情 報 保 護 學 會 誌
第 12 券 第 3 號, 2002. 6

암호제품 평가체계 분석

이 성 재*, 김 영 백*, 홍 시 환*, 김 승 주*

요 약

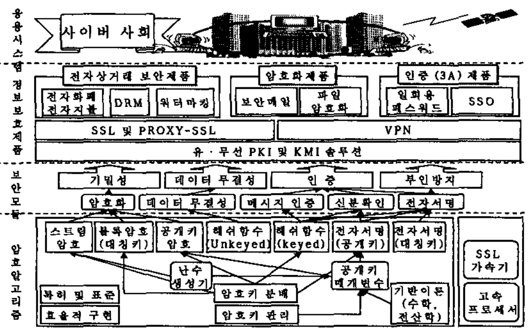
인터넷의 발달로 사회의 기반구조가 종이사회에서 사이버 사회로 전환됨에 따라 정보보호제품이 중요한 역할을 담당하게 되었다. 이러한 정보보호제품의 안전한 선택 및 사용을 위한 기본적인 선택기준은 신뢰 기관의 안전성 평가 결과일 것이다. 이러한 안전성 평가는 현재 세계적으로 공통 평가를 위한 체계를 준비중에 있으며, 가장 대표적인 것이 CC(Common Criteria)기반의 정보보호제품 평가이다. 그러나 CC기반의 평가기준에서는 정보보호분야의 핵심기술인 암호알고리즘에 대한 평가는 수행하지 않고 각 국이 독자적으로 하도록 규정하고 있으며, 이를 구현한 암호모듈에 대한 평가 또한 독자적으로 하도록 하고 있다. 암호모듈에 대한 안전성 평가로 가장 널리 참조되는 것은 미국의 NIST(National Institute of Standards and Technology)가 수행하는 CMVP(Cryptographic Module Validation Program)이며, 세계적으로 인정받고 있다. 본 고에서는 현재까지 수행되고 있는 정보보호제품에 탑재된 암호모듈의 평가체계에 대해 비교 분석하여 정리하고자 한다.

1. 서 론

인터넷의 발달은 과거 대면사회에서 사이버 사회로의 전환을 가져왔다. 우리는 현재 이러한 전환의 과도기에 있으며, 대면사회에서 행하던 일을 사이버 사회에도 똑같이 하기를 원한다. 전자상거래가 바로 이러한 것이며, 가상공간의 비대면 특성으로 인해 사이버 사회의 구현은 많은 문제점과 기술적 어려움을 가지고 있다. 이러한 문제를 해결하기 위한 가장 핵심적인 기술이 바로 암호기술이다. 이제 암호기술은 정보보호제품의 기본기능이 되었으며, 국가에서 지정한 신뢰기관에서 안전성에 대한 평가를 실시하고 있다. 이러한 암호기술의 안전성 평가는 가장 기본이 되는 안전성 요구이므로 국내외적으로 암호알고리즘의 안전성 분석 및 암호모듈의 안전성 평가에 대해 많은 관심을 보이고 있으며, 평가체계 및 제도를 마련 중에 있다. 본 논문은 정보보호제품에 탑재된 암호모듈의 안전성 평가체계에 대해 분석하고자 한다.

1.1 암호알고리즘과 기능

암호기술은 크게 암호알고리즘과 암호프로토콜로 나눌 수 있다. Alfred J. Menezes, Paul C.van Oorschot 및 Scott A. Vanstone 등의 저서 "Handbook of Applied Cryptography"[2]에 따르면, 암호기술은 다음 5개의 기본 서비스를 제공하기 위한 기술로서 그림 1과 같이 나타내어진다.



〔그림 1〕 사이버 사회와 암호기술

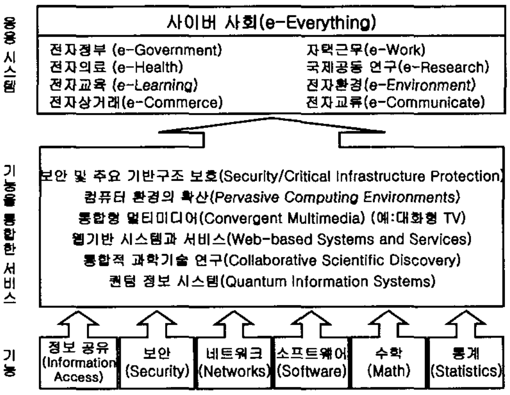
○ **기밀성**: 문서를 해독 불가능한 형태로 변형하거나 또는 암호화된 통신문을 해독 가능한 형태로 복원할 수 있도록 해주는 것. 암호의 가장 기본적인 목표라고 할 수 있으며, 이러한 기밀성은 암호화에 사용된 키 값을 알고있는 사용자만이

---

* 한국정보보호진흥원(KISA) ({sjlee,ybkim,shhong,skim}@kisa.or.kr)

원래의 데이터를 해독해낼 수 있도록 하여야 함.

- o **데이터 무결성**: 전송 도중에 문서의 내용이 부당하게(불법적으로) 변경되지 않고 정확하고 완전하게 수신되었음을 보증하는 것.
- o **메시지 인증**: 전송된 문서의 출처 및 문서내용의 무결성을 보증하는 것.
- o **사용자 인증 (신분확인)**: 원격지에서 접속한 사용자가 본인임을 신원 확인하는 것.
- o **부인방지**: 문서의 송·수신 후 송·수신자가 자신이 송신하거나 수신한 문서의 송·수신 사실을 부인하는 것을 방지할 수 있도록 하는 것.



〔그림 2〕 사이버사회와 기반기술

다음은 암호 알고리즘에 대한 간단한 설명이다.

- o **블록암호(대칭키)**: 기밀성 서비스를 제공하기 위한 대표적인 원천기술로 블록 암호 시스템은 고정된 크기의 입력 블록을 고정된 크기의 출력 블록으로 변형하는 암호 알고리즘에 의해 암호화 및 복호화 과정을 수행하는 암호 시스템이다. 대표적인 알고리즘으로는 DES, 3-DES, AES, BLOWFISH, RC2, RC5, RC6, Safer, MARS, TWOFISH(이상 미국), CAST-128, CAST-256(이상 캐나다), SERPENT(유럽), IDEA(스위스), SEED(한국) 등이 있다.
- o **스트림 암호(대칭키)**: 블록암호와 달리 평문을 블록으로 나누지 않고 평문과 비밀키로부터 유도된 키 스트림(Key stream)을 서로 XOR (exclusive or)하여 암호문을 생성하는 알고리즘이다. 대표적인 알고리즘으로는 RC4, SEAL(이상 미국), A5, LEVIATHAN, ISSAC, PANAMA, Sober, WAKE(이상 유럽) 등이 있다.
- o **해쉬함수(Unkeyed)**: 데이터의 무결성 서비스를 제공하기 위한 원천기술로 해쉬함수는 임의의 길이의 입력 메시지를 고정된 길이의 출력값으로 압축시키는 함수이다. MD5, SHA1(이상 미국), RIPEMD-160, TIGER(이상 유럽), HAS-160 (한국) 등이 있다.
- o **해쉬함수(Keyed)**: 메시지 인증코드인 MAC (Message Authentication Code)으로 널리 알려진 이 기술은 메시지의 무결성 기능 뿐 아니라 인증기능을 제공하는 함수이다. 키가 없는 해쉬함수는 메시지를 알고있는 사람은 누구든지 해쉬값을 계산할 수 있는 반면 MAC은 키가 있는 사람만이 데이터에 대한 해쉬값을 계산할 수 있으므로 메시지에 대한 인증기능을 갖고 있다. 기반 함수에 따라 다음과 같이 분류할 수 있다.
  - 일반적인 해쉬 함수 기반 : HMAC, KMAC
  - 곱셈을 이용하는 Universal 해쉬 함수 기반: UMAC
  - 블록암호 기반: CBC-MAC, XCBC, RIPEMAC
- o **공개키 암호**: 공개키 암호시스템은 비대칭키 암호 시스템(Asymmetric Cryptosystem)이라고도 불리며, 수학적 함수를 기반으로 하여 비밀키 암호 시스템과 달리 키 쌍이 존재하여 하나의 키는 누구든지 사용할 수 있도록 공개하며 다른 하나는 자신만이 비밀스럽게 보관하는 방식을 일컫는다. 이때 공개하는 키를 공개키(Public key)라고 하며 비밀스럽게 보관하는 키를 개인키(Private key)라고 한다. 대칭키(스트림, 블록)암호에서는 어떻게 송신자와 수신자에게 대칭키(비밀키)를 분배하는지가 커다란 문제였다. 이러한 문제를 한 쌍의 키를 사용함으로써 해결한 것이 공개키 암호이다. 공개키 암호는 기반 논리에 따라 다음과 같이 분류할 수 있다.
  - 소인수분해: RSA, Rabin encryption(이상 미국)
  - 유한체의 이산대수: Elgamal, Diffie- Hellman, XTR
  - 타원곡선의 이산대수: Elliptic Curve Cryptosystem(ECC)
  - 부호이론(Coding theory): McEliece
  - 배낭문제 : Knapsack 암호
  - 기타: NTRU(격자이론), Braid-group Cryptosystem(매듭이론, 한국)
- o **전자서명 (공개키)**: 사용자 인증과 부인방지 서

비스를 제공할 수 있는 원천기술로 현재 사용되고 있는 도장이나 사인을 디지털 정보로 구현한 것이다. RSA, DSA, ECDSA(이상 미국), ESIGN(일본), KCDSA, EC-KCDSA(이상 한국) 등이 있다.

- **전자서명 (대칭키)**: 사용자 인증 및 메시지 인증을 수행하는데 있어 대칭키 암호 기법을 이용한 디지털 서명 방식은 검증자가 이용자의 비밀키를 관리할 필요가 있는 문제점이 있으나, 특정 시스템 내에 국한하여 사용자 인증 및 메시지 인증에 적합한 방식이다.

1.2 정보보호제품

국내외 정보보호제품은 그림 2와 같이 전자 상거래 보안제품, 암호화 제품, 인증 제품, SSL(Secure Socket Layer), 가상사설망(VPN), PKI(Public Key Infrastructure) 및 KMI(Key Management Infrasturcture) 솔루션, 암호칩과 암호라이브러리로 크게 분류할 수 있다.

위에서 크게 분류한 암호 제품들에 대하여 간단하게 살펴보면 다음과 같다.

- **암호화제품**: 자료를 암호화하여 비밀키를 가진 사용자이외에는 그 내용을 볼 수 없도록 하는 전자 데이터의 기밀성 서비스를 제공하기 위한 기술과 그에 필요한 제품을 포함한다(보안전자메일, 데이터/파일 암호화, 암호화장치, 암호라이브러리/암호툴킷 등).
- **가상사설망(VPN)**: 인터넷과 같은 공공망에서 서로 다른 두 지점간에 안전한 망을 설정하여 전용회선을 사용하는 것처럼 안전하게 정보를 주고 받을 수 있는 사설망 기능을 제공한다.
- **인증 제품**: 페스워드 등을 이용해 사이버 공간에서 자신이 합법적이고 정당한 실체임을 나타내는 사용자 신원 확인 기능을 제공하여 시스템의 부당한 사용이나 정보의 부당한 전송 등을 방어할 수 있으며, SSO(Single-Sign-On), 일회용 패스워드 등이 포함된다.
- **PKI 관련 제품**: 공개키 암호 응용에 이용되는 공개키 값의 안전하고 효율적인 유통을 위해 인증서의 발행, 획득, 조회 검증 등을 수행하는 인증서 관리 기반구조를 PKI라고 하며, PKI 관련 제품에는 PKI 기반 구축 솔루션, PKI 기반 인증 서비스, PKI 기반 응용 제품 등이 포함된다.
- **전자상거래**: 인터넷상에서 물품 및 서비스 거래시 전통적 구매대금 결제방식의 전자적 형태로서 거래정보의 기밀성 제공 및 지적재산권 보호 등 전자상거래의 안전·신뢰성 확보기술. 전자 결제장치, 디지털 콘텐츠 보호기술 등이 포함된다.

II. 암호기술 표준 및 평가

2.1 암호기술 표준

오늘날 산업에서 암호기술의 중요성을 인식하기 위해, 현재 암호기술이 갖는 폭넓은 역할뿐만 아니라 표준의 발달 이전의 조건을 재조명하는 것이 필요하다. 정보가 천공 카드를 통하여 중앙의 대형 컴퓨터들에 수동으로 입력되던 때의 유일한 보안문제는 개개의 대형 컴퓨터로의 물리적인 접근이나, 중앙 집결된 컴퓨터로의 접근 권한이었다. 보안은 물리적 수단을 통하여 설비/컴퓨터들에 접근하는 것을 제한함으로써 생성되었다(잠겨진 문 뒤에 장비를 안전하게 하는 것). 안전을 보장하는 더 세련된 수단은 코드화된 정보에 대한 접근을 허락하기 위한 패스카드의 배급으로 이루어졌다. 전자 조합 키인 패스카드는 안전성을 높일 수 있다.

1970년대 이후 개인용 컴퓨터는 정보 시스템에 있어서 더 큰 중요성을 맡게 되었다. 독립형 계산장치의 등장은 암호화 상품과 서비스의 많은 수요를 만들었다. 이렇게 크고 새로운 컴퓨터들 집합체는 점차적으로 네트워크화 되고, 상호연결 되었다. LAN (Local Area Network), WAN(Wide Area Network)과 게시판 서비스는 평범하게 되었다. 1990년의 보편적인 URL(Uniform Resource Locator)의 소개와 더불어 월드 와이드 웹(www; World Wide Wep)은 컴퓨터들 연결성의 혁명을 야기 시켰다. 이런 환경은 인터넷의 사용에 많은 변화를 주었으며, 인터넷의 개방성으로 인해 암호기술의 필요성은 증가하였다.

암호기술의 표준화는 IT(Information Technology) 산업의 발전에 직접적인 영향을 미친다. 미국의 정부기관인 NIST는 1977년 DES(Data Encryption Standard)를 미연방 정보처리 표준인 FIPS 46(Federal Information Processing Standards Publications)으로 제정하였다.[12] 그 이후로 DES는 컴퓨터 산업과 금융 서비스와 관련된 여러 분야에서

의 안전성을 위한 기반 기술로 자리를 잡았다. 이를 통하여 미국의 소프트웨어/하드웨어 제조회사들은 표준 알고리즘인 DES를 상업용으로 구현하기 시작하였으며, NIST는 이러한 표준 알고리즘을 탑재한 제품이 시장에서 원할한 수요와 폭넓은 시장확보를 하기 위해서 시장의 안정화 및 암호 제품 수요증가를 위한 여러 가지의 노력을 해왔다. 그 결과, DES의 표준화는 정보보호제품을 생산하는 산업 영역의 빠른 성장을 유도하였으며, 특히 금융거래에서 폭넓게 이용되었을 뿐만 아니라 컴퓨터 네트워크에서 안전한 연결 및 전자상거래의 발전에 큰 역할을 하였다[1].

〔표 3〕 국가별 표준화 현황

분야	한국	미국	일본	유럽	ISO
블록	○	○	○	○	○
스트림	×	×	○	○	○
공개키	×	○	○	○	○
전자서명	○	○	○	○	×
고정길이 해쉬	○	○	○	○	×
가변길이해쉬	×	○	○	○	×
MAC	×	○	○	○	○
사용자 인증	×	○	○	○	○
의사난수 생성기	×	○	○	○	○

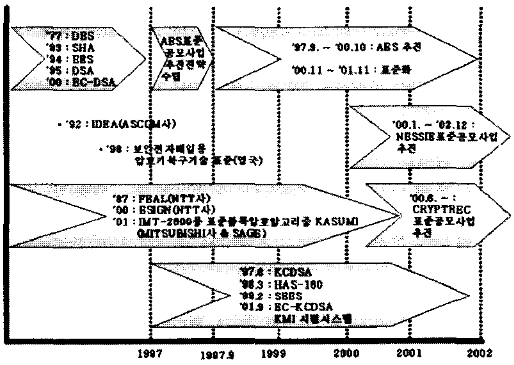
암호기술의 표준화로 인하여 정보보호업체들은 표준화된 암호기술을 채택하여 안전하고 신뢰성 있는 제품을 생산할 수 있게 되었다. 그러나 이러한 암호기술의 이해 부족으로 인해 실제로 제품에 탑재하는데 어려움이 있어 암호기술의 운영기술에 대한 가이드라인이 필요하였다. 이는 보다 신뢰할 수 있는 암호기술의 사용을 확보하기 위한 노력이다.

이러한 암호기술의 표준화는 IT산업의 발전뿐만 아니라 사용자의 프라이버시와 신뢰성을 확보에 직접적인 영향을 주었다. 그러나 표준암호기술을 탑재하였다 하더라도 잘못된 구현이나 표준과 일치하지 않을 경우, 또는 민감한 정보(암복호화 키)에 대한 무분별한 생성/사용/파기로 인해 암호기술 자체의 기능을 상실할 수도 있다. 따라서 구현된 암호기술에 대한 안전성 평가는 이러한 문제에 대해 검토하고 인증함으로서, 사용자의 제품선택에 대한 기준을 제시하고 업체의 제품개발의 가이드 라인을 제시할 수 있었다.

또한, 암호기술의 경우 과거에는 정부가 주도적으로 표준암호기술을 개발하였으나, 이런 경우 정부가 원할 때 암호기술을 우회할 수 있는 Backdoor 등에 대한 논란이 많이 제기됨에 따라 현재는 전 세계적으로 공모를 통한 민간주도의 표준암호기술을 개발하고 있는 추세이다[23,24].

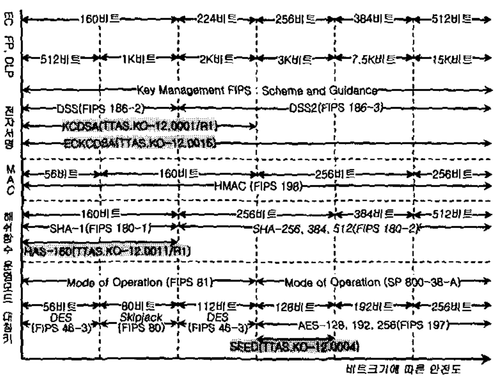
미국 NIST는 DES를 대체할 AES를 공모형식을 통하여 선정하였다.[22] 공모된 21개의 후보 알고리즘 중에서 5개를 최종후보 알고리즘으로 선정한 후 이중 벨기에에서 제안한 Rijndael을 2000년 10월 AES(Advanced Encryption Standard)로 선정하였으며, 2001년 12월 FIPS 197로 표준화되어 2002년 3월부터 CMVP(Cryptographic Module Validation Programe) 평가를 진행하고 있다.

이와 유사하게 일본에서도 암호기술평가위원회(CRYPTREC)을 통하여 전자정부에 사용할 암호 알고리즘을 7개 분야(블록암호, 스트림 암호, 공개키 암호, 전자서명, 해쉬함수, MAC, 사용자인증)에 걸쳐 평가중이며, 유럽에서도 암호평가 프로젝트(NESSIE)가 진행중이다.



〔그림 3〕 국내외 암호기술 개발 및 표준화 현황

또한 미국의 NIST는 각 암호기술의 키 길이에 따른 안전도 비교를 통하여 사용자가 자신이 원하는 안전한 암호알고리즘을 사용할 수 있도록 권고하고 있다. 그림 4에서 128비트 대칭키 암호(AES-128)를 사용할 경우 256비트 해쉬함수(SHA-256), 256비트 MAC, 3K비트 전자서명(DSS2), 256비트 ECDSA 타원곡선기반 전자서명(DSS2) 알고리즘을 사용해야 안전도가 같다. 즉 사용자가 원하는 안전도보다 높은 안전도의 알고리즘을 사용하여야 한다.



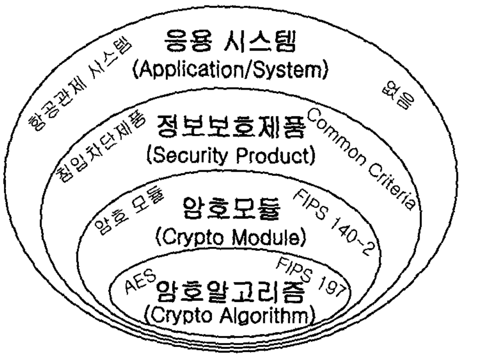
(그림 4) 키길이에 따른 안전도 비교

현재 국내의 경우 128비트 블록암호알고리즘 SEED, 전자서명알고리즘 KCDSA, EC-KCDSA, 160비트 고정길이 해쉬함수 HAS-160 등이 표준으로 사용되고 있다[17-20].

2.2 암호기술 평가

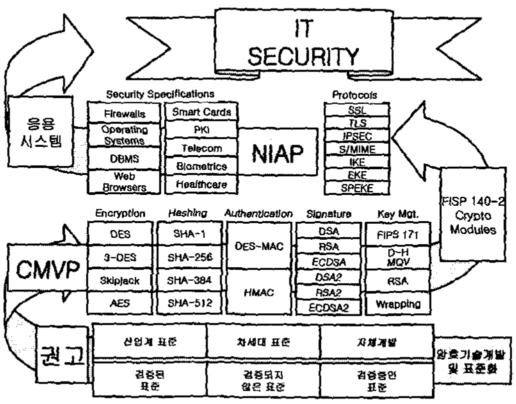
정보보호관련 평가기술은 크게 다음의 4가지로 나눌 수 있다.

- **암호알고리즘 평가**: 정보보호제품에 탑재된 암호알고리즘에 대한 안전성 평가. 알고리즘 자체만을 평가하므로 탑재된 제품이나 시스템과 독립적으로 평가가 가능하며, 일반적으로 알고리즘자체의 이론적 안전성만을 평가한다.
- **암호모듈 평가**: 암호알고리즘을 이용하여 제공되는 암호서비스(기밀성 기능 모듈, 무결성 기능 모듈)에 대한 안전성 평가. 암호알고리즘들로 구성되므로 알고리즘자체의 이론적 안전성과 별도로 암호서비스 기능을 제공하는 암호모듈의 안전성에 대한 평가이다. 암호모듈의 평가는 제품과 독립적으로 수행가능하며, 평가받은 암호모듈은 다른 제품에 제사용이 가능하다.
- **정보보호제품 평가**: 암호모듈을 탑재한 정보보호 제품(예: 침입차단시스템, 침입탐지시스템)에 대한 안전성을 평가. 제품별로 다른 평가기준이 적용되며, 제품을 구성하는 각 모듈의 안전성과 별도로 제공되는 기능 및 성능에 대한 안전성 평가이다.
- **응용시스템 평가**: 각 제품을 상호 연동하여 구성되는 시스템(예:국가기관망의 네트워크 망에 대한 보안성 평가, 항공관제센터의 안전성 평가)에 대한 안전성 평가. 각 시스템마다 독립적이며, 평가받은 제품을 사용하여 구성한다 하더라도 시스템 자체의 안전성을 보장할 수는 없다. 따라서 시스템의 안전성 평가가 가장 어려우며, 같은 시스템이라 하더라도 사용환경이나 구성환경에 따라 평가기준이나 방법이 다르다.



(그림 5) 응용시스템의 구성 및 평가

안전성 평가는 응용시스템의 안전성을 평가하는 것이 가장 바람직하나 이에 대한 평가기준, 방법, 체계를 마련하는 것이 상당히 어렵고, 시스템에 탑재된 기술을 개별적으로 평가해야하는 어려움이 있다. 그러므로 응용시스템의 안전성은 응용시스템의 가장 기본이 되는 암호알고리즘에 대한 안전성 평가가 우선되어야 한다. 결국 암호알고리즘에 대한 이론적 안전성 평가 → 검증된 알고리즘을 구현한 암호모듈의 안전성 평가 → 검증된 암호모듈을 탑재한 정보보호 제품의 안전성 평가 → 각각의 제품으로 구성된 응용시스템의 안전성 평가 순으로 응용시스템의 안전성 평가를 수행하는 것이 바람직하다.



(그림 6) IT 보안과 평가

그림 6은 미국의 NIST가 수행중인 CMVP의 평가 철학을 그림으로 나타낸 것으로 IT 보안을 달성하기 위해 각 알고리즘, 암호모듈, 제품의 평가 체계 및 흐름을 잘 보여주고 있다.

현재 세계적으로 암호알고리즘, 암호모듈, 정보보호제품에 대한 평가는 수행 중에 있으며, 응용시스템의 경우 각각의 시스템에 따라 안전성 기준이 다르므로 독립적으로 안전성을 평가 수행 중에 있다. 암호알고리즘에 대한 안전성은 이미 안전성을 검증받은 표준암호기술의 사용여부를 검증함으로서, 사용자가 판단할 수 있으나, 정보보호제품 및 암호모듈의 경우 앞에서 언급한 바와 같이 표준암호기술의 사용과는 별개로 안전성에 대한 검증이 필요하다.

III. 정보보호제품의 안전성 평가

3.1 정보보호제품 및 암호모듈의 안전성 평가

정보보호제품의 평가 체계는 세계적으로 기준과 적용이 다르다. 따라서 제품의 수출에 관련하여 자국에서 평가를 마친 제품이라 하여도 수입국의 기준에 따른 평가를 다시 받아야 하는 등, 비용과 시간의 손실이 상당하다는 문제점으로 인해 평가기준의 통합 필요성이 자연스럽게 생겨나게 되었다. 따라서 세계 각 국의 평가기준을 통합하기 위해 미국 등 6개국이 1993년 국제공통평가기준인 CC를 개발하는데 합의하고 1999년 국제표준(ISO/IEC 15408)으로 승인된 CC 버전 2.1을 발표하였다. CC는 크게 5가지 부분으로 구성되어 있는데 Part1에서는 소개 및 일반모델을 제시하고, Part2는 보안기능 요구사항, Part3는 보증 요구사항, Part4는 이미 정의된 보호 프로파일, Part5에서 보호 프로파일을 등록하는 절차를 포함하고 있다. CC의 핵심은 Part2와 Part3로써 정보보호제품이 구비해야 하는 기능 및 보증 요구사항을 기술하고 있으며 기술된 요구사항을 참조하여 정보보호제품을 개발할 수 있다. CC평가 등급은 EAL1~EAL7까지 있으며, EAL1부터 EAL4 등급까지는 사용된 특별한 암호기술을 소개하지 않고 일반적으로 기존에 있었던 제품과 시스템을 재정비하기 위한 관점에서 적용될 수 있으며, EAL4 이상의 등급은 응용기술로 사용된 보안기술까지 평가대상 범위를 넓히고 있다. 평가등급의 국제간 상호인증은 국제 협약에 의해 EAL 4 등급 이하만을 인정하기로 하였다. 또한 CC의 경우 암호알고리즘에 대한 평가는 수행하지 않으며, 암호모듈의 경우 관련 표준을 따를 것을 권고하고 있으나, 현재 암호모듈 안전성 평가 관련 표준은 FIPS 140-2만이 표준으로 제정되어 있는 상태여서 미국의 CMVP를 참조모델로 하고 있는 실정이다.

국내 정보보호제품 평가 체계는 정보화 촉진 기본법 15조 및 동법 시행령 15조 및 16조에 의거하여 실시되는 정보보호제품 평가인 '침입차단시스템(Firewall)'과 '침입탐지시스템(IDS: Intruder Tracing System)'에 대하여 한국정보보호진흥원(KISA)에서 실시하고 있다[25]. 각 제품에 대한 평가 등급은 K1~K7까지의 등급체계로 운영되고 있으며, 비밀성 기능을 제공하는 경우 각 평가등급에 'E'를 붙여 등급을 표기하고 있다. 그러나 비밀성 기능은 정보보호제품에 탑재된 암호기능 중 가장 기본이 되는 기능이며, 나머지 부분에 대한 평가는 아직 평가기술 개발 단계에 있는 실정이다. 암호기술자체에 대한 평가기술은 암호알고리즘에 대한 평가만을 수행 중에 있으며, 암호모듈에 대한 평가는 없는 실정이다. 따라서 이에 대한 대책 마련이 시급하다.

3.2 암호모듈의 안전성 평가(CMVP)

암호모듈의 안전성 평가인 CMVP는 1995년 7월 미국 NIST와 캐나다 주정부의 CSE(Communications Security Establishment)가 공동으로 개발한 암호 모듈의 안전성 검증을 위한 프로그램으로 1994년 미국의 NIST가 제정한 'Security Requirement for Cryptographic Modules'(FIPS 140-1)와 2001년 개정된 FIPS 140-2, 암호알고리즘 관련 FIPS 표준문서를 근간으로 만들어 졌다. CMVP는 시험평가 후 Level 1~4를 부여하고, 'List of Validated FIPS 140-1(FIPS 140-2) modules'에 등재되어 평가제품으로서 효력을 발휘할 수 있게 된다. 2002년 1월 현재 약 250여 개의 암호모듈이 검증을 받았다[3,21].

각 등급은 사용자가 제품을 선택할 수 있는 기준을 제시하며, 사용환경에 따라 적절한 제품을 선택하면 된다.

(1) **보안등급 1**: 가장 기본 등급의 안전성을 보장하며, 승인된 암호알고리즘을 사용해야 한다. 물리적 보안은 만족하지 않으며, 일반적으로 H/W 보다는 S/W 기반의 모듈 구현에 대한

안전성 수준이다.

(2) **보안등급 2**: 보안등급 1에 물리적 보안 기능을 추가한 등급이다. 키와 CSPs(Critical Security Parameters)에 물리적 접근시도를 탐지하면 키와 CSPs가 파괴되어야 한다. 이 등급은 CC 평가 등급 EAL2이상의 안전성 수준을 의미한다.

(3) **보안등급 3**: 보안등급 2에 물리적 보안, 신원기반 인증을 보안시킨 등급이다. 이 등급에서의 물리적 보안은 암호키와 CSPs에 대한 침입자의 접근을 막고, 모든 입/출력에 대한 인가되지 않은 공격자의 논리적 공격도 막을 수 있어야 한다. 이 등급은 CC평가 등급 EAL3이상의 안전성 수준을 의미한다.

(4) **보안등급 4**: 보안등급 3에 물리적 보안을 보완시킨 등급이다. 이 등급에서는 인가되지 않은 어떠한 물리적 접근에 대해서도 완벽하게 방어, 봉쇄 기능을 제공해야 한다. 일반적으로 암호모듈이 물리적으로 보호받지 못하는 환경에서 동작하는 암호모듈의 보안에 효과적이다. 이 등급은 CC 평가 등급 EAL4이상의 안전성 수준을 의미한다.

NIST는 산업계에서 많이 활용되고 있는 표준 등의 암호기술에 대하여 안전성을 검증하여 안전한 암호기술 선정하고 정부기관에서 사용할 암호기술로 권고한다. 또한 이러한 권고 암호기술을 사용하여 구현된 암호모듈에 대한 구현 적합성을 검증하여 정부의 암호이용 신뢰기반을 구축한다. 제품의 안전성은 안전한 암호기술을 사용하여도 암호모듈에 대한 암호키 운용, 물리적 보안등의 안전성 검증이 필수적으로 수행되어야 한다.

CMVP에서 요구하는 암호모듈의 안전성 평가는 크게 ① 암호기술의 구현 적합성 평가, ② 암호키 운용 및 관리, ③ 물리적 보안으로 나눌 수 있으며, 각 항목에 대한 안전성 등급을 설정하여 기준을 마련하고 이에 대한 보안성 평가를 수행한다.

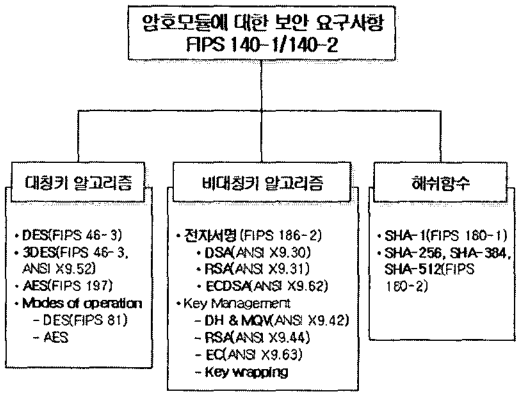
① **구현 적합성 평가**: 구현적합성 평가는 구현된 암호기술이 표준에 따라 제대로 구현되었는지를 평가하며, 이는 각 표준에 따라 평가하는 방법이 다르다.

② **암호키 운용 및 관리 평가**: 암호 키 운용 및 관리에 대한 평가는 암호기술의 안전성에 직접적인 영향을 미치는 암호키의 생성, 확립, 분배, 입/출력, 저장, 파기 등에 대한 방법 및 과정을 평가함으로서 잘못된 암호키 운용 및 관리에 따른 암호키의 유출 가능성을 평가하는 것이다. 이는 암호모듈의 안전성 평가 중 가장 중요한 부분이라고 할 수 있다.

③ **물리적 보안 평가**: 물리적 보안 평가는 암호모듈의 사용환경에 대한 평가로 암호모듈의 운영환경, EMI/EMC(electromagnetic interference/electromagnetic compatibility), 자기테스트 등에 대한 평가를 말한다. 이는 암호모듈의 운용환경에 따라 암호모듈을 직접적 혹은 간접적으로 물리적인 공격을 할 수 있기 때문에 이에 대한 평가를 한다.

다음은 NIST의 표준인 FIPS 140-2의 보안 요구조건 및 FIPS 140-1과 달라진 점이다.

미국의 NIST는 다음 그림에서와 같이 정부기관에서 사용 가능한 암호기술을 선정하여 권고하고 있다[7,8].



〔그림 7〕 보안요구사항에서 권고하는 암호기술

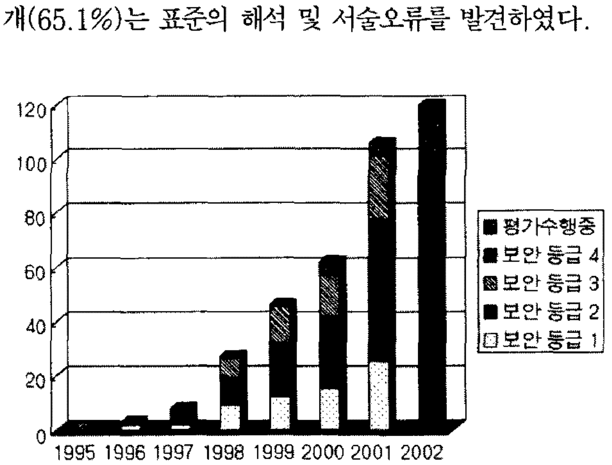
CMVP는 정보보호제품의 가장 핵심 모듈인 암호모듈의 안전성을 평가하는 것으로 보안 모듈의 표준 적합성, 물리적보안, 암호키 운용 및 관리, 운영환경 등에 대한 종합적인 평가를 수행한다. 암호모듈은 사용자의 환경에 따라 예측하지 못하는 취약성이 존재할 수 있으며, 이에 대한 평가는 필수적이라고 할 수 있다.

〔표 4〕 FIPS 140-2의 보안요구조건

보안요구조건	FIPS 140-1과의 비교
암호모듈명세	암호알고리즘 및 보안기능 추가
암호모듈 포트와 인터페이스	물리적으로 분리된 포트와 신뢰할수 있는 경로의 물리적 포트를 가지는 지역적으로 분리된 포트
역할, 서비스들과 인증	인증에 대한 메커니즘의 강도를 강화
유한 상태 모델	Hardware, Firmware, Software 모듈에 대한 모델 상세 설명
물리적인 보안	일관성 및 투명성을 위한 개선
운영 환경	TCSEC(Trusted Computer System Evaluation Criteria) 요구조건을 CC로 대체
암호키 운용	무선키관리 기능 추가 및 키확립에 대한 보안 강도 강화
EMI/EMC	FCC(Federal Communications Commission) 요구조건 반영
자기 테스트	난수생성기의 시험과 오류시 기능을 수행하지 않는 모드의 요구조건 강화
설계의 확실성	설정 관리, 정확성 명시, 문서 가이드 확장
다른 공격들의 완화	새로운 형태의 암호공격에 대한 정보, 권고 및 요구조건 제공

3.3 CMVP 평가 현황

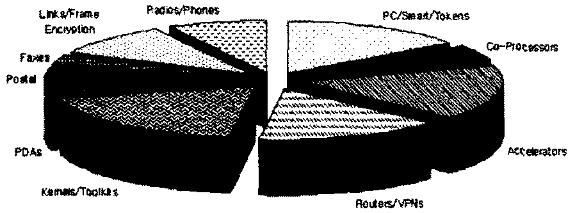
CMVP는 현재 164개의 암호모듈을 시험하여 80개(48.8%)는 보안 취약성을 발견하였으며, 158개(96.3%)는 표준의 해석 및 서술오류를 발견하였다. 또한 시험과정에서 암호모듈에 탑재된 암호알고리즘(DES, 3-DES, DSA, SHA-1)을 332건 검증하였으며 이중 88개(26.5%)는 보안취약성을, 216개(65.1%)는 표준의 해석 및 서술오류를 발견하였다.



〔그림 8〕 연도별 FIPS 140-2 승인 제품 수

또한 시험과정에서 가장 힘든 부분은 물리적 보안, 자체시험, 의사난수생성기, 암호키 운용 및 관리부분이 가장 시험하기 힘든 것을 나타났다. 이는 구현물의 취약성부분이 가장 높은 부분이기도 한 것으로 판단된다.

미국정부는 정부기관의 경우 검증된 암호모듈만을 사용하도록 규정하여 평가에 대한 신뢰도 및 필요성을 강조하고 있다. 암호모듈에 대한 평가는 매년 그 수요가 증가하고 있다.



〔그림 9〕 구현물의 형태에 따른 승인 모듈

Ⅳ. 결 론

앞에서 살펴 본 바와 같이 암호모듈의 안전성 평가는 암호알고리즘의 안전성과 무관하게 잘못된 암호기술의 사용 및 해석에 대한 취약성을 검증하여 안전한 암호이용을 위한 기반을 마련할 수 있다. 또한 제품과 독립적으로 검증이 가능하며, 이를 여러 제품에 탑재할 경우 암호모듈에 대한 안전성 평가를 생략할 수 있어 제품의 안전성 평가에 대한 시간 및 비용을 절감할 수 있다. 그러나 제품의 안전성을 검증 받는다 하더라도 이러한 제품들로 구성되는 시스템의 안전성 평가는 상당히 어려우며, 현재까지 제시된 평가방법도 없다. 따라서 사용자가 안전한 시스템을 구축하기 위한 가이드라인으로 검증 받은 제품을 사용하는 방법이 현재까지는 최선으로 판단된다.

암호모듈의 안전성 평가는 이러한 안전한 시스템을 구축하는 가장 기본이 되는 평가로 사용자가 안전하다고 절대적으로 신뢰하는 암호기술이 구현상의 잘못으로 취약할 수 있음을 인식하고 이에 대한 평가를 수행하여 한다.

국내의 경우 현재 가장 기본이 되는 비밀성 기능 제공 알고리즘인 블록암호알고리즘에 대한 안전성 평가만을 수행중이며 이 또한 구현물의 안전성이 아닌 이론적 안전성 평가에 그치고 있다. 앞에서 살펴본 바와 같이 표준암호알고리즘을 구현한다 하더라도 구현된 제품은 표준의 잘못된 해석, 의사난수 생성기의 잘못된 사용 등으로 인하여 상당히 취약할

수 있음을 보았다. 그러나 국내의 경우는 구현물에 대한 평가는 수해하지 않고 있어 이에 대한 보안이 시급한 실정이다.

따라서 국내에서도 국내 표준암호기술을 탑재한 암호모듈의 안전성 평가를 실시하여 사용자의 신뢰도 및 국내 정보보호제품의 시장경쟁력을 강화할 필요가 있다.

참 고 문 헌

[1] Economic Impacts of NIST's DES Program, 2001. 10, NIST

[2] Alfred J. Menezes, Paul C.van Oorschot, Scott A. Vanston, "Handbook of Applied Cryptography",CRC, 1996

[3] "Cryptographic Module Validation Program Conference", March 2002

[4] Bruce Schneier, "Applied Cryptography", WILEY, 1996

[5] "Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry", ANSI, X9.31, 1998

[6] "Public Key Cryptography for the Financial Services Industry : The Elliptic Curve Digital Signature Algorithm (ECDSA)", ANSI, X9.62, 1998

[7] "Security Requirements for Cryptographic Modules", NIST, FIPS 140-1, 1994

[8] "Security Requirements for Cryptographic Modules", NIST, FIPS 140-2, 2001

[9] "Derived Test Requirements for FIPS PUB 140-1, Security Requirements for Cryptographic Modules", NIST, 2001

[10] "Implementation Guidance for FIPS PUB 140-1 and the Cryptographic Module Validation Program", NIST, 2001

[11] "Digital Signature Standard(DSS)", NIST, FIPS 186-2, 2000

[12] "Data Encryption Standard(DES)", NIST, FIPS 46-3, 1999

[13] "DES Modes of Operation", NIST, FIPS 81, 1980

[14] "Secure Hash Standard", NIST, FIPS 180-1, 1995

[15] "Standard Specifications for Public-Key Cryptography", IEEE, P1363

[16] "Standard Specifications for Public-Key Cryptography: Additional Techniques", IEEE, P1363a

[17] "부가형 전자서명 방식 표준-제2부 : 인증서 기반 전자서명 알고리즘", TTA, TTAS.KO-12.0001/R1, 2000

[18] "해쉬함수표준 - 제2부 : 해쉬함수알고리즘표준(HAS-160)", TTA, TTAS.KO-12.0011/R1, 2000

[19] "128비트 블록암호알고리즘 표준", TTA, TTAS.KO- 12.0004, 1999

[20] "부가형 전자서명 방식 표준 - 제3부 : 타원곡선을 이용한 인증서 기반 전자서명 알고리즘", TTA, TTAS.KO- 12.0015, 2001

[21] "Cryptographic Module Validation (CMV) Program", NIST, http://csrc.nist.gov/cryptval/

[22] "Advanced Encryption Standard", NIST, http://csrc.nist.gov/encryption/aes/

[23] "Cryptographic Toolkit Standards", NIST, http://csrc.nist.gov/encryption/

[24] "NESSIE", https://www.cosic.esat.kuleuven.ac.be/nessie/

[25] "정보보호시스템 평가제도", KISA, http://www.kisa.or.kr/sysevaluation/menu2/sub1/index.html

〈著者紹介〉

이 성 재 (Sungjae Lee)
정회원
1996년 2월 : 고려대학교 수학과 이학사
1999년 2월 : 고려대학교 수학과 이학석사
2002년 현재 : 고려대학교 정보보호대학원 박사과정
1999년 9월~현재 : 한국정보보호진흥원(KISA) 연구원

김 영 백 (Youngbaek Kim)
정회원
1995년 2월 : 순천향대학교 정보통신공학과 졸업
1997년 2월 : 순천향대학교 정보통신공학과 석사
1996년 12월~2000년 3월 : 한전KDN
2000년 4월~현재 : 한국정보보호진흥원

홍 시 환 (Sihwan Hong)
정회원
1999년 2월 : 동서대학교 컴퓨터공학과 공학사
2001년 2월 : 동아대학교 컴퓨터공학과 공학석사
2001년 7월~현재 : 한국정보보호진흥원(KISA) 연구원

김 승 주 (Seungjoo Kim)
본호의 "고속 암호연산 프로세서 개발현황" 저자 소개 참조.