computer Operation, Audit, and Security Technology), UC Davis, 기타 연구기관 들에서 침입탐지시스템을 연구하고 있다. GSA를 중심으로 각 연방기관이 참여하는 침입탐지시스템 네트워크인 FIDnet(Fedal Intrusion Detection Network)을 구성하는 계획을 수립했다. 국내 업체들은 침입탐지시스템의 일부 기술을 확보하고 있으며, 2001년부터 K4 인증제품을 출시하고 있다. 국산제품들은 윈도우즈, 솔라리

스, 리눅스 등 다양한 운영체제 기반으로 개발되어 운용되고 있다. 리눅스에서 개발된 제품은 커널을 이용한 최적화를 통해 기가비트 환경을 지원하는 제품으로 발전하고 있다. 또한 침입차단시스템과 침입탐지시스템을 연동화하는 연동기술이 상용화하고 ESM을 사용하여 침입탐지시스템과 침입차단시스템의 통합적 관리 시스템을 구축하고 있다.

3. 응용체계 보호기술

3.1 해킹 · 바이러스 대응기술

해킹 · 바이러스 대응기술은 그동안의 단품적인 개별 운용, 수동적인 방어 기술에서에서 상호 복합적인 통합화가 이루어지고 있으며, 능동적이고 적극적인 예방기술이 개발되는 추세에 있다. 악성코드를 탐지하는 기술은 기존에는 특정한 문자열을 찾아 악성 코드 여부를 판정하는 것이었으나, 최근에는 악성 코드의 제작 기법이 발전함에 따라 가상 실행형태의 진단 방법으로 발전하고 있다. 또한, 다형성 악성 코드의 출현에 따라 이를 탐지 · 제거하는 기술개발이 이루어지고 있으며, 알려지지 않은 악성 코드를 탐지하기 위한 기술 개발이 국내·외적으로 활발하고 이루어지고 있다. 알려지지 않은 악성 코드를 탐지하기 위한 기술은 이미 알려진 패턴을 분석하고, 알려진 악성 코드의 행위를 분석하여 새로운 악성 코드를 탐지하는 기술과 가상 환경에서 실행하여 악성 코드 여부를 탐지하는 기술이 개발되고 있다.

침입자 역추적 기술은 미국의 DARPA를 중심으로 추진 중인 CITRA(Cooperative Intrusion Traceback & Response Architecture)를 비롯해 라우터 등을 이용하여 침입자를 역추적하는 방안들이 제시되고 있다. Honeynet과 같은 해커유인체계와 접목하여 역추적을 시도하는 연구도 진행되고 있다. 또한 기본 네트워크 인프라에 변경을 가하지 않고 역추적 에이전트를 이용한 추적에 대해서도 연구가 진행되고 있다. 침해 복구 기술 및 취약성 탐지 · 제거 기술은 특히 가용성을 침해하는 해킹 위협에 대한 인식이 확대되면서 활발한 연구가 진행되고 있다. 우리나의 경우 Anti-Virus 백신제품은 국제경쟁력을 확보하고 있다. 안철수 연구소, 하우리 등에서는 바이러스 대응 기술을 확보하고 있으며 온라인 검사등의 서비스를 시행중이다. 국가주도로 사이버 테러 대응기술 개발, 선도 기술개발을 위하여 2000년 7월부터 ETRI, KISA와 산업체를 중심으로 취약성 분석, 침해대응 복구 기술 등의 개발을 국책 사업으로 중점 추진 중에 있다. 사이버 테러 대응 기술은 선진국과 평균 2년에서 4년 정도 격차를 보인다.

3.2 응용 서비스 보호기술

1994년에 미국정부는 전자서명 방식인 DSS(Digital Signature Standard)를 표준으로 채택하여 정부기관이 사용하고 있다.

사용자 인증방법은 X.509를 기반으로 하는 인증방식과 Non-X.509를 기반으로 하는 인증 방식이 있다. X.509의 인증방식은 인증서가 기반이 되며 PEM, PGP, S-HTTP, SSL, S-MIME 등에서 지원되고 있다. SPKI는 Non-X.509 방식으로 개발 중인 인증방법이며 최소한의 필요 정보만을 가진 인증서를 만드는 것을 목표로 하고 있다.현재 우리나라에서는 전자서명알고리즘으로 우리나라에서 개발하여 1996년 1월에 개발되어 이후 지속적인 수정 · 보완작업을 거쳐 1998년 10월에 TTA 표준으로 제정된 KCDSA와 역시 ECC와 KCDSA를 응용하여 우리나라에서 개발한 EC-KCDSA 등이 있다.

현재 우리나라도 역시 전자서명의 상호인정을 위해 노력하고 있다. 우리정부는 양자 또는 다자간 국제회의를 통해 국가간 전자서명 상호인정 추진을 위한 정책적 협의를 지속적으로 추진하고 있으며, PKI 관련 민간단체를 통한 민간차원의 국가간 협력에도 적극적으로 지원하는 한편, 상호인정을 실현하기 위한 기술적인 기반을 조성하기 위해 노력하고 있다. 2001년 6월에는 우리나라, 일본, 싱가폴 3국이 전자서명상호인증추진을 위한 양해각서를 체결하였으며, 이의 후속조치로서 3국간 전자서명상호인증 테스트베드를 구축하는 등 기술적 기반을 조성하기 위한 프로젝트를 추진 중이다.

Ⅳ. 정보보호 기술 발전 전망

사이버공간을 통한 정보침해양상이 다양화 · 지능화되고, 새로운 정보통신서비스가 등장함에 따라 정보보호기술의 발전도 더욱 가속화 될 전망이다. 정보통신망의 고도화함에 따라 정보보호기술의 고속 · 고비도화가 진전되며, 통신기술과의 융합화 현상도 가속화될 전망이다.

IMT-2000, 무선 LAN 등을 이용한 무선인터넷의 보급이 급증하여 유 · 무선 통합 환경이 보편화될 것으로 예측됨에 따라 유 · 무선 통합 환경의 보안

취약점을 해소하는 방향으로 발전할 것이다. 또한 인터넷이 IPv4에서 IPv6망으로 전환되고 궁극적으로는 전체 통신망이 All IP망으로 단일화될 것으로 전망됨에 따라 이에 대한 정보보호 기술연구도 활발히 진행되고 있다.

1. 정보보호 기반기술

1.1 암호기술

최근에는 전 세계적으로 민간주도의 개발로 패러다임이 변화하고 있다. 앞으로도 암호기술은 컴퓨터 성능의 향상이나 예기치 않은 암호 해독기술의 개발 등으로 일거에 무력화 될 가능성이 상존하기 때문에 민간의 적극적인 참여를 유도하여 암호의 강도를 지속적으로 높이기 위한 방안을 마련할 필요가 있다. 암호 알고리즘은 현재 타원곡선 알고리즘과 IMT 2000 정보보호 알고리즘 기술이 개발되고 있으며 2000년대 중반에는 고속·고비도 암호 알고리즘 기술, 초고속 타원곡선 알고리즘 기술, 4G 이동통신 정보보호 알고리즘 기술, 광암호 기술이 개발되고 2000년대 말 이후에는 양자암호와 생체기반 암호가 개발될 것으로 전망된다.

1.2 인증기술

인증기술은 단순한 기능에서 복합적인 기능을 제공하는 접근 통제 시스템으로 발전하고 있으며, IC 카드, 지문, 홍채, 음성 등을 활용한 인식기술 개발이 적극 추진 중이다. 인증기술은 현재의 유무선 PKI 기술, 단일 생체 기반 인증에서 2000년대 중반에는 멀티캐스팅 키 관리 기술, PMI 기술, AAA 인증기술, 다중생체 인증기술로 발전되고 2000년대 후반에는 인공지능 인증으로 발전할 것으로 전망된다.

1.3 정보보호 평가기술

현재는 시스템 기반 평가 기술, 인터넷 보안 표준화, 사이트 취약성·위험분석 적용기술, 단독·단말 제품 EAL4 이하 비정형 평가기술이 개발되고 있으며, 2000년대 중반에는 네트워크 기반 평가, 4G 이동통신 정보보호 알고리즘 표준화 기술, 네트워크·상호연동·실시간·멀티미디어 기반 보안기술 표준화, 생명주기(kife cycle)기반 사이트 평가기술, 평가 및 인증 개발 도구 표준화가 이루어지고 2000년대 후반에는 CEM 기반 평가, 차세대 네트워크 기술 표준화, 소스 코드 레벨의 정형화 기술, 대응기술을 포함한 사이트 평가기술이 개발될 것으로 전망된다.

2. 시스템·네트워크 보호기술

2.1 시스템 보호 기술

IC 카드 기술은 보안 O·S 기반 IC 카드 기술과 키 관리 메카니즘을 내장하는 IC 카드가 주류를 이루면서 발전할 것으로 예상된다. 현재는 개방형 IC 카드가 개발되고 있으며 2000년대 중반에는 생체 데이터를 내장하는 기술이 적용된 생체정보기반 IC 카드로 발전하고 2000년대 후반에는 고성능 IC 카드가 개발될 것으로 전망된다.

보안 O·S는 수요에 따라 고등급 및 저등급의 차별화된 개발경향을 보이고 있으며, 국가의 정보기반구조를 보호하기위한 강력한 도구로써 활용될 전망이다.

보안데이터베이스는 다단계접근제어기술과 자율적인 접근 제어기술이 소개되고 있으나, 앞으로는 서로 통합된 형태의 기술로 단계별 자율 접근제어기술이 선보일 것으로 전망되며, 보안 O·S와 더불어 국가기반정보의 데이터를 저장하는 데이터베이스의 안정성을 확보한다는 측변에서 매우 중요한 기술이다. 현재는 보안 운영체제 기술이 개발되고 있으며 2000대 중반에는 차세대 보안 운영체제, 보안 DBMS 기술로 발전하고 2000년대 후반에는 센서 운영체제가 개발될 전망이다.

2.2 네트워크 보호기술

침입탐지시스템과 침입차단시스템은 바이러스 백신등과 연동하는 분야로 발전할 것이다. 침입탐지시스템은 현재 단순한 시스템의 오남용 등의 경우를 탐지하는 형태를 가지고 있으나, 사용자의 정상행위를 모델링하는 신경망 등의 기술이 도입되고 있으며 다른 시스템과의 연동도 모색되고 있다. 정보보호 관리시스템은 인터넷에서 망관리를 위해 QoS와 보안성을 제공하는 서비스를 통합하는 형태로 발전하고 있으며, 이들 서비스에는 침입차단시스템, Network Address Translation, VPN, User Authentication, Bandwidth Control 등이 포함될 것으로 전망된다. 또한 정보보호기술의 패러다임도 침입차단시스템, 침입탐지시스템 등의 단일 기술을 이용

한 현재의 수동적 보안기술에서 새로운 침입에 대한 실시간 탐지와 차단이 가능하고 복구 역추적, 대응 공격 등을 망차원에서 수행할 수 있는 능동형 네트워크 정보보호기술로 변화할 전망이다.

현재는 IPv4상에서 VPN 서버 기술, 통합관리 기술이 개발되고 있으며 2000년대 중반에는 능동 보안관리 기술, IPv6상의 VPN 서버기술, 보안 networking 기술, 차세대 무선네트워크 보안기술이 개발될 것이며 2000년대 후반에는 인증기술, 보안 운영체제, 침입탐지, 역추적 기술 등이 통합된 액티브 센서네트워크 기술로 발전할 것으로 예측된다.

3. 응용체계 보호기술

3.1 해킹 · 바이러스 대응기술

현재는 침입탐지기술, 침입차단기술이 단일 시스템기반으로 개발되고 있으나 바이러스 백신 등과 연동하는 분야로 발전하여 2000년대 중반에는 악성코드 탐지기술, 자동 면역 백신기술이 적용된 네트워크 침입탐지/차단 시스템과 역추적 및 능동대응 기술이 개발될 것이다. 2000년대 후반에는 인공지능 기반 해킹기술과 바이러스 대응 기술이 개발 될 것이다.

3.2 응용 서비스 보호기술

전자서명은 기술적인 측면에서 장소에 구애받지 않고 전자서명을 사용할 수 있도록 이동성 확보와 신기술을 이용한 전자서명으로 발전할 것으로 예측된다. 이동성을 확보하기 위해 스마트 카드나 USB 토큰 등 하드웨어 장치를 활용하는 경우 보급비용 문제 때문에 용이하지 않다. 따라서 이용자에게 패스워드만을 이용하여 중앙의 신뢰서버에 위탁 · 보관된 전자서명용/암호 키 분배용 키를 안전하게 이용할 수 있도록 하는 키로밍 서비스 등 새로운 전자서명 수요가 늘어나고 있다. 신기술을 이용한 전자서명인식 기술의 급속한 발전에 따라 생체인증, 수기서명 등 신기술에 바탕을 둔 다양한 전자서명기술이 출현할 것으로 예상된다. 공개키 암호방식을 이용한 디지털 서명을 대체할 수 있는 기술에 대한 연구가 미국을 중심으로 개발 중이다. 미국의 Signature Dynamics는 전자펜 혹은 터치 스크린을 이용한 수기서명에 기초한 생체인식 기술을 개발 중이다. 기타 응용서비스 보호분야로 현재는 인터넷 뱅킹 보안 서비스기술이 개발되고 있으며 2000년대 중반에는 전자정부 보안 서비스 기술, 생체 응용 IC 카드 기술, IMT-2000 정보보호서비스 기술이 개발되고 2000년도 후반에는 원격진료 보안서비스 기술, 차세대 네트워크 응용서비스 보안기술이 개발될 것이다.

V. 결 론

사이버공간에서의 정보침해는 더욱 다양해지고 지능화되고 있으며 정보통신망이 발달함에 따라 통신망이 고도화되고 새로운 정보통신서비스가 등장할 것이며 유무선 통합환경이 보편화할 것이다. 또한 인터넷이 IPv4에서 IPv6망으로 전환되고 궁극적으로는 전체 통신망이 All IP망으로 단일화될 것으로 전망된다. 따라서 이러한 정보통신환경의 변화에 따라 정보보호기술의 발전도 더욱 가속화 될 전망이다. 정보보호기술은 고속 · 고비도화가 진전되며, 통신기술과의 융합화 현상도 가속화될 전망이다. 또한 유 · 무선 통합 환경에서의 보안 취약점을 해소하는 방향으로 발전할 것이며 All IP망에 대한 정보보호 기술연구도 활발히 진행될 것이다.

참 고 문 헌

[1] 선진국의 정보보호기술 개발사업 동향분석 및 국내대응방안연구, 한국전자통신연구원I, 1999.

[2] 정보통신 기술 · 산업 전망, 한국전자통신연구원 2002.

[3] 정보보호시스템, 한국전자통신연구원, 2000.

[4] 중장기 정보보호 기본계획(안) 정보통신부 2002.

[5] Biometrics 기술&시장 동향, 한국전자통신연구원 2000

[6] 정보보호백서, 국가정보원, 2002

[7] 이종후, 김지선 류재철, 인증실무준칙 분석, 한국통신정보보호학회 학회지, 제8권 제3호, 1998. 9.

[8] "Minimum Interperability Specification for PKI Componnents", NIST MISPC, 1997.

[9] http://www.ietf.org

[10] http://www.kisa.or.kr/

[11] http://www.nis.go.kr/

[12] http://ins.go.kr/

[13] http://www.rootca.or.kr/
[14] http://www.ietf.org/
[15] http://www.gpka.gov.au/
[16] http://csrc.nist.gov
[17] http://niap.nist.gov
[18] http://www.nsa.gov/isso/

〈著 者 紹 介〉

김 배 현 (Bae-hyun Kim)
학생회원

1995년 2월 : 호원대학교 전자계산학과 (이학사)
1997년 2월 : 수원대학교 전자계산학과 (이학석사)
2001년 3월~현재 : 경희대학교 컴퓨터공학과 박사과정
관심분야 : 컴퓨터 네트워크, 정보통신 정보보호

나 원 식 (Won-shik Na)
학생회원

2002년 3월~현재 : 경희대학교 컴퓨터공학과 박사과정
관심분야 : 네트워크 보안, 모바일 네트워크

유 인 태 (In-Tae Ryoo)
정회원

연세대학교 (공학사, 공학석사, 공학박사)
1997년 : The University of Tokyo
1999년 3월~현재 : 경희대학교 전자정보학부 조교수
1997년 10월~1999년 3월 : 삼성전자 선임연구원
관심분야 : 차세대 네트워크/인터넷, 무선 및 이동통신, 멀티미디어 트래픽 관리, 네트워크 QoS, 정보보호

권 문 택 (Moon-Taek Kwon)
정회원

육군사관학교 졸업
University of Iowa/Iowa city (공학 석사)
University of Wisconsin/Madison (경영정보학 박사)
현재 : 경희대학교 산업정보대학원 정교수
관심분야 : 정보전, C4I, DSS 등