情 報 保 護 學 會 誌
第 12 券 第 5 號, 2002. 10

# 암호화 제품의 개발현황

주 학 수*, 김 승 주*

요 약

암호화 제품은 데이터의 기밀성 서비스를 제공하기 위한 것으로 크게 PC보안, 전자우편보안 제품 등으로 구분할 수 있으며 최근에는 키 복구 기능, 스테가노그라피 기능이 추가된 제품들이 나타나고 있다. 본 고에서는 암호화 제품들의 국내·외 현황을 알아보고 비교·분석함으로써, 국내 암호화 제품들의 새로운 시장을 개척하는데 도움이 되는 자료를 작성하고자 한다.

## Ⅰ. 서 론

통신 및 네트워크 기술의 발전은 전자 상거래 등 새로운 서비스를 창출하게 되었고, 통신 및 네트워크 상에서 이러한 서비스 제공을 위한 안전성 및 신뢰성 확보가 주요 요소로 부각되었다. 암호 기술은 이러한 서비스 제공의 핵심 요소기술로, 크게 데이터 보호를 위한 기밀성 관련기술과 신원 확인, 내용 인증, 부인 방지를 위한 인증 기술 등 두 분야로 양분된다.

이 중에서 기밀성이란 공격자가 전송되고 있는 메시지에 대한 정보를 얻을 수 없다는 것을 보장해주는 것으로 현재까지 제시된 기법은 크게 두 가지로 구분할 수 있다.

- 암호화(Encryption) : 암호키와 수학적인 함수를 이용하여 평문을 알아보기 힘든 암호문의 형태로 변환시키는 것으로, 안전하게 구현된 암호시스템에서는 키를 알지 못하는 사람은 암호화된 데이터를 복호할 수 없는 기능을 말한다. 예를 들어, 암호화 키와 복호화 키가 같은 대칭키 암호로는 DES, SEED, AES 등을 들 수 있으며 암호화 키와 복호화 키가 다른 공개키 암호로는 RSA, ElGamal 등을 들 수 있다.

- 스테가노그라피(Steganography) : 비밀 메시지의 내용 뿐 아니라 존재까지도 공격자가 알 수 없게 비밀 메시지를 커버정보[1]안에 숨기는 기법이다. 예를 들어 숨기고자 하는 메시지를 이미지(커버정보)의 최하위 비트로 바꾸어 줌으로써 원본 이미지와 비밀메시지가 삽입된 이미지를 공격자가 구분할 수 없게 만드는 기법이 있다. (더 많은 스테가노그라피 기법들에 대해서는 [1]을 참고)

기밀성 서비스에 사용되는 암호 기술의 사용은 정보의 누출을 방지하고 개인의 프라이버시를 보호해 주는 등 많은 장점을 가지고 있다. 그러나 암호의 부당한 사용은 국가의 기본질서를 위협할 수 있으며(예 : 미국 세계무역센터 폭파사건의 경우 암호통신으로 지령을 받아 수사기관의 수사권을 방해, 일본 오옴진리교 사건의 경우 범죄관련 내용의 암호화로 법정 증거 확보 곤란, 등이 있음), 또한 사용자의 부주의로 인한 암호키의 분실 및 손상시 정보의 손실을 예방하는 대책 확보 또한 절실히 요구되고 있다.

스테가노그라피 기술의 사용도 기밀성 서비스 이외에 해커와 같은 허가받지 않은 사용자의 접근을 방지해주는 접근권한 기능을 제공해 주는 등 많은 장점을 가지고 있다. 그러나 스테가노그라피 기술의 부당한 사용은 테러리스트들이 미국의 법집행(Law Enforcement)을 피해 통신하는 수단[2]으로 이용하고 있어 이에 대

* 한국정보보호진흥원(KISA) ({hsju,skim}@kisa.or.kr)

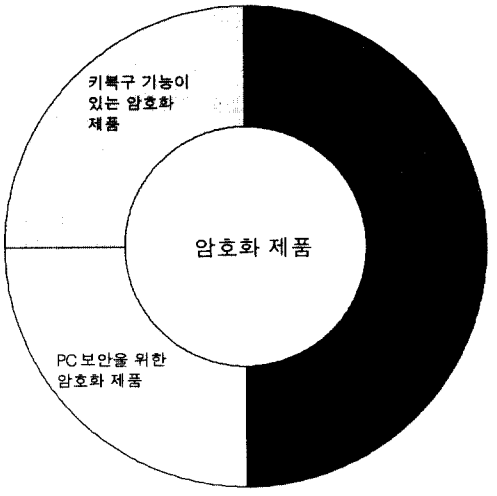
1) 커버정보란 비밀정보가 숨겨질 데이터로 이미지, 테스트, 동영상 등을 말함

2) 2000년 2월 USA Today[6]는 테러리스트들이 법 집행(Law Enforcement)로부터 자신들의 통신사실을 숨기기 위해 스테가노그라피 기술을 사용하고 있다는 것을 보도함. 또한 Wired News[7]는 eBay 혹은 Amazon과 같은 인터넷 경매 싸이트에 올려져 있는 이미지들에 메시지가 숨겨져 있다는 것을 보도함.

한 대책 방안도 절실히 요구되고 있다.

이에 따라 본 고에서는 기밀성 서비스를 제공하는 기술들의 제품현황을 살펴보기 위해서 암호 기술이 탑재된 암호화 제품들과 스테가노그라피 기능이 탑재된 제품들을 비교·분석해본다. 또한 사용자의 부주의로 인한 암호키의 분실 및 손상시 정보의 손실을 예방해 줄 수 있는 기술로 키복구 기술의 제품현황을 살펴보고 스테가노그라피의 기술을 구현한 소프트웨어들을 비교·분석한다.

전체 암호화 제품들을 다음 그림과 같이 분류하여 전개하고자 한다.




본 고의 구성은 다음과 같다. 2장에서는 국외의 PC 보안을 위한 암호화 제품현황, 3장에서는 전자우편 보안을 위한 제품현황을 알아보고 비교·분석한다. 4, 5장에서는 새로운 서비스를 제공하는 암호화 제품들 중 스테가노그라피 기능이 있는 것과 키복구 기능이 있는 제품들의 현황을 살펴보고 비교·분석한다. 그리고 나서 6장에서는 국내의 암호화 제품 현황에 대해 살펴보고 7장에서 결론을 내린다.

## II. PC 보안을 위한 암호화 제품 현황분석

대부분의 PC보안 제품들은 허가되지 않은 사용자의 접근과 사용으로부터 민감한 정보가 들어있는 폴더, 디스크, 하드 드라이브를 보호하기 위해 암호알고리즘을 사용하고 있었다. 초기의 제품들은 DES나 RC2의 낮은 비도(56 비트 이하의 키를 사용)의 암호알고리즘만을 지원하고 있었으나 DES의 짧은 키 길이에 대한 전수조사 공격의 위험이 컴퓨팅 파워의 증가로 커짐에 따라, 현재 PC 보안 제품들은 DES 이외에도 3DES, AES, Blowfish, Twofish와 같은 고비도(112비트 이상의 키를 사용) 암호알고리즘을 지원하고 있었다. 또한 키 길이가 증가된 암호알고리즘의 사용하는 것 이외에도 암호제품의 암호모듈 보안요구사항(FIPS 140-1)의 level 1 승인을 받은 제품들이 다소 증가하고 있는 추세이다. 그 중 대표적인 제품이 Infosec사의 Document Security, Entrust사의 File plugin 제품으로 이 제품들은 PC에서 Swap file 및 Temporary file 들로부터 유출될 수 있는 비밀정보(암호키, 패스워드 등)의[3] 완전 삭제 및 관리를 위해 국방부의 기밀정보를 보호하기 위한 산업보안매뉴얼(DOD 5220.22-M)을 따르고 있다는 것을 알 수 있다.

또한, 대부분의 제품들이 사용자들이 편리하고 안전하게 암호알고리즘을 사용할 수 있게 하기 위한 파일의 자동화된 암/복호 기능, 손쉬운 정책관리, 키 분실 시 복구해 줄 수 있는 키복구 기능이 첨가되고 있었다. 또한 해커로부터의 사용자 프라이버시 보호를 강화하기 위하여 기존의 암호화 기능 외에 스테가노그래피 기능을 추가로 접목한 제품들이 출시되고 있다. 스테가노그래피 기능이 추가된 제품들은 3절에서 다루기로 한다. 표 1,2,3은 각 PC 보안을 하는 제품들의 data sheet를 조사하여 비교·분석한 것이다.

3) · 도스/윈도우의 삭제명령어는 디스크로부터 파일을 삭제하는 것이 아니라 파일의 첫 번째 문자를 특수한 바이트로 변경하여 연결되지 않게 하는 기능만을 제공하는 것임. 따라서 겹쳐쓰기(Overwrite)가 되지 않으면 기존의 문서가 남아있을 수 있음.
· 윈도우는 멀티태스킹 시스템이라서 암호화되지 않은 데이터가 swap file로 저장될 수 있는 위험이 있음.
· 많은 어플리케이션들이 임시 백업 파일들이나 그 복사본을 하드 드라이브에서 생성하거나 저장하여 완벽한 삭제 기능을 보장하지 않고 있음.

〔표 1〕 PC 보안을 위한 암호화 제품들의 특징

| 회사 (나라) | 제품명 | 특징 |
|---|---|---|
| Entrust (미국) | Entrust File Plug in | • 특정폴더의 자동화된 암/복호 기능<br>• 완벽한 파일 삭제 기능<br>• 사용자의 패스워드 분실시 키 복구 기능 지원<br>• FIPS 140-1 level 1의 검증을 통과한 파일보호기법 |
| PC Guardian (미국) | Encryption Plus Hard Disk | • 디스크를 암호화하기 위해 블록암호알고리즘 AES를 사용하고 AES의 암호키는 RSA의 개인키로 보호<br>• 관리자에 의한 사용자 키복구 기능 지원<br>• 부트섹터보호<br>• SSO 기능 지원 |
| | Encryption Plus Folders Enterprise | • removable disk(CD-RW, Floppy disk, Zip, 등)에 있는 폴더 암/복호 기능<br>• 키복구 기능 지원<br>• 2명이상의 사용자가 암호화된 폴더를 공유할 수 있게 함<br>• 관리자에 의한 무제한 보호되는 폴더 설정가능 |
| Cerberus Systems (미국) | Document Security | • 문서 보안관리를 위한 암/복호 소프트웨어<br>• DOD 5220.22-M에 따른 기밀자료의 완벽한 삭제기능 제공<br>• FIPS 140-1의 Level 1을 검증을 받음<br>• 암호, 해쉬 검증 테스트 및 FIPS 140-1에서 요구하는 키생성 검증테스트 자체수행기능 탑재<br>• 암호학적으로 안전한 ANSI 9.17 키 생성기 사용<br>• 자동화된 암/복호 기능 및 암호화된 파일관리의 용이<br>• 파일의 암/복호 과정 중 파워의 정지 혹은 프로그램 충돌이 있는 경우 파일이 훼손되지 않음 |
| Safe House (미국) | Safe House | • 하드 드라이브 암호화 장치<br>• 관리자의 공개키 암호를 사용한 키복구 기술 지원<br>• Windows95,98,ME,NT,XP, 2000과 호환<br>• 2048GB의 볼륨지원<br>• 암호화된 볼륨파일의 안전한 백업<br>• X.9 휴대용 하드웨어 인증디바이스 지원 |
| Norman (유럽) | Norman Privacy 3.0 | • cut and paste한 임의의 평문, 파일 , 전자우편 및 전자우편에 첨부된 화일, 디렉토리, 디스크 등에 암/복호화 기능을 제공<br>• 암호화하기 전의 메시지 압축 기능 제공 |
| Public (미국) | SFS | • 디스크 암호화 장치<br>• FIPS 180(SHA), ANSI X9.30 (SHA),ISO10116: 1991(Modes of operation for an n-bit block cipher) 등의 표준 지원 |
| Public (free) | Cryptext | • 파일 암/복호화 프로그램<br>• 160비트 키를 갖는 암호알고리즘을 사용 |
| Public (free) | Cloak | • 암/복호 프로그램<br>• OTP(one time pad)를 사용 |

※ DOD 5220.22-M : 기밀정보를 보호하기 위한 산업 보안 매뉴얼

※ DOD5200 : 국방부의 신뢰된 컴퓨터 시스템 평가원리

〔표 2〕 PC 보안을 위한 암호화 제품들의 암호알고리즘 지원

| | Entrust File Plug in | PC Guardian | | Document Security |
|---|---|---|---|---|
| | | Encryption Hard Disk | Encryption Folders Enterprise | |
| DES | Y | N | N | Y |
| 3DES | Y | N | N | Y |
| RC2 | Y | N | N | N |
| RC4 | N | N | N | N |
| CAST | Y | N | N | N |
| IDEA | Y | N | N | N |
| Blowfish | N | Y | Y | N |
| Twofish | N | N | N | N |
| AES | N | Y | N | N |
| RSA | Y | Y | Y | N |
| DSA | Y | N | N | N |
| ECC | Y | N | N | N |
| DH | Y | N | N | N |
| SHA | Y | N | N | Y |
| MD5 | Y | N | N | N |
| FIPS 140-1 level 1 | Y | N | N | Y |
| 기타 | - | - | - | DOD 5220.22M DOD 5200.28 -STD ANSIX9.17 의 키생성기법 FIPS 74 FIPS 81 |

〔표 3〕 PC 보안을 위한 암호화 제품들의 암호알고리즘 지원

| | Safe House | Norman Privacy | SFS | CryptoEx | Cloak |
|---|---|---|---|---|---|
| DES | Y | Y | N | N | - |
| 3DES | Y | N | N | N | - |
| RC2 | N | N | N | N | - |
| RC4 | N | N | N | Y | - |
| CAST | N | N | N | N | - |
| IDEA | N | N | N | N | - |
| Blowfish | Y | Y | N | N | - |
| Twofish | Y | N | N | N | - |
| AES | Y | N | N | N | - |
| RSA | N | N | N | N | - |
| DSA | N | N | N | N | - |
| ECC | N | N | N | N | - |
| DH | N | N | N | N | - |
| SHA | N | N | Y | Y | - |
| MD5 | N | N | N | N | - |
| FIPS 140-1 level 1 | N | N | N | N | - |
| 기타 | - | - | MDC | - | - |

※ - : 공개되어 있는 자료만으론 알 수 없음을 의미

## Ⅲ. 전자우편 보안을 위한 제품현황분석

전자우편은 가장 빠른 통신수단이 되어 가고 있다. IDC보고서에 따르면 하루 평균 전자우편의 수가 2005년에는 360억을 넘어설 것으로 전망하고 있다.[2] 전자우편 보안을 위해 많은 회사들이 방화벽을 설치하고 있지만 방화벽은 들어오고 나가는 전자우편 보안을 제공하지 못하고 있다. 본 절에서는 국외의 전자우편 보안도구에 대해 조사해 보고자 한다.

전자우편 보안도구란 전자우편 소프트웨어에 암호기능, 내용 검사 및 악성 콘텐츠 방지 기능, 기타 보안 기능 등을 추가하여 보안성을 강화한 암호화 제품이다. 국외의 전자우편 보안 제품들은 현재 표준화되고 있는 S/MIME v3와 OpenPGP를 지원하고 있으며 RSA사의 PKCS 표준을 지원하는 제품들이 대다수였다. 또한 암호기술을 활용하여 SPAM 방지, 정보 유출 및 부적절한 콘텐츠 감시, 바이러스로부터의 보호, 필터링 기법, 서비스거부공격방지, 전자우편 중계 보호 등 다양한 기능을 제공하고 있었다.

〔표 4〕 전자우편 보안을 위한 암호화 제품들의 특징[4]

| 회사(나라) | 제품명 | 특징 |
|---|---|---|
| Baltimore/ Content Technologies (미국) | SECRETs weeper | • 인증서기반의 암호화/서명(컨텐츠 분석, 컨텐츠 검증기능, 클라이언트 서명 게이트웨이 암호화, 모바일 및 유동사용자를 위한 암호/서명 기능 제공<br>• 정책관리4)를 이용한 전자우편 보안관리 |
| Entrust Technologies (미국) | Entrust/ E-mail Plug in | • Micorsoft Exchange, Microsoft Outlook 등과 같은 어플리케이션을 통합운영<br>• 인증서, CRL의 자동 검증, 전송중인 메시지 변경 자동 검증<br>• 암호화 및 서명에 사용된 인증서 관리<br>• 컨텐츠 스캐닝 통합(컨텐츠 필터링, 바이러스 감지 기술 등)<br>• S/MIME, PKCS#12, X.509를 지원함으로써 다양한 호환성 제공 |
| PC Guardian (미국) | Encryption Plus Email | • Microsoft Outlook과 Lotus Notes와 통합운영<br>• 자동화된 복호화 기능을 제공하여 송신자는 특별한 소프트웨어를 필요로 하지 않음<br>• 고비도 암호화 기능 지원 |
| RSA (미국) | BSAFE S/MIME-C | • 개발자들은 RSA BSAFE S/MIME-C API(SDK)를 이용함으로써 구현시간을 절약할 수 있음<br>• X.509의 인증서 서비스 지원<br>• 안전한 인증서 관리, 키 관리, CRL관리 등<br>• LDAP 지원, 다양한 CA들과의 인터페이스를 지원<br>• S/MIME지원 |
| Authentica (미국) | Mailrecall | • Microsoft Outlook, Lotus Notes, Eudora Pro와 통합운영<br>• 전자우편의 자동 보호 및 통제기능<br>• 허가받지 않은 사용자에게 전달되지 못하게 하는 전자우편 전달방지기능<br>• 메시지 추적기능(누가 열어보고 인쇄하였는지 등) |

4) 암호화된/서명된 메시지를 받고 보낼 수 있는 사용자 결정, 인증받지 못한 키와 인증서 방지 등을 말함.

| | | |
|---|---|---|
| Vanguard Security Technologies (이스라엘) | Mail Guardian Enterprise | • 전자서명과 tampering탐지기능<br>• 사용자 인증기능<br>• 자동화된 키 관리기능 |
| Aliroo (이스라엘) | PrivaWall | • 자동화된 암/복호기능<br>• 바이러스 스캐닝<br>• 콘텐츠 필터링<br>• 자동 전자서명기능<br>• 조직적인 키 및 인증서 관리 |
| Norman Data Defense Systems (유럽 : 노르웨이) | Norman Privacy 3.0 | • 전자우편 및 전자우편에 첨부된 화일, 디렉토리, 디스크 등에 암/복호화 기능을 제공<br>• 암호화하기 전의 메시지 압축기능 제공 |

〔표 5〕 전자우편 보안을 위한 암호화 제품들의 알고리즘 지원

| | SECRETsweeper | Entrust/E-mail Plug in | Encryption Plus Email | BSAFE S/MIME-C |
|---|---|---|---|---|
| DES | Y | Y | N | Y |
| 3DES | Y | Y | N | Y |
| RC2 | Y | N | N | Y |
| RC4 | N | N | N | N |
| RC5 | N | N | N | N |
| CAST | N | Y | N | N |
| IDEA | N | Y | N | N |
| Blowfish | N | N | Y | N |
| Twofish | N | N | N | N |
| AES | N | Y | N | N |
| RSA | Y | Y | - | Y |
| DSA | N | Y | N | - |
| ECC | N | Y | N | N |
| ECDSA | N | Y | N | N |
| DH | N | N | N | N |
| SHA | Y | Y | - | Y |
| MD5 | Y | Y | - | Y |
| 기타 | S/MIME PKCS#2 PKCS#7 PKCS#11 PKCS#12 인증서호환 (Baltimore,Verisign,Entrust 등) | S/MIME PKCS#12 X.509 | - | PKCS12 PKCS7 PKCS10 X.509 S/MIME |

〔표 6〕 전자우편 보안을 위한 암호화 제품들의 알고리즘 지원

| | Mailrecall | Mail Guardian | PrivaWall | Norman Privacy |
|---|---|---|---|---|
| DES | N | Y | N | Y |
| 3DES | N | Y | Y | N |
| RC2 | N | N | Y | N |
| RC4 | N | N | N | N |
| RC5 | Y | N | N | N |
| CAST | N | N | N | N |
| IDEA | N | N | N | N |
| Blowfish | N | Y | N | Y |
| Twofish | N | N | N | N |
| AES | N | N | N | N |
| RSA | Y | - | Y | - |
| DSA | N | - | N | - |
| ECC | N | N | N | N |
| ECDSA | N | N | N | N |
| DH | N | N | N | N |
| SHA | N | N | Y | N |
| MD5 | N | N | Y | N |
| 기타 | - | S/MIMEv3 | S/MIME LDAP X.509 인증서 지원 | - |

※ PKCS#1 : RSA Encryption Standard
PKCS#2 : Password based encryption standard
PKCS#7 : Cryptographic Message Syntax Standard
PKCS#12 : Personal Information Exchange Syntax Standard

※ - : 공개되어 있는 자료만으론 알 수 없음을 의미

## Ⅳ. 스테가노그라피 기능이 탑재된 암호화 제품 현황분석

대부분의 정보보호제품들이 허가받지 않은 사용자들의 접근을 통제하기 위해 일회용 패스워드(OTP)를 많이 사용하고 있으나 이것만으로 해커와 같은 불법 사용자들로부터 개인의 비밀정보를 보호하기에는 미약하다.

이로 인해, 스테가노그라피 기능이 있는 암호화 제품들은 사용자의 기밀정보에 대한 높은 수준의 보호 기능을 제공하기 위해 암호화 알고리즘을 사용하여 사용자의 비밀정보에 대한 기밀성을 제공할 뿐 아니라 스테가노그라피 기능을 추가함으로써 허가받

지 않은 사용자들의 접근권한을 통제할 수 있는 접근권한 방지 기능들을 추가 제공하고 있다. 즉 스테가노그라피 기능이 있는 암호화 제품들은 사용자가 패스워드와 파일명을 알면 파일 접근이 허용되고 그렇지 않다면 파일이 있는지 조차 알 수 없게 한다. 제품들의 주요 보호대상은 파일, 폴더, 하드 디스크, 전자우편 첨부문서 등이었으며 사용자들이 손쉽게 이용할 수 있도록 마우스 버튼의 클릭만으로 암호화 및 스테가노그라피 기능을 사용할 수 있게 하고 있다.

또한, 안전성 측면에서 독일의 Steganos와 Neo-Byte Solutions 제품들은 PC 보안을 위한 암호화 제품들처럼 윈도우 상의 파일삭제 기능이 안전하지 않다는 이유로 DOD 5220.22-M을 따르는 파일 삭제기능을 지원하는 제품들이 있으며 향후 이런 표준을 따르는 제품들이 늘어날 것으로 추정된다.

〈표 7,8〉은 스테가노그라피 기능이 있는 암호화 제품들의 data sheet을 조사하여 비교 분석한 것이다.

〔표 7〕 스테가노그라피 기능이 있는 암호화 제품들의 특징

| 회사(나라) | 제품명 | 특징 |
|---|---|---|
| Steganos (독일) | Steganos 4 Security Suite | • 전자우편 첨부화일 암/복호<br>• 암호화 및 문서 숨기기<br>• 1GB 데이터를 1초 안에 암호화<br>• 사용자가 방문한 웹사이트를 다른 사용자들이 볼 수 없음<br>• 컴퓨터 잠금장치 지원 |
| SecurStar (독일) | DriveCrypt (ScramDisk) | • 하드디스크 및 하드디스크 파티션을 암/복호화<br>• 패스워드 보호기능<br>• 패스워드 스니핑 방지<br>• 잊어버린 사용자 패스워드 복구기술 지원<br>• 안전한 디스크 삭제<br>• 스마트카드 리더, USB 토큰 지원 |
| Invisible Secrets 3 (유럽) | NeoByte Solutions | • 비밀정보를 패스워드와 암호시스템을 사용해서 암호화 한 뒤 암호문을 이미지 및 음악파일에 삽입 |
| StealthDisk (미국) | StealthDisk | • 파일 및 폴더 숨기는 기능 지원<br>• Win95,98,ME,Win2000 지원 |
| Stealencrypt (미국) | Stealencrypt | • 임의의 파일을 숨기는 기능<br>• 암호화 기능 지원 |
| Security Software Development Ltd (미국) | S-Mail | • 임의의 파일을 암호한 후, 암호화된 데이터를 EXE 혹은 DLL파일에 숨김 |

〔표 8〕 스테가노그라피 기능이 있는 암호화 제품들의 암호 알고리즘 지원 및 기능 비교

| 제품명 | 암호지원 | 스테가노그라피 기능 | | 비고(지원 포맷 및 프로토콜) |
|---|---|---|---|---|
| | | 비밀 정보 | 커버 정보 | |
| Steganos 4 Security Suite | AES (128) | file | 이미지 오디오 | DOD 표준 5220.22-M에 따른 파일 삭제 |
| DriveCrypt (ScramDisk) | AES Blowfish Tea 16 Tea 32 Des 3Des | file | 음악파일 | - |
| NeoByte Solutions | Blowfish Twofish RC4 Cast128 GOST AES Diamond 2 | file | JPEG PNG BMP HTML WAV | DOD 표준 5220.22-M에 따른 파일 삭제 |
| StealthDisk | - | file | - | - |
| Stealencrypt | Blowfish 3DES | file | BMP TIF | - |
| S-Mail | - | file | EXE DLL | - |

※ - : 공개되어 있는 자료만으론 알 수 없음을 의미

스테가노그라피 기능을 탑재하여 PC나 전자메일을 보호하는 제품 이 외에 단지 스테가노그라피 기능만을 탑재하고 있는 스테가노그라피 제품들이 있다. 〈표 9〉는 스테가노그라피 기능을 탑재하고 있는 국외 소프트웨어를 조사하여 비교·정리한 것이다.

〔표 9〕 스테가노그라피 제품들의 비교·분석

| 저자(나라) | 제품명 | 제공형태 | 커버정보 | 비고 |
|---|---|---|---|---|
| Media Technology Research Center (미국) | Blindside | file | 이미지 (BMP) | - |
| Darkside Technologies (오스트레일리아) | gifshuffle | file | 이미지 (GIF) | • 메시지압축기법으로 허프만 인코딩 기법 지원<br>• 블록암호알고리즘 ICE(64비트) 지원 |
| | Snow | file | ASCII text | • 블록암호알고리즘 ICE 지원 |
| Heinz Repp (독일) | Hide4 PGP | file | Image (BMP) Audio (WAV) VOC files | - |
| Intar.com (-) | InThe Picture | file | BMP Image | - |
| Allan Latham (-) | JPHIDE & JPSEEK | file | Jpeg visual image | • 암호알고리즘을 사용하지 않음 |
| Fabien A. P. Petitcolas (미국) | MP3 Stego | file | MP3 | • 압축 알고리즘 Zlib 지원<br>• 블럭암호알고리즘 3DES를 지원 |
| Mark Chapman (미국) | NICE TEXT | file | Text | • 임의의 파일을 Pseudo-natural-language text로 변환할 수 있는 패키지 |
| Smaller Animals Software, Inc (미국) | Stash-it | file | BMP TIFF PNG PCX | - |
| Compris Text Technologies (독일) | TextHide | file | Text | • 블록암호알고리즘 Twofish(256비트), AES(128) 지원<br>• 공개키암호알고리즘 RSA 지원 |
| wbStego/ Werner Bailer (독일) | wbStego4 | file | BMP Text HTML PDF | • 블록암호알고리즘 Blowfish, Twofish, CAST, AES 지원 |

※ - : 공개되어 있는 자료만으론 알 수 없음을 의미

## V. 키복구 기능이 있는 암호화 제품 현황분석

키 복구 제품이란 사전에 약속된 어떤 특정한 조건 하에서 허가된 사람에게 복호화가 가능한 능력을 제공하는 암호 제품을 말한다. 여기서 특정한 조건이라는 것은 여러 가지 상황이 될 수 있는데, 예를 들면 법 집행기관이 범죄 수사를 목적으로 암호문을 복호해야 한다거나, 암호문의 소유자가 키를 분실해서 복호를 할 수 없는 경우를 말한다.

키복구 방식은 크게 위탁방식과 캡슐화 방식으로 나누어진다. 키복구 방식을 분류하면 〈표 10〉과 같다.

〔표 10〕 키 복구 방식에 따른 장단점 비교·분석

| 구분 | 정의 | 복구대상 | 비교 |
|---|---|---|---|
| 키위탁방식 | • 복구될 사용자의 비밀키, 비밀키의 부분 또는 키 관련 정보를 하나 이상의 신뢰기관(TTP)에 위탁하는 방식 | long term key | • 개인의 프라이버시가 각 기관들의 신뢰성에 절대적으로 의존<br>• TTP 사이의 키생성 방식이 통일된다면 국가간 호환성이 뛰어날 수 있음 |
| 캡슐화방식 | • 키위탁 방식과는 달리 암호문을 생성하는 각 세션마다 키를 복구해 낼 수 있는 정보를 포함하는 필드를 생성해서 해당 암호 메시지에 부가시키는 방식으로 실제적인 키 위탁이 일어나지는 않음 | 세션키 | • 복구되는 키가 사용자의 long-term 키가 아니라 세션키가 되도록 할 수 있기 때문에 도청 기관의 복구 능력을 제한할 수 있게 되어 사용자의 입장에서는 키위탁 방식보다는 안전에 대한 확신을 가질 수 있음. |

〈표 11, 12〉는 〈표 10〉의 분류된 키 복구 방식에 따라 키 복구기능을 지원하고 있는 암호화 제품들을 조사하여 비교·정리한 것이다.

〔표 11〕 키 복구 기능이 탑재된 암호화 제품들의 특징

| 회사 (나라) | 제품명 | 특징 |
|---|---|---|
| MS (미국) | Window 2000 EFS | • 공개키 암호화 기법을 사용하여 파일 및 디렉토리를 암호화<br>• 데이터 복구 정책을 설정할 수 있는 능력 제공<br>• 데이터 복구기능 제공, 복구된 데이터만을 드러내고 사용자의 키는 드러내지 않음<br>• 암호화된 파일 백업 및 복구 기능 제공<br>• 디스크에 파일을 읽고 쓸때의 암/복호화의 자동화<br>• 북미버젼은 56비트 DES키 지원, 북미 이외의 지역은 40비트 DES지원 |
| RSA (미국) | RSA Keon Desktop | • 강한 파일암호기술로 파일 보안을 수행<br>• 파일 시스템의 민감한 데이터에 대한 시스템 관리자의 접근을 효과적으로 방지함<br>• 표준 PKI 기반의 다른 시스템과 공동 이용가능(예, Netscape, VeriSign, Baltimore 등)<br>• PKI의 복잡성은 사용자에게 숨기는 반면 강력한 보안성을 제공 |
| F-Secure (핀란드) | File Crypto | • F-Secure Policy Manager와 통합되어 소프트웨어 배포 및 암호화 대상 파일 또는 폴더의 통제가 원격지에서 가능<br>• 완전파일삭제 기능은 삭제된 파일들이 절대 복구될 수 없도록 파일 오버라이트를 통한 완전삭제 기능 제공<br>• F-Secure의 Anti-Virus 및 F-Secure VPN과 통합 운영되어 모든 제품의 보안 기능들이 상호 유기적으로 작동<br>• 전원차단시의 파일보호 대책 제시<br>• Temporary 파일들에 대한 암호화 제공<br>• 관리자를 통한 키 복구 기능지원<br>• Windows의 Shell에 통합 운영되어 복잡한 기능을 사용자에게 숨김 |
| 미국 | Clipper Chip | • 미국의 1994년에 EES(Escrow Encryption Standard)라는 표준을 구현<br>• Tamper-resistant 특성을 지니는 클리퍼 칩이 내장된 암호 단말 장치, 암호문을 감청하여 키복구의 요청 및 암호문의 복호를 수행하는 법 집행 기관의 Law Enforcement Decryptor, 키를 복구할 수 있는 정보를 제공해 주는 위탁 기관 세부분으로 구성 |

〔표 12〕 키 복구 기능이 탑재된 암호화 제품들의 암호알고리즘 지원

| 회사(나라) | 제품명 | 키복구 기능 | 암호 알고리즘 | 비고 |
|---|---|---|---|---|
| MS (미국) | Window 2000 EFS | 캡슐화[4] | DESX 3DES | - |
| RSA (미국) | RSA Keon Desktop | 캡슐화[4] | RC5 (128) DES (56) | - |
| F-Secure (핀란드) | File Crypto | 위탁[4] | AES (128) Blowfish (256) | Secure Computing Magazine 의 Millenniu m Awards 2000 수상. |
| 미국 | Clipper Chip | 위탁[5] | SKIP JACK (비공개) | - |

※ - : 공개되어 있는 자료만으론 알 수 없음을 의미

## Ⅵ. 국내 암호화 제품 현황분석

대부분의 국내 암호화 제품들은 PC보안과 전자우편 보안을 위해 국외의 블록암호알고리즘으로는 DES, 3DES, Blowfish 등을 지원하고 있었으며, 국내 블록암호알고리즘으로 SEED를 지원하고 있거나 혹은 자체 개발된 블록암호알고리즘을 사용하고 있었다. 하지만 앞 절에서 조사된 국외 암호화 제품과는 달리 스테가노그라피 기능이 탑재된 암호화 제품들은 전무한 실정이었으며, 키복구 기능이 탑재된 제품들도 극히 드물다는 것을 알 수 있었다. 〈표 13〉~〈표 17〉은 국내 암호화 제품들의 data sheet를 조사하여 정리한 것이다.

〔표 13〕 국내 암호화 제품들(PC 보안)의 특징

| 회사명 | 제품 (PC 보안) | 특징 |
|---|---|---|
| 디지털 이지스 | F-Secure File Crypto | • F-Secure의 파트너로서 F-Secure의 제품을 지원 |
| 니츠 | PC Shield | • PC 사용통제 및 사용자 식별/인증 기능<br>• 파일/폴더 암호기능<br>• 암호화된 파일을 수정 편집한 후 다시 암호화 된 상태로 자동 저장함<br>• 보안정책을 설정함으로써 파일을 자동 암호화<br>• 파일 완전 삭제 기능지원<br>• 악성프로그램 점검/삭제 기능<br>• 실시간 네트워크 모니터링/침입탐지 점검 기능<br>• 개인 PC 방화벽 기능<br>• 공유폴더 접근차단현황 보기/ 감사 기능 목록 보기 |
| 안철수 연구소 | 앤디 Pro | • PC 보안제품<br>• 허락되지 않은 사용자의 시스템 접근 차단<br>• 주변기기를 통한 자료 유출 방지<br>• 암호 파일의 공유를 위해 공개키 암호기술을 사용하여 서로 모르는 사용자들끼리도 서로의 공개키를 주고 받음으로써 중요한 파일을 전달함<br>• 클라이언트 불법 접근 기록 추적, 분석<br>• 마우스 끌어놓기만으로 데이터 자동 암호화/복호화 |
| 펜타 시큐리티 | ISSAC -File | • 스마트 카드 기반으로 PC사용의 접근통제<br>• 윈도우 로그인 과정을 자체개발한 사용자 인증기법을 이용<br>• 공개키 암호를 사용하여 첨부파일을 수신자만 풀어볼 수 있도록 암호화<br>• 완전한 파일 삭제기능<br>• 공개키 기반 암/복호화<br>• 전자서명기능 지원 |
| 퓨쳐 시스템 | Say Safe | • 대상 컴퓨터에 대한 접근 제한<br>• PC의 취약한 부분을 찾아내는 포트 스캔기능<br>• 불법적 내/외부 사용에 대해 실시간 알림기능<br>• 소중한 정보의 보호를 위한 바이러스 진단 치료<br>• 스마트카드, USB 키 디바이스 지원<br>• 국내 공인 인증서 관리 기능 탑재 |
| 소프트 프로텍 | S-Cop | • 하드웨어 방식의 접근제한 기능지원<br>• 마우스의 클릭만으로 파일 또는 폴더를 암/복호화<br>• 128bit 암호화 알고리듬 지원 |
| F&F Secure | SecuX ACE | • 허가받은 사용자 키에 의한 컴퓨터 전원을 통제하는 방식으로 불법사용자 의 접근방지<br>• 128 비트 암호화 알고리즘 지원 |
| 에스디 아이티 | Insider Keeper | • 하드 디스크의 암/복호화<br>• 사용자 인증을 위한 생체인식 솔루션 및 스마트 카드와 연동<br>• 윈도우 부팅시 자동적으로 암호화 모드로 전환되어 데이터를 암호화<br>• 암호화 키를 PC가 아닌 전용 하드웨어 보안장치에 저장<br>• 원본파일이 서버에 보관되어 비상시 파일복구가 가능<br>• 부정 사용자의 접근을 차단 |
| 지란지교 소프트 | File Safe | • 암/복호 기술을 이용한 파일보호<br>• 실시간 바이러스 차단기능<br>• 유추 단어를 이용한 키복구 기능<br>• 중요한 데이터를 암호화하여 백업<br>• 완전한 파일 삭제기능 |

〔표 14〕 국내 암호화 제품들(전자우편 보안)의 특징

| 회사명 | 제품 (전자우편 보안) | 특징 |
|---|---|---|
| 소프트 포럼 | XecureExpress | • 전자우편 및 첨부화일 암호화, 전자우편 내용 위·변조 방지, 부인방지, 송신자 신원확인 가능<br>• 기존의 PKI 인프라와 연동 : 사설인증서, 공인 인증서 연동<br>• 수신확인 기능 지원<br>• MAC기반으로 등록된 단말기에서만 전자우편을 열어 볼 수 있음<br>• 전용브라우져 환경으로 다양한 메일 클라이언트 환경 지원 |
| 장미디어 인터렉티브 | JK Mail | • 인증서 기반의 암/복호화와 전자서명 지원<br>• S/MIME표준을 따름 |
| 비씨큐어 | CQ Mail | • 메시지 및 첨부파일에 대한 전자서명/암호화 기능지원<br>• S/MIME 표준 지원<br>• 공인 인증서를 이용한 전자우편 보안 메시지 지원 |

〔표 15〕 국내 암호화 제품들(PC보안 제품)의 암호알고리즘 지원

| 암호 알고리즘 | PC 보안 제품 | | | | |
|---|---|---|---|---|---|
| | Sky Safe | S-Cop | SecuK ACE | Insider Keeper | File Safe |
| DES | - | - | - | Y | N |
| 3DES | - | - | - | Y | N |
| SEED | - | - | - | Y | Y |
| RC2 | - | - | - | N | N |
| RC4 | - | - | - | N | N |
| CAST | - | - | - | N | N |
| IDEA | - | - | - | N | N |
| Blowfish | - | - | - | N | Y |
| Twofish | - | - | - | N | N |
| AES | - | - | - | N | N |
| RSA | - | - | - | N | N |
| DSA | - | - | - | N | N |
| ECC | - | - | - | N | N |
| DH | - | - | - | N | N |
| SHA | - | - | - | N | N |
| MD5 | - | - | - | N | N |
| FIPS 140-1 level 1 | N | N | N | N | N |
| 기타 | - | - | S-Pass 자체개발 블럭암호 | - | Bush2 자체개발 블럭암호 |

〔표 16〕 국내 암호화 제품들(PC보안 제품)의 암호알고리즘 지원

| 암호 알고리즘 | PC 보안 제품 | | | |
|---|---|---|---|---|
| | F-Secure File Crypto | PC Shield | 엔터 Pro | ISSAC -File |
| DES | - | - | Y | - |
| 3DES | - | - | Y | - |
| SEED | N | - | Y | - |
| RC2 | N | - | N | - |
| RC4 | N | - | N | - |
| CAST | N | - | N | - |
| IDEA | N | - | N | - |
| Blowfish | Y | - | Y | - |
| Twofish | N | - | N | - |
| AES | Y | - | N | - |
| RSA | N | - | N | - |
| DSA | N | - | N | - |
| ECC | N | - | N | - |
| DH | N | - | N | - |
| SHA | N | - | N | - |
| MD5 | N | - | N | - |
| FIPS 140-1 level 1 | N | N | N | N |
| 기타 | - | - | - | - |

〔표 17〕 국내 암호화 제품들(전자우편 보안 제품)의 암호 알고리즘 지원

| 암호 알고리즘 | 전자우편 보안제품 | | |
|---|---|---|---|
| | Xecure Express | JK-Mail | CQ Mail |
| DES | Y | - | - |
| 3DES | Y | - | - |
| SEED | Y | - | - |
| RC2 | Y | - | - |
| RC5 | Y | - | - |
| CAST | N | - | - |
| IDEA | N | - | - |
| Blowfish | N | - | - |
| Twofish | N | - | - |
| AES | N | - | - |
| RSA | Y | - | - |
| DSA | N | - | - |
| ECC | N | - | - |
| DH | - | - | - |
| SHA | - | - | - |
| MD5 | - | - | - |
| FIPS 140-1 level 1 | N | N | N |
| 기타 | ELGalmal KCDSA | - | S/MIME |

※ - : 공개되어 있는 자료만으론 알 수 없음을 의미

## Ⅶ. 결 론

본 고에서는 암호기술의 대표적인 서비스에 해당하는 기밀성을 제공해주는 암호화 제품들의 개발현황을 조사하여 비교 분석하였다. 또한 암호화 제품의 사용시 쉽게 발생할 수 있는 사용자의 부주의로 인한 암호키의 분실 및 손상시 정보의 손실을 예방하는 대책으로 국외에서 제시되고 있는 키복구 기능을 갖는 암호화 제품들에 대해 조사하여 비교분석 하였으며, 기밀성 이외의 해커와 같은 불법 사용자들로부터의 접근을 방지할 수 있는 스테가노그라피 기능이 탑재된 암호화 제품들의 현황을 조사하여 비교정리 하였다. 이는 국내 암호화 제품들의 새로운 시장을 개척하는데 도움이 되는 자료로 활용될 것으로 판단된다.

〔표 18〕 조사된 암호화 제품의 URL

| 구분 | 회사 | URL |
|---|---|---|
| PC 보안을 위한 암호화 제품 | Entrust Technologies | http://www.entrust.com/entelligence/file/faqs/htm |
| | PCGuardian | http://www.pcguardian.com |
| | Cyberus Systems | http://www.cerberussystems.com/INFOSEC/index.htm |
| | Safe House | http://www.pcdynamics.com/SafeHouse/Features.asp |
| | Norman Data Defense Systems | http://www.norman.com/ |
| | SFS (Secure File encryption) | ftp.ox.ac.uk:/pub/crypto/misc/sfs**.zip |
| | Cryptext | http://www.pcug.org.au/~njpayne/ |
| | Cloak | http://cloak.binarynet.com/ |
| 전자우편 보안을 위한 암호화 제품 | Baltimore/ Content Technologies | http://www.contenttechnologies.com |
| | Entrust E-mail | http://www.entrust.com/entelligence/email/index.htm |
| | PC Guardian | http://www.pcguardian.com |
| | RSA | http://www.rsasecurity.com/products/bsafe/smimec.html |
| | Authentica | http://www.authentica.com/ |
| | Vanguard Security Technologies | http://www.vguard.com |
| | Aliroo | http://www.aliroo.com |
| | Norman Data Defense Sysemts | http://www.norman.no/index.shtml |

〔표 19〕 조사된 암호화 제품의 URL

| 구분 | 회사 | URL |
|---|---|---|
| 스테가노그라피 기능이 있는 암호화 제품 | Stegnos | http://www.steganography.com/english/steganos/download.htm |
| | Secur Star | http://www.scramdisk.clara.net/ |
| | Invisible Secrets | http://www.neobytesolutions.com/invsecr/ |
| | Stealth Disk | http://www.stealthdisk.com/ |
| | Steal encrypt | http://www.stealthencrypt.com/index2.html |
| | Security Software Development | http://www.ssdltd.com/english/ourphilo.htm |
| 스테가노그라피 제품 | Blind side | http://www.blindside.co.uk/ |
| | gif shuffle | http://www.darkside.com.au/gifshuffle/ |
| | Hide4 PGP | http://www.heinz-repp.onlinehome.de/index.html |
| | InThe Picture | http://www.intar.com/ITP/itpinfo.htm |
| | JPHIDE & JPSEEK | http://linux01.gwdg.de/~alatham/stego.html |
| | MP3 Stego | http://www.cl.cam.ac.uk/~fapp2/steganography/mp3stego/ |
| | NICETEXT | http://www.ctgi.net/nicetext/ |
| | Snow | http://www.darkside.com.au/snow/index.html |
| | Stash -it | http://www.smalleranimals.com/stash.htm |
| | Text Hide | http://www.compris.com/TextHide/en/ |
| | WbStego | http://www.wbailer.com/wbstego |
| 키 복구 기능이 있는 암호화 제품 | MS | http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winxppro/reskit/prnb efs qaji.asp |
| | RSA | http://www.rsasecurity.com/products/keon/techpecs/rsakeondesktop.html |
| | F-Secure | http://www.datafellows.com/wireless/pocketpc/compare-filecrypto.shtml |
| | Cliffer chip | http://www.cosc.georgetown.edu/~denning/crypto/clipper/Key-Escrowing-Today.txt |

〔표 20〕 조사된 암호화 제품의 URL

| 구분 | 회사 | URL |
|---|---|---|
| 국내 암호화 제품 | 디지털 이지스 | http://www.aegis.co.kr/aegis/main/index.html |
| | 니츠 | http://www.nitz.co.kr/ |
| | 안철수 연구소 | http://home.ahnlab.com/productionfo/ende_pro.html |
| | 펜타 시큐리티 | http://www.pentasecurity.com/ |
| | 퓨쳐 시스템 | http://www.future.co.kr/index.php |
| | 소프트 프로텍 | http://www.softprotec.com/ |
| | F&F Secure | http://www.ffstek.com/korean/index.html |
| | 에스디 아이티 | http://www.sdit.co.kr/ |
| | 소프트 포럼 | http://www.softforum.com/ |
| | 지란지교 소프트 | http://www.jiran.com/ |
| | 장미디어인터렉티브 | http://www.jmi.co.kr/ |
| | 비씨큐어 | http://www.bcqre.com/ |

## 참고문헌


〔1〕 Neil F.Johnson, "Information Hiding Steganography and Watermarking Attacks and Countermeasures", 2000.

〔2〕 IDC, Email Usage Forecast and Analysis 2001-2005, Mark Levitt and Rober Mahowald, August 2001〕

〔3〕 한국정보보호진흥원, "키복구 기능을 갖는 파일 암호화시스템 개발", 2000.12

〔4〕 한국정보보호진흥원, "키복구 시스템 제품 및 활용사례 분석", 2000.12

〔5〕 Jack Kelley. Terror groups hide behind Web encryption. USA Today, Feburary 2001.

〔6〕 Declan McCullagh. Secret Messages come in. Wavs. Wired News, February 2001. http://www.wired.com/news/poltics/0,1283,41861,00.html


## 〈著者紹介〉


**주 학 수 (Hak-Soo Ju)**

1997년 8월 : 고려대학교 수학과 이학사

1999년 8월 : 고려대학교 수학과 이학석사

2001년 8월 : 고려대학교 수학과 박사과정 수료

2001년 9월~현재 : 한국정보보호진흥원(KISA) 연구원

**김 승 주 (Seungjoo Kim) 종신회원**

1994년 2월 : 성균관대학교 정보공학과 공학사

1996년 2월 : 성균관대학교 대학원 정보공학과 공학석사 (암호학 전공)

1999년 2월 : 성균관대학교 대학원 정보공학과 공학박사 (암호학 전공)

1998년 12월~현재 : 한국정보보호진흥원(KISA) 암호기술팀장

2000년 6월~현재 : 한국정보통신기술협회(TTA) 정보통신기술위원회 암호기술연구반 의장

2002년 4월~현재 : 한국정보통신기술협회 국제 표준화 전문가