전자결재시스템의 기능복원을 위한 비밀분산 방식의 키복구 시스템

진 현 수*

◈ 목 차 ◈

1. 서 론

컴퓨터를 이용한 정보처리가 일반화되고 컴퓨터 통신망을 통한 문서 양식의 통폐합 및 간소화는 되었지만 문서의 결재는 여전히 수작업으로 이루어지고, 컴퓨터의 역기능이 급증하면서 문서에 대한 보안 사항들의 부정 유출도 심해서 기업의 비밀이 타기업으로 넘어가 커다란 타격을 받는 경우가 발생하나 최근 정보처리 기술이 급격히 진보되어 컴퓨터 통신 회선을 통해 서로 연결되고 수많은 단말기들이 근거리 또는 원거리에 부착됨에 따라 명실상부한 종합적 정보시스템이 구축되고 있으며 이러한 정보시스템의 보급 확대로 우리사회는 고도의 정보화 사회로 진입되고 있다. 그런데 이러한 모든 정보들은 점차적으로 종이 문서의 형태에서 전자적 형태로 변환되어 있으니 개인간의 전화, 팩스, E-mail등의 이용은 보편화되었으며 개개인의 건강/인사 기록과 같은 사적인 정보에서부터 은행간의 거래, 중요한 사업상의 정보등의 기밀성을 요하는 자료 및 비행관제 시스템, 교통정보 시스템등과 같은 국가 기간망에 이르는 많은 정보들이 전자적 형태로 이동되고 있다. 이처럼 전자적인 정보의 유통량이 증가하고 정보의 가치가 높아질수록 정보보호의 문제가 부각된다. 정보보호란 보다 안전하고 신뢰성 있게 정보를 전달할 수 있도록 하는 것으로 암호학에 그 기반을 두고 있다. 암호란 키와 수학적인 알고리즘을 이용하여 평문을 알아보기 힘든 암호문의 형태로 변환시키는 것으로 안전하게 구현된 암호시스템에서는 키를 알지 못하는 사람은 암호화된 데이터를 복호할 수 없다는 것을 전제로 한다.

암호의 사용으로 인한 정보의 누출 및 오용을 방지하고 상대의 신원 확인을 가능케하나 본래 가지고 있는 키관리의 어려움 때문에 다음과 같은 문제를 발생시킬 수 있다.

첫째, 키의 분실이나 손실로 인해 사용자가 자신의 키(또는 암호문)에 접근할 수 없을 경우

둘째, 국가가 범죄 수사등의 적법한 이유로 키에 접근해야 할 필요성이 있을 경우 범죄자는 암호문을 사용함으로써 합법적인 수사를 방해 할 수 있다.

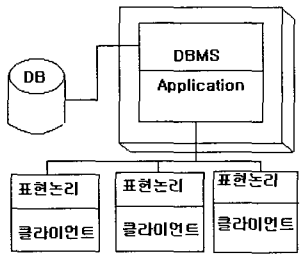
셋째, 암호가 오용됨으로써 발생할 수 있는 잠재적인 위협이다. 사업장에서 피고용인이 중요한 정보를 암호화하고 키를 담보로 금품을 요구할 수 있는데 본 분에서는 이와 같은 위협에 대응하기 위하여 비밀 분산에 기반한 안전한 키복구 방식을 전자 결재 시스템에 적용하여 위와 같은 문제점을 해결하고자 함이다. 전자 결재 시스템은 현 업무가 갖고 있는 보안 사항들의 부정 유출이 심각한 문제들로 대두되면서 적절한 결재 시스템에서 중요한 부분중의 하나가 데이터의 보안이므로 보안상의 특징과 전자결재 시스템에서 암호화 방법에 대해서 연구한다.

전자 결재 시스템구성의 특징은 네트워크상에 트래픽을 줄이기 위해서 단위 부서별로 브리지/라우터 기능이 있는 LAN장비를 도입했으며 문서관리용 결재

* 천안대학교 정보통신학부 조교수

(표 1) Client/Serve의 기능

클라이언트	서버
사용자 인터페이스 담당	결재경로변경
기안 문서 작성	결재진행상태관리
문서 결재	부서별 문서관리
문서 조회	부서별문서 조회



(그림 1) 전자결재 시스템의 네트워크 구성도

서버를 단위 부서별로 두는 클라이언트/서버간에 기능을 분담하도록 데이터 베이스를 설계하였고 사용자별 PC로 구성된 클라이언트에서는 안내 및 에러화면과 같은 사용자 인터페이스 기능, 기안 문서작성기능, 결재처리 조회등 관리기능을 담당하고 서버 시스템에서는 결재진행상태관리, 부서별 문서관리의 기능을 담당한다.

시스템 하구 구조인 네트워크는 그림 1과 같이 PC간에 통신 기술을 활용하기 위해서 윈도우즈 NT3.51 환경에서 윈도우즈 프로그래밍 언어인 Visual Basic을 이용하여 문자 도형등이 포함된 복합 정보에 대해서는 문서의 보관 및 전송이 쉽고 편리하게 하였고 결재권자가 문서의 반송을 위해 사용한 음성 합성의 원리를 이용한 녹음기 기능은 사운드 카드를 사용하였으며 문서 처리 기능에서는 윈도우즈 워드프로세서를 사용할 수 있게 구성하였다.

2. 전자 결재 시스템의 암호문 관리

정보에 대한 접근은 기본적으로 읽기, 쓰기, 실행 등의 유형이 있다. 각 사용자들이 각 파일에 대해서 읽기, 쓰기, 실행 중 어떤 종류의 접근을 할 자격이 있는지 적절한 기준에 따라 명시하여야 하며 접근의 통제를 위해서는 사용자에 대한 3가지 통제의 개념이 필요하다.

1) 식별(Identification):입력된 패스워드가 정당한 패스워드인가를 체크하고 패스워드의 주인을 식별한다.
2) 인증(Authentication):패스워드를 입력한 사람이 그 패스워드의 정당한 주인인가를 인증 한다.
3) 허가(Authorization):패스워드를 입력한 사람이 요구하는 작업이 그 패스워드의 주인에게 인가된 작업인가를 확인한다, 이는 각 부서원에 대해 각 파일에 대한 접근 유형별 자격을 미리 컴퓨터에 입력 저장하여 둠으로써 수행된다.

3. 전자 결재 시스템의 설계

문서 양식의 통폐합 및 간소화로 전산 자료의 전송 체제와 전자우편을 이용한 정보의 전달과 의사소통은 신속성과 간편성을 이룩해 왔으나 문서의 결재 과정은 여전히 인쇄된 문서에 서명을 하는 체제를 유지하고 있다. 이로 인한 기안자와 수신자의 결재 과정을 공통적으로 인쇄기를 통해 출력된 문서에 서명을 하는 결재 과정을 유지하면서 문서를 별도로 보관하는 이중 보관 체제를 가질 수밖에 없으며 특히 지점이 원거리에 있는 경우에 결재권자에게 결재를 위해서 우편발송이나 결재권자에게 직접가야 하는 소요시간 및 인적 낭비가 있을 뿐만 아니라 보안의 여러 측면을 고려하여 사원들이 알고 있는 정보를 교체하기 위해서 각 부서를 강제로 이동시키는 것은 당연한 것으로 생각했다. 기존의 많은 기업들은 사원들간에 신뢰를 기본으로 중요한 결재 문서를 결재권자의 손으로 서명을 하면서 개인에 대한 프라이버시의 침해뿐만이 아니라 이미 결재된 보관 문서의 내용이 사원들에게 공개되어서 기업의 기밀이나 보안 유지가 되지 않아 쉽게 경쟁기업으로 넘어가 자회사에 커다란 타격을 받는 경우가 발생했다. 이런 수작업으로 작성된 문서 등을 보관 또는 이관하는 작업을 효율적으로 이용하고 기밀이나 보안 유지의 해결 방법으로 전자결재 시스템을 이용하다 전자 결재 시스템의 기본 기능은 표 2와 같다.

3.2 전자결재의 키복구기능

3.2.1 키복구 시스템

키복구 방식의 정의는 사전에 약속된 어떤 특정한 조건하에서 허가된 개체에게 암호문의 키나 평문의

(표 2) 전자결재시스템의 기본 기능

기본설계	주요기능
문서작성	기안을 위한 양식 사용, 문서지정, 결재경로의 지정, 문서의 발송등을 한다.
문서결재	결재권자의 미결문서에 대해 문서보기, 결재, 반송, 결재 경로 변경 등의 작업 관리를 한다
문서정보	미결재 문서 및 이관전의 반송 서류에 대한 정보를 가진다
부재정보	사용자의 출장등에 대비하여 자신의 부재를 등록.결재권자의 부재정보를 참조할수 있다.
문서이관	결재 문서에 대해 완결이 되고 참조가 완료된 후 기안자가 따로 보관하고자 할 경우의 해당 문서에 대한 이관 작업을 한다
작업종료	전자결재의 모든 작업을 종료한다

복구가 가능한 능력을 제공하는 기법이라고 할 수 있다. 이러한 키복구 시스템은 크게 두가지로 분류할 수 있다, 첫 번째는 비밀키 위탁방식으로 자신의 비밀키의 일부 또는 전부를 특정한 방법으로 복구기관이나 기타 신뢰기관에 위탁하는 것이다. 이 방법은 복구가 필요할 때 비밀키를 얻게 되므로 유사이에 키(또는 평문)을 얻을 수 있는 확실한 보장이 되며, 해당 사용자의 모든 암호화에 관련된 행동에 대한 확인이 가능하다. 이러한 속성은 범죄수사나 범죄 방지 등에는 매우 용용하게 사용될 수 있으나 일반 사용자의 입장에서는 프라이버시의 침해에 대한 우려와 같은 이유로 인해 거부감을 느낄 수 있다. 또한 키가 유출되면 해당 사용자가 키를 바꾸기 전 까지는 복호화 뿐만이 아니라 키를 사용한 인증이나 다른 기능에 대한 위/변조가 가능하기 때문에 위탁된 키를 고관하는 보관 기관이 신뢰성과 보관 방법의 안전등이 보장되어야 한다. 이러한 방식으로는 Clipper라고 불리우는 미국의 EES(Escrow Encryption Standard),영국의 GCHQ프로토콜등이 있으며 이에 대한 여러 가지 문제점과 개선 방향에 대한 연구가 진행되었다.

두 번째로는 키 복구 필드를 생성해서 암호문에 부가한 후, 복구가 필요한 경우 이 영역에 포함된 정보를 바탕으로 암호화에 사용된 키나 평문을 복구하는 캡슐화 방식이 있다 이방식은 키위탁 방식과는 달리 비밀키 정보의 위탁이 일어나지 않고, 해당 암호문을 복구할 수 있는 세션키만을 이용하기 때문에 키 복구 시에 발생할 수 잇는 문제점을 줄일수 있다, 하지만 이 방식의 경우 사용자가 생성하여 암호문에 부가하기 때문에, 복구 필드에 대한 수정이나 조작이 가능해서 유사시에 키를 얻을 수 없는 경우가 발생할 가능성을 내포하고 있다. 일반적으로 TIS사의 Recovery Key, IBM사의 Secure Way 등과 같은 상용시스템에서 이런 방식을 적용하였다.

3.2.2 비밀 분산 방식

비밀 분산에 대한 개념은 Shamir와 Blakley가 각각 소개한 이후로 많은 방식에 대한 연구가 진행되었다. 비밀 분산이란 어떠한 비밀 정보가 있을 때 이것을 여러개의 정보로 분할 한 후 각각의 참여자에게 분배하고 모든 사용자에게 분할된 정보를 모으면 다시 비밀 정보를 복원할 수 있는 방식을 말한다. 각각의 분할된 정보를 shadow라고 한다. 이것은 안정성과 효율성을 위해 n개의 shadow가 있을 때 k($\leq$n)개의 shadow만을 모으면 비밀 정보가 복구 가능하도록 구성 될 수 있다. 이것을 [k,n] threshold방식이라고 하며 다음과 같은 성질을 갖는다.

- 비밀정보 S 는 n개의 shadow로 분할된다.
- k개 이상의 shadow를 모으면 s는 쉽게 계산된다.
- k-1이하의 shadow는 S에 대한 아무런 정보도 주지 않는다.

3.2.3 비대화형 증가가능한 비밀 분산 방식

이 방법은 shadow의 수신자가 분배자나 다른 수신자와 상호 작용하지 않고 자신의 shadow 가 올바른 것이지 확인할 수 있다.

위의 위탁 방법과 같은 g, h $\in z_q$를 선택한 후 s $\in Z_p$를 다음과 같이 분배한다.

1) 분배자는 다음과 같을 S를 위탁하기 위한 E_0를 계산한다.
   $E_0 = E(s, t) = g^s h^t$($t \in Z_q$는 랜덤)
2) 분배자는 F( )=S를 만족하는 k-1차의 다항식 F $\in Z_q[x]$를 선택하고 다음의 shadow 정보 S_i 를 계산한다.
   S_i=F(i)(i=1,.....,n)

3) 위에서 선택된 임의의 다항식을
F(x)=s+ $a_1 x + \ldots + a_{k-1} x^{k-1}$이라 하자 분배자는 $b_1, \ldots, b_{k-1} \in Z_q$를 랜덤하게 선택하고 b_i 를 이용해서 다항식의 지수 a_i (i=1,...,k-1)를 위탁하기 위한 E_i 를 다음과 같이 계산한다.
$E_i = E(a_i, b_i)(i = 1, \ldots, k-1)$
4) G(x)=t+ $b_a x + \ldots + b_{k-1} x^{K+1}$이라고 할때 다음과 같은 shadow확인정보 t_i를 계산한다
$t_i = G(i)(i = 1, \ldots n)$
5) 분배자는 (s_i, t_i)와 $E_i(i = 0, \ldots, k-1)$를 수신자 p_i (i=1,2,..,n)에게 안전하게 전송하다. p_i가 자신의 shadow와 확인정보 (S_i, t_i)를 받으면 다음을 양변의 결과가 일치하는지 확인한다
$E(S_i t_i) = \prod_{j=0}^{k-1} E_j^{i^j}$
6) 이후에 비밀 정보는 다음과 같이 계산된다
$S = \sum_{i \in S} a_i s_i (a_i = \prod \frac{i}{i-j})$

4. 전자 결재 시스템의 기능 복원을 위한 키복구 시스템

4.1 기존키 복구 방식의 안전성

기존의 방식의 키복구 시스템은 무결성과 기밀성을 만족해야 했고 널리 사용될 수 있도록 유연한 방식을 가져야 하였다 또한 사용자가 안전도를 확신할 수 있도록 복구방식의 상세한 부분들은 공개되는 것이 바람직했다, 또한 법집행을 방해해서는 안되었고 오용이 어려워야 하였고 오용의 감지는 쉽게 할 수 있었다. 그리고 마스터키로 도청이 시작되면 그 이후의 통신은 모두 노출되므로 도청시간의 제한에 대한 보장이 필요하였다. 또한 새롭게 개발된 알고리즘의 적용이 용이해야 하였다. 이러한 일반적인 공개키를 이용하면 사용자의 암호화된 메시지는 다음과 같은 요소로 구성되어 간단하게 키 복구를 구현할 수 있다.

1) 랜덤한 세션키를 선택한 후 그 키를 이용해서 암호화된 메시지
2) 수신자의 공개키로 암호화된 세션키
3) 복구기관의 공개키로 암호화된 세션키

이와 같이 구성된 복구정보를 메시지에 부가하면, 복구기관이 메시지를 복원할 필요성이 있을 경우에 자신의 공개키로 세 번째 영역을 복구해서 세션키를 얻을 수 있다. 이 방법에서는 사용자의 키를 위탁할 필요가 없다. 단지 통신에 사용되는 임시적인 세션키에 대한 접근 능력을 부여해 주면 된다. 이와 같은 개념은 몇 가지 복구 방식의 기반을 이루고 있다, 그러나 이 개념의 중요한 약점은 세 번째 영역이 정말로 올바른 세션키를 포함하고 있는지를 검사할 수 없다는 것이다. 이것은 복구 기관이 복호를 시도해 볼 때까지는 알 수 없다. 제안 방식에서는 이러한 검사 시점을 암호문을 평문으로 바꾸는 복호 시점에서 좀더 앞당길 수 있도록 한다.

4.2 구성 방식

본 절에서는 제안된 방식에서 키복구 필드를 구성하는 방법을 소개한다

○ 사전 계산 단계
1) 송신자는 자신이 전송하고자 하는 평문을 랜덤한 세션키를 가지고 암호화한다.
c= $E_s(M)$ (s:세션키)
2) 송신자는 암호화에 사용된 키를 이용해서 다음과 같은 위탁방식에 근거해서 키를 위탁한 정보 E_0를 계산한다
$E_0 = E(S, t) = g^s h^t$
(g,h $\in G_q, s \in Z_p t \in Z_q$는 랜덤)
여기서 g, h는 사전에 복구기관에 의해 선택되어 모두가 알고있는 공개 파라미터이다
3) 송신자는 F(0)=S를 만족하는 타함수 F $\in Z_q[x]$를 선택한 후 다음을 계산한다
$S_i - F(i)(i = 1, 2, 3)$
4) F(x)=s+ax이라 하자 송신자는 b $\in Z_q$을 랜덤하

게 선택하고 b를 이용해서 a를 위탁하기 위한 정보 E_1을 계산한다.

$E_1 = E[a, b] = g^a h^b (i = 1, \ldots, k-1)$

5) G(x)=t+bx 라고 할 때 다음의 확인 정보 t_i를 계산한다.

$t_i = G(i)(i = 1, 2, 3)$

○ 복구필드 생성 단계

1) (S_i, t_i)을 수신자의 공개키로 암호화한다.

2) ($s_2 t_2$)를 보구기관의 공개키로 암호화한다.

3) (s_3, t_3)와 계산된 s와 a의 위탁 정보 E_0, E_i를 연접(concatenation)한다

4) 1, 2, 3 항목을 연접하고 송/수신자의 식별자, 복구기관의 식별자, 사용된 암호 알고리즘 등과 같은 부가 정보를 붙인 후 자신의 공개키로 서명한다.

5) 위와 같이 구성된 복구 필드를 1단계에서 암호화한 암호문 c와 연접한다.

○ 세션키 정보 확인

다음과 같은 연립 방정식의 해를 구함으로써 수신자나 복구기관은 세션키 S를 얻을수 있다

1) 수신자 : 영역 1과 3의 정보를 이용해서 세션키를 재조합 한다.

$S=S_1-a*1, s= S_3-a*3$

2) 복구기관: 영역 2와 3의 중보를 이용해서 세션키를 재조합 한다.

$S=S_1-a*2, s= s_3-a*3$

5. 결 론

제안된 방식은 다음과 같은 안전도를 갖는다. 첫 번째 영역은 수신자만이 자신의 비밀키로 복구할 수 있다. 두 번째 영역은 복구 기관만이 자신의 비밀키로 복구할 수 있다. 비밀 분산의 개념에 의해서 세 번째 영역에 공개된 shadow는 키에 대한 어떠한 정보도 포함하지 않는다. 즉 복구 필드는 전체 시스템의 비도에 영향을 미치지 낳는다. 송신자의 위와 같은 복구 프로토콜에 따른다면 복구기관은 두번째와 세 번째 영역의 shadow를 조합해서 키를 재구성 할 수 있다. 세번째 영역에 대한 shadow를 조작한다면 수신자조차도 암호와에 사용된 키를 얻을 수 없다.

송신자가 복구 기관에게 전송되는 정보를 조작하면 확인 단계에서 shadow를 확인 가능한 성질에 따라 암호문을 해독하지 않고도 조작 여부를 알수 있다. 복구기관은 자신의 공개키로 암호화된 정보를 비밀키로 복호한 후에 올바른 shadow인지를 확인하고, 저장해 두거나 랜덤하게 추출된 임의의 통신문에서 이와 같은 작업을 수행함으로써 사용자의 부정 조작을 검출하거나 방지할 수 잇다.

본문에서는 암호 사용시에 발생 할 수 있는 키의 분실 및 암호의 오용이나 악용을 방지하기 위한 새로운 키 복구 방식을 제안하였다. 키에 대한 적법한 접근이 필요할 때 올바른 키를 얻을 수 있도록 키 복구 필드의 구성 방법 및 복구 필드의 조작에 대한 방지와 검출이 가능하도록 한 방식을 제안하였다. 이 방식은 앞서 살펴 본 바와 같이 암호문을 복호하지 않고서도 복구키의 조작 여부를 알 수 있다 또한 키를 사용하는 모든 암호화 알고리즘에 적용가능하며 다양한 암호정책과 모델에 적용 할 수 있다. 구현은 소프트웨어나 하드웨어 모두 가능하며. 프로토콜의 확장과 가상의 수신자를 지정함으로써 복구기관을 쉽게 추가하거나 바꿀 수 있다. 그리고 복구기관의 신뢰도를 높이기 위해서는 복구기관의 비밀키를 비밀 순산을 사용하여 분배하거나 암호문의 성격에 따라 복구기관 의 선택을 사용자가 하는 등 기존에 제안되었던 방식의 적용이 가능하다.

참고문헌

[1] j.p Anderson, "Computer Security Technology Planning Study", EDS-TR_73-51,prepared for Deputy for Command and Management Systems,Hq Electronic System Davissio(AFSc), L.G.Hanscom Field Bedford, Mass, October 1972, Vol. 1, 2.

[2] Anderson, J.Computer Security Threat Monitoring and Surveillan ce. Fort Washington, PA:James P. An-

derson Co., april 1980.

[3] Bauer, D., and Koblentz, M. NIDX-An Expert System for Real-Time Network Intrusion Detection. Proceedings, Computer Networking Symposium, April 1988.

[4] Denning, d. An Intrusion-Detection Model. IEEE Transactions Software Engineering, February 1987.

[5] hEBERLEIN, L.:Mukherjee, B.:and Levitt, K. Internetwork Security Monitor : An Intrusion Detection System for Large-Scale Networks. Proceedings, 15th National Computer Security Conference, October 1992.

[6] Lunt, T., and Jangannathan, R.A Prototype Real-Time Intrusion_Detection Expert System. Proceedings, 1988 IEEE Computer society Symposium on Research in Security and Privacy,April 1988.

[7] Porras, P.STAT: A Stat Transition Analysis Tool for Intrusion Detection. Masters Thesis, University of California at Santa Barbara, July 1992.

[8] Simon Garfinkel and Gene Spafford, "Practical UNIX Security", O'Relilly and Associates, Inc, 1994.

[9] Snapp, S., et al., A System for Distributed Intrusion Detection. Proceedings, COMPCON Spring 91, 1991.

[10] Silvana Castano, Maria Grazia Fugini, Giancarlo Martella, Pieranglela Samarati, "Database Security", ACM Press,1995.

◐ 저 자 소 개 ◑

진 현 수

1982년~1986년 서울시립대학교 전자공학과(공학사)
1990년~1992년 서울시립대학교 전자공학과(공학석사)
1993년~2000년 서울시립대학교 전자공학과(공학박사)
2001년 3월~현재 : 천안대학교 정보통신학부 조교수
관심분야 : 퍼지시스템, 정보보안. 인공생체면역시스템, 로봇