情 報 保 護 學 會 誌
第 14 券 第 4 號, 2004. 8

암호시스템의 키 관리 기술

송 기 언*, 이 진 우*, 곽 진*, 양 형 규**, 원 동 호***

요 약

암호시스템의 안전성은 사용하는 키의 안전성을 기반으로 하기 때문에, 키 관리 기술은 암호시스템의 안전성을 제공하기 위한 가장 중요한 요소이다. 그러나 이러한 키 관리 기술의 중요성에도 불구하고 키 생명주기에 따라 이루어지는 통합 키 관리 기술에 대한 연구는 거의 전무한 상태이다. 이에 본 고에서는 암호시스템의 설계 시 적용 가능한 통합 키 관리 기술에 대해 서술한다. 본 고에서 기술하는 키 관리 기술의 구조는 클라이언트·서버 구조의 소켓을 이용한 통신 시스템과 유사한 형태를 갖고 있기 때문에, 암호시스템에 효율적으로 적용할 수 있는 장점을 가지고 있다. 본 고에서는 먼저, 키 생명 주기와 키 관리의 개념 등에 대하여 설명하고, 이러한 내용을 바탕으로 암호시스템에 효율적으로 적용할 수 있는 통합 키 관리 기술에 대하여 설명하고자 한다.

Ⅰ. 서 론

최근, 정보통신 기술의 발전과 함께 정보시스템이 각 분야에서 매우 중요한 요소로 자리 잡고 있다. 특히 금융분야에서의 거래를 비롯한 기업 간의 거래와 개인 사용자간의 통신에서 매우 중요한 요소로 자리 잡고 있다. 이렇게 정보의 처리와 전송되는 정보의 형태가 다양해짐에 따라 사회 각 분야의 정보시스템의 안전성 확보의 필요성 및 정보보호의 중요성 또한 증대되고 있다. 그러므로, 정보시스템의 다양한 역할과 함께 개인의 프라이버시(privacy)나 기업 간의 거래 정보와 같은 경영상의 기밀 내용에 대한 정보보호와 통신 상태의 보호 및 사용자 정당성 확인을 위한 방법으로 암호기술이 요구되고 있다. 이러한 암호기술의 사용은 보호하고자 하는 정보를 작은 길이의 키로 관리 및 보호하는 것에 기반을 두고 있으므로, 키를 중심으로 이를 안전하게 관리하기 위한 키 관리(key management) 기술은 매우 중요한 요소이다.

키 관리는 인가된 두 개체간의 공통된 키 정보를 유지할 수 있는 관계를 설정하고 이를 지속시키는 모든 절차를 포함하며 키 재료의 생성, 등록, 인증, 말소, 분배, 설치, 저장, 보관, 취소, 파생, 파기 등과 같은 서비스의 관리를 말한다. 즉, 키 관리는 키 관련 데이터를 생성하는 키 생성 과정, 생성된 키가 비인가된 사용자에게 노출되지 않고 인가된 개체 사이에서만 키를 공유하는 키 분배 과정, 프로토콜 수행 과정에서 생성된 키와 키 관련 데이터를 안전하게 저장하는 키 저장 과정, 키 정보의 노출이나 유효기간이 만료되었을 때 키를 안전하게 폐기하는 키 폐기 과정, 그리고 인가된 사용자의 키가 손상되거나 분실되었을 경우 키를 복구할 수 있는 키 복구 과정 등으로 분류할 수 있다[1,2].

본 고에서는 암호시스템에서 안전하고 효율적인 키 관리 기능을 제공할 수 있는 통합 키 관리 기술에 대하여 기술한다. 키 관리 기술은 키의 생명주기(Key Life-cycle)에 따라 키의 통합적인 관리 기능을 제공한다.

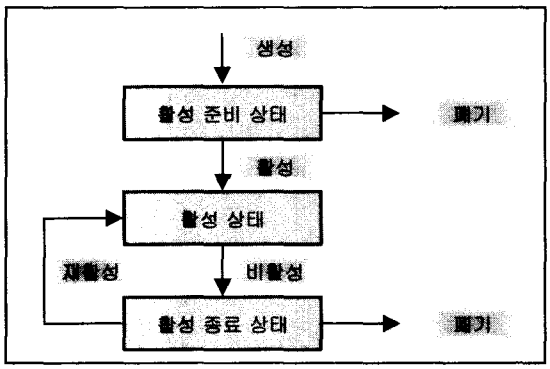
본 고의 구성은 다음과 같다. 2장에서는 키 관리 기술의 바탕이 되는 키 생명주기와 키 관리 개념에 대해 알아보고, 키 생명주기에 따른 키 관리 서비스에 대해 소개한다. 3장에서는 키 관리 기술에 대하여 설명하고, 마지막 4장에서 결론과 향후 연구 방향에 대하여 제시한다.

* 성균관대학교 컴퓨터공학과 정보통신보호연구실(kesong, jwlee, jkwak@dosan.skku.ac.kr)
** 강남대학교 컴퓨터미디어공학과 부교수(hkyang@kangnam.ac.kr)
*** 성균관대학교 컴퓨터공학과 정교수(dhwon@dosan.skku.ac.kr)

Ⅱ. 키 관리

1. 키 생명주기

키의 생명주기는 키가 암호화나 복호화와 같은 작업을 위해 사용될 수 없는 활성 준비 상태와 키가 정보를 암호학적으로 처리하는데 사용되는 활성 상태, 그리고 키가 단지 복호화나 검증을 위해서만 사용되는 활성 종료 상태로 구성되며, 그림 1은 키 생명주기를 도식화한 것이다.



〔그림 1〕 키 생명 주기

1.1 키 상태의 전이

키가 한 상태로부터 다른 상태로 진행되는 것을 전이라고 하며, 생명주기 모델에서는 크게 5가지의 전이로 나누어 생각할 수 있으며 각각에 대한 설명은 다음과 같다.

- □ 생성 : 키를 생성하는 과정으로 키 생성 규칙에 따라서 생성되어야 한다. 키 생성 과정은 생성된 키 값에 대한 검사도 포함한다.
- □ 활성 : 암호화 작업을 위한 키를 유효하게 만든다.
- □ 비활성 : 키의 사용을 제한하는 과정으로 키의 유효기간이 지나거나, 취소될 때 발생한다.
- □ 재활성 : 키 사용 후 키가 다시암호화 작업에 사용될 수 있게 한다.
- □ 폐기 : 키의 생명주기가 끝나는 과정으로 키의 논리적 폐기부터 물리적 폐기까지 포함한다.

키 상태 전이는 새로운 키가 필요하거나, 키의 유효기간 경과, 그리고 키 생명주기 완료 등에 일어나게 되며, 모든 전이는 키 관리를 위한 여러 가지 서비스를 제공한다.

2. 키의 보호

키는 암호학적 기술에 의존하는 암호시스템에서 가장 중요한 요소로서 사용되는 응용의 형태, 위협, 키 자체의 상태 등에 따라 노출, 변경, 파괴, 재사용 등의 공격으로부터 적절하게 보호되어야 한다. 또한 키는 유효기간 동안에만 사용되어야 하는데, 소모적 공격을 행하는데 요구되는 시간, 키가 사용되어지는 기간동안에 전송되는 암호화된 정보의 양 그리고 시간이 지난 정보에 대한 가치를 고려하여 보호되어야 한다[3].

2.1 키 보호 종류

앞서 설명한 바와 같이, 암호시스템에서 사용하는 키의 보호는 안전한 서비스를 제공하기 위해 매우 중요한 요소이다. 이러한 키를 보호하는 방법으로는, 크게 암호기술을 이용하는 방법과 암호기술을 이용하지 않는 방법, 물리적 방법을 이용하는 방법, 그리고 유기적인 방법 등 4가지로 나누어 생각할 수 있으며, 각각에 대한 설명은 다음과 같다.

(1) 암호기술을 이용하는 보호

키 자료에 대한 위험 요소는 암호화 기술을 사용하여 막을 수 있다. 키 노출의 방지를 위해 암호화 기술을 사용하고, 키의 변경을 방지하기 위해 데이터 무결성 메커니즘을 사용하며, 위조방지를 위해 데이터 인증 메커니즘 또는 객체 인증 메커니즘을 사용한다.

(2) 암호기술을 이용하지 않는 보호

암호 기술을 이용하지 않는 기술 중에서는 대표적인 방법으로 타임스탬프(Timestamp)를 이용하는 방법이 있다. 타임스탬프는 동기화된 시간을 참조하여, 특정 시점을 알 수 있도록 시간에 따라 변하는 매개변수이다. 유효기간을 제공함으로서 키의 사용을 제한하며, 특히 특정 순서를 가진 수와 함께 사용되면 기록된 키의 재사용을 방지할 수 있다.

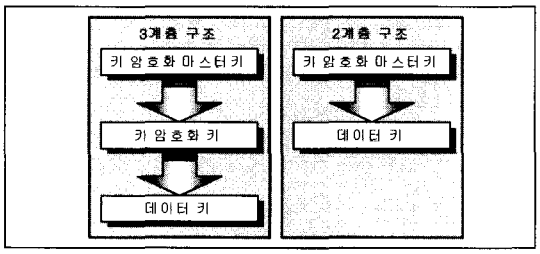
(3) 물리적 방법을 이용한 보호

암호시스템내의 각 암호 장치는 키 자료를 보호하는데 필요하다. 그 장치는 전형적으로 키 저장, 키 사용, 그리고 암호 알고리즘 구현을 위한 보안영역을 제공한다. 이러한 장치는 별도의 안전한 키 저장 장치로부터 키 자료를 로드하는 방법, 별도의 보안 장치(스마트카드, 메모리카드 등)에 구현된 암호 알고리즘과 상호작용 할 수 있는 방법 그리고 오프라인으로 저장될 수 있

는 방법 등을 제공한다.

(4) 유기적 방법을 이용한 보호

키는 전형적으로 키 계층의 조직으로 이루어진다. 계층의 1단계에 있는 키 암호화 마스터 키(master key)는 아래 단계에 있는 키의 보호를 위해 사용되고, 계층의 가장 낮은 단계에 있는 데이터 키는 데이터 보안 서비스를 제공하는데 이용된다. 즉, 데이터 키는 실제 데이터를 암호화에 사용하는 키를 말하며, 키 암호화 키는 데이터 키의 안전한 저장을 위해 암호화하는 키를 말한다. 마스터키는 키 계층 구조에서 최종 암호화에 사용하는 키를 말한다. 이러한 계층적 접근은 해당 키의 사용을 제한하며, 이렇게 함으로써 키 노출을 제한하고, 공격자의 공격을 어렵게 만든다. 보안영역의 사용으로 비인가 된 객체에 의한 키의 노출, 변경, 삭제와 같은 위협을 막을 수 있다. 시스템 관리자는 자신의 접근권한으로 마스터 키(키 계층구조에서 최상위 단계에 있는 키)를 알아낼 수 있다. 하지만 마스터 키의 노출은 잠재적으로 프로세서(processor)가 그 키에 의해 보호되고 있는 다른모든 키를 노출시키거나 조작될 수 있게 하기 때문에, 일반 사용자는 물론 시스템 관리자에 대해서도 마스터 키에 대한 접근권한은 제어되어야 한다. 그림 2는 키 계층 구조도를 나타낸 그림이다[4].



〔그림 2〕 키 계층 구조도

3. 키 관리의 개요

키 관리는 키 자료의 생성, 등록, 인증, 말소, 분배, 설치, 저장, 보관, 취소, 파생, 파기 등과 같은 서비스의 관리를 말한다. 키 관리의 목적은 이들 키 관리 서비스에 대한 안전한 관리이며, 키 관리 절차는 사용된 알고리즘, 키의 의도적인 사용, 그리고 사용에 대한 보안 정책에 의해 좌우된다[5,6].

3.1 키 관리 서비스

키 관리는 생성, 등록, 인증, 분배, 설치, 저장, 파생, 파일보관, 취소, 말소, 폐기 등의 기본적인 키 관리 서비스를 포함한다. 이러한 서비스는 키 관리 시스템에 의해 제공되거나 신뢰성 있는 제 3의 서비스 제공자에 의해 제공될 수 있다. 이 때 서비스 제공자는 모든 객체가 신뢰할 수 있도록 보안 요구사항을 만족시키는 범위 내에서 서비스를 제공해야 한다.

여러 가지 키 관리 서비스는 서로 다른 사용자에 의해 사용된다. 이들 사용자는 서로 다른 용도로 키를 사용하거나 서로 다른 키 관리 시스템을 사용할 수 있으며, 필요로 하는 서비스만을 이용할 수 있다[7-10]. 표 1은 키 관리 서비스를 정리한 표이다.

〔표 1〕 키 관리 서비스

키 관리 서비스	내 용
키 생성	안전한 키의 생성 절차
키 등록	키와 정당한 사용자와의연관
인증서 생성	공개키와 객체의 연관성보장
키 분배	인가된 객체 사이에 키의 안전한 공유
키 설치	안전한 키의 설치
키 저장	키의 사용과 복구를 위한 안전한 저장
키 유도	원본키로부터 파생키 유도
키 보관	키의 문제 발생 시 사실증명에 사용
키 복구	유사시 허가된 사용자만이 복호화
키 취소	키를 안전한 비활성 상태 유지
키 말소	키와 객체의 관계 제거
키 폐기	사용이 끝난 키의 안전한 폐기

□ 키 생성 : 키 생성은 암호학적으로 안전한키를 생성하는 절차를 의미한다. 이 때 예측이 불가능하고 위조할 수 없는 랜덤수(random number)를 사용해야 하며, 재사용해서는 안된다. 이는 하나의 키의 노출로 인해 그 키와 관련된 정보뿐만 아니라 노출된 키로부터 파생되었거나 관련되어 있는 다른 모든 키에 대한 접근권한도 임의의 사용자에게 제공될 수 있기 때문이다.

□ 키 등록 : 키 등록은 생성된 키를 정당한 사용자와 관련시키는 것으로 등록기관(RA : Registration Authority)에 의해 이루어지며, 등록기관은 키와 관련된 정보의 기록을 안전하게 유지해야 한다. 또한, 키 등록기관은 키 등록뿐만 아니라 키를 말소시키는 역할도 수행한다.

□ 키 인증서 생성 : 키 확인서는 보통 공개키와 객체의 연관성을 보장하는 인증서(certificate)라 하며, 인증기관에 의해 생성된다. 인증기관은 키 인증에 대

한 요구를 받은 경우 키 인증서를 생성한다[11,12].

□ 키 분배 : 키 분배는 인가된 객체 사이에 키 또는 키 자료가 안전하게 공유되는 것을 의미한다. 비대칭 암호 방식에서는 키를 분배하는 특정 메커니즘을 사용하고, 대칭 암호 방식에서는 KTC(Key Translation Center), KDC(Key Distribution Center)에 의해 분배가 이루어진다.

□ 키 설치 : 키 설치는 키를 사용하기 전에 필요한 절차로 키 관리 시스템 내에서 안전하게 제공되어야 한다.

□ 키 저장 : 키 저장은 키를 사용하거나 복구를 위해 키를 안전하게 저장하는 것을 의미한다. 이 때, 키는 물리적으로 안전한 장치에 저장되는 것이 바람직하며, 이렇게 저장된 키 자료는 기밀성 및 무결성을 제공한다. 키 저장은 키의 생명주기 동안의 모든 상태(활성 준비, 활성, 활성 종료 등)에서 발생할 수 있다.

□ 키 유도 : 키 유도는 원본키(original key)로부터 파생키(derivation key)를 유도하는 것으로 유도된 키가 원본키를 노출시키지 않도록 하기 위해 유도 연산은 역변환이 불가능하고 예측 불가능해야 한다.

□ 키 보관 : 키 보관은 키의 일반적인 사용이 중단된 이후 그 키의 오용 등의 문제가 발생했을 경우 그러한 사실을 증명하는데 키가 사용될 수 있도록 하기 위해 이루어진다.

□ 키 복구 : 키 복구는 합법적 상황에서 암호문을 복호화 하거나, 사용자가 자신의 비밀키를 분실했을 경우 등과 같은 유사시에 허가된 사용자만이 복호화를 할 수 있는 기능을 제공하기 위해 이루어진다.

□ 키 취소 : 키 취소는 키의 오용이 의심되거나 알려진 경우, 키의 안전한 비활성 상태를 유지하기 위해 이루어진다. 키 취소는 키 삭제라고도 하며, 유효기간이 만료된 키나 소유자의 환경이 변경된 경우 발생한다. 키가 취소된 후에는 단지 복호화나 검증만을 위해 사용된다.

□ 키 말소 : 키 말소는 키와 객체의 관계를 제거하는 것으로, 키 등록기관에 의해 제공된다. 이는 폐기 과정의 일부분이다.

□ 키 폐기 : 키 폐기는 더 이상 사용될 필요가 없는 키의 안전한 폐기를 위해 이루어진다. 키를 폐기한다는 것은 모든 기록을 제거함으로써 폐기 후에 남아있는 어떠한 정보를 가지고도 폐기된 키를 다시 복구시킬 수 없도록 하는 것을 의미한다. 또한 이는 사용되는 키뿐만 아니라 보관된 모든 복사본에 대한 폐기도 포함한다. 보관된 키를 폐기할 때는 보관된 키에 의해 보호된 자료가 더 이상 필요 없는지의 여부를 사전에 확인해야 한다.

4. 지원 서비스

키 관리 서비스는 보안에 관련된 다른 서비스에 사용될 수 있는데, 이러한 서비스에는 다음과 같다[5]. 표 2는 키 관리의 지원 서비스를 나타낸 표이다.

〔표 2〕 키 관리 지원 서비스

지원 서비스	내용
접근 제어	인가된 객체만이 자원 접근
감시	키의 오용 감지
인증	정당한 객체인지 검증
암호학적 서비스	무결성, 기밀성, 부인방지 제공
시간 서비스	시간 파라미터 생성

□ 접근 제어 : 객체가 키 관리 시스템의 자원에 접근할 때 인가된 객체에 의해서만 접근되어질 수 있도록 보장되어야 할 경우에 사용된다.

□ 감시 : 키 관리 시스템에 나타나는 보안에 관련된 행위의 추적에 사용된다.

□ 인증 : 객체를 보안 도메인의 구성원으로 구축하기 위해 사용된다.

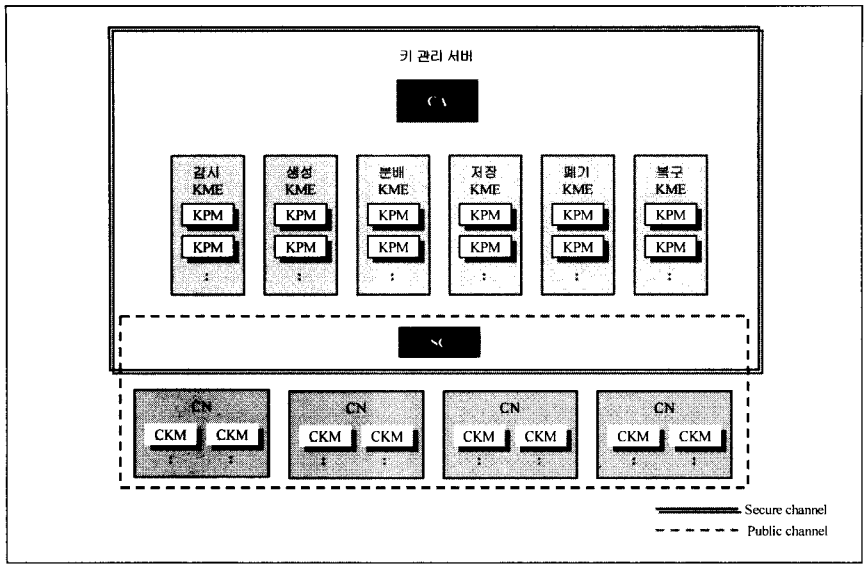
□ 암호학적 서비스 : 무결성, 기밀성, 부인방지 등을 제공하는 키 관리 서비스에 의해 사용된다.

□ 시간 서비스 : 유효기간과 같은 시간 파라미터(parameter)을 생성하는데 사용된다.

Ⅲ. 암호시스템에서의 키 관리

현재 대부분의 응용 암호시스템은 체계적이거나 가시적으로 명확하게 나타낼 수 있는 키 관리 기술을 적용하지 못하고 있다. 이는 암호시스템의 설계자들이 키 관리의 중요성을 인식하고 있지만 체계적인 키 관리 기술에 대한 연구가 부족하기 때문이다.

키는 암호시스템의 안전성에 직접적인 영향을 주는 중요한 사항이기 때문에, 키 관리 기술은 암호시스템의 안전성과 신뢰성을 나타내는 중요한 요소이다. 따라서, 암호시스템 설계 시 체계적이고 가시적인 키 관리를 고려한 설계가 이루어 져야 하며, 이러한 키 관리를 통해



〔그림 3〕 키 관리 구조

보다 향상된 안전성을 보장할 수 있다. 또한, 암호시스템의 안전성 평가 시 안전한 키 관리 기술을 적용하였음을 체크함으로써 보다 객관적이고 정확한 평가가 이루어질 수 있다[13,14].

본 절에서는 암호시스템 설계 시 효율적이고 안전한 키 관리 기술을 기술한다.

1. 키 관리 기반구조(KMI : Key Management Infrastructure)

KMI의 구성은 암호시스템의 특성에 따라서 다르게 구성된다. KMI의 구성에 영향을 미치는 암호시스템의 특성은 다음과 같다.

- 사용되는 암호알고리즘
- 각 구성 요소 사이의 통신 방법
- 시스템의 목적
- 암호 통신을 하는 객체의 수와 관계

암호시스템에 사용되는 알고리즘이 대칭키 기반 또는, 비대칭키 기반인지에 따라서 KMI의 구조와 구성요소의 기능이 달라지게 된다. 또한 응용 프로토콜의 특성도 KMI에 영향을 준다. 암호시스템을 구성하고 있는 각 객체 사이의 통신 환경도 KMI를 결정하는 중요한 요소 중 하나이다. 즉, KMI의 구조가 암호시스템의 통신 환경이 유선인가, 무선인가, 유무선 통합 환경인가에 따라 변할 수 있다. 암호시스템의 사용 목적 또한 KMI를 결정하는 중요한 요소이다. 뿐만 아니라 암호시스템의 객체의 수가 많고 적을 때의 KMI의 구성은 달라지게 된다.

본 고에서는 KMI에서 키 관리를 위해 기능을 수행하는 구성 요소로는 CA(Central Authority), KME (Key Management Element), SC (Service Connector), CN(Client Node)가 있으며, 그 구조는 그림 3과 같다.

1.1 CA(Central Authority)

CA는 KMI의 모든 구성 요소의 동작을 감시한다.

1.2 KME(Key Management Element)

KME은 키 관리 구성 요소별로 나누어진다. 각각의 KME은 SC로부터 동작 요청을 받으면 KPM(Key Processing Module)을 통해서 요청을 수행하게 된다. KPM은 KME를 이루는 구성 요소로서 실제 키와 관련된 동작을 하는 프로세스를 말한다.

- ❑ 감시 KME : 키에 대한 모든 작업의 로그 파일을 분석을 통한 감시를 하며, 키 관리 정책에 따라 감시 범위가 결정된다.
- ❑ 생성 KME : 키와 관련된 모든 정보의 생성에 관계된 KPM이 생성 KME에 속한다. 데이터의 생성요청과 요청 객체의 인증을 통해 생성된 정보의 전송으로 구성된다.

□ 분배 KME : 생성된 키의 분배는 대칭키 방식의 키 분배 프로토콜을 사용할 경우에만 필요하게 된다. 비대칭키 방식의 키 분배는 키 관리 서버의 개입 없이 클라이언트 간에 이루어진다.
□ 저장 KME : 키와 관련된 모든 데이터의 저장은 저장 KME를 통해 수행된다. 데이터를 보안 요구사항에 따라 분류하여 보안 요구 레벨을 부여하고, 필요한 보안 수준에 따라 다른 저장 방식을 적용한다.
□ 폐기 KME : 폐기 KME는 키와 관련된 모든 데이터의 폐기를 처리한다. 키 복구 기능을 제공하는 시스템에서는 복구를 위한 폐기 방식이 다르게 된다. 따라서 폐기될 데이터의 특성에 따라 다른 폐기 방식이 적용 가능해야 한다.
□ 복구 KME : 키 복구 요청 객체의 인증을 수행하고 복구를 위한 기능을 지원한다.

1.3 SC(Service Connector)

SC는 CN의 서비스 요청에 따라서 KME을 연결 시켜주는 기능을 한다. SC는 클라이언트와의 통신 기능을 수행하는 통신 프로세스와 요청 받은 서비스를 분류하는 프로세스로 구성된다.

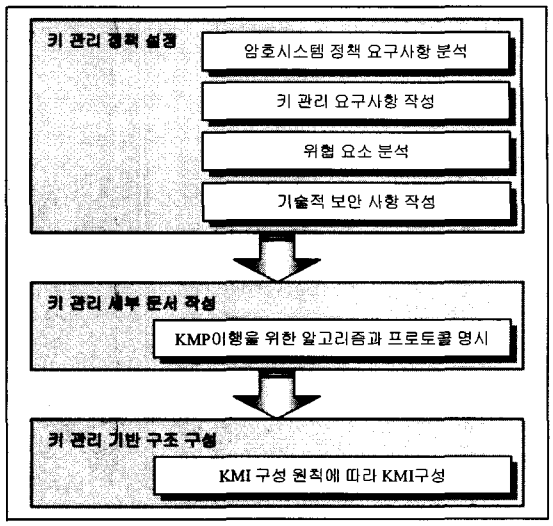
1.4 CN(Client Node)

CN은 사용자와 관리자를 위한 인터페이스(interface)를 제공하는 부분이다. CN은 암호화 모듈과 키 관리 서비스를 제공하는 모듈인 CKM (Client Key management Module)로 구성된다.

□ CKM : CN을 구성하는 구성 요소로서 CN 안에서 실제 암호 기능을 수행하는 프로세서의 그룹이다. 여러 개의 프로세스가 하나의 일을 수행하는 Entity로 구성된다. 즉 서버의 KME와 같은 기능을 수행하게 된다. CN의 기본 CKM은 SC와의 통신을 위한 통신 CKM이 있고, 서버의 KME와 같이 키 관리 구성 요소에 따라 생성·분배·저장·폐기·복구 CKM이 있다. 또한 CN 내의 키 관련 프로세서의 작동을 감시하고 이를 통신 KME를 통해SC에 전송하는 감시 CKM이 존재한다.

2. 키 관리 단계

암호시스템에 적합한 키 관리를 위해서는 암호시스템의 설계 초기 단계부터 키 관리를 고려해야 한다.



〔그림 4〕 키 관리 단계

키 관리 단계는 암호시스템의 요구사항을 만족하는 키 관리 정책(KMP : Key Management Policy)을 설정하고 이를 기반으로 키 관리 세부 문서(KMSS : Key Management Specific Statement) 작성한다. KMSS를 바탕으로 KMI 구성하게 된다. 그림 4는 키 관리 단계를 나타낸 그림이다.

2.1 KMP 설정

KMP는 키 관리의 목적과 키 관리에서 수행해야 할 의무 그리고 키 관리에 필요한 요구사항을 명시해야 한다. KMP의 설정 과정은 암호시스템 정책 요구사항을 명시하고 이에 따라 키 관리 요구사항을 작성하게 된다. 또한 위협 요소와 그의 대응 방안에 대해서 기술한다.

(1) 암호시스템 정책 요구사항

KMP가 적용될 암호시스템의 정책의 요구사항을 명시해야 한다. 암호시스템의 정책의 요구사항에 따라 KMP의 방향이 정해진다.

(2) 키 관리 요구사항

키 관리를 위해 고려해야 할 사항에 대해 다음 사항을 기술한다.

□ 보호 대상 종류 : 암호시스템의 기반 알고리즘이대칭키 방식 또는 비대칭키 방식임을 명시하며 인증서 사용에 따른 요구사항을 작성한다.
□ 키와 키 재료 생성 주체 : 키 또는 키 재료의 생성

주체가 정의 되어야한다. 키 생성 주체가 사용자일 경우에 사용자 신분 확인 방법과 생성된 키의 검증 과정에 대한 요구사항이 포함된다. 키 관리 서버가 키를 생성할 경우는 사용자 신분 확인 방법과 서버에서 생성된 키를 사용자에게 분배하는 방식에 대한 요구사항이 포함된다.

□ 관리자와 사용자의 권한 : 관리자와 사용자의 시스템 사용 환경을 명시하고 그에 적절한 키에 대한 권한을 정의한다. 관리자의 사용 환경은 공개채널(public channel)을 통해 원격 관리를 지원 유무와 사용자의 프라이버시 보호 수준을 결정하고 이에 따른 관리자의 키 관리 권한을 정의한다. 사용자의 권한 정의에는 사용자의 보안 지식 수준, 사용자 암호시스템 사용기간, 비인가된 사용에 대한 제약, 보안 지침과 같은 내용을 기술한다.

□ 키의 재사용에 관한 요구사항 : 키의 재사용은 암호시스템의 안전성과 효율성을 모두 만족해야하기 때문에 재사용 키의 사용 목적, 암호시스템의 네트워크 환경, 재사용 빈도, 암호 단말 기기의 연산 능력 등을 고려하여 키의 재사용에 관한 요구사항이 작성된다.

□ 키 복구 요구사항 : 키 복구 방식에 따라 KMI의 구성이 결정된다. 키 복구 시기, 요청 방법, 복구 방식, 사용자의 프라이버시 등을 고려하여 키 복구 요구사항을 작성한다.

(3) 위협 요소

암호 기술적인 위협 요소와 물리적인 위협 요소로 분류한다.

□ 기술적 위협 요소 : 기술적인 위협 요소는 키 관리 구성 요소에 따라 공격 방법을 기술하며 그에 따른 보안 요구사항을 작성한다.

□ 물리적 위협 요소 : 정전 또는 화재와 같은 위급한 상황 발생 시 처리 방식의 요구사항과 백업(back-up)된 정보를 통해 KMI를 다시 구성하기 위한 요구 사항이 명시된다.

(4) 기술적 보안

키 관리 요구사항과 기술·물리적 위협 요소의 안전성 요구사항을 만족하기 위한 세부 기술을 작성한다.

□ 키 생성 : 키 크기(size), 비밀·개인키 생성 시 안전성 보장, 공개키 분배시 무결성 보장, 키 생성 관리 방식 등을 명시한다.

□ 비밀·개인키 보호 : 비밀·개인키 백업, 저장, 폐기, 복구시 안전성 보장을 위한 방법을 기술한다.

□ 키 관련 정보 보호 : 키 생명 주기 동안에 발생하는 키와 관계된 모든 정보의 보호를 위한 방법을 기술한다.

□ 감시 기능 : 개인의 프라이버시와 조직의 안전성에 대한 요구 사항을 모두 만족하도록 감시 방식에 대해 명시한다. 서버내의 동작과 사용자의 정보 보호 기기의 동작까지 감시가 가능해야 한다.

2.2 KMSS 작성

KMSS에서는 KMP에서 정의된 항목에 따라서 암호시스템에서 이행하기 위해 실제 필요한 알고리즘과 프로토콜을 명시한다. KMSS의 기본 항목은 다음과 같으며, KMP의 요구사항에 따라 추가된다.

- 키 관리 객체들간의 관계와 교환 정보에 대한 정의
- 키 생성과 키 획득
- 키 동의
- 인증서의 상호 인증
- 키 분배와 복구
- 유효기간
- 키 재료 관리
- 키 재료 보호
- 유사시 키 재료 복구
- 감시 기능
- 키 재료 폐기
- 키 저장과 복구

2.3 KMI 구성

KMSS의 각 항목들의 기능 수행을 위해 하나 또는 그 이상의 KPM과 CKM을 생성한다. 생성된 KPM과 CKM을 키 관리 구성 요소에 따라서 분류를 하고 각 KPM과 CKM 사이의 연관성을 고려하여 KME, CN, SC를 생성한다. KME, CN, SC은 KMP의 요구사항에 따라 KMI을 구성하게 된다.

3. 키 관리 기술의 특징

키 관리 기술은 KMP를 기반으로 작성된 KMSS에 따라서 키 관리 구성 요소별로 프로세스를 분류하여 KMI를 구성하기 때문에 안전성과 효율성이 향상된다. 표 3은 키 관리 기술의 특징을 정리한 것이다.

〔표 3〕 키 관리 기술의 특징

특 징	내 용
안전성	■ 일괄적인 KMP의 적용 가능 ▸ KMP의 적용이 각 단계를 거쳐가며 구체화 ■ 가시적인 통합 키 관리가능 ▸ 키의 흐름 파악에 용이 ▸ 사용자에게 더 높은 신뢰성 제공
효율성	■ KMP 변경이 쉬움 ▸ 변경된 KMP의 적용은 KMSS와 KMI의 부분적인 수정으로 가능 ■ KMI가 암호시스템의 구조에 쉽게 적용 가능 ▸ 소켓을 이용한 클라이언트·서버 모델과 같음

3.1 안전성

(1) KMP의 적용이 각각의 단계를 거쳐가며 구체화되기 때문에 암호시스템의 다양한 요구사항에 따른 일괄적인 KMP 적용이 가능하다. 일괄적인 정책 적용이 가능한 암호시스템은 안전한 키 관리를 지원한다.

(2) 키의 생명주기에 따라 가시적인 키 관리가 가능하다. 키 관리 구성 요소에 따라 KMI가 구성되기 때문에 키관리자는 키의 흐름을 쉽게 파악할 수 있다. 따라서 암호시스템에서 키에 대한 공격에 취약점 분석이 용이해지며 공격에 따른 신속한 대응이 가능하기 때문에 시스템의 안전성이 향상된다. 또한, 가시적인 키 관리는 시스템의 사용자에게 더 높은 신뢰성을 제공할 수 있다.

3.2 효율성

(1) 시스템을 사용하는 동안에 추가적으로 발생하는 요구사항에 의해 KMP는 변경될 수 있다. 본 고에서 기술하는 키 관리 기술을 적용한 암호시스템은 KMP가 변경되더라도 쉽게 KMI의 변경이 가능하다. KMP가 변경되었을 경우 변경 부분만 KMSS에서 수정하고 이를 바탕으로 KMI를 부분 수정하는 것으로 변경된 KMP가 적용된다.

(2) 키 관리 기술의 KMI는 많은 암호시스템에 사용하는 소켓을 이용한 클라이언트·서버 모델과 같다. 따라서 설계 시 KMI가 암호시스템의 구조에 쉽게 적용이 가능하다.

Ⅳ. 결 론

본 고에서 기술하는 키 관리 요소에 대한 통합 키 관리 기술은, 암호시스템의 안전성 향상과 관리 측면에서의 효율성을 제공한다. 키 관리 기술을 암호시스템의 설계 단계부터 적용함으로써 암호시스템의 안전성을 향상시킬 수 있으며, 또한 가시적인 키 관리가 가능하기 때문에 사용자의 암호시스템에 대한 신뢰도를 향상시킬 수 있다.

현재 대부분의 암호시스템은 통합 키 관리 기능을 지원하지 않는다. 통합 키 관리를 위해 기존에 사용하는 암호시스템을 통합 키 관리가 가능한 시스템으로 대체하는 것보다 기존 암호시스템에 키 관리 기술을 적용하는 것이 더욱 효율적이다. 본 고의 연구 결과는 향후 키 관리 기술을 기반으로 암호시스템을 설계할 경우, 키 관리에 대한 가이드라인을 제시할 것으로 기대되며, 기존의 암호시스템에 적용하기 위한 추가적인 연구를 통해 추가적인 비용을 최소화하기 위한 연구를 진행해야 할 것이다.

참 고 문 헌

〔1〕 D.W.Davies, W.L.Price, "Security for Computer Networks", John Wiley & Sons, New York, 2nd edition, 1989

〔2〕 W.Fumy, P,Landrock, "Principles of key management", IEEE Journal on Select- ed Areas in Communications, pp. 785- 793, 1993

〔3〕 Alfred J.Menezes, Paul C.van Oorschot, Scott A.Vanstone, Handbook of Applied Cryptography, pp. 543-590, 1996

〔4〕 R.A.Rueppel, "Criticism of ISO CD 11166 banking key management by means of asymmetric algorithms", Proceedings of the 3rd Symposium on State and Pro- gress of Research in Cryptography, pp. 191-198, 1993

〔5〕 M.Abadi, R.Needham, "Prudent engineering practice for cryptographic protocols", Digital Equipment Corporation, DEC SRC report #125, 1994.

〔6〕 R.Anderson, E.Biham, "Robustness principles for public key protocols", Advances in Cryptology-CRYPTO '95, LNCS 963, pp. 236-247, 1995

〔7〕 S.M.Matyas, C.H.Meyer, "Generation,

distribution, and installation of cryptographic keys", IBM Systems Journal, 17, pp. 126-137, 1978
[8] ISO/IEC 11770-1, Information technology-Security techniques-Key Management-Part 1 : Framework, ISO, 1996
[9] IEEE P1363, Standard Specifications For Public Key Cryptography, IEEE, 2001
[10] ISO 10202-7, Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards - Part 7: Key management, ISO, 1998
[11] Russ Housley, Tim Polk, "Planning for PKI", Wiley Computer Publishing, New York,2001
[12] NIST, Guideline for the Certification and Accreditation of Information Technology Systems, NIST Special Publication 800-37, 2003
[13] NIST, Key management guideline - Part 2: Best Practices for Key Management Organization, NIST Special Publication 800-57, 2003
[14] NIST, Guideline to Federal Organizations on security Assurance and Acquisition /Use of Tested/Evaluated Products, NIST Special Publication 800-23, 2000

〈著 者 紹 介〉

송 기 언 (Kieon Song)
학생회원

2003년 2월 : 성균관대학교 정보공학과 졸업(학사)
2003년 3월~현재 : 성균관대학교 컴퓨터공학 석사과정

이 진 우 (Jinwoo Lee)
학생회원

2003년 2월 : 성균관대학교 정보통신공학부 졸업(공학사)
2003년 3월~현재 : 성균관대학교 컴퓨터공학과 석사과정

곽 진 (Jin Kwak)
학생회원

2008년 8월 : 성균관대학교 바이오메카드로닉스 공학과 졸업(공학사)
2003년 2월 : 성균관대학교 대학원 전기전자 및 컴퓨터 공학부 졸업(공학석사)
2003년 3월~현재 : 성균관대학교 정보통신공학부 박사과정

양 형 규 (Hyungkyu Yang)
정회원

1983년 2월 : 성균관대학교 전자공학과 졸업(공학사)
1985년 2월 : 성균관대학교 대학원 전자공학과 졸업(공학석사)
1984년 12월~1991년 2월 : 삼성전자 선임 연구원
1995년 2월 : 성균관대학교 대학원 정보공학과 졸업(공학박사)
1995년 3월~현재 : 강남대학교 컴퓨터미디어공학부 부교수

원 동 호 (Dongho Won)
종신회원

성균관대학교 전자공학과 졸업 (학사, 석사, 박사)
1978년~1980년 : 한국전자통신연구원 전임연구원
1985년~1986년 : 일본 동경공대 객원연구원,
1988년~1999년 : 성균관대학교 교학처장, 전기·전자 및컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장
1996년~1998년 : 국무총리실 정보화추진위원회 자문위원,
2002년~2003년 : 한국정보보호학회장
2002년~2004년 : 성균관대학교 연구지원처장
현재 : 성균관대학교 정보통신공학부 교수, 정통부 지정 정보보호 인증기술 연구센터 센터장, 성균관대학교 연구지원처장