The Journal of Korean
Institute of CALS/EC
Vol. 7, No. 1, April. 2002

PC상의 암호파일의 안전한 복구를 위한 키복구 시스템의 개발 및 평가

장수진*, 고정호**, 이강수*

Development and Evaluation of Key Recovery System for Secure Recovery of Cryptographic Files in PC

Soo-Jin Jang, Jeong-Ho Ko, Gang-Soo Lee

Abstract

The encryption of a file on a PC before saving can maintain security of the file. However, if the key for the encrypted file is lost or damaged, the encrypted file can not be decrypted, resulting in serious economical loss to the user or the user group. In order to minimize the economical loss a secure and reliable key recovery technology is required. Presented in this paper is the development and evaluation of PKRS (PC based Key Recovery System) which supports encryption and decryption of file and recovery of the encrypted file in emergency. The encapsulating method, which attaches key recovery information to encrypted file, is applied to the PKRS. In addition, the PKRS is developed and evaluated according to the requirements of Requirements for Key Recovery Products proposed by NIST and requirements of Common Criteria 2.0 to prove the safety and reliability of the information security system. This system is applicable to a PC and can be further extended to internet or intranet environment information system where in encryption and recovery of file is possible.

***Key Word** : file encryption, key recovery, security*

* 한남대학교 컴퓨터공학과
** 영진전문대학 컴퓨터정보기술계열

1. 서론

정보화 사회가 발전함에 따라 정보의 가치에 대한 인식이 새로워지고 정보를 보호해야 할 가치로 인정하고 있으며, 초기의 오프라인 형태이던 컴퓨팅 환경이 인터넷의 발전으로 개방화되면서 더 많은 위협을 가지게 되었다. 따라서, 이에 대한 기술적인 측면에서 정보보호의 필요성이 커지게 되었다. 정보보호란 보다 안전하고 신뢰성 있게 정보를 전달할 수 있도록 하는 것으로 암호기술에 그 기반을 두고 있다. 암호기술은 암호 알고리즘을 사용하여 평문을 알아보기 힘든 형태로 변화시키는 방법으로 암호를 수행할 때 사용된 키를 소유한 사람만이 암호문을 해독하여 평문을 얻을 수 있다.

암호의 이러한 속성은 데이터의 노출 위험을 제거한 반면, 사용자의 키가 분실 및 손상되었을 때, 사용자는 암호문을 복호화할 수 없다는 문제가 발생한다. 예를 들어, 어떠한 이유로든 사용자가 키를 갱신했을 때 갱신 이전에 암호화된 암호문을 복호화하는 것이 불가능하게 되며, 문서를 암호화하여 보관해 놓은 직원의 갑작스런 퇴사나 휴가 등의 이유로 문서에 접근할 수 없게 되었을 때 개인 및 기관에 경제적 손실을 초래하게 된다. 이러한 문제를 해결하여 경제적 손실을 최소화하고 안전한 암호 사용을 보장하기 위한 대책이 필요하게 되었으며, 그 대책으로 마련된 기술적 방안이 "키복구 기술"이다[TCKRA, 1997]. 따라서, 개인 PC 상의 저장된 정보의 보호를 위한 파일 암호 시스템에도 유사시에 암호문을 복호화할 수 있는 키복구 기능을 포함하는 것이 필요하다.

본 논문에서는 PC내의 파일 암호 시스템이 유사시(즉, 개인키의 손상)에도 파일의 복구를 지원할 수 있는 PC기반의 키복구 시스템(PKRS ; PC based Key Recovery System)을 개발하였다. 본 시스템은 사용자 시스템(UCS ; User Cryptographic file System)과 키복구 센터(KRC ; Key Recovery Center), 키복구 기관(KRA ; Key Recovery Agent)의 부 시스템으로 구성되며 이들간의 통신으로 키복구가 수행되고, PKI와 연동하여 각 부 시스템을 인증할 수 있도록 구현하였으며, PKRS도 정보보호시스템이므로 정보보호시스템의 평가스킴(ITSEM, CEM)[NIST, 1998 : 이강수, 1998]을 적용하여 개발 및 평가하였다.

논문의 구성은 다음과 같다. 2장에서는 기존의 파일 암호 시스템과 키복구 시스템에 대해서 간략히 기술하며, 3장에서는 PC 기반의 키복구 시스템의 키복구 요구사항과 보안 요구사항을 기술한다. 4장에서는 PKRS의 구조와 파일의 암·복호 및 키복구 프로토콜 설계를 기술하며, 5장에서 시스템의 구현을 기술한다. 6장에서는 PKRS의 보안기능 평가 결과와 기존 시스템과의 비교한 내용을 보이며, 7장에서 결론을 맺는다.

2. 관련 연구

2.1 파일 암호 시스템

파일 암호 시스템은 1996년대 유닉스 운영체제 기반에서 파일 암호를 지원하던 CFS (Cryptographic File System)가 대표적이다. 기존에는 서버 중심의 보안을 제공하던 것이 현재는 개인 PC 보안의 중요성이 부각되면서, 데스크탑을 위한 파일 암호 시스템들도 개발되고 있으며 공개키 기반구조(PKI ; Public

Key Infrastructure)와 연동되는 통합 형태의 파일 암호 시스템들이 개발되고 있다. 파일 암호는 다음과 같이 분류될 수 있다. 본 논문에서 개발한 시스템은 파일 암호 시스템의 부류에 속하며 PKI 기반의 애플리케이션 계층에서 파일 암호를 수행한다.

- **볼륨 암호 시스템** : 디스크 암호 시스템으로, 디스크로부터 송·수신된 데이터의 암·복호를 위하여 디바이스 드라이버 계층을 사용하는 것이 가능하다. 볼륨 암호 시스템에는 Network Associates의 PGP Disk, 오클랜드 대학의 Perter Gutmann의 SFS, Alexander Tormasov의 TorDisk 등이 있으며, 이것은 전체 디스크 볼륨을 보호하기에는 편리하지만 디렉토리나 파일 단위의 개별적인 접근 제어가 불가능하다[Peter, 1996].
- **파일 암호 시스템** : 단대단 암호를 획득하기 위하여 암호를 표현 계층이나 애플리케이션 계층에서 실행할 수 있도록 애플리케이션 암호를 제공한다. 파일 암호 시스템에는 기존의 Phil Zimerman의 PGP와 최근의 Baltimore Technology의 SecureFile, Nova-Stor의 DataSAFE, IBM의 PC Data Protection, 안철수 컴퓨터바이러스 연구소의 앤디Pro, 지란지교의 FileSafe 2.0 등이 있다. 이것은 애플리케이션 계층에서 파일 암호를 수행하는 것으로써, 보안이 네트웍에 접근하는 데이터에만 요구되던 때에는, 사용의 불편함과 고유의 위험 요소(예, 사용자의 실수)로 인해 많이 사용되지 않았다. 그러나 최근에 인터넷의 사용 증가로 인한 컴퓨터 환경의 변화로 개인 및 기업 컴퓨터의 보안 요구가 증대되고, PKI를 기반으로한 암호 애플리케이션이 개발되면서 많은 업체에서 개별적인 형태 또는 다른 시스템과의 통합적인 형태로 개발되고 있다[Novastor, 2000].
- **파일 시스템 암호** : 이것은 주로 네트웍상의 파일 시스템으로 원격 접근에 대한 보안에 초점을 둔다. 애플리케이션 계층에서 파일 암호의 불편함과 위험 요소(사용자의 실수 등)를 제거하기 위해 파일 시스템 자체에 암호 서비스를 추가한 형태이다. 애플리케이션 계층의 파일 암호 시스템과는 달리, 장기간 암호파일을 저장하며 다중 사용자에게 적합하다는 장점이 있다. 예로는 AT&T의 CFS, Salerno 대학의 TCFS, Microsoft의 EFS 등이 있다[Blaze, 1993 : TCFS, 2000 : Shamir, 1979 : Microsoft, 2001].

2.2 키복구 시스템

키복구 시스템은 미국에서 1993년 '클리퍼 칩'이라는 키 위탁 프로젝트에서 시작되었으며 이후 키 위탁의 프라이버시 침해라는 문제가 대두되었다. 이에 대한 대안으로 나온 것이 키복구인데, 키복구는 키 위탁과는 달리 제삼자에게 모든 정보를 제공하지 않기 때문에 안전하다고 볼 수 있다. 1997년 키복구 동맹(KRA ; Key Recovery Alliance)이 결성되었고, 이들의 연구에 의해서 1999년 키복구 요구사항 문서가 발행되었다[TCKRA, 1997 : 유준석, 2000].

현재까지 제안된 암호키 관리 방식은 크게 위탁(escrow) 방식과 캡슐화(encapsulation) 방식, TTP(Trusted Third Party) 방식으로 나눌 수 있다.

- **키 위탁**(Key escrow, 예 ; 클리퍼 칩이나 위탁 암호 표준[채승철, 1999 : Dorothy, 1996 : Escrow, 1996 : Jingmin,1995 : Lee,

1997]) : 사용자 비밀키의 전부 또는 일부를 신뢰받는 제삼자에게 위탁하는 방식으로 유사시에 키를 확실하게 얻을 수 있다는 장점이 있는 반면에 키를 위탁하는 제삼자의 신뢰도에 많은 영향을 받는다.

- **키 캡슐화**(Key encapsulation, 예 ; TIS RecoveryKey[Stephen, 1996], CyKey [Mark -owitz, 1997], SecretAgent[Cylink, 1998], IBM SKR[Gennaro, 1999]) : 각각의 메시지 전송 또는 파일 저장시마다 키복구 필드를 생성해서 해당 메시지를 복구할 수 있는 정보를 데이터에 부가하는 방식으로 실제적인 키 위탁은 일어나지 않는다는 장점이 있다. 이 방식에서는 유사시에 키의 복구가 필요한 경우 사용자의 비밀키가 아닌 복구 기관 자신의 비밀키를 이용해서 키복구 필드를 복호화한 후 세션키를 얻을 수 있다. 이 방식의 문제점은 복구 필드의 생성이 대부분 사용자 측(사용자의 암호화 제품 등)에서 일어나게 되므로, 제품을 조작하거나 수신자와 공모한다면 복구 필드의 수정과 조작이 다른 방식에 비해 쉽다는 점이다. 따라서 필요시에 키를 복구할 수 있는 확실성이 저하될 수 있다.
- **신뢰된 제삼자**(Trusted Third Party, 예 ; Yaksha system [Ravi, 1996 : Jefferies, 1995], ANSI X9.17[NIST, 1992]) : 영국의 Royal Holloway 대학에서 개발된 방식으로 위탁방식의 변형이다. 이 방식에서는 키를 사용자가 생성해서 위탁하는 것이 아니라, 위탁 기관이 생성한 후에 사용자에게 알려주는 방식이다. 그러므로, 사용자는 암호 서비스를 사용하기 위해 항상 서버에 접속해서 작업을 수행하고, 서버는 사용자의 작업마다 필요한 키를 생성해 주어야 한다.

키위탁 방식과 TTP방식은 트랜잭션 오버헤드와 대량의 메모리를 요구하므로 정보시스템상의 병목이 될 수 있으며, 키 캡슐화 방법에서는 키의 소유자가 키복구의 권한을 가지므로 개인 비밀의 침해로부터 비교적 자유롭고 다른 방법에 비해 많은 장점을 가진다.

"키복구 시스템"은 복호화 키를 사용할 수 없는 경우에 정당한 권한이 있는 사람으로 하여금 암호화 데이터에서 평문을 복호화할 수 있도록 하는 시스템으로 '키복구'라는 용어는 다양한 키복구 기술에 광범위하게 적용 될 수 있다[유희종, 2000]. 본 논문에서는 복구의 목적인 키 즉, 사용자가 파일을 암호화한 키(이하 세션키)를 복호화할 수 없을 때를 대비하여 키복구 정보(KRI ; Key Recovery Information)를 생성하여 암호파일에 첨부하므로 신뢰기관에 개인의 정보를 위탁할 필요가 없는 키 캡슐화 방식을 사용하였으며, 키복구시 키복구 정보에 대응되는 인증정보(공개키 인증서)와 함께 해당 키복구 정보를 키복구 기관에 전송하며 키복구 기관은 인증절차에 따라 검증한 후에 세션키를 복구하여 그 세션키를 사용자의 공개키로 암호화하여 전송하므로 사용자가 파일을 안전하게 복구할 수 있는 키복구 시스템을 제안한다.

키복구를 위해서는 다수의 키복구 기관이 참여하며 사용자가 모든 키복구 기관들 중에 몇 개(기관의 수는 정책에 따라 결정)를 임의로 선택하는 새로운 기능을 추가하였으며, 이것은 키복구 기관들이 모두 공모하지 않는 한 세션키 정보를 노출시킬 수 없다는 장점을 가진다. 또한 캡슐화 방식의 단점인 키복구 정보의 변조가능성을 해결하기 위하여 키복구 정보의 해쉬값을 키복구 정보와 함께 암호화하므로 키복구 정보의 무결성 기능을 추가하였다.

3. 키복구 시스템의 요구사항

3.1 키복구 요구사항

NIST에서 제정한 키복구 제품의 요구사항에 관한 표준안인 RKRP(Requirements for Key Recovery Products)는 키복구 구성요소를 위한 요구사항들을 명세하였으며, 이들 구성요소들은 암호문으로 저장되거나 통신하기 위한 암호키를 사용할 수 없을 때 암호화에 사용되는 키의 복구를 제공한다. 키복구 제품 요구사항은 모두 208가지의 항목으로 구성되며 다음과 같이 분류될 수 있다[유희종, 2000 : RKRP, 1998].

- **기능 요구사항(요구사항 5 ~ 24)**
  - 키복구 시스템의 동작에 필수적인 기능적 요구사항 제시
- **보안 요구사항(요구사항 25 ~ 174)**
  - 각 키복구 시스템 기능에 대해 적용
  - 암호 알고리즘의 강도, 감사 사항 등에 대한 요구사항
  - 세 개의 레벨로 분류(level 0, level 1, level2)
- **보안 확신 요구사항(요구사항 175 ~ 208)**
  - 키복구 시스템 기능을 구현하는 데 적용되는 요구사항(level A, level B, level C)
  - 제품의 구성, 배달, 작동법, 안내문서 등에 관한 사항으로 구성
- **기타 요구사항(요구사항 1 ~ 4)**
  - 다른 키복구 기술간의 상호 운용에 대한 요구사항 및 키복구 시스템에 대한 일반적 요구사항 제시

본 시스템에서는 적용한 키복구 시스템의 기능 요구사항은 다음과 같다. 제안한 시스템의 각 기능에 적용된 키복구 기능 요구사항들을 키복구 시스템의 기능별로 분류하여 기술하였으며 내용은 다음과 같다.

(1) 키복구 정보 생성(KRI Generation) 기능

- 키복구 정보 생성 기능의 각 객체는 KRI의 부분 또는 모두를 생성해야 하고 모든 KRI 생성 기능은 키복구를 위해 충분한 KRI를 생성해야 한다.
- KRI 생성 기능의 한 객체는 다른 키복구 기능이 사용할 KRI의 일부 또는 전부를 암호문과 연관시킬 수 있도록 조립, 구성해야 한다.
- KRI 생성 기능은 출력의 유효성을 보장해야 한다.
- KRI 생성 기능은 생성된 KRI를 KRI 전달 기능에 제공해야 한다.
- KRI 생성 기능은 둘 이상의 KRA로 TKI를 나눈다.

(2) 키복구 정보 전달(KRI Delivery) 기능

- KRI 전달 기능은 저장된 암호문에 대응하는 KRI를 지속적으로 사용할 수 있도록 저장해야 한다.
- KRI 전달 기능은 KRI가 KRR 기능이나 KRA, 또는 양쪽 모두에서 이용될 수 있도록 (KRI를 KRR이나 KRA에게 전송하거나 그들이 접근할 수 있는 곳에 둠) 해야 한다.
- KRI 전달 기능은 KRI가 KRI 검증 기능에서 이용될 수 있도록(통신 채널이나 저장 장치를 통해) 해야한다.

(3) 키복구 정보 검증(KRI Validation) 기능

- KRI 검증 기능은 활성화(turn on) 또는 비활성화(turn off) 될 수 있어야 한다.
- KRI 검증 기능은 검증 기능이 활성화 되어 있는 상태에서 유효성 검사가 실패하면 암호

단말 장치에서 평문으로의 접근은 거부되어야 한다.

(4) 키복구 요청(Key Recovery Requestor) 기능

- KRR 기능은 주어진 KRI에 대해 하나 이상의 KRA 기능들과 상호 작용함으로써 target key를 복구할 수 있어야 한다.
- KRR 기능이 전송하는 암호화 데이터는 복구 가능해야 한다.

(5) 키복구 에이전트(Key Recovery Agent) 기능

- KRA 기능은 target key 복구 시 필요한 키, 키 요소 또는 다른 정보를 저장한다.
- KRA 기능을 작동시키기 위해 필요한 모든 정보와 KRA 기능을 사용하는 모든 암호 모듈은 가용성을 위해 안전하게 복사되어야 한다.
- KRR 기능이 제공하는 KRI를 처리하여 요청자가 얻은 데이터를 복호하는데 필요한 부분 또는 모든 정보를 보내야 한다.
- KRA 기능이 전송하는 암호화 데이터는 복구 가능해야 한다.

3.2 보안 요구사항

본 논문에서는 국제공통 평가기준인 CC 2.0 [NIST, 1998]을 기반으로 정보보호시스템의 평가와 인증 맥락에서 PKRS의 보안 요구사항을 분석하였다. 보안 요구사항이란 정보보호시스템이 행해야 할 기능과 그 기능의 보증 수준이며, 시스템 개발시 요구사항 명세서 및 보안목표 명세서 상에 포함되어야 한다. 보안 요구사항은 정보보호시스템이 설치되어, 방어해야 할 어떤 시스템의 보안 정책, 보안 목적 및 이들에게 가해질 수 있는 각종 보안 위협을 분석하므로 얻어질 수 있으며, 보안목적 및 보안기능은 시스템내의 파일을 각종 위협으로부터 보호하기 위한 것이다. 보안목적이란 각종 위협을 고려하여 시스템이 추구하는 보안 관련 목적을 의미하고, 하나의 보안목적은 하나 이상의 위협을 대처하기 위한 것이며, 보안기능 요구사항은 보안목적을 달성하기 위한 정보보호관련 대책 또는 기능이라 할 수 있다.

PKRS 역시 정보보호시스템의 유형이므로, CC의 평가방법론을 적용하여 <표 1>에서는 PKRS의 보안위협과 보안목적을 보이며, <표 2>에서는 보안기능 요구사항을 보인다. 특히, 보안기능 요구사항은 CC 2.0의 보안기능 요구사항들 중에서 본 시스템에서 필요로 하는 기능들을 선택한 것이며 이에 대한 평가는 6장에서 기술하였다.

4. PC 기반의 키복구 시스템의 설계

4.1 PC 기반의 키복구 시스템의 구조

PKRS는 사용자가 파일의 암·복호 및 키복구 요청시 사용하는 사용자 암호 시스템(UCS ; User Cryptographic System)과 전체 세션키를 복구해주는 키복구 센터(KRC ; Key Recovery Center), 부분 세션키를 복구해주는 키복구 기관(KRA ; Key Recovery Agent)들의 부 시스템으로 구성되도록 제안하였으며, 사용자는 UCS를 사용하여 KRC와 KRA들과 상호 연동하여 키복구를 수행한다.

PKRS의 전체 구조는 <그림 1>과 같으며, 본 시스템은 다음과 같은 표준에 근거하여 설계 및 구현하였다. 첫째, 국제공통평가기준인

<표 1> PKRS의 보안위협과 보안목적

T1 : 보안 데이터의 불법적인 수정 및 노출	O1 : 인가된 접근
T2 : 보안 사건 기록의 파괴 및 장치 결함 발생	O2 : 보안감사
T3 : 기밀 데이터, 키, 감사자료에 대한 수정 및 삭제	O3 : 시스템관련 행동결과 보증
T4 : 시험되지 않은 암호 알고리즘의 사용	O4 : 기밀성 메커니즘 제공
T5 : 기밀 데이터, 키, 감사자료의 노출로 불법적인 접근 시도	O5 : 암호연산을 위한 모듈
T6 : 키에 대한 노출	O6 : 잔여 정보의 안전한 삭제
T7 : 악의적인 관리자의 시스템 환경 수정	O7 : 식별 및 인증
T8 : 악의적인 사용자에 의한 정보 삭제 및 노출	O8 : 무결성 메커니즘 제공
T9 : 인가된 사용자로 가장한 행동	O9 : 키복구정보의 생성 및 유지
T10 : 보안기능을 손상시키는 잘못된 데이터 삽입	O10 : 기밀 데이터의 누출 방지
T11 : 악의적인 KRA에 의한 키 공개	O11 : 키관리
T12 : 키복구정보의 생성 및 유지 실패	O12 : 보안정책 우회침투 방지
T13 : 키의 불법적인 수정	O13 : 키복구 증거생성 및 사용자 식별 메커니즘 제공
T14 : 검증된 인증 데이터를 재사용	O14 : 독립된 도메인 유지
T15 : 데이터 공간의 반복적인 탐색	
T16 : 시스템의 불법 접근	
T17 : 시스템 자원을 손상시켜 탐지되지 않는 행동	

<표 2> PKRS의 보안기능 요구사항

FAU_GEN.1~2	: 보안감사 데이터 생성 및 사용자 신분연관	FIA_ATD.1	: 사용자 속성 정의
FAU_SAR.1~2	: 보안감사 검토	FIA_SOS.1	: 비밀 정보의 검증
FAU_STG.1	: 감사 추적 데이터 보호	FIA_SOS.2	: 비밀 정보의 생성
FCS_CKM.1~4	: 암호키 관리	FIA_UAU.1~7	: 사용자 인증 : 인증시기, 모든 행동이전의 사용자인증, 인증 무결성, 일회용 및 다중 인증 메커니즘, 재인증, 안전한 인증 피드백
FCS_COP.1	: 암호 연산		
FDP_ACC.1	: 부분적인 접근통제	FIA_UID.1~2	: 식별 시기
FDP_ACF.1	: 보안속성 기반 접근통제	FIA_USB.1	: 사용자-주체 연결
FDP_DAU.1	: 보증인 신분을 포함한 데이터 인증	FPT_TDC.1	: 키복구 정보 복구
FDP_RIP.1	: 부분적인 잔여 정보보호	FTA_TAB.1	: 디폴트 시스템 접근경고
FDP_SDI.1	: 저장된 데이터의 무결성 감시	FTA_TAH.1	: 시스템 접근이력
FIA_AFL.1	: 인증 실패 처리	FPT_SEP.1	: 영역 분리

(주) FAU(Security audit) : 보안감사, FCS(Cryptographic support) : 암호지원, FDP(User data protection) : 사용자 데이터 보호, FIA(Identification & authentication) : 식별 및 인증, FPT(Protection of the PKRS security functions) : PKRS 보안기능의 보호, FTA(PKRS access) : PKRS 접근

CC V2.0 [NIST, 1998]을 따랐으며 CC는 1999년 ISO/IEC 15408 국제표준으로 채택된 국제 공통평가기준으로써 정보보호시스템에 대한 보안기능과 보증 요구사항에 관한 개발 및 평가 지침서이다. 둘째, 암호표준인 FIPS PUBs [FIPS Pub.,2001], 셋째, 공개키 암호화를 위해

RSA에서 제안한 PKCS[RSA Data Security, 1991], 넷체, NIST에서 제안된 키복구 시스템의 요구사항을 규정한 RKRP[RKRP, 1998] 등의 표준을 따르고 있다.

<그림 1> PKRS의 프레임워크

이와 같이 입증된 보안 표준에 근거하여 사용자에게 기밀성, 무결성, 식별 및 인증, 접근제어, 보안 감사와 같은 보안 서비스를 제공하여 준다. 주요 기능으로는 키복구, 파일 보안, 감사, 인증, 키 관리 등의 기능들이며 내용은 다음과 같다.

- 키복구 기능 : 이 기능은 키복구 정보(KRI ; Key Recovery Information)의 생성 및 관리, 복구 기능을 수행한다. KRI 관리 기능은 다시 KRI 전달과 검증 기능으로, KRI 복구 기능은 키복구 요청과 수행 기능으로 세분화된다.
- 파일 보안 기능 : 이 기능은 파일 암호 및 복호, 관리 기능을 수행한다. 키 관리 기능으로부터 랜덤하게 생성된 세션키와 사용자의 공개키를 전달받아 평문의 암호화를 수행하며, 복호시 사용자가 제공한 개인키에 의해 복호화를 수행한다. 파일 관리 기능은 암호화된 파일의 저장과 이것의 반환 등의 파일 관리를 수행한다.
- 키 관리 기능 : 키 관리 기능은 파일 암호화를 위한 세션키 생성과 사용자의 개인키/공개키 쌍을 생성하기 위한 키 생성 기능, 생성된 키를 안전하게 취소하고 삭제하는 키 취소/삭제 기능 그리고 키 저장 기능과 키 전달 기능을 수행한다. 키의 보관은 보안정책에 따라 특정한 하드웨어에 보관이 가능하다.
- 인증 기능 : 인증 기능은 인가된 사용자에게 인가된 데이터 접근을 허가하기 위한 주체 확인 및 식별에 의한 접근 제어를 수행하게 된다. 사용자는 패스워드와 개인키 입력을 요구받으며, 시스템은 입력된 값으로 사용자 인증과 패스워드 인증을 수행하게 된다.
- 감사 기능 : 감사 기능은 사용자의 행동에 대한 활동을 기록하여 기록된 자료와 활동의 연결 및 증거를 생성하여 책임성을 제공한다. 감사 관리는 감사 기록에 대한 조회 및 침입에 대한 탐지를 분석하게 된다.

4.2 PKRS의 파일 암·복호 수행과정

파일을 암·복호화하기 전에 먼저 UCS는 PKI와 연동하기 위하여 키쌍을 생성한 후 인증기관(CA ; Certification Authority)에게 공개키를 등록하여 CA로부터 공개키 인증서를 발급 받고 KRC 및 KRA들의 인증서를 전송받아 <표 3>과 같이 시스템 초기화를 수행하므로 다음과 같은 파일 암·복호화를 수행할 수 있게 된다. 이러한 파일 암·복호화 과정은 사용자의 키 손실이 없다면 KRC와 KRA들의

연동이 전혀 필요 없으며 UCS 내에서만 수행이 가능하다.

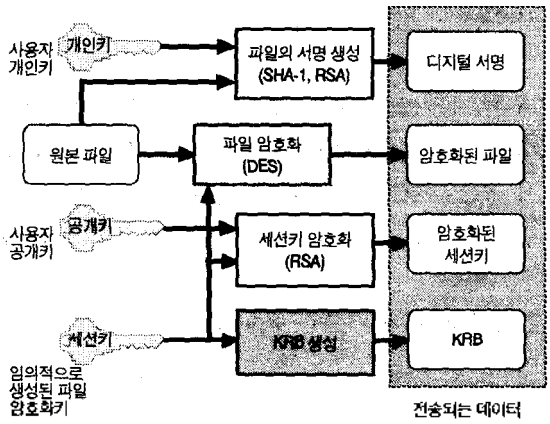
<표 3> 시스템 초기 설정 인증서

UCS	KRC	[illegible]
자신의 인증서 KRC의 인증서 KRA들의 인증서	자신의 인증서 KRA들의 인증서	자신의 인증서 KRC의 인증서

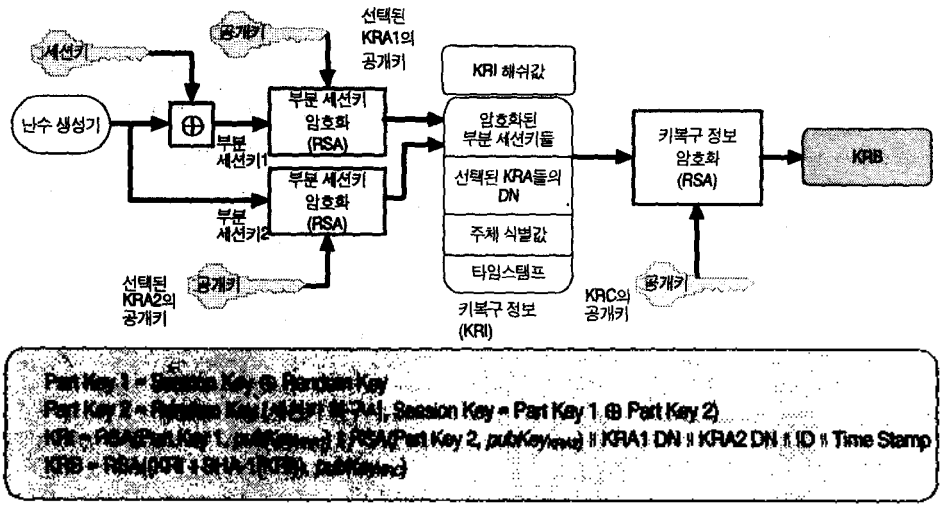
● **파일 암호화 과정**

PKRS에서 파일을 암호화하는 과정은 다음과 같이 수행된다.

먼저, 파일의 기밀성을 제공하기 위해 난수 발생기를 이용해 세션키를 생성한 후 <그림 2>와 같이 세션키로 파일을 암호화하고 세션키의 안전한 보관(혹은 전달)을 위해 사용자의 공개키로 세션키를 암호화한다. 파일의 주체 인증 및 무결성을 제공하기 위해 파일에 서명하여 디지털 서명을 생성한다. 그리고 키복구 기능을 지원하기 위하여 키복구 블록(KRB ; Key Recovery Block)을 생성하여 암호화된 파일과 함께 저장하는 키 캡슐화 방법을 사용하였다. 저장되는 암호파일은 디지털 서명과 암호화된 파일, 암호화된 세션키, KRB를 함께 파일의 형태로 저장한다.



<그림 2> PKRS의 파일 암호화 과정



<그림 3> 키복구 블록 생성과정

● 키복구 블록(KRB) 생성과정

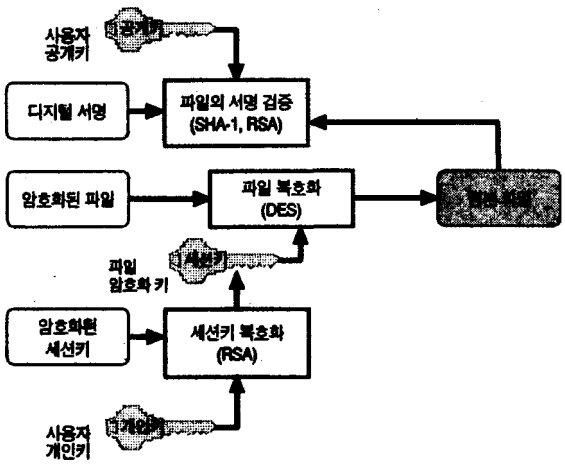
키복구의 대상은 파일을 암호화한 키인 세션키이며, KRB는 세션키 복구를 위한 정보로서 암호파일과 함께 저장되며 KRB의 생성과정은 <그림 3>과 같다.

UCS는 각 세션(즉, 파일 암호)마다 등록된 모든 KRA들 중에서 몇 개를 임의로 지정하여 사용한다. KRA의 수는 정책에 따라 달라질 수 있으며 본 논문에서는 n개의 KRA 중에 2개를 비밀리에 지정하도록 가정하였으며 이에 대한 정보를 KRI에 삽입한다. 세션키는 난수와 XOR 연산으로 부분 세션키들로 분할되며 선택된 KRA의 공개키로 암호화하여 KRI에 추가한다.

KRI의 내용은 두 개의 암호화된 부분 세션키와 선택된 KRA들의 식별값, 주체 식별값(인증서의 subjectUniqueID), 타임스탬프 등을 포함한다. 주체 식별값은 파일의 소유자를 식별하는 값으로 키복구 요청시 요청한 사람이 파일의 소유자인지를 확인하는 값(예 ; 주민등록번호)으로 사용된다. 그런데 KRI가 공격자에게 노출되어, KRI를 변경할 수 있다면 암호파일을 습득한 공격자는 누구나 키복구를 요청하여 평문에 접근할 수 있게 된다. 그러므로 본 시스템에서는 KRI의 변조가능성을 해결하기 위해 해쉬 함수를 이용하여 KRI의 해쉬값을 생성하여 KRI와 함께 KRC의 공개키로 암호화하여 KRB를 생성한다.

● 파일 복호화 과정

파일을 복호화하는 과정은 <그림 4>와 같이 수행된다. 먼저, 암호화된 세션키를 사용자의 개인키로 복호화하여 세션키를 획득하고, 세션키를 이용하여 암호화된 파일을 복호화하여 원본 파일을 획득하게 된다. 그리고 사용자의 공개키를이용하여 디지털 서명을 복호화하고 복호된 파일의 해쉬값을 생성하여 파일의 서명을 검증하므로 파일 복호화를 수행한다.

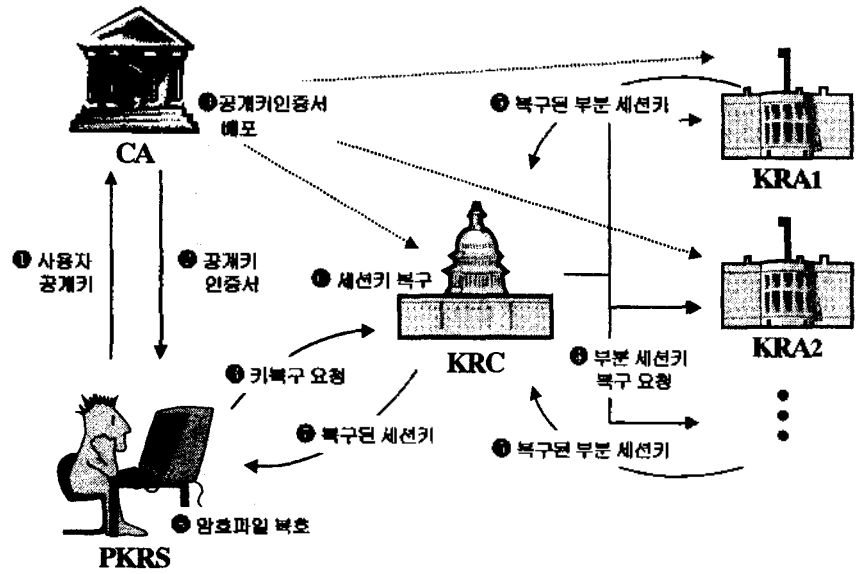


<그림 4> 파일 복호화 과정

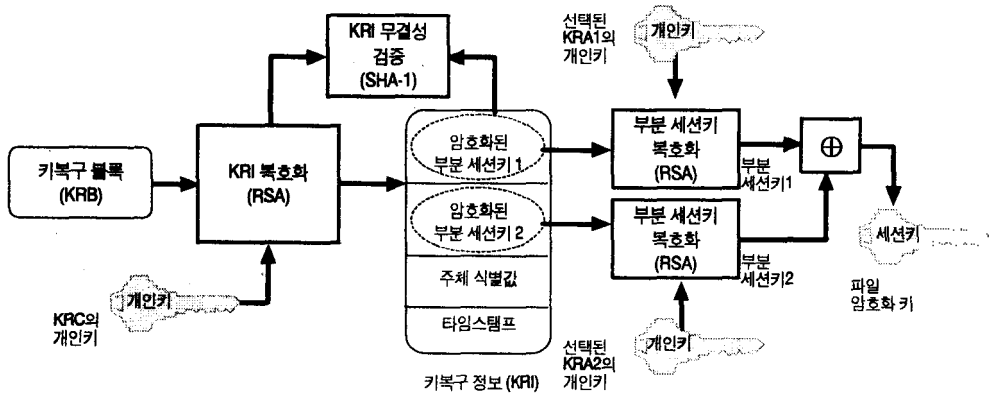
4.3 PKRS의 키복구 수행과정

사용자 개인키의 손상이나 유실, 갱신으로 인하여 암호화된 파일을 복호화할 수 없을 때, 키복구 기능을 수행하게 되며 <그림 5>와 같은 수행과정을 거쳐 세션키를 복구하여 암호파일을 복호화하게 된다. 이때, 각 부 시스템들 사이의 통신은 모두 암호화하여 안전하게 전송되며 키복구 프로토콜 내용은 다음과 같다.

(1) 키복구를 수행하기 전에 KRC와 KRA들이 PKI와 연동하여 서비스를 수행하기 위하여 CA로부터 인증서를 ⓪과 같이 발급 받아 초기화를 수행하여 키복구 서비스를 지원한다. 전체 KRA의 수는 보안정책에 따라 정해지며 그 중 2개의 KRA를 각 세션(즉, 파일 암호)마다 임의적으로 비밀리에 지정하



<그림 5> PKRS의 키복구 수행과정



<그림 6> 세션키 복구 과정

여 KRI내에 이에 대한 정보를 삽입한다. 이로써, 파일의 노출시 사용된 키복구 기관의 정보를 알 수 없도록 하며 부 시스템들 간의 공모공격 가능성을 줄일 수 있다.

(2) 먼저 사용자는 ①과 ②를 통하여 CA로부터 새로운 인증서를 발급 받아 UCS의 초기화를 수행한다.

(3) 키복구 요청을 위해 복구할 파일에 해당하는 KRB를 포함하며 사용자의 서명이 첨부된 키복구 요청서와 사용자의 인증서를 함

께 KRC에게 전송하므로 ③과 같이 키복구 요청을 수행한다.

(4) KRC는 사용자의 인증서에 대하여 CA의 서명을 확인하고 사용자 공개키를 추출하여 키복구 요청서의 서명을 검증하므로 사용자 인증을 수행한다. 그리고 KRB를 KRC의 개인키로 복호화하여 KRI의 무결성 검증과 KRI의 소유자 검증을 수행한 후 암호화된 부분 세션키들을 ④와 같이 각각의 KRA에게 부분 세션키 복구를 요청한다.

(5) 각각의 KRA들은 부분 세션키를 복호화하여 KRC의 공개키로 암호화하여 KRC에게 ⑤와 같이 전송한다.

(6) ⑥에서 KRC는 복구된 세션키들을 모두 수신하여 세션키를 <그림 6>과 같이 복구한 후 복구된 세션키를 사용자의 공개키로 암호화하여 ⑦과 같이 전송한다.

(7) UCS는 복구된 세션키 정보를 사용자의 개인키로 복호화하여 ⑧과 같이 암호파일을 복호화하게 된다.

5. PKRS의 구현

5.1 구현환경

PKRS는 CPU 800MHz, 메모리 128M의 PentiumIII(Windows 2000)으로 구현하였으며, 구현도구로는 JBuilder 3.0과 JDK 1.2.2 컴파일러를 사용하였다. DES와 RSA, DSA, SHA-1, MD5 등의 암호 알고리즘을 구현하기 위한 API로는 Java Security API인 DSTC (Distributed Systems Technology Centre)의 JCSI(Java Crypto and Security Implementation) V1.0[JCSI, 2000]을 이용하여 개발하였다. 또한 PKRS는 Java로 구현하여 높은 호환성을 가지며, PC(Windows95/98/2000/NT)기반에서 저장된 파일의 암·복호 및 복구가 가능하도록 구현하였다.

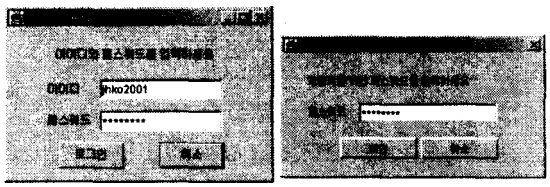
5.2 구현 결과

<그림 7>은 구현된 PKRS의 사용자 인터페이스이다. (a)는 시스템의 접근통제를 위해 사용자의 ID와 패스워드를 입력받는 화면과 개인키 사용을 위한 패스워드 입력 화면이다. 사용자의 개인키는 파일을 암·복호시에 서명 및 세션키 복호를 위해 반드시 요구되므로 개인키 사용을 위한 패스워드 입력 화면이 필요하다. (b)는 보안정책을 설정하는 화면으로 암호 알고리즘과 키 크기, 그리고 키복구 여부를 설정할 수 있다. (c)는 다중 파일을 동시에 처리할 수 있는 화면으로 사용자는 파일 암·복호 기능을 수행하고 유사시 파일 복구를 요청하는 기능을 수행한다. (d)는 KRC에서 수행할 수 있는 감사로그 조회 화면으로서 시스템의 접근상황과 파일 복구의 이력을 볼 수 있으며, 이력파일로 보관하는 것이 가능하다.

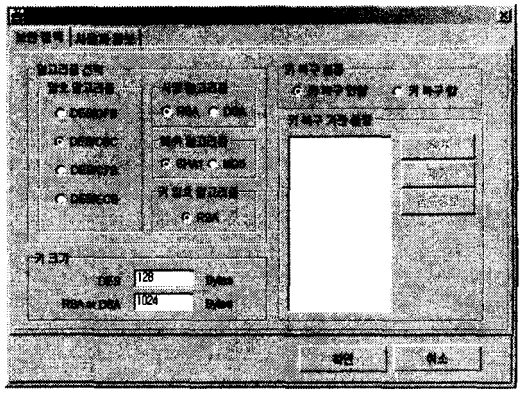
6. PKRS의 평가

6.1 보안 기능 평가

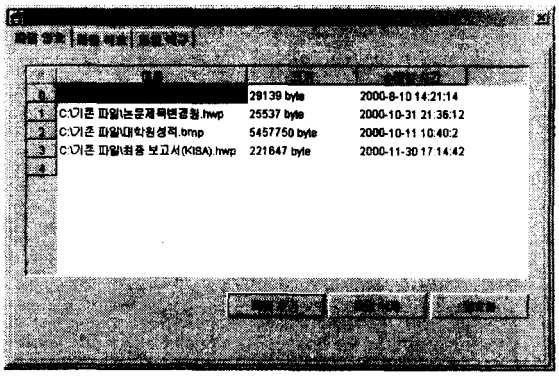
보안 기능 평가란 개발된 시스템이 키복구 가능한 파일 암호 시스템의 보안 요구사항 명세대로 올바른 기능을 수행하며 이 기능들의 보장성을 평가하는 것이다[이강수, 1998]. 3.2절에서 주어진 보안 요구사항(즉, 보안위협,



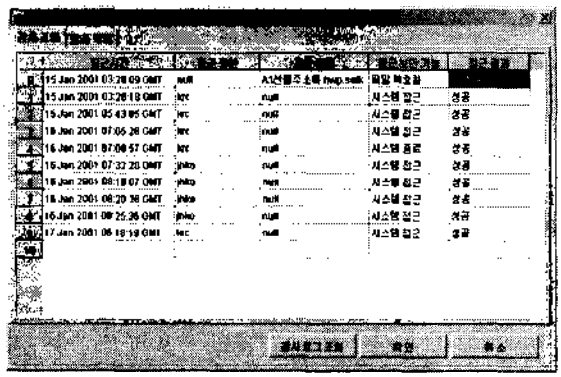
(a) 사용자 로그온 및 패스워드 입력 화면



(b) 보안정책 설정 화면



(c) 파일 암·복호 및 복구 화면



(d) 감사로그 조회 화면

<그림 7> PKRS의 사용자 인터페이스 구현

보안목적, 보안기능)에 대해, <표 4>에서는 키복구와 관련된 보안위협들과 보안목적(<표 1>을 참조)들간의 대응성, <표 5>에서 보안목적들과 보안기능들간의 대응성 그리고, <표 6>에서는 제시된 보안기능 요구사항들을 PKRS에서 어떻게 대응되고 있는지를 보이므로 이것은 국제공통평가기준인 CC 2.0의 평가스킴에 따라 평가한 결과를 보인 것이다.

<표 4> 보안목적과 보안위협간의 대응성

	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17
O1																O	
O2	O	O					O	O									O
O3	O																
O4					O												
O5				O													
O6																O	
O7									O					O			
O8			O														
O9												O					
O10											O						
O11						O							O				
O12																O	
O13									O								
O14										O							

<표 5> 보안목적과 CC 2.0의 보안기능간의 대응성

O1	O	O				O	O		O		O	O			O		O		O	O	
O2	O	O	O														O				
O3	O		O																		
O4				O	O	O	O	O	O					O							
O5				O	O																
O6				O					O												
O7								O			O	O	O	O	O	O	O				
O8			O	O	O	O	O			O			O								
O9					O			O		O								O			
O10	O					O	O														
O11				O																	
O12	O		O			O		O	O		O		O	O	O						
O13	O							O									O				
O14																					O

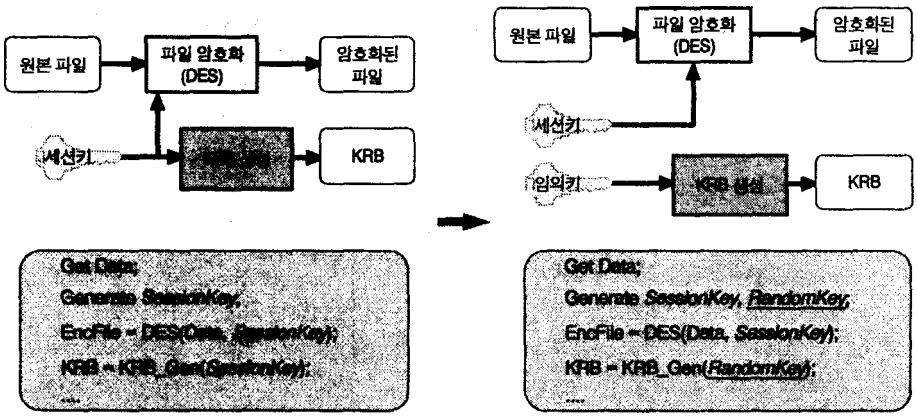
<표 6> CC 2.0의 보안기능 요구사항과 PKRS 모듈간의 대응성

보안감사 모듈	O	O	O																		
암호 모듈					O																
키 관리 모듈				O																	
접근통제 모듈						O	O												O	O	O
식별·인증 모듈											O	O			O	O	O				
데이터보호 모듈								O	O	O			O	O							
키복구 모듈								O		O			O	O				O			

6.2 PKRS의 취약성 분석

본 시스템은 키 캡슐화 방식을 사용하므로 복구 필드의 수정이나 조작할 수 있는 취약성[Kim, 1999]을 가진다. 즉, <그림 8>과 같이 세션키 대신 임의키로 KRB를 생성(여기서, SessionKey≠RandomKey)시, 암호화된 파일(EncFile)을 복호화할 수 없다는 것이다. 이와 같은 취약성에 대한 공격방법은 소스코드를 변경하는 방법이 있을 수 있다. <그림 8>과 같이 원래의 소스코드를 공격자는 임의키를 생성하여 KRB를 생성하도록 변경해야만 한다.

이러한 암호파일 생성시 KRB의 공격을 위해서는 소스코드의 변경 또는 명령어 추가가 필요하다. 그러나, 사용자(공격자)에게 배포되는 것은 자바코드가 아니라 바이너리코드이므로 소스코드의 변경은 어려우며, 소스코드의 변경여부(즉, 무결성)를 확인하기 위해 배포된 코드를 해쉬함으로써 무결성을 확인할 수 있다. 배포코드에 대한 무결성 체크는 본 시스템의 범위를 벗어나며 배포된 코드는 무결성이 보장된다는 가정이 필요하다. 이 문제(즉, 소스코드의 변경을 통한 공격)는 모든 정보보호시스템에서도 유사하게 적용되는 것이다. 또한 이미 생성되어 있는 암호파일의 KRB를 수정하려고 시도한다면 KRB의 복호화가 불가피하



(주) SessionKey : 세션키, RandomKey : 임의키(난수 등) EncFile: 암호화된 파일

<그림 8> 키복구 시스템의 취약성을 이용한 소스코드의 변경방법

며, 본 시스템에서는 KRI와 KRI의 무결성 값을 포함하여 KRC의 공개키로 암호화하여 KRB를 생성하였으므로 KRC 이외에는 KRB를 복호화할 수 없다. 그러므로 암호파일의 생성 시 뿐만아니라 암호파일 생성 후에도 키복구 정보의 변경으로부터 안전하도록 구현하였다.

6.3 기존 시스템과의 비교 및 시스템 특성

본 논문에서는 검증되고 잘 알려진 암호 알고리즘들을 포함하고 있는 범용 암호 라이브러리를 이용함으로써 시스템의 유지보수성을 높였으며, 국제공통평가기준인 CC 2.0을 기반으로 정보보호시스템의 개발 및 평가 과정을 준수함으로써 다른 정보보호시스템의 개발 시 본 과정을 적용하여 개발할 수 있도록 하였다. 그리고, 개발된 암호파일 복구 기능을 PKRS와 기존의 파일 암호 시스템과 비교할 때 다음과 같은 특성을 가지며, <표 7>은 기존의 시스템과 기능을 비교한 것이다.

첫째, PKRS에서는 파일 암호시 KRI를 생성할 때 여러 개의 KRA들 중에 사용할 KRA들을 비밀리에 지정할 수 있다. KRA를 여러 개 두는 것은 어느 한 기관에만 권한이 집중되는 것을 방지할 수 있으며, KRA들이 공모한다 하더라도 사용자가 선택한 KRA는 KRC 이외에 제3자가 알 수 없다. 또한 KRC는 KRA의 도움 없이는 세션키를 복호할 수 없으므로 이들 KRC와 KRA들의 권한을 정책에 따라 조정할 수 있는 장점을 가지며 부 시스템들 간의 공모공격 가능성을 줄일 수 있다.

둘째, 키복구 기능을 지원하기 위한 KRI에 해쉬값을 첨부하여 KRB를 생성하므로 무결성을 지원하도록 하였다. KRI의 무결성은 외부 침입자가 암호화된 파일을 강제 복구하기 위하여 KRI의 내용을 변경하거나 교체할 위협으로부터 보호하는 기능이다.

셋째, 시스템의 안전을 위해 2개의 사용자

<표 7> PKRS와 기존 시스템과의 비교

제품명 / 항목	PKRS(본 시스템)	제품 B	제품 C	F-Secure의 FileCrypto
운영체제	Windows 95/98/2000/NT	Windows 2000	Windows 95/98/2000/NT, NetWare	Windows 95/98/2000/NT
알고리즘(키 길이) (bits)	DES(64/128) RSA(512/1024) SHA1, MD5	DES(40/56) RSA(1024)	DES(56) RC4(128) RC5(56/128)	Blowfish(256) DES(128)
표준 수용	CC v2.0, FIPS PUBs, RKRP, PKCS	N/A	ITU X.509	N/A
공개키 암호	●	●	●	×
다중 인증	●	×	×	×
패스워드 만료시기	●	N/A	●	×
임시 파일 삭제	●	N/A	임시파일 없음	●
보안 감사 제공	●	×	×	×
데이터 무결성 제공	●	×	×	×
키복구 기능	●	●	●	●
키복구 방식	캡슐화 방식	캡슐화 방식	캡슐화 방식	TTP 방식
키복구 필드 검증	●	×	×	×
사용자 키복구기관 설정	●	×	N/A	N/A

출처 [Microsoft, 2001 : RSA Security, 2001 : F-Secure, 2000]

패스워드를 사용하도록 하였다. 하나는 UCS의 접근 제어를 위해 로그인 과정시 사용하며 다른 하나는 개인키 암호화용으로 사용된다. 개인키는 패스워드로 암호화되어 안전하게 보관되므로 사용시 패스워드를 입력받아 복호화하여 사용 후 메모리에서 삭제하므로 개인키를 안전하게 관리할 수 있다.

넷째, KRC에서는 안전한 키복구를 지원하기 위하여 다음과 같은 여러 가지 인증을 동시에 처리하여 보안성을 증대하였으며 내용은 다음과 같다.

- **사용자 인증** : 키복구 요청시 사용자의 서명이 첨부된 키복구 요청서와 사용자의 인증서를 함께 KRC에 송신하면, KRC는 사용자 인증서에 대하여 인증기관의 서명을 확인하고 사용자 공개키를 추출하여 키복구 요청서의 서명을 확인하므로 사용자 인증을 수행한다.
- **파일 소유자 인증** : 키복구 요청시 첨부된 키복구 정보내에는 파일 소유자의 유일한 식별값을 포함하므로 인증서내의 subject-UniqueID와 비교하여 파일 소유자를 인증하므로 비인가 소유자가 키복구 요청을 할 수 없도록 하였다. 최악의 경우, 파일 소유자가 아닌 외부 침입자가 가로챈 암호파일과 소유자의 인증서를 이용하여 키복구를 요청할 경우, 파일 소유자의 개인키가 없으므로 키복구 요청서에 서명을 할 수 없으며 다른 키로 서명할 경우 사용자 인증서에 에러를 발생하므로 키복구가 진행되지 않는다.

7. 결론

본 논문에서는 저장된 정보의 직접적인 보호를 위하여 파일 암호 시스템을 설계 및 구현하였으며, 사용자의 개인키의 손상 및 분실, 갱신으로 암호화된 파일을 복호화할 수 없음으로 인한 경제적 손실을 최소화하기 위하여 키복구 기능을 추가하였다. 키복구의 대상은 개인키가 아닌 파일을 암호화한 키인 세션키이며 키복구 정보를 특정기관에 위탁하지 않고 암호파일 내에 첨부시키는 캡슐화 방식을 적용하였다.

PKRS가 제공하는 보안기능은 보안 감사와 키 관리, 접근 통제, 식별 및 인증, 데이터 보호, 키복구 기능이며, 보안정책에 맞게 키 크기 및 암호 알고리즘 등을 설정할 수 있는 유연성을 부여하였다. 그리고 시스템에 여러 가지 새로운 기능들 즉, 사용자의 KRA 임의 지정과 2개의 패스워드 사용, KRI의 무결성 지원, KRC의 다중인증 등의 특성을 부여하여 보안성을 높였다.

PKRS의 프로토콜과 알고리즘들은 다음과 같은 보안 표준을 수용하여 개발하였다. 보안기능을 위해 정보보호시스템의 국제공통평가기준인 CC 2.0의 보안기능 요구사항과 키복구 기능을 적용하기 위해 NIST에서 제안한 RKRP의 요구사항을 기반으로 하여 분석, 설계 및 평가하였다. 또한, 정보보호시스템의 평가스킴(ITSEM, CEM)을 적용하여 개발하였으므로, 각종 정보보호시스템의 개발(설계, 구현, 평가)시 참조할 수 있도록 하였다.

본 시스템은 PC 환경에서의 키복구 솔루션으로 개발되었으므로, 상용화하기 위한 성능개선 즉, 패키지화, 인터넷 및 인트라넷 환경의 정보시스템에서 파일의 암호 및 복구가 가능한 시스템으로의 확장 등을 향후 연구과제로 남기고 있다.

참고문헌

[유준석, 2000] 유준석외 4인, "키 복구 시스템 및 안전성에 관한 고찰", *통신정보보호학회지*, Vol. 10, No. 1, pp.21-37, Mar. 2000.

[유희종, 2000] 유희종외 4인, "키 복구 시스템의 요구사항에 관한 고찰", *통신정보보호학회지*, Vol. 10, No. 1, pp.1-19, Mar. 2000.

[이강수, 1998] 이강수, *선진국 정보보호시스템의 평가제도에 관한 연구*, 정보통신학술연구지원국, 정보통신부, 1998년 3월.

[채승철, 1999] 채승철, 이임영, "안전한 키 위탁 시스템에 관한 연구", *한국통신정보보호학회논문지*, Vol.9, No.2, pp.83-92, Jun. 1999.

[Blaze, 1993] Blaze, M., "A Cryptographic File System for Unix," *Proc. First ACM Conference on Computer and Communications Security*, Fairfax, VA, November 1993.

[Cylink, 1998] Cylink Corp., "CyKey, A Key Recovery System for Commercial Environments," *http://www.cylink.com*, 1998.

[Dorothy, 1996] Dorothy E. Denning and Dennis K. Branstad, "A Taxonomy for Key Escrow Encryption Systems," *Comm. ACM*, pp.34-40, Vol.39, No.3, 1996.

[Escrow, 1996] Ravi Ganesan, "How To Use Key Escrow," *Comm. ACM*, Vol.39, No.3, pp.33, Mar. 1996.

[FIPS Pub., 2001] Federal Information Processing Standards Publications, *http://www.itl.nist.gov/fipspubs/*, 2001.

[F-Secure, 2000] F-Secure Corp., FileCrypto, *http://www.datafellows.com/products/tech-info/*, 2000.

[Gennaro, 1999] R. Gennaro, et. al., "Secure Key Recovery," *IBM Thomas J. Watson Research Center*, 1999.

[JCSI, 2000] JCSI homepage, *http://security.dstc.edu.au/projects/java/jcsi.html*, Aug. 2000.

[Jefferies, 1995] Jefferies, N., Mitchell, C. and Walker, M., "A Proposed Architecture for Trusted Third Party Services," *Lecture Notes in Computer Science*, Vol. 1029, pp.98-104, 1995.

[Jingmin, 1995] Jingmin He and Ed Dawson, "A New Key Escrow Cryptosystem," *Lecture Notes in Computer Science*, Vol. 1029, pp.105-113, 1995.

[Kim, 1999] S.J.Kim, I.S.Lee, M. Mambo and S.J.Park, "On the difficulty of key recovery systems," *Proc. of ISW'99, Information Security Workshop*, Springer-Verlag, LNCS 1729, Kuala Lumpur, Malaysia, pp.207-224, November 6-7 1999.

[Lee, 1997] Yung-Cheng Lee, Chi-Sung Laih, "On the key recovery of the Key Escrow System," *Proc. of 13th Annual Computer Security Applications Conference*,

pp.216-220, 1997.

[Markowitz, 1997] M. Markowitz and R. Schlafly, "Key Recovery in SecretAgent," *Digital Signature*, 1997.

[Menasce, 2000] D. A. Menasce, V. A. F. Almeida, *Scaling for e-business : technologies, models, performance, and capacity planning*, Prentice Hall, Upper Saddle River, NJ, 2000.

[Microsoft, 2001] Microsoft, Encryption File System, *http://www.microsoft.com/korea/ntserver/*, 2001.

[NIST, 1992] National Institute of Standards and Technology, *Key Management Using ANSI X9.17*, Federal Information Processing Standard(FIPS) Publication 171, Apr. 1992.

[NIST, 1998] National Institute of Standards and Technology, "Common Criteria v2.0," *http://csrc.nist.gov/cc/*, 1998. 11.

[Novastor, 2000] Novastor. Corp,. DataSAFE, *http://www.novastor.com/*, 2000.

[Peter, 1996] Peter Gutmann, University of Auckland, New Zealand. The Secure FileSystem (SFS) for DOS/Windows, *http://www.cs.auckland.ac.nz/~pgut001/sfs/index.html*, Sep. 1996.

[Ravi, 1996] Ravi Ganesan, "The Yaksha Security System," *Comm. ACM*, Vol.39, No.3, pp.55-60, Mar. 1996.

[RKRP, 1998] Requirements for Key Recovery Products, Final Report, Federal Information Processing Standard for Federal Key Management Infrastructure, *http://csrc.nist.gov/key recovery*, Nov. 1998.

[RSA Data Security, 1991] RSA Data Security Inc., Public Key Cryptography Standards #1~9, June 3, 1991.

[RSA Security, 2001] RSA Security Inc. Desktop Keon, *http://www.rsasecurity.com/products/keon/*, 2001.

[Shamir, 1979] A. Shamir, "How to Share a Secret," *Comm. ACM*, Vol. 24, No. 11, Nov. 1979.

[Stephen, 1996] Stephen T. Walker, Steven B. Lipner, Carl M. Ellison and David M. Balenson, "Commercial Key Recovery," *Comm. ACM*, Vol.39, No.3, pp.41-47, 1996.

[TCFS, 2000] Salerno Unv. TCFS, *http://tcfs.dia.unisa.it/*, Sep. 2000.

[TCKRA, 1997] Technology Committee of Key Recovery Alliance, Cryptographic Information Recovery using Key Recovery, A Working Paper, Version 1.2, *http://www.kra .org*, Aug. 1997.

저자소개

장수진(sjjang@tjhealth.ac.kr)
충남대학교 계산통계학과 학사
충남대학교 대학원 이학석사
충남대학교 전자계산소 시스템 개발실장
현 한남대학교 컴퓨터공학과 박사과정, 대전보건대학 컴퓨터정보처리과 조교수
관심분야 : 소프트웨어공학, 정보보호시스템 평가

고정호(jhkont@yjc.ac.kr)
한남대학교 전자계산공학과 학사
한남대학교 컴퓨터공학과 공학석사
한남대학교 컴퓨터공학과 공학박사
현 영진전문대학 컴퓨터정보기술계열 전임강사
관심 분야 : 전자상거래, 정보보호, 객체지향 프로그래밍

이강수(gslee@eve.hannam.ac.kr)
홍익대학교 전자계산학과 학사
서울대학교 대학원 전산학과 이학석사
서울대학교 대학원 전산학과 이학박사
대전산업대학 전임강사
일리노이대학 객원교수
전자통신연구원 초빙연구원
한남대학교 멀티미디어학부장
현 한남대학교 컴퓨터공학과 교수
관심 분야 : 소프트웨어공학, 병행시스템모델링 및 분석, 정보보호시스템 평가,
멀티미디어교육 커리큘럼