제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

전자상거래를 위한 사용자 인증 기술

김 지 은*, 전 현 정*, 윤 동 식*
* 안동과학대학 사이버테러대응학과

요 약

인터넷 속의 산업구조는 1:1 대면 방식의 구조에서 네트워크 상의 On-line 구조로 변화되어 가고 있다. 이러한 인터넷상에서의 전자상거래는 네트워크의 발달에 힘입어서 거대한 시장을 형성하게 될 것이다. 인터넷에서 상거래가 일어나는 것은 오히려 자연스러운 현상이라고 할 수 있다. 인터넷을 통한 전자상거래는 많은 사람들의 관심을 증대시킬 것이다. 그런데 여기에는 제도적, 기술적 여러 가지가 선결되어야 한다. 이중에서도 가장 먼저 해결되어야 할 것이 사용자 인증에 대한 기술력이다. 이 논문에서는 안전한 전자상거래 쇼핑몰 구축 및 운영을 위해 필요한 세 가지의 주된 목적을 갖는다. 먼저 전자상거래의 보안 해결방법이며 둘째, 그들의 문제점들을 분석하고 이를 바탕으로 하여 실제 전자상거래 쇼핑몰에서 사용자 인증을 할 때, 필요한 각종 위협요소 및 취약점을 파악하고 이에 대응하는 방안을 제시하고자 한다.

Customer authentication service method for E-commerce

Kim Ji Eun*, Jun Hyun Jung*, Yun Dong Sic*
*Andong Science College Dept. of Cyberterror Defense

ABSTRACT

The industrial structure with Internet is changing from offline to online. By developing of network, E-commerce will be big market. It is natural to increase of E-commerce and interest of people. but, it is supported by system and technics. First of all, we need customer authentication service method. In this paper, we described about Electronic shopping mall Security by three main categories. One is general security solution of E-commerce, Second is analyzing about various threats, vulnerability and countermeasures to that. Third is security consideration of directory service in E-commerce circumstance.

1. 서 론

인터넷(Internet) 이란 거대한 네트웍들이 모인 것이다. 즉, 네트웍들의 네트웍이다. 인터넷은 몇 가지 특징을 가지고 있고 그에 따라 여러 가지 문제점을 가지게 되었다.

첫째, 개방성이다.

둘째, UNIX, TCP/IP 등의 소스 코드가 개방되어 있다. TCP/IP 프로토콜이나 UNIX 시스템은 많은 학교나 연구소 등에서 소스코드를 보유하고 있고, 서점에서도 교재로 판매하고 있을 뿐만 아니라, 인터넷에서 이러한 문서들을 무료로 배포하고 있다.

셋째, 상호 정보 교환이 쉽다. 인터넷에서는 게시판(BBS)과 온라인 정보 교환을 위한 방법들이 제공되므로, 새로운 침입 방법들이 침입자들 간에 손쉽고 은밀하게 서로 교환되어 사용되는 것이다.

이러한 인터넷의 취약점을 이용하는 불법 침입자라고 알려진 해커들은 주로 정보의 비밀성을 위반하는 경우이다. 비밀성이나 무결성을 보장하려면 가용성이 낮아지게 된다. 그 반대도 마찬가지이다. 이들을 위반한 해킹 사전은 외국뿐만이 아니라, 최근 국내에서도 급격히 증가하고 있는 추세이다. 이는 아직은 관리자들의 인식이 부족하고 보안 시스템에 대한 투자가 적어서 제대로 된 보안 시스템을 갖춘 곳이 거의 없기 때문이기도 하다. 하지만, 이러한 보안 시스템을 아무리 잘 갖춘다고 해도 관리자의 인식이 부족하다면 무용지물이 되고 만다.

이 논문에서는 "전자상거래를 위한 사용자 인증 기술"에 대하여 현재의 기술과 개선된 새로운 기술을 대하여 고찰하고자 한다.

2. 전자상거래 사용자 인증 기술

전자 상거래 인증은 전자문서를 작성한 자의 신원과 전자 문서의 변경 여부를 확인할 수 있도록 비대칭 암호화방식을 이용하여 전자서명 생성키로 생성한 정보로서 당해 전자문서에 고유한 것임을 인정하고 증명한다.

2.1 전자상거래 전자서명

2.1.1 전자서명의 해쉬 알고리즘

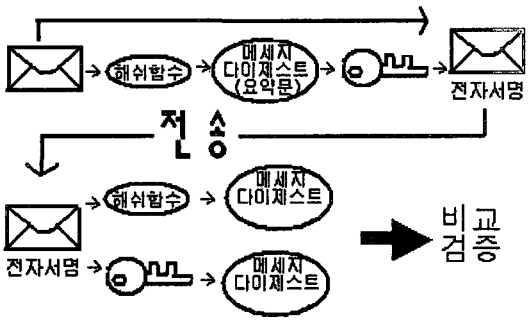
해쉬 함수는 메시지 다이제스트라는 코드를 작성하기 위해 텍스트(예: 전자 우편 메시지)를 사용하는 수학 공식이다.

공개키 암호화 방식을 이용하여 문서에 전자서명하고 이를 검증하는 경우, 공개키 암호화 방식의 특성으로 인해 많은 시간이 소요되기 때문에 문서를 사전에 작게 압축하여 전자서명을 한다면, 문서의 검증에 걸리는 시간을 많이 절약할 수 있게 된다.

디지털 인증에 사용되는 해쉬 함수는 암호용으로 사용할 수 있을 정도로 안전한 속성을 가지고 있어야 한다. 특히 다음 항목에 해당되지 않아야 합니다.

- 메시지 다이제스트를 알고 있는 경우에도 메시지 내용을 해독할 수 없어야 한다.
- 동일한 해쉬값을 두 개의 서로 다른 메시지가 생성하면 안 된다.
- 제공된 해쉬값에 대응하는 메시지를 찾을 수 있으면 침입자는 서명된 진짜 메시지를 가짜 메시지로 대체할 수 있다.
- 실제로는 동일한 값에 해쉬하는 다른 메시지에 서명했다고 주장하여 거짓으로 메시지를 부인할 수 있게 되어 디지털 서명의 부인 방지 속성을 침해할 수 있다.
- 동일한 해쉬값을 생성하는 두 개의 다른 메시지를 찾을 수 있으면 동일한 값에 해쉬하는 메시지를 내용이 다른 메시지로 착각하여 서명하게 할 수도 있다.

● 전자서명 생성 및 검증과정



<그림1>전자서명 및 생성과정

인터넷에서 전자상거래인증 서비스를 받는 사이트는 개인정보, 사업정보 및 신용카드 등 각종 정보를 암호화해 줌으로써 도청에서부터 해방될 수 있다.

전자상거래인증은 안전한 인터넷 이용을 위해 필수적이다. 전자상거래인증은 암호화와 전자서명으로 전자상거래의 신뢰를 높여주며 전자상거래 인증은 다음과 같은 위험요소를 제거해 준다.

- 신원확인
- 무결성
- 기밀성
- 부인방지

2.1.2 암호화

전자우편이나 전자상거래를 포함해 일반적으로 정보를 보안하기 위한 가장 안전한 방식은 정보를 암호화하는 방법이다.

암호화 기술은 모든 정보통신 분야에서 적용할 수 있다. 즉, 디지털 정보를 다루는 모든 분야에서 보안이 필요하다면 암호화를 응용할 수 있다는 것이다. 네트웍 상에서 주고받는 정보 혹은 컴퓨터에 저장된 정보를 보호하는 암호화시스템에서 중심적으로 고려하는 내용은 다음과 같다.

첫 번째, 비밀보장(Confidentiality) 기능이다. 정보를 보호하는데 있어 비밀을 보장하는 것은 가장 기본이 되는 사항이다.

두 번째, 무결성(Integrity)의 보장 기능이다.

세 번째, 부인방지(Non-Repudiation) 기능이다.

일반적으로 암호화 정보를 네트웍상의 상대편에게 보낼 때는 암호키까지 보내게 된다. 이러한 대칭형 암호화 방식의 경우 이 암호키를 보호할 방법이 없게 되는데, 이러한 문제를 해결하기 위해 개발된 기술이 비대칭 암호화 방식이다.

중간에 데이터가 변조되는 것을 막는 보안 기능이 바로 메시지 인증기능이다. 메시지 인증기능은 메시지를 송수신하는 A가 B외에 제 3자인 C가 메시지 내용을 수정하지 못하게 하는 것에 초점을 맞추고 있다. 메시지 인증기능을 통해 메시지가 수정되지 않았는지, 메시지의 순서가 바뀌었는지에 대한 확인을 할 수 있다.

인증의 방식에는 퍼블릭 키를 이용해 메시지를 암호화하는 방법과 암호화 체크섬 이용, 해쉬함수 이용 등이 있다.

비대칭 알고리즘에서 두드러지는 점은 공개키 알고리즘이 해시 값(해시 값은 일반적으로 128~256 비트임)만 암호화하거나 해독하면 된느 서명을 만들고 확인하기에는 좋은 방법이지만 다량의 데이터를 암호화하기에는 대단히 취약한 방법이라는 것입니다. 즉, 공개 키는 디지털 서명을 만들고 대칭 키(세션 키라고도 함)를 교환하는 두 가지 용도로 사용됩니다.

2.2 보안기술

전자상거래라고 하는 것은 실제 생활에서 나타나고 있는 모든 거래, 즉 쇼핑, 금융거래, 기업간거래, 보험, 법률 등이 모든 것을 컴퓨터 네트웍 상에서 시뮬레이션을 통해 거래가 가능하도록 하는 것을 말하는 것이다.

전자상거래에서 보안이란 실제 거래를 통해 돈이 오고 간다는 점에서 그 중요성을 찾을 수 있다. 전자상거래 사이트는 개인의 손익과 직결되는 사항들로 이루어져 있기 때문에 보안과는 별개로 생각할 수 없는 분야이다. 바꾸어 말하면 전자상거래에 관련한 특별한 보안 조치가 있는 것이 아니라 전자상거래 시스템 자체가 보안 기능을 수행해야만 하는 것이다. 다양한 유형들을 가지고 있지만 실제 인터넷상의 비즈니스나 전자상거래가 활성화되기 위해서는 선결돼야 하는 여러 가지 문제들이 있다. 네트웍 접속, 소프트웨어, 하드웨어 플랫폼, 물품의 배달, 멀티미디어 정보, 지불방식, 법률적 제약 등이 그 문제들로 이것들의 해결을 통해 인터넷상의 거래가 실제 활성화될 수 있을 것이다.

전자상거래 사이트 보안에서 특징적인 부분이라 하면 거래를 하면서 돈을 지불해야 하는 관계로 지불 방법에 대한 프로그램들 자체가 보안에 대한 기능을 수행하게 된다. 즉, 지불 방법에 따라 거래의 안정성을 보장하게 되는 것이다.

2.3 전자지불

전자지불 방법은 크게 두 가지로 나누어질 수 있다. 그 하나가 지불 브로커 시스템이고, 또 다른 하나는 전자화폐를 이용하는 것이다. 지불 브로커 시스템은 신용카드나 은행의 계좌번호를 이용해 네트웍 상에서 대금을 지불하는 방법을 말한다.

그러나 이와 같은 시스템은 신용카드의 사용자들의 개인정보나 거래정보 등의 자료가 쉽게 노출될 수 있기 때문에 비밀보장이 되지 않는다는 단점이 있다.

전자화폐의 경우는 아직 실용화되기에 이른 감이 있지만 이것을 이용하는 것은 신용카드를 이용해 발생할 수 있는 단점들을 개선할 목적으로 만들어졌기 때문에 전자상거래에서 보안의 또 다른 방법이라 말할 수 있다. 전자화폐의 장점은 사용자 측면에서 현금과 같은 익명성을 보장받을 수 있고, 사용자와 인가된 상점 간의 거래뿐만 아니라 사용자간 화폐의 이동도 가능하다.

2.3.1 전자지불시스템보안

안전하고 효율적인 전자상거래가 행해지기 위해서는 특히 전자 지불시스템의 보안이 필수 불가결한 요소이다. 전자상거래의 운영에 있어서 전자적인 형태로 구현된 지불시스템이 없이는 거래처리의 전 과정이 자동화 될 수 없기 때문에 거래 대금의 처리를 위한 전자지불시스템은 전자 상거래의 효율성을 결정하는 중요한 요소 중의 하나이다. 그러나 전자시스템은 해커들이 공격을 통하여 금전적인 이익을 직접적으로 억을 수 있는 부분이기 때문에 이에 대한 보안 대책의 강구는 매우 중요하다. 종래의 전자지불방법은 은행 등의 업계 내부 시스템을 폐쇄했지만 현재 기업이나 개인이 자유롭게 접근 가능한 개방형 통신망인 인터넷에서 안전한 전자지불을 낮은 비용으로 실현하는 것은 정보보안의 대책 없이는 불가능할 것이다.

2.3.2 신용카드기반 전자지불시스템 보안

신용카드는 일반 상거래에서도 가장 보편적으로 이용되고 있는 지불 수단으로 신용카드의 기반의 전자상거래 지불시스템은 다음과 같은 요구사항을 만족하여야 한다.

- 비밀성 : 신용카드 계정 정보, 거래금액, 거래 내역 등의 비밀정보에 대한 비밀성이 제공되어야 한다.
- 인증 : 상점은 카드 소지자가 제시한 사용카드의 계정이 유효한지를 확인할 수 있어야 하며, 카드 소지자는 상점이 해당 신용카드의 금융 기관과의 거래처인지를 확인할 수

있어야 한다.

- 무결성 : 전송되는 주문 정보가 임의로 변경되지 않아야 한다.
- 암호 알고리즘 및 프로토콜 : 위의 세 가지 요구사항에 대한 보안 서비스를 제공하기 위한 암호 알고리즘과 프로토콜이 정의 되어야 한다.
- 상호 운용성 : 다양한 전자상거래 관련 응용 프로그램간의 상호운용성과 네트워크 제공자와의 상호 운용성이 제공되어야 한다.
- 수용성 : 다양한 신용카드, 금융 기관 및 상점에서 쉽게 사용되어야 한다.

2.3.3 SET 프로토콜 개요

SET은 인터넷에서 신용카드 거래를 안전하게 하기 위한 프로토콜을 말한다. SET은 보안상의 허점을 보완하기 위해서 신용카드 회사인 비자, 마스터카드와 IBM, Netscape, 마이크로소프트 그리고 VeriSign 이 협력 하여 개발하였다.

2.3.4 SET 지불 시스템 참여자

SET에서는 종래의 대면 거래나 우편 주문 거래 방식에서의 대금 지불 관련자들 간의 상호 접촉 방식을 전자적으로 구현하고 있는데, 주요 참여자들은 다음과 같다.

①소비(카드소유자)
②신용카드 발급 기관
③상인
④상인 측 금융기관(Acquirer)
⑤지불 게이트웨이
⑥카드 상표

2.3.5 SET에서의 거래 처리

SET를 이용한 전자상거래의 흐름은 먼저 소비자가 인터넷상에 있는 상인의 쇼핑몰에 접속하여 상품을 선택하고 대금 결제를 위한 정보를 전송한다. 이때 상인 시스템에서 가동 메시지를 웹 브라우저에 전송하고, 웹 브라우저는 주어진 MIME 타입에 해당하는 소비자 측의 응용 프로그램을 가동한다. 소비자는 다시 상인의 전자 지불 서버로 대금 결제 메시지를 전송하고 응답을 기다린다. 상인 측의 대금 결제 서버는 소비자로부터 대금 결제 메시지를 받고 소비자의 대금 결제 요구가 해당 상품에 대한 구매가 확실한지 확인하기 위해 쇼핑몰 서버에서 구매 정보를 얻는다. 소비자의 대금 결제 요구가 해당 구매 정보에 해당하는 것이 확실하면 전자 지불 서버는 지불 게이트웨이 서버에 접속하여 거래 승인을 요구한다. 지불게이트웨이는 금융 네트워크에 접속하여 은행이나 신용카드 회사에 거래 승인을 요구하고 응답을 기다린다. 지불 게이트웨이가 금융 네트워크로부터 받은 응답을 상인의 전자 지불 서버로 전송하면 전자 지불 서버는 거래 승인 여부에 따라 승인되었을 경우에는 전자영수증을 소비자에게 전송하고 쇼핑몰 서버에 거래 승인을 알리면 쇼핑몰 서버는 그 결과에 따라 상품을 배송하거나 서비스를 실시한다. 만일 거래 승인이 거부되었다면 소비자에게는 거래 승인 거부 메시지만이 전송되어 다른 지불 방법은 선택하거나 대금 결제를 취소할 것인지의 여부를 질의하고 응답에 따라 다시 대금 결제 흐름이 진행되거나 중단된다.

2.3.6 SET의 전자서명 처리 과정

- 1단계 : 갑(구매자)은 거래 내역에 대해서 일방향 해쉬 알고리즘을 이용하여 메시지 다이제스트라는 특정 값을 생성한다. 이것은 거래 내역에 대한 전자적인 지문과 같으며, 향후 메시지의 무결성을 시험하는데 이용된다.
- 2단계 : 갑은 전자서명을 생성하기 위하여

메시지 다이제스트를 비밀키로 암호화 한다.

- 3단계 : 대칭키를 무작위적으로 생성하여 거래 내역, 전자서명 및 증명서를 암호화 한다. 갑의 증명서에는 공개키가 포함되어 있다. 을(판매자)이 거래 내역을 복호화 하기 위해서는 안전하게 전송된 대칭키가 필요하다.
- 4단계 : 갑이 사전에 입수한 을의 인증서에는 을의 공개키가 들어있다. 대칭키를 안전하게 전송하기 위해서 갑은 을의 공개키를 이용하여 암호화한다. 전자봉투라고 불리는 암호화된 키는 암호화되어 메시지와 함께 을에게 전송된다.
- 5단계 : 값은 을에게 갑의 대칭키로 암호화된 거래 내역, 전자서명, 인증서 및 전자봉투(을의 공개키로 암호화된 갑의 대칭키)를 보낸다.
- 6단계 : 을의 갑으로부터 메시지를 받아서 을의 비밀키로 전자봉투를 복호화하여 갑의 대칭키를 복구한다.
- 7단계 : 을은 대칭키를 이용하여 거래 내역과 갑의 전자서명 및 인증서를 복호화 한다.
- 8단계 : 을은 갑의 인증서에 포함된 공개키를 이용하여 갑의 전자서명을 복호화하여 거래 내역에 대한 원래의 메시지 다이제스트를 복구한다.
- 9단계 : 을은 갑이 사용한 일방향 해쉬 알고리즘을 이용하여 복호화된 거래 내역에 대한 특정 값(메시지 다이제스트)을 생성한다.
- 10단계 : 을은 갑의 인증서에서 입수한 갑의 공개키를 이용하여 2단계에서 갑이 비밀키로 암호화한 메시지 다이제스트를 복호화한 다음, 9단계에서 그가 생성한 메시지 다이제스트와 비교한다. 두 값이 일치하면 메시지 내용이 통신 중에 변조되지 않았음을 알 수 있으며, 또한 갑의 비밀키로 서명되었음을 알 수 있다.

3. 제안한 인증기법

3.1 기본 인증

본 시스템은 암호의 체크 섬을 이용하는 방법으로 MAC(Message Authentication Code)를 구해 사용한다.

사용자 이름과 패스워드에 의한 접근 관리 방법으로는 웹의 초기 때부터 제공되어 온 방법인 기본 인증과 HTTP/1.1에 새롭게 추가된 다이제스트 인증 방법이 있지만, 기본 인증은 사용자 이름과 패스워드가 아무런 암호화 과정없이 네트워크를 통해 서버로 전달되는 것이어서 탈취 및 공격의 가능성이 있으므로, 인증을 위한 정보를 보다 안전한 방법으로 전달하기 위해 다이제스트 인증 방식을 사용하는 것이 좋다.

3.2 기본 인증의 동작 방법

NCSA의 서버를 사용할 경우에, 먼저 서버의 관리자는 특정한 사용자에게만 보여줄 문서들을 하나의 디렉토리에 모아 놓고 그 디렉토리 밑에 .htaccess란 파일을 만들어 접근을 허용할 사용자들의 사용자 이름을 지정해 주고, 패스워드가 드르어있는 파일의 패스를 지정한다. 패스워드는 .htpasswd라는 파일에 암호화하여 저장되는데 이들 파일의 이름은 access.conf 파일에서 정해준다. 각각의 사용자 이름을 지정해 주는 것이 불편할 때는 그룹으로 묶어 사용자 이름은 .htgroup이라는 파일에 저장한다.

기본 인증의 절차는 매우 가난한 방법으로 사용자별 접근제어를 구현하지만, 패스워드가 네트워크상에 평문으로 전송된다는 단점이 있따. 평문으로 전송되는 패스워드는 스니핑(sniffing)과 같은 방법에 의해 쉽게 가로챌 수 있는데, 이 침입방법은 네트워크에 연동되어 있는 호스트 뿐

만 아니라 외부에서 내부 네트워크로 접속하는 모든 호스트에게도 위협이 된다. 다른 단점으로는 등록되어 있는 사용자의 수가 매우 많거나, 이들의 패스워드를 자주 변경해 주어야 할 때, 서버 관리자에게 너무 큰 부담이 될 수 있다.

3.3 다이제스트 인증

다이제스트 인증 방식도 기본 인증 방식과 마찬가지로 단순한 challenge-response 메커니즘으로 동작한다. 이 방식에서는 타임스템프(timestamp)를 사용하고 있으며, 응답 메시지 속에 MD5 검사합(checksum) 방식에 의해 인코딩 된 사용자 ID, 패스워드, 주어진 타임스템프, HTTP method, request-URI 등이 들어가지만, 패스워드는 절대 평문의 형태로 전달되지 않는다. 이 과정에서 서버에게 검사합이나 다이제스트를 생성하는 데 쓰이는 알고리즘을 지정할 수 있게 하는 옵션 헤더가 있다. 여기서는 MD4 알고리즘이 기본적으로 설정되어 있으며 128-비트 MD5 다이제스트가 32개의 ASCII 문자로서 표현된다.

따라서 MD5 알고리즘에서 알려진 문제점들이 그대로 다이제스트 인증 방식에서도 나타나지만 다이제스트 인증은 기본 인증을 대치하기 위해 만들어진 것이며, 서버 측면에서의 패스워드 시스템이 공통적으로 겪고 있는 문제점이기도 하다. 대부분의 다른 인증 프로토콜에서 보더라도 공격에 대한 위험은 프로토콜 자체에 있는 것이 아니라 이것을 사용하는 데 있어서의 보안 정책이나 절차에 의해 좌우된다. 다이제스트 인증을 하더라도 이의 보안 강도는 구현 방식에 달려 있게 된다. 이러한 다이제스트 인증 방식을 위해 "WWW-Authenticate" 헤더 필드와 "Authorization" 헤더 필드를 수정하였다. 여기에다 "Authentication-info"라고 하는 새로운 헤더 필드 하나가 다이제스트 인증을 위해 추가되었다.

4. 결 론

국내 전자상거래 사이트 상의 정보보호 및 관리 기술 분야는 많은 발전을 가져오고 있다. 본 논문에서는 비대칭적 암호화 기법 및 SET을 이용한 암호화 거래 방법을 이용하였으며, 호스트의 비대칭적인 스위칭 시스템으로 사용자가 웹 사이트에 접속 시에는 데이터 서버는 닫혀있는 상태이고 비동기적으로 사용자가 웹 사이트에서 인증을 취득한 후에 데이터 서버로 접속이 가능하며 데이터의 액세스가 끝난 후에는 웹 사이트의 접속을 재게 시키고 데이터 서버의 액세스는 무효화시킴으로써 서버의 데이터 보안 및 관리를 효율적으로 수행한다. 또한 SSL 실행 방법을 검토하고 서버측 인증서를 얻어서 설치하는 방법을 사용하였으며 IIS 메타베이스의 보안 설정을 간단히 알아보았다. 차후에는 모든 형태의 클라이언트 인증을 다루고, 주어진 상황에 따라 어떤 형태를 선택할지를 결정하는 데 도움이 되는 팁을 제공하고자 한다. 이 시스템은 한가지 단점을 가지고 있다. 실시간 접속이 부자연스럽고 사용자의 대기 시간이 부여되므로 처리 시간이 다소 지연되어진다. 이 문제를 해결하는 것이 향후 연구 과제이다.

참고문헌

[1] 김병천 "암호기술 및 전자상거래보안", 한국정보보호센터 기술개발부기반기술팀, 1999년 2.

[2] Paul Timmers, " Business Models for Electronic Markets", Electronic Market, Vol.8, No2, April 1998.

[3] Ravi Kalkota, Andrew B. Whinston, readings in Electronic Commerce, A

ddison-Wesley Publishing Company, 1997.
[4] 개방형 통신망 환경에서의 인증 및 접근 통제 기술, 한국정보보호센터 기술본부 기술응용팀, 1998년 4.
[5] 인터넷 전자상거래의 물결-뉴글로벌시장, 한국 전자통신 연구원 1998년 6.
[6] 전자상거래를 위한 보안 기술 체계 및 요소 기술에 대한 이해 한국 전산원 1999년 6.
[7] 김기병, 김수홍, "전자상거래를 위한 지불방법" 한국정보처리학회지, Vol.6, No1, January. 1999.
[8] 이만영, "전자상거래 보안기술", 생능출판사
[9] 전자지불 표준 동향 분석에 관한 연구, 한국전산원, 1998년 9.
[10] 한국형 전자화폐를 이용한 유통시스템 모델 연구, 한국정보통신진흥협회. 1997년 12.
[11] 염흥열, 홍기융, "공개키 기반구조", 통신정보보호학회 학회지(PKI 특집). 8권3호,1998.
[12] 공개키 기반 구조 전개를 위한 유럽 신뢰서비스 분석, 한국정보보호센터 정책기획본부 정책연구팀, 1998년 6.

김 지 은

2004년 ~ 현재 안동과학대학 사이버테러대응학과 재학

전 현 정

2004년 ~ 현재 안동과학대학 사이버테러대응학과 재학

윤 동 식

1992년 관동대학교 전자계산학과(공학사)
1994년 관동대학교 컴퓨터공학과(공학석사)
2000년 관동대학교 컴퓨터공학부(공학박사)
1999년 ~ 현재 안동과학대학 사이버테러대응학과 교수