식별정보를 이용한 보안서버시스템의 전자서명 모델 및 응용

김 영 수[†] · 신 승 중[††]

요 약

서명시스템은 오늘날 전자상거래의 활성화를 위한 필수적인 기술로 인식되고 있으나 이의 응용시스템은 사용이 불편하고 보안성이 취약하여 사용자가 이의 사용을 꺼리고 있다. 따라서 사용자의 편의성과 보안성을 동시에 고려하는 서명시스템이 제공되어야 한다. 이의 해결을 위해서 사용자가 서명시스템에 투명하게 접근하여 서명과 검증을 할 수 있도록 식별정보를 사용하는 서버기반의 응용 모델을 제안하고 서명키를 생성하는 구성요소를 클라이언트와 서버에 분산하여 유지하도록 함으로써 서버공격으로부터 야기되는 위험을 감소시킬 수 있는 서명시스템을 설계하고 검증하였다. 서명시스템의 응용 모델은 경량급 서버시스템을 인프라로 사용함으로써 경제성을 높이는 동시에 보안성도 고려되도록 설계되어 있어서 전자상거래의 활성화에 이바지하고 기업의 경쟁력을 향상시킬 수 있을 것으로 기대된다.

Electronic Signature Model and Application of Security Server System using Identity Information

Young-Soo Kim[†] · Seung-Jung Shin[††]

ABSTRACT

Electronic signature system is required to be used in the promotion of the e-Commerce. Because the application system for electronic signature system has inconvenience and vulnerability of security, users are reluctant to use it. Therefore, the electronic signature system should give a guarantee of convenience and security. In this paper, we propose server-based application model, which uses identity information and makes users access transparently to solve electronic signature problems. We also design and verify electronic signature system that reduces threats to security, which cause server attack by distributing the part of signature key to both server and client. The application model with lightweight server system based on the electronic signature system is expected to be used in the promotion of the e-Commerce and help to make its business more efficient and competitive.

키워드 : 보안성(Security), 전자서명(Electronic Signature), 식별정보(Identity Information), 응용모델(Application Model), 서명키의 조각(The Part Of Signature Key)

1. 서 론

인터넷에 대한 사용자수가 급속히 증가하면서 인터넷을 이용한 전자상거래가 확대되고 있다. 인터넷을 이용한 원격지간의 비대면 거래방식은 상거래 상대자의 신원을 확인하거나 거래내용에 대한 진정성을 보장하지 못한다[1]. 이는 사이버 공간에서의 거래정보의 불법적 유출과 위조 그리고 훼손에 따른 보안위험을 증가시키고 전자 상거래의 촉진을 저해한다.

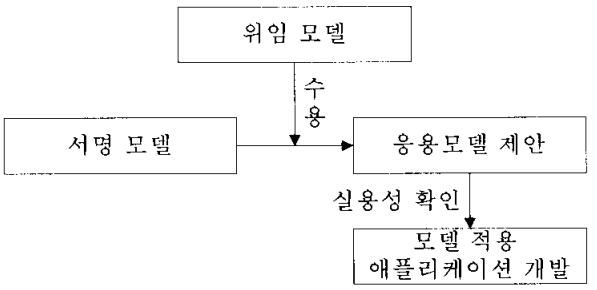
따라서 인터넷을 통한 전자적 문서의 결재와 계약과 같은 전자 상거래의 활성화를 위해서는 인증과 무결성 그리고 부인방지에 대한 보안기능을 제공하는 전자서명이 필수적으로 요구된다[2]. 전자서명 방식으로는 공개키 암호화방식에 기초를 둔 암호화 프로토콜이 사용되고 있다. 공개키 암호화 방식은 비밀키와 공개키라는 두 개의 키를 사용해서 서명값의 생성과 검증을 수행한다[3]. 그러나 공개키 암호화시스템의 가장 큰 문제점은 사용의 복잡성과 키 관리의 어려움으로 사용자가 사용을 꺼리고 외면한다는 점이다[4].

이와 같은 문제점을 해결하는 서명시스템의 개발 및 구현을 목표로 (그림 1)과 같은 방식에 따라 디렉토리를 사용하는 공개키 암호화시스템의 서명모델과 사용자를 대신하여 보안서버시스템이 서명을 수행하는 위임 모델을 분석하고 문제점을 도출해서 이를 해결할 수 있는 서명시스템의 응용모델을 제안한다.

본 논문의 구성은 다음과 같다. 제2절에서는 서명시스템의 연구모델로 디렉토리 기반의 서명모델과 위임서버시스템의 서명모델을 분석하고 개선방안을 도출한다. 제3절에서는 사용자에게 공개되어 있는 식별정보를 사용하는 서명시스템의 응용모델을 제안한다. 제4절에서는 모델의 실용성을 검

† 정 회 원 : 국민대학교 대학원 정보관리학과 박사
†† 정 회 원 : 한세대학교 IT학부 부교수
논문접수 : 2004년 12월 4일, 심사완료 : 2005년 1월 27일

증하기 위하여 식별정보를 응용한 서명시스템을 구현하고 검증한다. 제5절에서는 결론과 시사점을 기술한다.



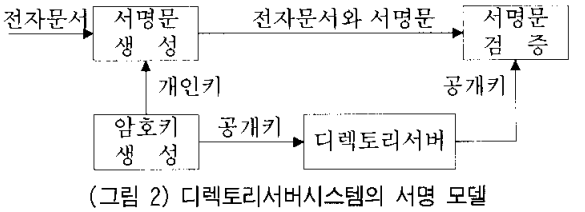
(그림 1) 연구 모델

2. 서명시스템의 연구모델

2.1 디렉토리서버시스템의 서명 모델

인터넷을 이용한 전자상거래가 확산되면서 거래정보의 보호를 위해서 암호화의 필요성이 확대되고 있다. 암호화는 인터넷을 통해서 전달되는 전자문서의 불법적인 노출과 위조를 방지하고 사이버 공간에서의 신분확인을 위한 해결책을 제공한다[5]. 공개키 암호화 시스템은 공개키와 개인키라는 두개의 상이한 키를 사용함으로써 비밀키 암호화 시스템이 가지고 있는 비밀키의 노출에 따른 키분배 문제[6]를 해결하고 개인키로 서명된 전자문서를 이용해서 송·수신자의 신원과 송·수신 사실에 대한 부인을 봉쇄하는 전자서명의 응용에 널리 사용된다[7]. 전자서명은 송신자가 보낸 전자문서를 수신자가 송신자 이외의 사람에 의해서 서명하지 않았음을 검증할 수 있도록 하는 암호통신 응용이다.

전자서명을 위한 디렉토리서버시스템의 서명모델은 (그림 2)와 같이 공개키는 사용자가 공동으로 사용하는 정보근원지 역할을 하는 디렉토리에 보관하고 개인키는 사용자가 관리한다. 전자서명을 위하여 송신자는 자신의 개인키를 사용하여 서명문을 생성하고 수신자는 디렉토리로부터 송신자의 공개키를 획득하여 서명을 검증한다[8].



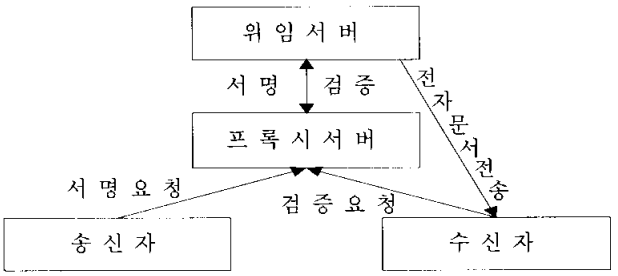
(그림 2) 디렉토리서버시스템의 서명 모델

디렉토리서버를 이용한 서명시스템은 전자서명을 위한 암호화작업에 많은 사간이 소요되고 공개키를 보관하는 디렉토리를 안전하게 유지해야 한다. 또한 사용자는 서명에 사용하는 개인키를 안전하게 보관해야 한다. 이는 전자서명서비스의 품질을 저하시키고 개인키의 분실에 따른 보안성을 위협한다. 따라서 보안성을 강화할 수 있는 서명시스템이 요구된다.

2.2 위임서버시스템의 서명모델

디렉토리서버시스템의 서명모델은 전자서명의 위·변조에 따른 보안위험을 감소시키기 위해서 서명키인 개인키의 관리를 위한 사용자의 많은 노력이 요구되고 또한 전자서명의 처리지연을 방지하기 위해서 사용자는 일정수준 이상의 시스템 사양을 구비해야할 뿐만 아니라 디렉토리서버의 신뢰성을 제고해야 하는 문제점을 가지고 있다[9].

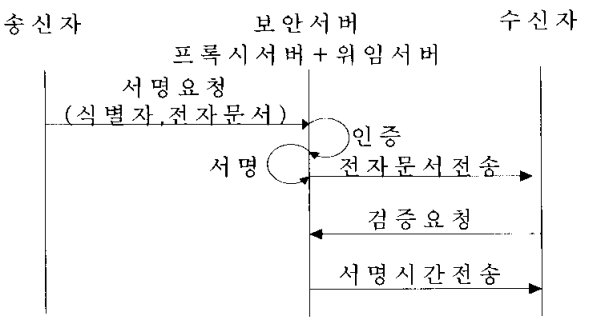
이의 해결을 위해서 사용자를 대신해서 전자서명과 검증을 수행하는 위임서버를 이용한 서명시스템이 사용된다[10]. 위임모델을 사용하는 서명시스템의 아키텍쳐는 (그림 3)과 같고 사용자가 개인키를 관리해야 하는 부담을 감소시키고 사용자가 사용하는 시스템의 사양과는 관계없이 일정수준의 전자서명서비스를 제공한다. 프록시 서버는 사용자를 식별하는 반면 위임서버는 사용자를 대신하여 서명을 수행하고 수신자에게 전자문서를 전송한다.



(그림 3) 위임서버시스템의 서명 아키텍쳐

위임서버시스템의 서명프로토콜은 (그림 4)와 같다. 전자서명을 위해서 사용자는 전자문서와 식별자를 프록시서버에게 전송한다. 프록시서버는 사용자를 인증한 후에 식별자와 인증정보를 위임서버에게 전송하고 위임서버는 서명시간을 생성하고 식별자와 전자문서 그리고 서명시간을 데이터베이스에 저장한 후에 수신자에게 전자문서를 전달한다.

수신자는 전자서명의 검증을 위하여 전자문서를 보안서버의 위임서버에게 전송하고 위임서버는 이와 매칭되는 서명시간을 데이터베이스에서 검색하고 수신자에게 이를 리턴한다.



(그림 4) 위임서버시스템의 서명 프로토콜

위임서버기반의 서명시스템은 디렉토리서버시스템의 서명모델에 비해서 사용자에게 편의성과 보안성을 제공한다[11]. 이는 위임서버시스템이 사용자를 대신해서 서명작업을 수행

하고 개인키를 보관하기 때문이다. 그러나 위임서버시스템은 사용자의 간섭없이 서명을 수행하기 때문에 보안서버의 신뢰성이 보장되어야 한다.

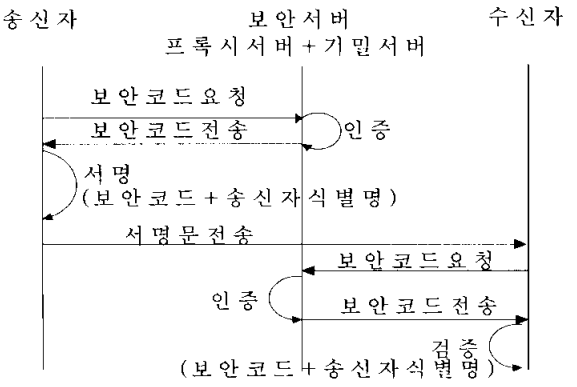
이를 위해서 위임서버시스템에 집중되어 있는 보안요소를 분산시켜서 보안성을 강화할 수 있는 방법이 요구된다.

3. 식별정보기반의 서명 모델 및 구조

3.1 식별정보서명시스템의 응용 모델

위임서버시스템이 불법적인 공격에 노출되는 경우에 개인키의 도용으로 인한 전자서명의 위·변조에 대한 보안위험은 크게 확대된다. 이러한 문제점을 해결하기 위하여 프록시서버와 기밀서버로 구성되는 보안서버시스템은 공개키와 개인키의 생성에 필요한 보안코드를 관리하는 반면 사용자는 공개되어 있는 자신의 식별정보와 보안서버시스템이 리턴하는 보안코드를 결합해서 서명키인 개인키를 생성하고 전자서명을 수행한다. 이는 보안서버시스템의 침해위험을 분산시키고 개인키의 노출로 야기되는 전자서명의 위·변조 가능성을 감소시키는 잇점을 제공한다. 이를 위한 서명시스템의 응용 프로토콜은 (그림 5)와 같고 식별정보와 보안서버시스템이 리턴하는 보안코드를 사용해서 송수신 문서에 대한 서명처리를 수행한다.

송신자는 보안시스템의 기밀서버로부터 리턴되는 보안코드와 자신의 식별정보를 이용하여 전자문서에 서명한다. 프록시서버는 기밀서버가 보안코드를 리턴하기 전에 사용자를 인증한다. 수신자는 전자서명을 검증하기 위하여 보안시스템에게 요청해서 수신한 보안코드와 송신자의 식별정보를 사용해서 서명을 검증한다.

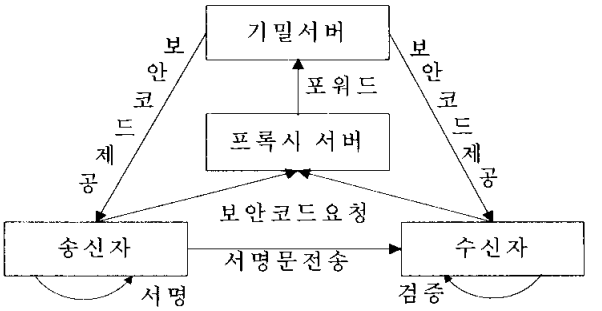


(그림 5) 식별정보서명시스템의 응용프로토콜

3.2 식별정보서명시스템의 응용아키텍쳐

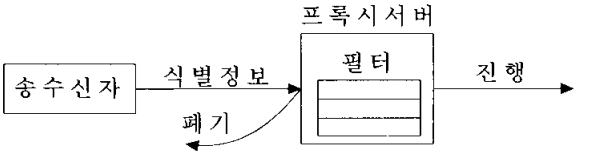
위임서버시스템의 서명방식이 개인키의 관리와 서명작업에 대한 사용자의 부담을 최소화하는 반면 사용자의 의도와는 달리 침입자나 서버관리자에 의해서 전자서명이 오용될 위험을 수반하고 있다. 식별정보를 응용한 서명시스템의 아키텍쳐는 (그림 6)과 같다.

식별정보서명시스템은 위임기반서명시스템과는 달리 송신자가 자신의 보안코드와 식별정보를 이용하여 서명문을 구성하고 전자문서와 함께 수신자에게 직접 전송한다. 기밀서버는 사용자의 인증정보를 사용하여 보안코드를 생성하고 이를 송·수신자에게 전송한다. 수신자는 서명을 검증하기 위하여 기밀서버로부터 보안코드를 리턴받고 송신자의 식별정보와 결합해서 서명을 검증한다. 이는 보안서버관리자에게 전자문서와 서명에 사용하는 개인키가 노출되는 것을 방지할 수 있고 개인키를 구성하는 요소를 서버와 사용자에게 분산시킴으로써 보안성을 강화할 수 있다.



(그림 6) 식별정보서명시스템의 응용아키텍쳐

식별정보서명시스템의 응용 아키텍쳐를 구성하는 프록시서버가 제공하는 주된 기능은 (그림 7)과 같고 사용자를 식별하고 합법적인 사용자인 경우에 서비스를 제공받을 수 있도록 포워딩하고 불법적인 사용자인 경우에는 서비스의 제공을 차단한다.

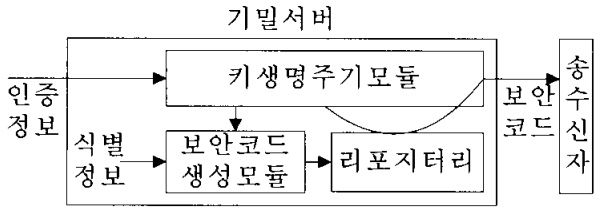


(그림 7) 프록시서버시스템의 서비스 구조

식별정보서명시스템의 기밀서버가 제공하는 서비스 구조는 (그림 8)과 같고 사용자의 인증정보를 사용하여 서명키를 구성하는 보안코드를 산출하고 이를 송·수신자에게 전송한다. 송신자의 서명키에 대한 보안정책은 기밀서버의 키생명주기모듈이 담당하고 서명키에 대한 생명주기의 보안정책에 따라서 갱신된 보안코드는 리포지터리에 보관한다. 서명키의 생명주기에 대한 디폴트 보안정책은 전자서명을 요청할 때마다 기밀서버가 새로운 보안코드를 생성해서 리턴한다. 위임기반 서명시스템은 길이가 긴 사용자의 서명키를 생성해서 저장하고 관리하는 반면에 식별정보기반 서명시스템은 서명키의 생명주기에 따라서 서명키의 조각을 보관하고 유지한다.

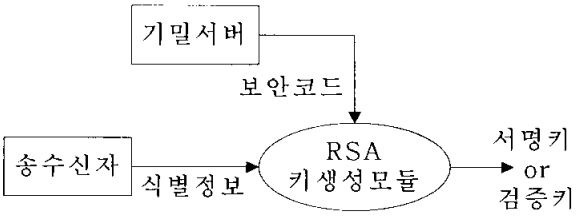
식별정보서명시스템은 서명메시지를 전송하는 시점에서 송신자가 기밀서버로 부터 리턴된 서명키의 조각인 보안코드와 자신의 식별자를 결합한 문자열을 사용하여 서명키를 생성함으로써 서명키의 노출과 훼손에 따른 위험을 감소시

킬 수 있는 장점을 갖는다.



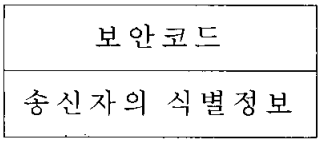
(그림 8) 기밀서버시스템의 서비스 구조

송신자는 (그림 9)와 같은 서명키의 생성 구조를 이용해서 이메일주소와 같은 일반인에게 공개되어 있는 자신의 식별자와 보안서버시스템이 리턴한 보안코드를 결합한 문자열을 RSA알고리즘의 입력 데이터로 사용해서 서명키인 개인키를 생성한 후에 서명 메시지를 구성하고 수신자에게 전송한다. 수신자는 서명의 검증을 위해서 보안서버시스템이 리턴한 보안코드와 일반인에게 공개되어 있는 송신식별자의 문자열을 RSA알고리즘의 입력 데이터로 사용해서 검증키인 공개키를 생성한 후에 서명 메시지를 검증한다.



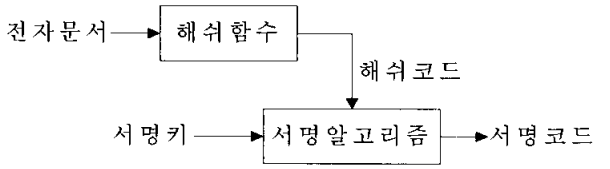
(그림 9) 서명키의 생성 구조

서명키와 검증키의 구조는 (그림 10)과 같고 송신자는 보안코드와 자신의 식별정보로 구성되는 서명키를 사용해서 전자문서에 서명하고 이를 수신자에게 전송한다. 수신자는 기밀서버로부터 수신한 보안코드와 송신자의 식별정보를 결합해서 검증키를 생성한 후에 서명을 검증한다.



(그림 10) 서명키 및 검증키의 구조

서명과 검증을 위해서 (그림 11)과 같은 해쉬기반의 서명방식을 사용한다[12]. 이는 전자문서를 대상으로 서명과 검증을 수행하는 대신 전자문서에 대해서 계산된 해쉬코드에 대해서 서명하고 검증하도록 하였다. 해쉬코드는 상이한 크기의 전자문서와는 관계없이 고정된 크기의 다이제스트로서 서명시간을 감소시키는 효과를 제공한다[13]. 이는 길이가 긴 전자문서에 서명하는 것보다 전자문서로부터 생성된 요약문인 해쉬코드에 서명하는 것이 서명을 위한 처리시간이 적게 소요되기 때문이다[14].

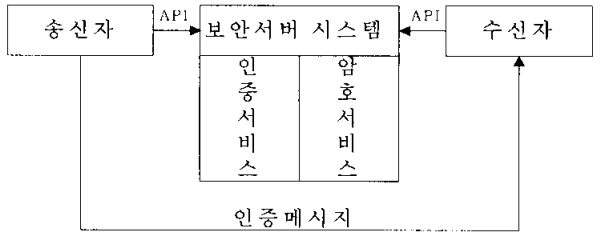


(그림 11) 식별정보서명시스템의 서명방식

4. 식별정보응용시스템의 설계 및 모델의 검증

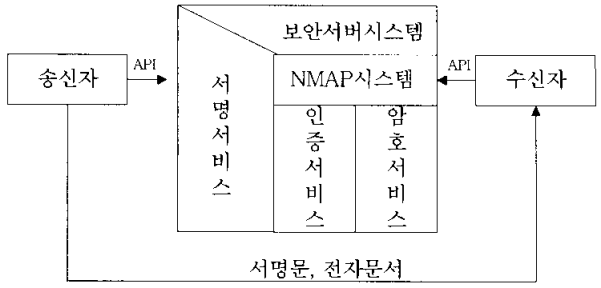
4.1 식별정보응용시스템의 설계

식별정보를 응용한 서명시스템의 적용 사례로서 메시지 보안 시스템의 인증 프로토콜 설계 및 구현[16]에 관한 연구개발 시스템인 NMAP(New Message Authentication Protocol)을 선정하였다. NMAP는 공개키 암호화 방식에 기초를 둔 인증프로토콜로 (그림 12)와 같이 송신자와 수신자는 보안서버시스템의 인증서비스와 암호 서비스를 사용하여 인증토큰의 구성과 검증을 수행한다.



(그림 12) NMAP시스템의 아키텍처

NMAP시스템에 식별정보를 응용한 서명시스템의 아키텍처를 통합한 응용구조는 (그림 13)과 같다. 응용시스템은 NMAP의 인증 및 암호서비스에 공개되어 있는 사용자의 식별정보를 사용해서 보안코드를 계산하는 서명서비스를 제공하는 시스템이다. 송·수신자는 전자문서에 대한 서명과 검증을 하기 위해서는 NMAP시스템의 인증서비스를 이용해서 적법한 사용자임을 확인 받은 후에 식별정보를 응용한 서명 프로토콜이 제공하는 서명서비스를 통해서 보안코드를 리턴받도록 설계하였다.

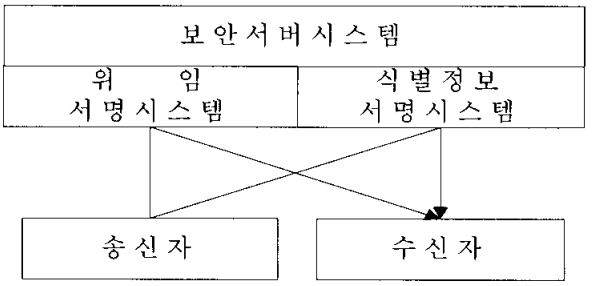


(그림 13) 식별정보응용시스템의 서명구조

4.2 식별정보서명시스템의 응용모델 검증

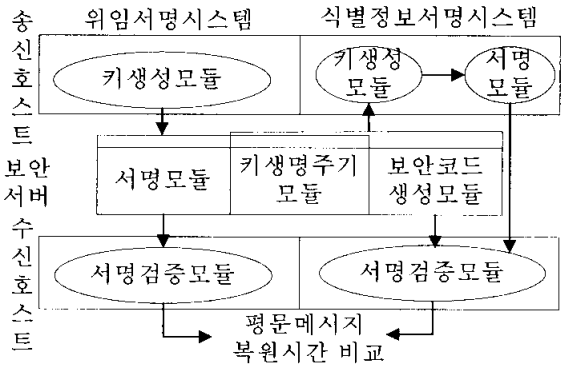
식별정보를 응용한 서명모델의 실용성을 확인하기 위한

검증방식은 서명의 주체와 송·수신방식이 상이한 위임서명 시스템과 식별정보서명시스템을 구현하고 시스템의 성능을 비교 분석하는 방식을 적용하였다. (그림 14)은 비교우위의 검증을 위한 실용성 평가 모델을 보여주고 있다.



(그림 14) 실용성 평가 모델

송수신 메시지의 서명과 전송 그리고 복원에 소요되는 서명 처리 시간을 측정하기 위한 시뮬레이션시스템에 대한 컴포넌트 보안모듈의 레이아웃은 (그림 15)와 같다. 위임서명 시스템과 식별정보서명시스템의 비교를 위해서 보안서버시스템의 키생명주기모듈에 디폴트 보안정책을 적용해서 평문 메시지의 복원에 소요되는 시간 데이터를 측정하였다.



(그림 15) 시뮬레이션시스템의 컴포넌트 레이아웃

모의실험 환경으로 셀러론 850MHz와 윈도우즈 2000운영체제 하에서 전자문서의 크기를 상이하게 하여 전자서명 메시지를 처리하는데 소요되는 시간을 측정하여 실험하였다.

<표 1>에서 보는 것과 같이 사용자에게 공개되어 있는 식별정보를 사용하는 서명시스템은 사용자를 대신해서 서명을 수행하는 위임서명시스템과 비교해서 서명 처리시간이 지연되는 것을 알 수 있다. 이는 식별정보서명시스템이 서명키를 구성하는 보안코드를 획득하기 위해서 보안서버와의 상호작용이 필요하고 서명키의 완성에 추가적으로 시간이 소요되기 때문이다. 또한 서명시스템의 응용모델은 서명프로토콜의 동작에 오류가 없고 침입자의 서버공격에 감내할 수 있는 해결 방안으로 사용될 수 있음을 확인하였다. 식별정보서명시스템은 서명처리시간이 다소 느린 반면에 서명키를 구성하는 조각을 기밀서버와 송·수신자가 분산 관리함으로써 불법적인 서버공격으로 부터 야기되는 보안위험을 감소시키는 장점을 제공한다.

〈표 1〉 서명처리시간

구분	식별정보 서명시스템	위임서명 시스템	차이
100K	0.6358	0.60	0.0358
200K	1.0818	1.038	0.0438
300K	1.5078	1.458	0.0498
400K	1.9436	1.8858	0.0578
500K	2.3796	2.3162	0.0634

5. 결 론

전자상거래의 활성화와 거래의 신뢰성을 확보하기 위해서는 전자문서의 수신자가 송신자를 사칭하는 사람이 아닌 실제 송신자로부터 전송되었다는 것과 수신한 전자문서는 전송도중 변경되지 않았다는 것을 확인할 수 있어야 하고 사후에 송·수신자가 전자문서의 송·수신 자체를 부인하는 것을 방지할 수 있는 방안이 제공되어야 한다[15]. 이를 위한 기술적인 요소로는 암호방식에 기초를 둔 서명 방식이 널리 사용된다. 서명서비스를 제공하기 위한 기반구조는 디렉토리 기반의 서명 모델과 위임기반의 서명모델이 있다. 디렉토리기반의 서명시스템은 보안서버시스템에 대한 인프라의 구축과 운영을 위한 비용이 과대하게 소요되고 사용자가 개인키를 안전하게 유지관리하는데 많은 노력을 요구한다.

이의 해결을 위한 방안으로 위임서버시스템에서 사용자를 대신해서 서명을 수행하는 서명시스템이 연구되었다. 그러나 위임서명시스템이 서명키를 관리함으로써 사용자가 개인키를 관리하는데 요구되는 노력을 감소시키는 반면 서버가 공격의 위험에 노출되는 경우에 이의 불법적인 사용을 제한하는 해결책이 없다는 단점이 있다.

따라서 이의 해결을 위한 대안으로 본 논문에서는 서명키를 구성하는 요소를 송·수신자와 기밀서버시스템에게 분산 배치함으로써 보안위험을 감소시킬 수 있는 서명모델을 제안하고 이의 실용성을 검증하였다. 서명시스템에 대한 식별정보 응용모델은 보안시스템의 기밀서버가 사용자에게 공개되어 있는 식별정보를 사용해서 서명키의 구성요소인 보안코드를 생성하고 송신자는 보안코드와 자신의 식별정보를 결합한 문자열을 사용해서 생성한 서명키를 이용해서 전자문서로부터 산출한 해쉬코드에 서명한 후에 수신자에게 직접 전송하는 방식을 사용한다.

제안한 서명모델은 디렉토리기반의 서명시스템이 가지고 있는 인증 프로토콜의 복잡성을 배제하고 위임서명시스템의 단점인 불법적인 사용자의 침입공격에도 보안성을 보장할 수 있는 서명프로토콜을 사용함으로써 오늘날 급속하게 증가하고 있는 서버시스템에 대한 보안위험으로부터 서명시스템의 신뢰성과 보안성을 높여줄 수 있을 것으로 기대한다. 향후 송·수신자시스템과 서명시스템에 대한 서비스거부공격을 차단하고 침입에 감내할 수 있는 서명시스템의 개발에 대한 연구가 필요하다.

참 고 문 헌

[1] Krawcyzk, H., "The Order of Encryption and Authentication for Protecting Communications", Proc. Crypto '01, 2001.

[2] Chokhani, S., "Towards a national public-key infrastructure", IEEE Communications Magagine, Vol.32, No.9, pp.70-74, 1994.

[3] Sarbari and Stephen, "Public Key Infrastructure: Analysis of Existingand Needed Protocols and Object Formats for Key Recovery," Computer and Security Vol.19(1), pp.56-68, April 2000.

[4] Merkle, R., "A Certified Digital Signature, Advances in Cryptology", CRYPTO.

[5] Fujisaki, E. and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes", Proc. Crypto '99 pp.537-554, 1999.

[6] Merkle, R. C., "A digital signature based on a conventional encryption function," in Advances in Cryptology-Crypto'87, pp.369-378, 1987.

[7] Rivest, R., A. Shamir and L. Adleman, "A Method for Obtaining Digital Signature and Public Key Cryptosystems", Comm. of ACM, 21, pp.120-126, 1978.

[8] Whittle, R., Public Key Authentication Framework : Tutorial, 1996. 6.

[9] Shamir, A., "Identity-based cryptosystems and signature schemes," In Advances in Cryptology, Crypto'84, Volume 196 of LNCS, 2001.

[10] Asokan, N. and G. Tsudik, and M. Waidner, "Server-supported signatures," Journal of Computer Security, Vol.5, No.1, 1997.

[11] Mambo, M. and K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," in Proc. of the Third ACM Conf. on Computer and Communications Security, pp.48-57, 1996.

[12] Lamport, L., "Constructing digital signatures from one-way functions", SRI intl. CSL-98, October, 1979.

[13] Damgard, I. B., "Collision Free Hash Functions and Public Key Signature Schemes", Eurocrypt, 1987.

[14] Rompel, J., "One-way functions are necessary and sufficient for secure signatures.", In Proceedings of the Twenty Second Annual ACM Symposium on Theory of Computing, pp.387-394, ACM Press, 1990.

[15] Fiat, A. and A. Shamir, "How to prove yourself: Practical solutions to identificati on and signature problems", Proc. Crypto'86, pp.186-194, 1986.

[16] 김영수, 메시지보안시스템의 인증 프로토콜 설계및 검증", 박사학위논문, 국민대학교 대학원, 2003.

김 영 수

e-mail : experkim@dreamwiz.com

1989년 전북대학교 회계학과 졸업(학사)

1992년 경희대학교 대학원(경영학석사)

2003년 국민대학교 대학원 정보관리학과 (정보관리학박사)

관심분야 : 전자상거래, 인터넷 응용, 분산 정보시스템, 정보보안

신 승 중

e-mail : expersin@hansei.ac.kr

1988년 세종대학교 대학원 졸업(경영학석사)

1994년 건국대학교 대학원 전자계산학과 (공학석사)

2000년 국민대학교 대학원 정보관리학과 (정보관리학박사)

1990년~1994년 태성 MIS 기술이사

1993년~1995년 중경공업전문대학 전자계산과 겸임교수

1995년~2003년 중부대학교 정보보호관리학과 부교수

2003년~현재 한세대학교 IT학부 부교수

관심분야 : 인터넷보안, 전송프로토콜, 소방방재시스템