通信情報保護學會誌
第 11 券 第 2 號, 2001. 4

키 복구 제품의 특징 및 활용 분야

황 보 성**, 이 임 영*, 김 지 연**, 권 현 조**

요 약

암호의 이용은 개방 네트워크상에서 보다 안전한 통신을 보장한다. 그러나 암호 이용이 이러한 긍정적 측면만 있는 것이 아니다. 암호용 비밀키를 유실했을 경우, 데이터를 복구할 수 없다. 또한 암호가 범법자에게 이용될 경우, 정부는 법 집행능력을 확보할 수 없게 된다. 이러한 문제점들을 해결할 수 있는 방법이 키 복구이고 여러 선진국들에 의해 많은 연구가 진행되고 있다. 본 논문에서는 키 복구의 기술적 동향을 파악하기 위해 실질적으로 개발되어 이용 중인 키 복구 기능이 포함된 제품들의 특징과 활용분야를 분석하고 이들을 비교하였다.

Ⅰ. 서 론

인터넷의 발달에 의해 사용자의 편리성을 증대하였지만 개인 정보 노출에 대한 위협은 커지고 있는 추세이다. 이를 해결하기 위한 암호는 이제 국내에서도 통신이나 정보 보호 등에 없어서는 안될 필수 도구로 자리잡고 있다. 그러나 암호 사용의 일반화가 이러한 긍정적 측면만 있는 것은 아니다. 암호 이용에 있어서 가장 중요한 점은 사용자의 비밀키에 대한 관리이다. 만약 사용자의 비밀키가 손실되거나 분실되었다면 암호화된 메시지를 복호할 수 없을 것이다. 또한, 강력한 암호 제품이 범법자들에게 이용될 때 정부는 법 집행능력을 확보할 수 없다는 부정적인 측면들을 동시에 가진다. 이를 해결하기 위한 대책 방법이 여러 가지가 존재하나 실제로 이용될 수 있는 방법은 제 3자에게 키를 복구할 수 있는 능력을 제공하는 키 복구 시스템을 이용하는 것이다[1]. 이미 외국의 선진국에서는 키 복구 시스템에 대한 정책, 기술, 제품, 표준들이 활발히 소개되고 있다. 본 고에서는, 이 중에서 실제상으로 개발되어 이용중인 키 복구 기능이 포함된 제품들을 분석한다.

2장에서는 키 복구에 대한 정의와 방식들을 살펴보고, 3장에서는 키 복구 기능이 포함된 제품들의 특징을 분석한다. 그리고 4장에서는 분석된 제품들의 특징을 비교하고 5장에서는 제품들의 활용 분야를 살펴본다. 마지막으로 6장에서 결론을 맺도록 한다.

2장에서는 키 복구에 대한 정의와 방식들을 살펴보고, 3장에서는 키 복구 기능이 포함된 제품들의 특징을 분석한다. 그리고 4장에서는 분석된 제품들의 특징을 비교하고 5장에서는 제품들의 활용 분야를 살펴본다. 마지막으로 6장에서 결론을 맺도록 한다.

Ⅱ. 키 복구의 개론

이장에서는 키 복구의 일반적 정의와 키 복구 방식을 분류하고 설명한다.

1. 키 복구 정의

키 복구(Key recovery) 시스템이란 사전에 약속된 어떤 특정한 조건하에서 허가된 사람에게 복호화가 가능한 능력을 제공하는 암호 시스템이라고 정의할 수 있다. 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 경우 등을 말한다. 허가된 사람은 사전에 미리 합의되어 복구 능력을 가질 수 있는 사람을 뜻하며 이것은 정부기관, 개인, 기업 등이 될 수 있다. 즉, 키 복구란 암호 시스템에서 키를 가지고 암호문을

* 순천향대학교 정보기술공학부 (hbs2593@kisa.or.kr)
** 한국정보보호센터

복호하는 정상적인 절차 외에 다른 방법으로 유사시에 암호문을 복호할 수 있는 방법이다[2][3].

2. 키 복구 방식

키 복구방식은 크게 위탁 방식과 캡슐화 방식으로 나누어진다.

위탁 방식은 사용자의 비밀키 전부 또는 일부를 신뢰받는 제3자(Trusted Third Party)에게 위탁하는 방식으로 유사시에 키를 확실하게 얻을 수 있다는 장점이 있다. 이 방식은 유사시에 키를 확실하게 얻을 수 있다는 장점이 있는 반면에, 키를 위탁하는 제3자의 신뢰도에 많은 영향을 받는다. 또한 이러한 키 위탁 방식에서 위탁되는 키는 대부분 한시적으로 사용되는 세션키(session key)가 아니라 사용자의 개인키(private key)와 같은 긴 주기동안 사용되는 키(long-term key)가 되므로 신뢰도가 낮은 보관기관을 사용하는 경우에는 많은 문제점이 발생할 수 있다.

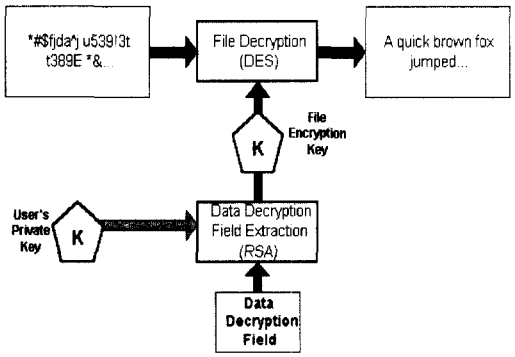
캡슐화(Encapsulation)방식은 각각의 메시지 전송 또는 파일 저장시 마다 키 복구 필드를 생성해서 해당 메시지를 복구할 수 있는 정보를 데이터에 부가하는 방식으로 실제적인 키 위탁은 일어나지 않는다는 장점이 있다. 이처럼 키 복구에 필요한 정보를 담은 영역을 키 복구 필드(Key Recovery Field, KRF) 또는 데이터 복구 필드(Data Recovery Field, DRF)라고 하며, 유사시에 키의 복구가 필요한 경우 복구 기관이 가지고 있는 복구키를 이용해서 키 복구 필드를 복호한 후 해당키를 얻을 수 있다.

Ⅲ. 키 복구 제품의 분석

본 장에서는 여러 가지 키 복구 제품의 특징을 분석한다.

1. Window 2000

마이크로소프트사에서 개발된 Windows 2000은 EFS(Encryption File System)을 통해 파일을 암호화/복호화 하고 키 복구를 제공한다[4]. EFS는 암호화된 NTFS(NT File System) 파일을 디스크에 저장할 수 있는 핵심적인 파일 암호화 기법을 제공하고 이 때 사용되는 암호화 기법은 사용자의 공개키와 비밀키에 독립적인 대칭키를 이용한다. 암호화된 NTFS 파일을 접근하기 위해선 사용자의 비밀키가 있어야 파일에 접근할 수 있다.



〔그림 1〕 Windows 2000의 파일 암호화 과정

각각의 화일은 랜덤하게 생성된 파일 암호용키(File Encryption Key)로 불려지는 키를 이용해서 암호화된다. 이 키는 사용자의 공개키/개인키와 독립된 것이다. FEK는 DES의 암호화 알고리즘을 이용한다. EFS는 사용자가 처음으로 파일을 암호화할 때 파일 암호화를 위해 자동적으로 공개키쌍과 file encryption certificate를 생성하고 개별 파일이나 폴더에 암/복호화를 지원한다. 사용자는 파일을 복호하기 위한 별도의 과정없이 EFS가 자동적으로 암호화된 파일을 검출하고 시스템의 키 저장소로부터 사용자의 FEK의 위치를 알아낸다. EFS는 캡슐화 방식의 키 복구 또한 제공한다. 이때 복구되는 키는 오직 FEK만이 복구되어지고, 사용자의 비밀키에 대한 정보는 recovery agent에 드러나지 않는다. 그림 1은 Windows 2000에서 파일에 대한 암호화과정을 보여주고 있다. 사용자는 파일을 암호화하기 위해 랜덤하게 FEK를 생성한다. 생성된 키와 DES를 이용해 파일을 암호화한다. 그리고 복호를 위해서 Data Decryption Field에 File Encryption Key를 자신의 공개키로 암호화하여 저장해 둔다. 그리고 키 복구를 위해 Data Recovery Field에 File Encryption Key를 키 복구 기관의 공개키로 암호화하여 저장해 둔다. DDF를 통해 FEK를 복호하고 DRF를 통해 FEK를 복구받을 수 있다.

2. Netscape Certificate Management System

Netscape에 개발된 Netscape Certificate Manage-

ment System는 PKI 솔루션을 지원하고 그 중 키 복구 기능을 포함하고 있다[5]. 이 제품은 위탁방식을 이용하고 있으며 서명용/암호화용 키쌍을 생성하고 이 중 위탁되는 키는 데이터 암호화용 비밀키이다. CMS는 위탁과정과 복구과정으로 나누어진다.

2.1 위탁 과정

① 사용자는 dual key-pair를 생성하고 RegIstration Manager로부터 제공받은 인증서 등록폼을 작성 후 제출한다. RM은 사용자의 인증서 요구의 키 위탁 옵션을 검사하고 사용자의 암호용 비밀키를 요청한다. 사용자는 자신의 암호용 비밀키를 DRM의 transport certificate의 공개키를 이용해 암호화한다.

② 사용자로부터 암호화된 암호용 비밀키를 받은 RM은 이것을 사용자의 공개키와 함께 DRM에게 전송하고 DRM의 증명을 기다린다.

③ DRM은 사용자의 암호용 비밀키를 자신의 transport certificate안의 공개키에 해당하는 비밀키로 복호하고 이것이 사용자의 암호용 공개키와 일치하는지 검사한다. DRM은 storage key로 암호화한 뒤 내부 데이터베이스에 저장한다.

④ 사용자의 암호용 비밀키가 성공적으로 저장되었다면, DRM은 RM에게 키 위탁 과정이 성공적으로 끝났다는 것을 알리기 위해 transport key pair의 비밀키를 이용해 토큰(키가 성공적으로 저장되었다는 증명)에 서명한다. 서명된 토큰은 RM에게 전달된다.

⑤ RM은 서명된 토큰을 증명 후, 인증서 요구를 Certificate Manager에게 전송한다.

⑥ CM은 두 개의 인증서를 생성하고, 암호용 인증서와 서명용 인증서를 각각 RM에게 전송한다.

⑦ RM은 인증서들을 사용자에게 전송한다.

2.2 복구 과정

① DRM agent는 절적한 인증서와 복구를 요구하는 사용자와 관련된 식별정보를 이용해 키 복구 폼에 접근하고 request를 제출한다.

② DRM은 이것을 받고 request가 적당한지 검사한다.

③ DRM은 confirmation HTML 페이지를 agent에게 보낸다. confirmation 페이지 안에는 다음과 같은 정보와 입력창이 있다.

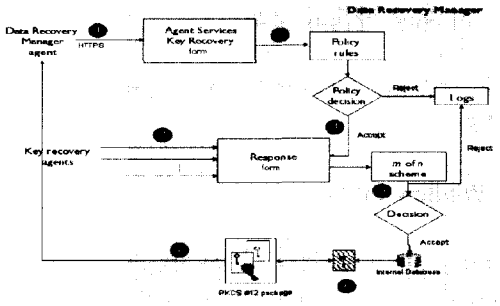
- Information section : 사용자 정보
- Input section : 복구할 키에 해당하는 사용자의 인증서, PKCS #12 package (사용자의 암호용 비밀키와 그에 따른 인증서를 포함)를 위한 패스워드, KRA의 패스워드

④ KRA들은 confirmation page를 검사하고 MIME-64 format의 인증서, PKCS #12 package를 위한 패스워드 그리고 그들의 식별정보와 패스워드를 입력한다. DRM agent는 이 페이지를 DRM에게 제출한다.

⑤ DRM은 KRA의 정보와 "m of n scheme"을 검사한다. 요구된 수의 KRA의 패스워드가 증명되었다면, Server는 키 저장소에 접근하기 위해 PIN을 생성하는데 KRA의 패스워드를 이용한다.

⑥ DRM은 키 저장소로부터 사용자의 암호용 비밀키를 가지고 오고 이것을 storage key pair를 통해 복호한다.

⑦ DRM은 사용자의 인증서와 암호용 비밀키를 PKCS #12 package로 생성하고 이것을 PKCS #12 패스워드를 통해 암호화한다. agent는 로컬 파일 시스템에 저장할 것인지 또는 플로피 디스크에 저장할 것인지 선택한다. 그리고 암호화된 PKCS #12 package와 이것과 일치하는 패스워드를 안전한 방법을 통해 사용자에게 전달한다.



〔그림 2〕 CMS의 키 복구 과정

3. CyKey

CyKey는 Cylink사의 키 복구 제품으로 통신

및 저장 데이터 복구를 모두 지원한다[6]. 이 제품은 캡슐화 방법을 이용하고 초기화 단계와 복구 단계로 나누어진다.

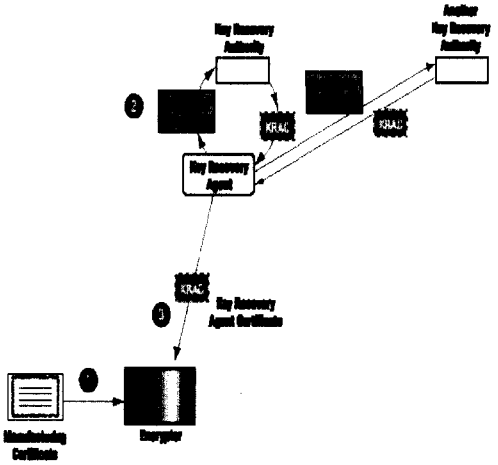
3.1 초기화 단계

이 단계는 KRA(Key Recovery Agent), 암호제품, 키 복구 기관(Key Recovery Authority) 사이의 신뢰관계를 설정하는 것이다.

① 제조시 암호제품에 인스톨된 제조 인증서(Manufacturing Certificate)는 암호제품이 KRA를 인가할 수 있는 키 복구 기관을 정의한다. 제조 인증서는 키 복구 기관의 공개키를 포함한다.

② KRA는 자신의 인증 정보(공개키, ID등)를 키 복구 기관에서 제출하고 키 복구 기관은 서명한 KRAC(Key Recovery Agent Certificate)를 KRA에게 되돌린다.

③ 사용자는 KRA에 등록하고 KRAC을 받는다.



〔그림 3〕 CyKey의 초기화 단계

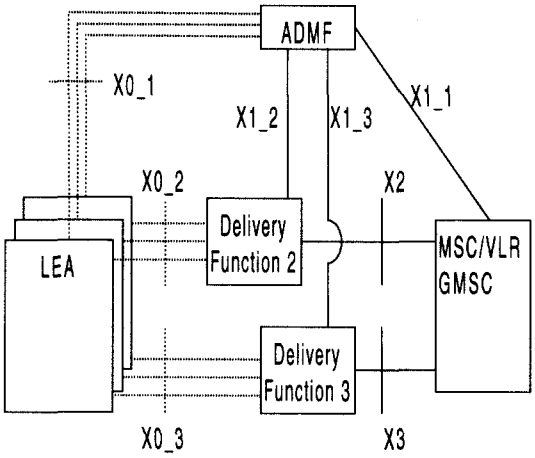
3.2 복구단계

복구 대상은 파일 암호화용 세션키와 통신을 위한 키 교환 프로토콜상의 키 요소가 된다. 파일 암호화는 사용자가 파일을 암호화할 때, 데이터를 암호화한 세션키를 KRA의 공개키로 암호화해 KRF를 생성한다. 만약, 세션키가 유실되었을 경우 KRF는 KRA에게 전송되고, KRA는 KRF를 복호화하고 복호된 세션키를 사용자에게 전송한다. 통신을 위한 키 복구는 통신 데이터를 암호화하는 세션키를 복구하는 것이 아니라 양 사용자가 키 교환 프로토콜 실행시 이 정보를 KRF에 포함함으로 해서 키를 복구할 수 있다.

4. 이동통신상에서의 키 복구 모델

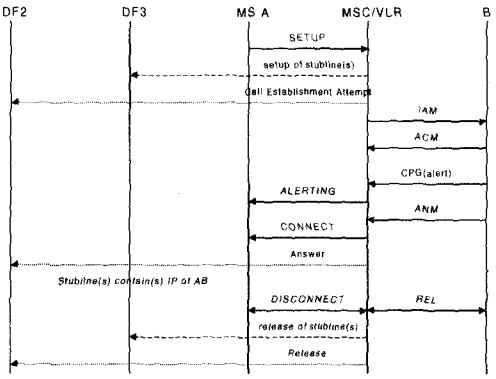
무선이동 통신의 발달로 인해 무선이동통신상의 보안문제가 중요시되고 있고 이를 해결하기 위해 많은 연구들이 진행 중에 있다. 본 모델은 제품은 아니지만 IMT-2000의 표준화작업을 하고 있는 3GPP (Third Generation Partnership Project)를 기반으로 하는 법 집행능력 확보 방법과 키 복구 프로토콜을 분석한다[7][8]. 감청은 목소리, SMS등에 대해서 가능하고 그림 4는 키 복구 모델의 구성요소와 인터페이스(X-interface)를 설명한다.

X-interface의 타입을 정의함으로써 이동통신상의 감청에 대한 법 집행능력을 확보할 수 있다.



〔그림 4〕 X-interface의 구성

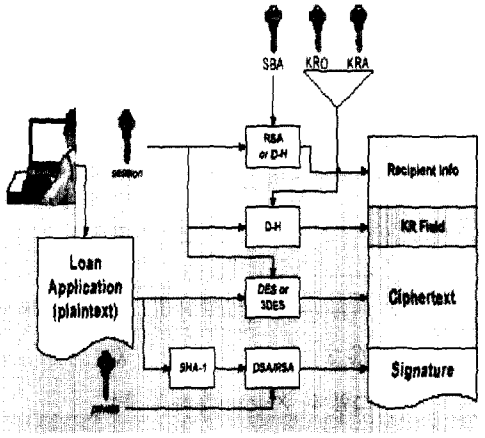
X1_1,2,3 인터페이스는 피감청 대상을 초기화하기 위해 교환국과 감청 데이터 전달 함수(DF2, DF3)를 설정하는 것으로 피감청자의 식별자, 감청 데이타의 종류등이 설정된다. X2, X3 인터페이스는 실제적 감청을 하는 것으로 감청된 정보는 DF2, DF3를 통해 LEA(수사기관)에게 전달된다. 그림 5는 A, B사이에 법 집행능력확보를 위한 단계를 도식화한 것이다. 사용자 A와 B가 Setup를 거친 후 DF2와 DF3에 의해 감청된 데이터와 그와 관련된 정보가 LEA에게 전송되는 과정을 보여준다.



〔그림 5〕 이동통신상의 일반적인 감청 절차

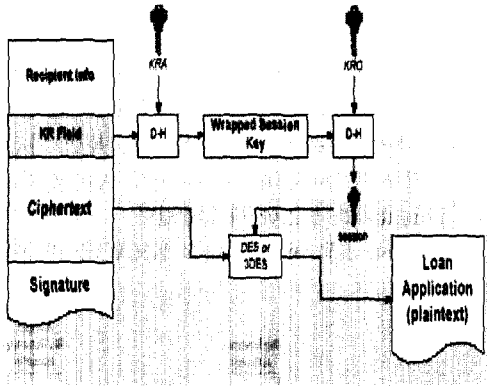
5. SecretAgent

이 제품은 Information Security Corporation 사에 의해 개발된 제품으로 키 복구의 기능을 가지고 있다[9]. SecretAgent는 사용자가 하나나 그 이상의 수신자를 위해 파일을 암호화하고 서명하는 것을 제공한다.



〔그림 6〕 SecretAgent의 키 복구 필드 생성과정

암호화 과정에서 랜덤 세션키들은 생성되어지고 수신자의 공개키를 이용해 암호화된다. 키 교환을 위해 SecretAgent는 RSA, Diffie-Hellman, Capstone KEA를 제공한다. 서명하기 위한 비밀키와 복호화하기 위한 비밀키의 저장을 위해 스마트 카드나 토큰들이 제공된다. 또한 SecretAgent는 VIM, MAPI, AT&T AccessPlus를 통해 메일에서도 가능하다. 또한, X.509 버전 3을 지원함으로써 PKI와의 연동 또한 가능하다. 키 복구 필드의 생성과정은 그림 6과 같다. 송신자의 Key Recovery Officer(또는 "key requestor")와 Key Recovery Center(또는 "Key Recovery Agent")로 구성되며 KRF는 세션키 K와 KRO와 KRA의 공개키로 구성된다. KRO와 KRA는 혼자만의 힘으로 K를 유도할 수 없고, 오직 협력을 통해 K를 얻을 수 있다. 키 복구는 그림 7과 같이 KRO와 KRA의 동의에 의해 M을 복구할 수 있다.



〔그림 7〕 SecretAgent의 키 복구 과정

SecretAgent의 특징은 다음과 같다.

- KRO 또는 KRA는 대칭키 암호나 키 교환 프로토콜을 깨지않는 이상 혼자서는 암호화된 메세지(M)을 복구할 수 없다.
- 각각의 메시지를 위해 생성된 데이터 암호화 키(K)와 KRO는 각각의 메시지마다 새로운 키 복구 요구를 생성해야 한다.
- SecretAgent는 쉽게 다른 KRO와 KRA를 연동할 수 있다.
- SecretAgent는 복수 개의 KRO와 KRA를 위해 비밀분산(threshold) 기법을 쉽게 적용할 수 있다.

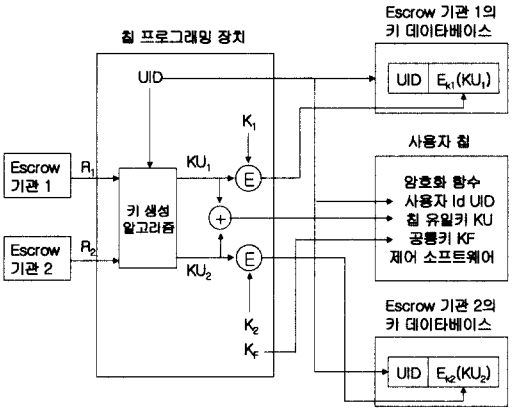
6. Clipper Chip

미국은 1994년 클리퍼 정책은 우선 연방기관이 사용 또는 운영하거나 연방기관과의 계약하에서 연방기관을 위하여 운영되는 암호제품과 시스템의 디자인 및 이행에 적용하도록 위탁암호표준(EES : Escrowed Encryption Standards)으로 제정되

어 공표 되었다[10][11]. 미국 행정부에 의해 EES (Escrowed Encryption Standard)로 정해진 Clipper Chip은 사용자들간의 통신을 암호화/복호화하고 해당 통신을 복구할 수 있는 확장필드를 제공한다. Clipper Chip은 비밀에 붙인 Skipjack 알고리즘을 사용하여 통신자의 내용을 암호화하고, LEAF(Law Enforcement Field)를 생성해 암호문과 함께 전송한다. Clipper Chip의 알고리즘은 64-bit block에 작용하는 Block Cipher이고 32-round의 과정을 거치게 된다. 암호화키는 80-bit를 사용한다. 이 알고리즘은 Skipjack이라고 부르는데 미국 정보의 새로운 정책에 따라서 비밀로 분류되어 있다. Block Cipher의 특정을 가지고 있어 네 가지의 작동 방식을 가지고 있다.

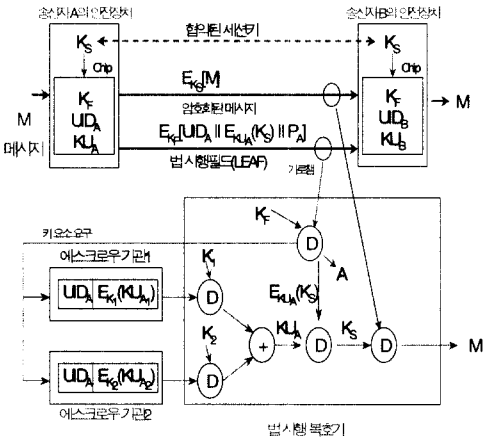
다음은 Clipper Chip에서 이용되는 시스템 계수들이다.

- KF : 80bit group key. group의 모든 장치에 저장되고 LEAF를 만드는 데 사용
- UID : Clipper chip에 대한 유일한 식별자.
- KU : 장치 유일키. 칩과 함께 암호화된 모든 메시지를 푸는데 사용되는 Clipper chip에 유일한 암호화키
- KU1, KU2 : 키 요소의 쌍(KU = KU1 ⊕ KU2)
- K1, K2 : 암호화 비밀키
- KS : 세션키
- P : 인증 코드, LEAF가 인정되지 않은 방법으로 바뀌거나 수정되지 않았다는 것을 확신하는데 사용되는 LEAF의 필드



〔그림 8〕 Clipper Chip의 키 위탁 과정

그림 8은 Clipper Chip의 키 위탁 과정이다. Clipper Chip은 동일한 알고리즘인 Skipjack을 안전하게 보관하고 각 칩은 식별번호(ID)를 가지고 있다. 각 칩을 초기화하기 위해서 보관자 A와 B는 독립적으로 난수를 선택하여 보관한다. 이 난수는 칩 회사에 전해지고 칩 회사는 이 두 개의 난수를 XOR 연산을 수행하여 개별 비밀 번호를 생성한 후 칩의 안전한 장소에 저장한다. 이 초기화가 끝나면 Clipper Chip이 가지고 있는 비밀키는 두 부분으로 나뉘어져 서로 다른 보관자가 보관하게 되므로 각 보관자는 Clipper Chip이 실제 비밀 통신시에 사용하는 비밀키는 알 수 없다. Clipper Chip을 사용하는 두 사용자는 그림 9과 같은 동작 과정을 거치게 된다. 암호통신을 하고자 하는 두 사용자는 우선 세션키 분배 프로토콜을 사용하여 암호 통신에 사용할 세션키 Ks를 공유한다. 암호문을 송신하고자 하는 사용자가 자신의 EES칩에 평문과 공유된 세션키 Ks를 입력하면, EES 칩은 암호문과 암호키 복구를 위한 LEAF(Law Enforcement Access Field)를 생성한다.



〔그림 9〕 Clipper Chip의 동작 과정

Chip 내부에서는 송신자의 메시지를 공통의 세션키로 암호화하고, 법 시행 필드를 만들어 수신자에게 전달함으로써 메시지의 암호화를 수행한다. 수신자의 Chip은 동일한 세션키를 이용하여 암호문을 복호화하게 된다. 법 집행기관은 Clipper Chip에서 생성되는 법 시행필드(LEAF)를 이용하여 사용자의 메시지에 접근할 수 있다.

이 복호화 과정은 법 집행기관이 법원의 승인을 받아 보관자로부터 사용자의 비밀키를 전달받고, Clipper Chip에서 생성되는 법 시행필드(LEAF)를 이용하여 사용자의 메시지를 복원하게 된다. 하지만, Clipper Chip은 SKIPJACK 알고리즘의 비공개, 하드웨어 구현, 사용자의 프라이버시 침해, 다양한 공격 방식 등의 많은 문제점들이 지적되었다.

7. PGP

기업의 요구에 의해 PGP는 ADK(Additional Key Decryption)라는 키 복구 모듈을 제공한다[12]. 기업은 다음의 파일들이나 이메일 메시지와 같은 것들에 기밀성을 제공하길 원할 것이다. PGP에서는 여러개의 공개키를 이용해 파일이나 메시지를 암호화한다. 회사내의 종업원들은 PGP를 이용해 암호화할 때 다른 키들뿐만 아니라 company key를 이용해 암호화한다. 이 company key와 이것의 passphrase는 일반적으로 회사의 security office에 의해 관리된다.

사용자의 공개키는 ADK를 이용할 수 있음을 가르키는 ADK ID를 포함한다.(키의 압축에 의해 생성된 20 바이트 ID) ADK ID는 사용자의 공개키에 post-it을 붙인 것과 같다. ADK ID가 있는 수신자의 공개키를 제공받은 송신자는 이 ADK를 쓸 것인지 아니면 수신자의 공개키만을 이용할 지는 자유이지만 ADK가 의무사용일 경우 송신자는 ADK를 이용해야지만 수신자에게 메시지를 전송할 수 있다.

송신자가 수신자의 요구에 받아들일 경우(ADK를 이용 할 때), 수신자와 ADK의 키 소유자는 메시지를 복원할 수 있다. 수신자가 이 키를 이용해 암호화할 때 지적된 ADK가 사용된다. 수신자의 공개키안에 additional flag는 ADK를 이용한 암호화가 필수적이라는 것을 나타낸다. 종업원은 ADK 없이 자신의 공개키를 이용해 암호화할 수 없다. PGP ADK의 특징은 송신자 및 수신자의 동의가 있어야지 ADK를 사용한다는 것이다. 송신자가 PGP 암호화 과정에서 ADK를 허가해야지만 2개의 키로 암호화된다. PGP의 freeware 버전에는 ADK의 기능이 없지만 commercial 버전에는 이 기능을 가진다.

PGP에서 수신자는 그의 공개키에 첨부된 ADK 정보에 서명하여야 한다. 하지만 PGP 버전 5.5에서 6.5.3까지는 이 서명을 항상 확인하지 않기 때문에 버그가 있다. 이것은 누군가 수신자의 공개키가 인가되지 않는 ADK를 첨부할 수 있다는 것이다. 다음의 시나리오는 인가되지 않은 ADK의 이용을 보여준다.

① A는 PGP 키 서버로부터 B의 공개키를 획득한다. A는 파일 에디터를 이용해 B의 키에 자신의 ADK ID를 첨부하고 ADK의 실행을 의무사항으로 설정한다. 그리고 A는 이것을 다시 키 서버에 등록하고 B의 키는 이것으로 갱신된다. A의 공개키는 이미 같은 키 서버에 있다고 가정한다.

② B는 C의 가게에서 물건을 사길 원한다. 이를 위해 B는 C에서 그의 비자 카드 번호와 최종 요금의 확인을 포함하는 암호화된 이메일을 전송한다.

③ C는 이전에 B와 통신하지 않았다면 B의 공개키를 키 서버로부터 다운 받는다. 하지만 이 키는 A의 의해 조작된 것이다.

④ C는 다운받은 B의 공개키를 이용해 계산된 카드번호 및 기타정보를 암호화해 전송하려 할 것이다. 하지만 C는 ADK가 필요하다는 경고를 받게 되고, C가 commercial 버전을 이용하고 있고 ADK에 친숙하다면 ADK ID에 해당하는 ADK를 키 서버로부터 다운 받는다. 그리고 A의 공개키와 ADK로 메시지는 암호화된다.

⑤ B의 이메일를 모니터하고 있는 A는 이 메시지를 도청할 수 있다. 이 부분을 아주 어려운 부분이지만 실제로 발생할 수 있다.

⑥ A는 B에게 가는 C의 메시지를 자신의 비밀키로 복호하고 여러 가지 지불정보를 알 수 있다.

이러한 인가되지 않은 ADK의 이용을 막기위해 Network Associates(NAI, the company that bought Zimmermann's PGP, Inc.)은 PGP 6.5.8에서부터 ADK ID에 키 소유자의 서명이 없으면 인증된 ADK로 허가하지 않는다. 또한, NAI는 유럽의 한 키 서버(약 1,200,000의 키들)를 대상으로 인가되지 않는 ADK가 존재하는지 테스트하였지만 아직 이러한 키는 발견되지 않았다.

Ⅳ. 키 복구 제품들의 특징 비교

표 1은 제품들의 특징을 비교한 것이다.

〔표 1〕 키 복구 제품들의 특징 비교

	대상 데이터	기술분류	대상 키	특징
Windows 2000	저장	캡슐화	세션키	-OS에 삽입 -단순한 파일 복구용
CMS	통신	위탁	long-term 키	-PKI와의 연동 -logn-term key 위탁 -m of n scheme
IMT -2000	통신	-	세션키	-IMT 2000용 키 복구 모델 -각 모듈에 대한 스팩 필요
Secure Way	통신	캡슐화	세션키	-2단계를 거쳐 위탁
Recovery Key	저장, 통신	캡슐화	세션키	-저장, 통신 데이터 모두 적용
Crypto Backup	저장	캡슐화	세션키	-단순한 파일 복구용
CyKey	저장, 통신	캡슐화	세션키	-저장, 통신 데이터 모두 적용 -제조 인증서, KR authority 이용
Secret Agent	저장, 통신	캡슐화	세션키	-KRO, KRA의 협동에 의해서 세션키 복구
Clipper	통신	위탁	long-term 키	-하드웨어상에서 구현 -두개 기관에 키 위탁
PGP	저장, 통신	캡슐화	세션키	-사용자 공개키에 ADK ID를 추가된 형태

복구되는 데이터의 대상은 크게 저장 데이터와 통신 데이터로 나눌 수 있고 Windows 2000과 Crypto Backup만이 단순한 저장 데이터 복구만을 지원한다. 하지만, 다른 제품들은 통신이나 저장 데이터의 복구를 지원하고 있다. 각 제품들이 이용하고 있는 키 복구의 기반기술은 CMS, Clipper를 제외한 모든 방식들이 캡슐화 방식을 이용하고 있다. 이것은 사용자들의 위탁에 따른 거부감과 위탁방식을 이용함으로써 생길 수 있는 여러 가지 문제점을 고려한 것이라 할 수 있다. 기술 방식에 따라 캡슐화를 기반기술로 채택한 제품들은 세션키를 복구 대상으로 하고 있고 위탁 방식을 이용한 제품들은 long-term 키를 복구 대상으로 하고 있다. CMS는 사용자가 PKI 참여시(인증서 생성시) 서명용 키쌍과 암호화용 키쌍을 생성하고 그 중 암호화용 비밀키를 위탁하는 특징을 가진다. 전체적으로 키 복구 제품들은 PKI와 연동되는 암호 솔루션의 중의 일부 함수로 제공되며 있으며 사용자의 키 유실에 대비한 키 복구의 성격이 강하다.

Ⅴ. 키 복구 제품의 활용 분야

3장에서 살펴본 것과 같이 키 복구 제품 및 키 복구 기능을 포함하고 있는 제품들은 다양한 분야와 기술을 이용해 개발되었고 이용되어 지고 있다. 본 장에서는 각 제품들의 특징 및 기술을 바탕으로 키 복구 제품들의 활용 분야를 알아본다[13][14][15].

표 2는 키 복구 제품들이 이용되는 분야별로 분류한 것이다. 이 중 몇 가지의 제품은 한 분야뿐만 아니라 여러 분야를 지원하고 있으나 주된 목적에 의해 하나로 분류하였다. 키 복구 기능을 가지는 제품들은 다양한 분야에 걸쳐 개발되고 이용되어 지고 있다. 암호의 이용이 기존 PC상의 파일 및 통신 데이터뿐만 아니라 Non-PC상의 mobile이나 wireless분야로 확대되고 있는 상황임으로 키 복구 또한 이러한 암호의 이용확대에 따라 그 중요성과 이용 분야의 확대가 기대된다.

〔표 5-1〕 키 복구 제품들의 이용 분야

		키 복구 제품	
파일용		위탁	-
		캡슐화	Windows2000 CryptoBackup
통신용	데이터 전송용	위탁	CMS Clipper
		캡슐화	SecureWay RecoveryKey CyKey SecretAgent
	e-mail용	위탁	-
		캡슐화	PGP
	mobile용	위탁	IMT-2000
		캡슐화	

지금까지 개발된 키 복구 제품의 활용 분야는 크게 저장 데이터용(파일용)과 통신용으로 나누어진다. 그리고 통신용은 다시 데이터 전송용, e-mail용, 이동 통신용으로 나누어진다. 파일용 제품들을 통해 파일을 안전하게 암/복호화하고 비상시 복구받을 수 있다. 또한 통신용 제품들을 통해 데이터 전송, e-mail등에 대해 유사시 사용자 및 법 집행 기관은 키 복구를 할 수 있다. 하지만 mobile용 IMT-2000 키 복구 모델은 사용자의 입장보다는 법

집행 기관의 키 복구를 중요시하고 있다. 그 이유는 음성 통화의 경우 사용자의 키 복구 요구는 미진할 것이기 때문이다.

키 복구 제품의 가장 큰 기술적 구분은 위탁 방식과 캡슐화 방식으로 구분하는 것이다. 분석된 제품들 중 파일용 키 복구 제품들에는 위탁방식을 이용한 제품이 없는 것으로 조사되었다. 통신용에서는 CMS와 Clipper만이 위탁방식을 이용하고 있는 것으로 조사되었다.

위에서 언급한 키 복구 제품들은 크게 활용분야 및 채용된 기술 방식으로 분류되어질 수 있지만 각각의 제품들은 그들만의 특징을 가진다. 각각의 제품들의 특징 및 활용분야가 상이하다 하더라도 상호호환성을 위해 사용자 인증기술, 전자서명기술, 대칭키/공개키 암/복호화 기술들은 공통의 암호 기술들로 이용되어야 한다. 또한, 국가 암호키 관리 기반구조와의 연계성을 가져야 한다. 공통의 암호 기술 이용은 각각의 제품들이 널리 이용되고 있는 암호 기술들을 이용해 개발하였으므로 상호호환성에 큰 어려움이 없다. 하지만, 각 제품의 특징적인 프로토콜과 그에 따른 데이터 이용 형태로 인해 국가 암호키 관리 기반구조와의 연계성을 가지는 것은 그렇게 쉽지는 않다.

Ⅵ. 결 론

사용자의 키 유실과 정부의 법집행 능력 확보를 위해 여러 가지 방법들이 존재하지만, 실질적으로 이용될 수 있는 방법은 키 복구 방법이다. 이에 따라 키 복구에 대한 많은 기술들이 소개되었고 그 기술들을 포함한 많은 제품들 또한 개발되었다. 본 고에서는 키 복구 기술의 동향 파악을 위해 키 복구 기능을 가지는 제품들과 이동통신상에서 키 복구 모델을 분석하였고 그 특징들과 활용 분야를 살펴보았다.

안전한 암호사용과 국가의 법질서 유지를 위해 키 복구는 꼭 필요한 사항이지만 정부와 사용자들의 요구사항이 아직 접점을 찾지 못하고 있다. 이러한 점을 해결하기 위해 키 복구 기술, 표준, 제품, 정책에 대한 더 많은 연구가 필요할 것이다.

참 고 문 헌

[1] 황보성, 이임영, "키 복구 제품 분석", 한국통신정보보호 학회지, pp633-642, 2000

[2] 이임영, 채승철, "Key recovery 시스템에 관한 고찰", 한국통신정보보호 학회지, 제7권 제4호, pp.45-58, 1997

[3] 이임영, 채승철, "Key recovery 시스템에 관한 고찰II", 한국통신정보보호 학회지, 제8권 제4호, pp.97-112, 1998

[4] Microsoft, "Windows 2000 Server-Encrypting File System for Windows 2000", http://www.microsoft.com, 2000

[5] Netscape, "Administrator's Guide-Netscape Certificate Management System Ver 4.1", http://www.netscape.com, 2000

[6] Cylink, "CyKey : Cylink's Key Recovery Solution", http://www.cylink.com, 1997

[7] 3GPP, "Digital cellular telecommunications system - Lawful Interception(stage 1)", http://www.3gpp.org, 2000

[8] 3GPP, "Digital cellular telecommunications system - Lawful Interception(stage 2)", http://www.3gpp.org, 2000

[9] Michael J. Markowitx and Roger S.Schafly, "Key Reovery in SecretAgent", http://www.isc.com, 1997

[10] Approval of FIPS 185 "Escrowed Encryption Standard(EES)", http://www.epic.org, 1994

[11] 최용락, 소우영, 이재광, 이임영, "통신망 정보보호", 도서출판 그린, 1996

[12] David E. Ross, "PGP:Additional Key Decryption(ADK)", http://www.vcnet.com/rossde, 2000

[13] IBM, "Secure Key Recovery", http://www.ibm.com/security/technologies/techkeyrec.html, 2000

[14] Stephen T.Walker, Steven B. Lipner, Carl M. Ellison and Dvid M. Balenson, "Commercial Key Recovery", Communications of the ACM, Vol.39, pp41-47, 1996

[15] David Paul Maher, "Crypto Backup and Key Escrow", Communications of the ACM, Vol.39, pp48-53, 1996

〈著者紹介〉

황 보 성 (Bo-Sung Hwang)
학생회원

1999년 2월 : 순천향대학교 전산학과 졸업
1999년 3월~2001년 2월 : 순천향대학교 대학원 전산학과 졸업
2001년 1월~현재: 한국정보보호센터 연구원
관심분야 : 암호 이론, 컴퓨터 보안

이 임 영 (Im-Yeong Lee)
정회원

1981년 8월 : 홍익대학교 전자공학과 졸업
1986년 3월 : 오사카대학 통신공학과 석사
1989년 3월 : 오사카대학 통신공학과 박사
1989년 1월~1994년 2월 : 한국전자통신연구원 선임연구원
1994년 3월~현재: 순천향대학교 정보기술공학부 부교수
관심분야 : 암호이론, 정보이론, 컴퓨터 보안

김 지 연 (Kim Jee Yeon)

1995년 2월 : 성균관대학교 정보공학과(학사)
1995년 3월~1997년 2월 : 성균관대학교 대학원 정보공학과(공학석사)
1996년 12월~현재: 한국정보보호센터 연구원
관심분야 : 암호 프로토콜, 암호키관리 기반구조

권 현 조 (Kwon Hyun Jo)

1997년 2월 : 성균관대학교 정보공학과(학사)
1998년 3월~2000년 8월 : 성균관대학교 정보통신대학원(석사)
1997년 1월~1997년 7월 : (주) 나라계전 기술연구소 연구원
1997년 7월~현재: 한국정보보호센터 연구원
관심분야 : 정보보호시스템 평가체계, 암호 프로토콜, 스마트카드, 정보보호 기술 표준화