C. Boyd 의 순차 다중서명 방식을 적용한 전자 결재 시스템*

최재영, 박선우, 전웅렬, 원동호**
성균관대학교 정보통신공학부 정보보호연구소
e-mail : fiffa01@gmail.com, {swpark, wrjeon, dhwon}@security.re.kr

Electronic Approval System Using C.Boyd Sequential Multisignature

Jae-Young Choi, Dongho Won
Information Security Group, School of Information and Communication Engineering
SungKyunKwan University

요 약

전자 결재 시스템은 오프라인 문서 결재보다 효율적인 문서 관리가 가능 하고 예산 낭비를 방지할 수 있으며, 작업 능률을 극대화 할 수 있다는 장점 때문에 현재 많은 기업에서 도입하여 사용하고 있다. 하지만 상용화되어 있는 전자 결재 시스템에서 사용되는 이미지 서명은 복제 및 위조가 가능하다는 위협이 존재한다. 이러한 문제를 해결하기 위해서 단순 서명 방식을 적용한 전자 결재 시스템이 제안되었다. 하지만 단순 서명 방식을 이용한 전자 결제 시스템은 단 한 명의 결재자만을 고려한 시스템으로 실제 기업에는 다양한 직책의 결재자가 존재하기 때문에 적용하기가 어렵다. 이에 본 논문에서는 C.Boyd 의 순차 다중서명 방식을 사용하여 다수의 결제자가 서명할 수 있는 전자 결제 시스템을 제안한다.

1. 서 론

전자 결재 시스템이란 기존의 종이 서류를 사용 한 오프라인 방식의 결재를 전산화한 것으로, 전산망을 이용해 문서의 승인이나 신고 등의 업무를 처리하는 시스템을 말한다. 전자 결재 시스템은 오프라인 문서 결재보다 효율적인 문서 관리가 가능하고 문서 출력 과정이 생략됨으로써 예산 낭비를 방지할 수 있으며, 작업 능률을 극대화 할 수 있다는 장점 때문에 현재 많은 기업에서 도입하여 사용하고 있다.

현재 상용화되어 있는 대부분의 전자 결재 시스템은 전자 펜을 이용하여 서명 이미지를 생성하거나 사전에 저장해놓은 서명 이미지를 사용하는 이미지 서명 방식을 사용하고 있다. 하지만 이러한 방식에 사용되는 서명 이미지는 쉽게 복제가 가능하기 때문에 서명 위조의 위협이 존재하며 따라서 서명 부인 방지 기능을 제공하기 어렵다. 뿐만 아니라 현 전자 결재 시스템에서는 서명의 대상이 되는 원문의 내용 역시 쉽게 변조가 가능하기 때문에 결재 내용에 대한 무결성을 제공하지 못하고 있다.[3]

이러한 문제를 해결하기 위해 김창수, 정희경은 RSA 공개키 알고리즘을 기반으로 하는 단순서명 (Single Signature) 방식을 적용한 전자 결재 시스템을 제안하였다. 그러나, 제안된 방식은 서명자가 한 명인 경우만을 고려하여 설계된 시스템 이기 때문에 실제 환경에 적용하기에는 어려움이 있다.

이에 본 논문에서는 다중서명(Multisignature) 기술을 적용한 전자 결재 시스템을 제안함으로써 이전에 제안된 단순서명 방식을 적용한 전자 결재 시스템의 문제를 해결하고자 한다.

본 논문의 구성은, 2장에서 단순서명 방식을 적용한 전자 결재 시스템과 C.Boyd 의 다중서명 방식을 설명하고, 3장에서 C.Boyd 의 다중서명 방식을 적용한 전자 결재 시스템을 제안한다. 마지막으로 4장에서 결론을 맺는다.

2. 관련연구

2.1 단순서명 방식 기반 전자 결재 시스템

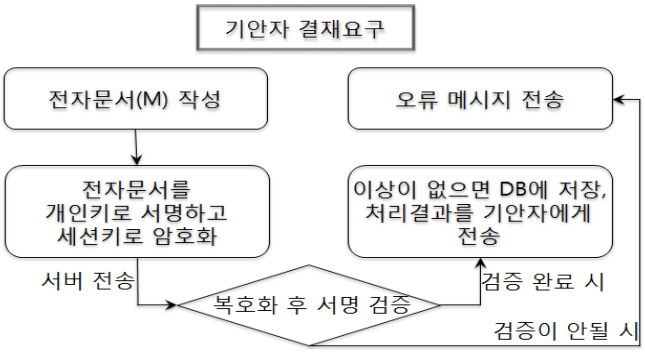
단순서명 방식을 적용한 전자 결재 시스템은 결재 문서를 XML 문서로 변환한 뒤 이미지 서명 대신 RSA 공개키 알고리즘을 기반으로 하는 전자서명을 이용한 시스템으로 과거의 시스템들이 지니고 있던 문서의 무결성, 서명 부인 방지, 기밀성 문제 등 여러 보안 문제를 해결하였다[1].

<표 1> 본 논문에서 쓰이는 표기 및 설명

표기	설명	표기	설명
Pri	개인키	Dec	복호화
Pub	공개키	Doc_Num	문서번호
S_key	세션키	Sign_Info	결재 정보
Sign	서명	IDcm	결재자 리스트
Verify	서명 검증	Drft	기안자
H()	해쉬값	Svr	서버
Enc	암호화	Signer	결재자

결재요구 및 처리는 다음과 같은 순서로 진행된다.

2.1.1 기안자의 결재 요구



(그림 1) 기안자의 결재 요구

①기안자는 전자문서(M)에 대한 해쉬값(H(M))을 생성하고 자신의 개인키로 전자서명을 수행한다. 전자문서를 세션키로 암호화한 뒤, 서명 값과 함께 서버에 전송한다.

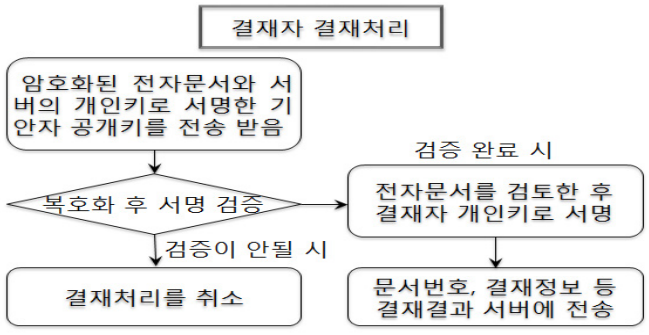
$$Sign_{Pri\_Drft}[H(M)]||Enc_{S\_key}(M)||Sign_{Pri\_Svr}[Pub\_Drft]$$

②서버는 암호화된 전자문서를 세션키로 복호화 한 뒤, 서명 값에 대한 서명 검증을 수행한다. 서명 검증을 성공하면 문서를 DB 에 저장한다.

$$Dec_{S\_key}[Enc_{S\_key}(M)] \rightarrow M \rightarrow H'(M)$$

$$Verify_{Pub\_Drft}[Sign_{Pri\_Drft}[H(M)]] \rightarrow H(M)$$

2.1.2 결재자의 결재 처리



(그림 2) 결재자의 결재 처리

① 결재자는 서버로부터 암호화된 전자문서와 서버의 개인키로 서명한 기안자의 공개키를 전송 받는다.

$$Sign_{Pri\_Drft}[H(M)]||Enc_{S\_key}(M)||Sign_{Pri\_Svr}[Pub\_Drft]$$

② 결재자는 암호화된 전자문서를 세션키로 복호화 한 뒤, 서버로부터 전송 받은 기안자의 공개키를 사용하여 서명 검증을 수행한다. 만약 두 값이 일치하지 않으면 결재는 취소 된다.

③ 결재자는 전자문서를 검토한 후 해쉬값(H(M))에 자신의 개인키로 전자서명을 수행한다. 서명 값, 문서번호(Doc_Num), 결재 정보(Sign_Info, 결재, 보류, 거부 등)를 서버로 전송한다.

$$Sign_{Pri\_Signer}[H(M)]||Doc\_Num||Sign\_Info||Sign_{Pri\_Svr}[H(M)]$$

단순서명 방식을 적용한 전자 결재 시스템은 한 사람의 결재자만을 고려한 시스템이다. 하지만 실제 업무 환경에서는 기안자, 중간결재자, 최종결재자가 단계별로 서명하는 것이 일반적이기 때문에, 단순서명 방식을 적용한 전자 결재 시스템은 실제 환경에 적합하지 않다.

2.2 C.Boyd 의 다중서명 방식

본 논문에서는 C.Boyd 의 순차 다중서명 방식을 사용하여 여러 명이 단계적으로 서명이 가능한 전자 결재 시스템을 제안하고자 한다.

C.Boyd 는 Ohata-Okamoto 의 다중서명 방식이 하나의 난수를 사용할 때, 서명자가 관리해야 할 비밀키의 수가 많아지는 점을 보완하여 여러 개의 난수를 이용하여 비밀키의 수를 줄인 방식이다[4].

2.2.1 C.Boyd 의 서명 생성 및 검증 알고리즘

<표 2> C.Boyd 서명생성 알고리즘

		서명자 1	서명자 i
서명생성 1	수신	M, X_1, …, $X_t = 1$	M, IDcm, X_1,…, X_t
	공통키 발생	i = 1 to t $R_i(i) \in Z_n$ $X_i(1)=R_j(1)^2 \pmod N$	i = 1 to t $R_i(i) \in Z_n$ $X_i(i)=R_i(i)^2 \pmod N$ $X_i(i)=X_i(1)X_i(2)\cdots X_i(i) \pmod N$
	송신	$X_i(1)$를 다음 서명자에게	$X_i(i)$ 를 다음 서명자에게, 마지막이면 첫 번째 서명자에게
서명생성 2	수신	M, IDcm, X_1,…,X_t	M, IDcm, X_1,…,X_t
	서명생성	i = 1 to t $(e_{i1}, \ldots, e_{ik})$ $=H(M, X_1, \ldots, X_t)$ $Y_i(1)=R_i(1)\prod_{e_{ij}=1} S_i(1) \pmod N$	i = 1 to t $(e_{i1},\ldots,e_{ik})$ $=(M, X_1, \ldots, X_t)$ $Y_i(t)=R_i(t)\prod_{e_{ij}=1} S_i(t) \pmod N$ $Y_i(t)=Y_i(t-1)Y_i(t) \pmod N$

	송신	(M, IDcm, X_1, …, X_t, Y_1, …, Y_t)를 다음 서명자에게	(M, IDcm, X_1, …, X_t, Y_1, …, Y_t)를 다음 서명자에게 마지막이면 서버로

이 서명생성 알고리즘 결과, 서명은 문서 M 과 $e_{i,j}$ 행렬 그리고 모든 y_i 로 이루어지게 된다. C.Boyd 의 서명 검증 알고리즘은 다음과 같이 실행한다.

$$V_i = \frac{1}{S_i(1)^2 S_i(2)^2 \cdots S_i(m)^2}$$

$$Z_i = Y_i \prod_{e_{i,j}=1} V_j(t) (\mathrm{mod}\ N) (\mathrm{for}\ j = 1, \cdots, k)$$

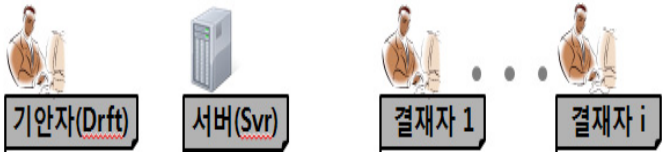
H(M, Z1, …, Zt)의 kt 비트가 e_{ii} 와 같은지 검사한다.[2]

3. 다중서명 방식을 적용한 전자 결재 시스템 설계

앞서 살펴본 단순서명 방식 기반 전자 결재 시스템은 RSA 암호 알고리즘을 도입하여 무결성, 서명 부인방지, 기밀성 문제 등 여러 보안 문제를 해결하였으나, 한 명의 결재자만 존재한다는 단점이 있다. 실제 기업환경에서는 결제자가 계층적으로 다수가 존재하기 때문에 단순서명 방식 기반 전작 결재 시스템은 적용이 어렵다.

이에 본 장에서는 C.Boyd 의 다중서명 방식을 기반으로 하는 전자 결재 시스템을 제안한다. 제안하는 전자 결재 시스템은 다수의 결재자를 허용하기 때문에 현실에 적용하기가 용이하다는 장점이 있다.

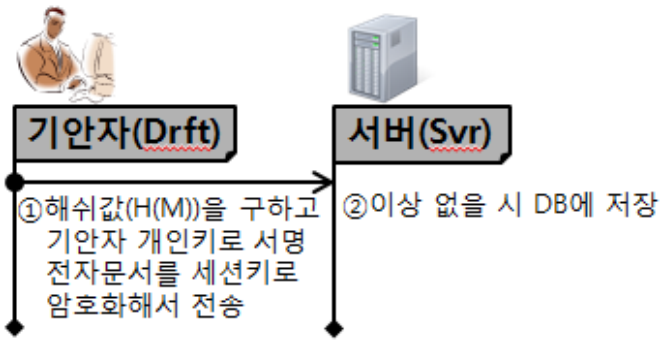
새로 제안된 전자 결재 시스템의 결재 요구 및 처리의 과정에 참여하는 객체들은 기안자와 서버 그리고 결재자 1 에서 i 까지 이다.



(그림 3) 다중서명 방식의 참여자들

다중서명 방식을 적용한 전자 결재 시스템의 결재 요구 및 처리는 다음과 같은 순서로 진행된다.

3.1 기안자의 결재 요구

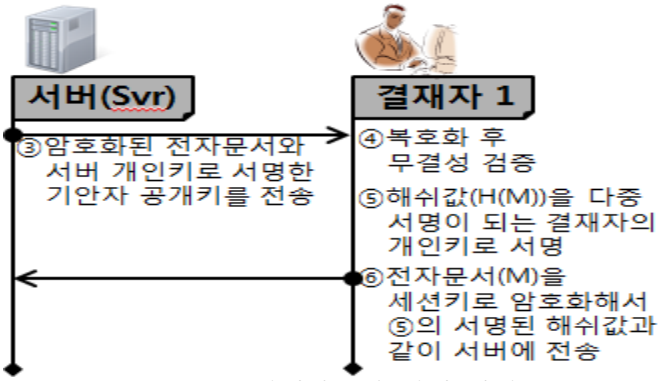


(그림 4) 기안자의 결재 요구

① 기안자는 전자문서(M)으로 해쉬값(H(M))을 구하고 자신의 개인키로 서명하고, 전자문서를 세션키로 암호화해서 서버에게 전달한다.

② 서버는 이상이 없으면 문서를 DB 에 저장한다.

3.2 결재자 1 의 결재 처리



(그림 5) 결재자 1 의 결재 처리

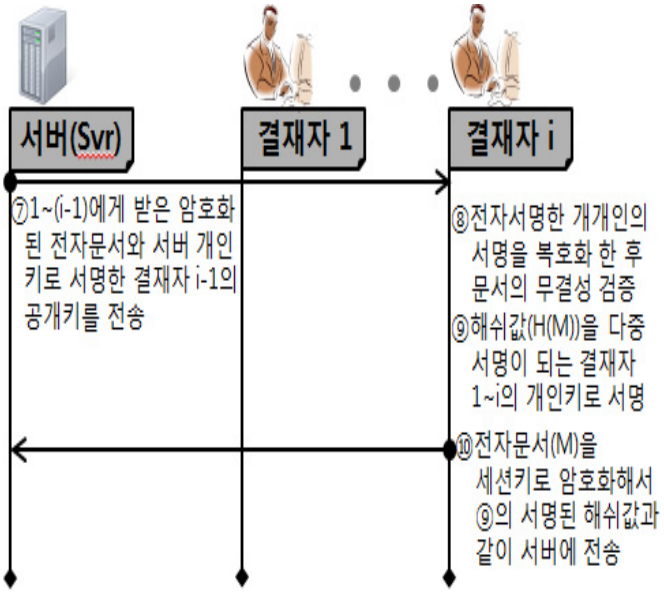
③ 서버는 기안자 개인키로 서명한 해쉬값 H(M), 세션키로 암호화된 전자문서 그리고 서버 개인키로 서명한 기안자 공개키를 결재자 1 에게 전송

④ 그 이후 이 기안자의 공개키로 복호화하고 나온 H(M)과 전자문서를 복호화하고 나온 M 으로 해쉬값(H(M))이 같은지 무결성 검증을 한다. 만약 두 값이 일치하지 않으면 결재는 취소가 된다.

⑤ 전자문서(M)을 검토한 후 해쉬값(H(M))에 다중 서명이 되는 결재자의 개인키로 서명한다.

⑥ 전자문서(M)을 세션키로 암호화하고 ⑤에서 만들어진 서명된 해쉬값과 같이 서버에 전송한다.

3.3 결재자 i 의 결재 처리



(그림 6) 결재자 i 의 결재 처리

⑦ 1~(i-1)에게 받은 암호화된 전자문서와 서버 개인키로 서명한 결재자 1~(i-1)의 공개키를 결재자 i 에게 전송한다.

⑧ 세션키로 암호화된 전자문서(M)을 복호화하고 해쉬값(H(M))을 구한다. 전자서명한 1 부터 i-1 의 서명

들을 복호화 한 후 나온 해쉬값들($H_1(M)$, …, $H_{i-1}(M)$)을 H(M)과 비교하여 문서의 무결성을 검증한다.
⑨ 해쉬값(H(M))을 다중서명이 되는 결재자 1~i 의 개인키로 각각 서명한다.
⑩ 전자문서(M)을 세션키로 암호화해서 ⑨에서 서명한 해쉬값과 같이 서버에 전송한다.

마지막 결재자 i 로부터 문서를 받은 서버는 결재처리 결과를 기안자에게 전송한다.

4. 결론

현재 상용화되어 있는 대부분의 전자 결재 시스템은 전자 펜을 이용하여 서명 이미지를 생성하거나 사전에 저장해놓은 서명 이미지를 사용하는 이미지 서명 방식을 사용하고 있다. 하지만 서명 이미지는 쉽게 복제가 가능하기 때문에 위조의 위협이 존재하며 따라서 부인 방지 기능을 제공하기 어렵다. 뿐만 아니라 현 전자 결재 시스템에서는 서명의 대상이 되는 원문의 내용 역시 쉽게 변조가 가능하기 때문에 결재 내용에 대한 무결성을 제공하지 못한다.

이에 김창수, 정희경은 RSA 공개키 알고리즘을 기반으로 하는 단순서명 방식을 적용한 전자 결재 시스템을 제안하였다. 그러나 제안한 방식은 서명자가 한 명인 경우만을 고려하고 있기 때문에 실제 환경에 적용하기에는 어려움이 있다.

이에 본 논문에서는 다중서명 기술을 적용한 전자 결재 시스템을 제안하였다. 본 논문이 제안한 방식은 다수의 결재자를 허용하기 때문에 실제 환경에 적용이 용이하다.

ACKNOWLEDGMENT

* “본 연구는 지식경제부 및 정보통신산업진흥원의 “대학 IT 연구센터 육성• 지원사업” 의 연구결과로 수행되었음" (NIPA-2011-C1090-1001-0004)
** 교신저자, dhwon@security.re.kr

참고문헌

[1] 암호 알고리즘을 이용한 XML 기반 비즈니스 문서의 전자 결재 시스템. 김창수, 정회경. Oct. 2006
[2] 다중 전자서명 알고리즘 연구 및 개발. C.Boyd 순차 다중서명 방식. Dec. 1999
[3] 보안향상을 위한 에이전트 기반 전자 결재 시스템 구현. 2010 by 김정훈
[4] C. Boyd "Multisignature based on zero-knowledge schemes"Electronic Letters, Vo1 27, 22, pp 2002-2004, Oct,1991