S/MIME을 적용한 안전한 지불 메커니즘 설계
(Design of a Secure Payment Mechanism based on S/MIME)

전 철 우 † 이 종 후 †† 이 상 호 †††
(Chul-Woo Chun) (Jong-hu Lee) (Sang-Ho Lee)

요 약 최근 등장한 메일 기반의 계좌이체 시스템은 송금인이 수금인의 계좌번호를 알 필요 없이 메일 주소만 알면 계좌 이체가 가능하도록 하여 사용자에게 많은 편의를 제공한다. 그러나 대부분의 메일 기반 계좌이체 시스템은 SSL 기반으로 동작하고 있어 거래 사실에 대한 부인이 가능하고, 영수증 발급이 불가능하다는 문제점이 있다.

이에 따라 이 논문에서는 기밀성, 무결성, 사용자 인증, 부인 봉쇄 등의 보안 서비스를 제공하고 인증서 기반으로 동작하는 국제 표준 메일 보안 메커니즘인 S/MIME을 적용한 메일 기반의 지불 메커니즘을 제안한다. 이 메커니즘에서는 'Check'라는 수표와 같은 역할을 하는 메시지를 통해 모든 계좌이체 정보가 송금인과 수금인 및 메일 결제 서버 사이에서 전달된다. 이 시스템은 기존의 시스템과 마찬가지로 수금인의 메일 주소만 알면 계좌이체가 가능한 편리성을 제공함과 동시에 S/MIME에 기반한 보안 서비스를 제공함으로서 기존 지불 시스템에서 가장 문제가 되는 송신 부인 문제를 해결하고 영수증 발급도 가능하다.

키워드 : 메일 보안 메커니즘, 보안 웹 메일 시스템, 지불 시스템, 암/복호화, 전자서명

Abstract In E-mail based accounting system, the remitter does not have need to find collector's account number. To transfer money to a collector's account, what remitter need is just a collector's E-mail address. But the current E-mail based accounting systems are built on SSL technology. Basically SSL provides some security services - confidentiality, user authentication and data integrity, but does not provide non-repudiation. So, in the current E-mail based accounting system, it is possible to deny transaction. And there is no receipt of transaction.

In this paper, we design and implementation of a S/MIME applied Secure Payment Mechanism. In our system, every account information - account number, receiver name, amount of money, etc. - is included in a 'check' message. And this message is protected under the Secure Web-mail using S/MIME. In a view point of the convenience, users using our system do not have need to find collector's account number. And in a view point of the security, our system provides confidentiality, user authentication, data integrity and non-repudiation. Moreover our system provides a receipt.

Key words : S/MIME, payment system, secure e-mail system, encryption/decryption, digital signature

1. 서 론

인터넷의 이용이 보편화되면서 인터넷 쇼핑몰이나 인터넷 뱅킹과 같은 전자상거래 서비스 또한 자주 활용되는 서비스로 자리잡아 가고 있다. 이와 같은 인터넷 뱅킹 등의 이용자가 증가하면서 최근의 전자상거래 서비스는 기능적인 면뿐만 아니라 사용자가 쉽게 서비스를 이용할 수 있도록 편리성을 극대화하는데 주력하고 있다.

전자상거래에서의 편리성을 추구하는데 있어서 최근 등장한 주목할 만한 서비스로 메일을 이용한 계좌 이체 서비스가 있다. 기존 인터넷 뱅킹에 의한 계좌 이체 서비스는 실세계에서의 계좌 이체와 마찬가지로 송금인이 수금인의 은행 계좌번호를 반드시 미리 알고 있어야 한다. 그러나 메일을 이용한 계좌 이체 서비스의 경우에는 상대방의 은행 계좌번호를 알지 못해도 수금인의 메일

† 학생회원 : 충북대학교 컴퓨터과학과
chun605@hanmail.net
†† 비 회 원 : (주)시큐컴 대표이사
jiongfu@cqcom.com
††† 종신회원 : 충북대학교 전기전자및컴퓨터공학부 교수
shlee@cbucc.chungbuk.ac.kr
논문접수 : 2002년 4월 13일
심사완료 : 2002년 6월 25일

주소만 알고 있으면 계좌 이체가 가능하다는 점에서 실세계에서의 계좌 이체나 현재의 인터넷 뱅킹에 비해서 매우 편리하다고 할 수 있다.

이와 같이 가장 대표적인 인터넷 응용이라고 할 수 있는 메일 시스템은 본래 메일 시스템이 갖고 있는 용도뿐만 아니라, 점차 다른 인터넷 응용의 기반기술로 작용하고 있다.

인터넷에서의 메일은 초기에는 UNIX TCP/IP (Transmission Control Protocol/Internet Protocol) 기반의 메일 시스템으로 출발하여 POP/IMAP (Post Office Protocol/Internet Message Access Protocol) 등을 이용한 메일 시스템이 주를 이루고 있다. 그러나 이러한 경우에는 전용 메일 클라이언트 프로그램이 있어야 하며 사용자가 반드시 자신만의 컴퓨터나 메일 계정을 소지하고 있어야 하는 단점이 있다. 따라서 일반인들은 메일 시스템을 사용하기가 다소 불편한데 최근에는 웹메일 시스템이 이러한 불편을 해소할 수 있는 차세대 인터넷 메일 시스템으로서 각광 받고 있다. 웹메일 시스템은 웹 브라우저만 사용할 수 있다면 누구나 쉽게 조작이 가능하고 자신의 컴퓨터가 아닌 다른 컴퓨터에서도 쉽게 메일을 주고받을 수 있어 이동성이 뛰어나다. 앞에서도 기술하였듯이 메일 시스템은 모든 인터넷 통신의 기반이 될 뿐만 아니라 전자상거래가 보다 활발하게 이루어질 경우 주문서, 계약서 등 여러 가지 중요한 정보들이 메일을 통해서 교환될 것으로 예측된다. 특히 높은 인터넷 보급률과 PC(Personal Computer)방 등의 영향으로 인해 일반인들의 사용이 늘고있는 웹메일 시스템은 이동성, 편리성 등 웹메일 시스템만이 갖는 장점으로 인해 향후 가장 널리 사용되는 인터넷 통신수단으로 자리잡을 것으로 예상된다.

그러나 웹메일 시스템을 포함한 인터넷 메일 시스템이 전자상거래에 본격적으로 적용되기 위해서는 반드시 보안 문제의 해결이 필요하다. 전자상거래 서비스를 성공적으로 운영하기 위한 보안기술의 중요성은 이미 널리 인식되고 있으며 인터넷의 발전과 함께 각종 보안 위협이 증가하고 있는 가운데 보안기술의 중요성은 더욱 강조되고 있다. 특히 앞에서 언급한 기존의 메일 기반 계좌 이체 서비스와 같은 경우에는 웹메일 시스템을 이용하여 계좌 이체가 이루어지는 가운데 보안 서비스 제공을 위해 SSL(Secure Socket Layer)을 사용하고 있는데 이로 인해 거래 사실의 부인이 가능해지는 등의 몇 가지 문제를 가지고 있다.

이에 이 논문에서는 인터넷 상에서의 전자 결제에 있어서 안전성과 편리성을 제공할 수 있는 메일 기반의 전자 지불 메커니즘을 제안하고자 한다. 이 논문에서 제안하고자 하는 지불 메커니즘은 보안 웹메일 시스템을 기반으로 하여 현재 인터넷 뱅킹이나 메일 기반 계좌 이체 서비스에서 제공하고 있는 계좌 이체 서비스를 제공한다. 즉, 송금인이 수금인의 계좌번호를 알지 못하더라도 메일 주소만 알면 계좌 이체가 가능하다. 또한 국제 표준 메일 보안 메커니즘인 S/MIME을 적용함으로써 기존의 메일 기반 계좌이체 시스템에서 발생하는 보안상의 문제점도 해결가능하다.

이 논문의 2장에서는 계좌 이체를 비롯한 인터넷 전자상거래에 대한 이해를 위해 전자지불 시스템에 대해서 살펴본다. 3장에서는 이 논문에서 제안하고자 하는 지불 메커니즘의 기반 기술로 작용하는 메일 보안 메커니즘에 대해서 분석하고 4장에서는 기존의 메일 기반 계좌 이체 시스템에 대해서 고찰하고, 5장에서는 안전한 전자 지불 메커니즘의 설계와 평가에 대해서 기술하고 마지막으로 6장에서 결론을 맺는다.

2. 전자지불 시스템의 개발동향

최근 몇 년 동안 국내외 전자상거래 시장이 급속하게 성장하면서 전자상거래의 필수 요소인 전자지불 시스템 개발이 활발하게 진행되고 있다. 이러한 전자지불 시스템은 크게 지불 브로커 시스템(일반적으로 PG(Payment Gateway) 시스템이라고 함)과 전자화폐 시스템으로 구분할 수 있다. 두 시스템 모두 전자상거래 분야, 특히 B2C(Business-to-Customer)로 대표되는 인터넷 쇼핑몰에서 고객이 상품을 구입할 때 편리하고 안전하게 대금 결제를 할 수 있도록 개발된 시스템이다. 경우에 따라 인터넷상에서 거래에 대한 대금결제를 계좌이체로 대신할 수 있는 인터넷 뱅킹 시스템을 전자지불 시스템에 포함시키기도 하지만 기존의 은행 거래 일부를 인터넷 서비스의 형태로 제공하기 위해 개발되었다는 점에서 전자지불 시스템과 다소 차이가 있다.

지불 브로커 시스템과 전자화폐 시스템은 인터넷을 통해 전자상거래에 사용되는 지불 수단이란 점에서는 동일하지만 내부적으로 동작하는 메커니즘은 매우 다르다.

지불 브로커 시스템은 고객이 신용카드를 이용해 인터넷상에서 거래에 대한 지불을 할 수 있도록 개발된 것이다. 신용카드를 이용한 거래가 일반화되어 있는 현재 가장 널리 이용되고 있는 시스템으로 고객과 인터넷 쇼핑몰이 서로를 신뢰할 수 없는 상황에서 지불 브로커가 고객과 쇼핑몰 사이에서 신용카드 결제에 대한 중개인 역할을 해 줌으로써 신용카드를 안전하게 이용할 수 있도록 하는 구조로 되어있다. 이 시스템은 신용카드를

소지하고 있는 사용자만 이용할 수 있다는 제약이 따르며 신용카드 이용에 따른 수수료 지불과 같은 제반 환경상 고액의 거래에 적합한 특성을 지니고 있다.

이에 비해 전자화폐 시스템에서 사용자는 은행 또는 신용카드사로부터 IC카드 형태의 전자지갑을 발급 받고 자신의 은행계좌의 금액 또는 현금을 전자화폐로 발행받은 후 인터넷 쇼핑몰에서 물건을 구입하고 이에 대한 결제를 할 수 있다. 이 전자화폐는 인터넷 쇼핑몰뿐만 아니라 기존의 오프라인 상점에서도 대금 결제 수단으로 이용이 가능하다. 즉, 기존의 대표적인 지불 수단인 현금의 사용 범위를 실세계는 물론 인터넷까지 확장한 전자지불 수단이라고 할 수 있다. 또한 거래 금액 면에서 신용카드를 이용한 지불 브로커 시스템과 비교해 볼 때 전자화폐 시스템은 현금과 같이 소액의 거래에 적합한 특성을 가지고 있다. 즉, 전자화폐 시스템은 기존의 현금과 동일한 가치를 지니는 디지털 정보 형태의 전자화폐를 고객에게 발행해 줌으로써 전자화폐를 거래에 항시 이용할 수 있도록 한 것으로 선불카드/직불카드를 한 단계 발전시킨 시스템이다. 이러한 전자화폐는 소액의 거래에도 적용하기 쉽고 기존의 현금과 사용이 거의 동일하기 때문에 누구나 쉽고 편리하게 사용할 수 있다는 장점을 지닌다[1][2].

초기에 개발된 전자화폐 시스템은 개인의 PC에 소프트웨어로 제작된 전자지갑을 설치하여 이용할 수 있는 형태로 개발되었는데 1994년 네덜란드의 DigiCash사에서 개발한 *Ecash*가 대표적인 전자화폐 시스템이다[3]. 그러나 이와 같은 소프트웨어 전자지갑 방식을 이용한 시스템은 모든 정보가 PC에 저장되어 관리되기 때문에 이동성이 떨어지는 단점을 지닌다. 또한 전자화폐 위조 및 이중 사용과 같은 보안 위협에 대처할 수 있도록 복잡한 보안 구조 및 프로토콜을 지닌 형태로 개발해야 하는 부담이 있어 널리 사용되고 있지 못한 상태이다.

최근의 전자화폐 시스템은 높은 보안성과 탁월한 휴대성을 지니고 있는 IC카드를 이용해 전자지갑을 구현하고 여기에 기존의 현금과 동일한 가치를 지니는 전자화폐를 저장하여 전자상거래에 즉시 이용할 수 있도록 한 IC카드 기반 전자화폐 시스템이 주목을 받고 있다. IC카드는 높은 보안성을 지니고 있음에도 불구하고 높은 개발비용과 다양한 어플리케이션을 제공하는데 어려움이 있어 제한적으로 사용되어왔다. 그러나 최근 IC카드 개발 기술의 발전과 함께 IC카드와 단말기 가격이 하락하고 Java 기술 등을 접목하여 다양한 어플리케이션을 수용할 수 있게 되면서 전자화폐 시스템은 IC카드를 기반으로 개발되는 것이 일반적이다[1][2].

전자화폐 시스템에서 금액 정보를 비롯한 모든 거래 정보는 디지털 형태로 저장되고 금융망 또는 인터넷과 같은 네트워크를 통해 전송되는데 디지털 정보는 특성상 불법적인 제3자에 의해서 위조되거나 변조될 가능성이 매우 높다. 따라서 전자화폐를 이용하기 위해서는 안전성과 신뢰성은 매우 중요한 요소인데 IC카드는 디지털 정보 형태의 전자화폐, 거래 내역 등과 같이 중요한 정보를 안전하게 보호하고 저장하는데 매우 적합한 기술로 평가되고 있다. 이에 최근 몇 년 사이 국내외적으로 IC카드를 이용한 전자화폐 시스템 개발을 서두르고 있으며 이와 함께 국제 표준화를 위한 활발한 행보가 진행되고 있는 상황이다.

3. 메일에서의 보안성 분석

3.1 메일 보안 서비스

일반적으로 메일 보안 서비스는 송신자 인증과 데이타의 기밀성 및 무결성 그리고 송신 부인봉쇄 등을 포함한다. 이 장에서 분석하고자 하는 메일 메커니즘인 S/MIME (Secure Multi-Purpose Internet Mail Extensions)과 PGP/MIME은 모두 사용자에게 이와 같은 보안 서비스를 제공한다. S/MIME은 처음에 RSA Data Security Inc.에서 개발되었다. 이 것은 메시지를 위해 ASN.1 *DER* 형식을 따르는 PKCS#7 데이타 형식과 공개키 인증서를 위한 X.509 v3 형식을 기반으로 한다. 또한 PGP/MIME은 PGP(Pretty Good Privacy)를 기반으로 하고 있는데 메시지 형식과 인증서 형식은 독자적으로 만들어 졌으며 단순한 이진 인코딩을 사용하고 있다.

S/MIME과 PGP/MIME은 메시지의 구조를 위해 모두 MIME 표준을 사용하며 또한 이 두 프로토콜은 전자서명된 메시지를 전송하기 위해 RFC 1847에 기술되어 있는 multipart/signed MIME 타입을 따른다[4].

또한 이 장에서는 기존의 웹메일 시스템에서 보안 서비스를 제공하기 위해 많이 사용되는 SSL(Secure Socket Layer)에 대해서도 살펴본다.

3.2 SSL 기반의 메일 보안

기존 웹메일 시스템이나 메일 기반 계좌이체 시스템에서 보안 메커니즘으로 사용하고 있는 SSL은 인터넷 환경에서 통신을 하는 두 응용 프로그램 사이에 안전한 채널을 형성함으로써 보안 서비스를 제공한다[5][6].

이와 같은 SSL을 이용한 보안 메일 시스템은 그림 1과 같이 구성된다.

(1)에서 송신자와 웹메일 서버는 SSL 핸드쉐이크를 통해 서버 인증을 수행하고 암호통신에 사용될 암호키를 교환한다. (2)에서 송신자는 메일을 작성하고 이를

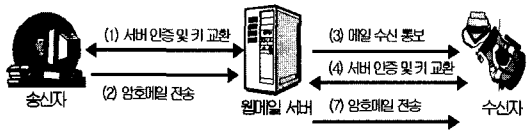

그림 1 SSL 기반의 보안 웹 메일 시스템

(1)에서 교환된 암호키를 이용해 암호화하여 웹메일 서버에게 전송한다. (3)에서 수신자는 자신에게 메일이 도착되었음을 알 수 있고 이를 읽기 위해 (4)를 진행한다. (4)에서 수신자는 SSL 핸드쉐이크를 통해 서버를 인증하고 암호키를 교환한다. 웹메일 서버는 (5)에서 송신자로부터 수신한 암호화된 메일을 복호화고 이를 수신자에게 송신하기 위해 (4)에서 교환된 키를 이용해 다시 암호화한다((6)). (6)에서 암호화된 메일은 (7)과 같이 수신자에게 전송된다.

이와 같은 SSL 기반의 보안 웹 메일 시스템은 크게 2가지 문제점이 지적된다.

첫 번째는 보안 메일 서비스가 제공해야 되는 보안 서비스인 사용자 인증, 데이타의 기밀성 및 무결성, 송신 부인 봉쇄 가운데 송신 부인 봉쇄 서비스가 제공되지 않는다는 점이다. 이는 SSL에서 데이타에 대한 암호화만을 제공하고 데이타에 대한 전자서명은 제공하지 않기 때문이다. 일반적으로 웹 통신에 적용되는 SSL의 경우 클라이언트와 웹 서버 사이에 교환되는 모든 데이타에 대해 전자서명을 제공할 경우에는 전자서명 연산에 너무 많은 시간이 소요되기 때문에 매우 비효율적인 통신이 될 수밖에 없고 따라서 SSL에서는 데이타에 대한 전자서명은 제공하지 않는다. 그러나 메일 서비스에서의 송신 부인 봉쇄는 기본적인 보안 서비스로 반드시 제공되어야 한다. 또한 현재 SSL 기반의 보안 웹 메일 시스템에서는 일반적으로 서버 인증은 인증서 기반으로 이루어지지만 클라이언트 인증은 ID와 패스워드에 기반한 인증방식을 사용하고 있다. 그러나 ID와 패스워드 기반의 인증방식이 취약한 것은 이미 잘 알려진 사실이며 따라서 클라이언트 인증도 좀 더 안전한 방식으로 개선할 필요가 있다.

SSL 기반 보안 웹 메일 시스템의 두 번째 문제는 웹 메일 서버 관리자가 사용자들의 메일의 내용을 얼마든지 볼 수 있다는 점이다. 그림 1에서 보는 바와 같이 송신자가 보낸 메일은 일단 웹 메일 서버에서 복호화된 뒤에 다시 웹 메일 서버와 수신자가 공유하는 키로 암호화되어 수신자에게 전송된다. 따라서 웹 메일 서버에서 메일이 복호화되는 과정에서 평문이 메일이 외부로 누출될 위험이 있으며 송수신자 모두와 키를 공유하는 웹 메일 서버의 관리자는 메일의 내용을 얼마든지 볼 수 있다. 또한 메일이 웹 메일 서버에서 보관될 때도 평문으로 보관되거나 관리자가 알고있는 키로 암호화되어 저장됨으로 웹 메일 서버 관리자는 사용자 메일의 내용을 쉽게 볼 수 있으며 경우에 따라서는 변조도 가능하다.

이와 같은 문제는 SSL을 기반으로 하는 메일 기반 계좌이체 시스템에도 그대로 적용되는데 이에 대해서는 4장에서 보다 자세히 분석하기로 한다.

3.3 S/MIME

RSA Data Security Inc.에서 개발된 S/MIME은 현재 S/MIME v3(Version 3) 개발이 완료단계에 있는 상태이며 표준화는 IETF(Internet Engineering Task Force)의 S/MIME W/G에서 담당하고 있다. IETF에서 정의한 S/MIME v3는 다음과 같이 4부분으로 구성되어 있다[7] [8] [9] [10].

- Cryptographic Message Syntax
- S/MIME Version 3 Message Specification
- S/MIME Version 3 Certificate Handling
- Enhanced Security Services for S/MIME

S/MIME W/G에서는 S/MIME v3을 IETF의 표준으로 만들기 위해 RSA 키 교환과 취약한 암호기법을 요구하지 않도록 프로토콜을 정의하고 또한 S/MIME의 보안 서비스 확장인 "Enhanced Security Services for S/MIME"를 S/MIME W/G에서 논의하고 있다.

"Enhanced Security Services for S/MIME"에는 기본적인 S/MIME에 추가적으로 송신자의 전자서명된 메시지를 수신한 후 수신자의 전자서명을 추가하는 "signed receipts", 원본 메시지의 접근 권한을 부여할 수 있는 "security labels", 메일링 서버로 보내진 메시지의 불법적인 변경 등을 막을 수 있도록 할 수 있는 "secure mailing lists" 등을 제공할 수 있도록 확장한 것이다.

"signed receipts", "security labels"는 S/MIME v2와 S/MIME v3 모두에서 동작할 수 있는 반면 "secure mailing lists"는 S/MIME v3 에서만 동작한다.

S/MIME v2와 S/MIME v3의 차이점을 비교하면 S/MIME v2와 v3가 유사한 MIME 형식을 사용하고 있기는 하지만 표 1에서 보는 바와 같이 메시지 기밀성, 해쉬 알고리즘 및 전자서명과 키 교환을 위한 공개키 암호 알고리즘 등을 교체하였다. 이와 같이 S/MIME v2에서 메일 보안 서비스 제공을 위해 사용되었던 암호 알고리즘을 전체적으로 수정한 이유는 메일 보안 시스템의 표준화에 걸림돌이 되는 보안에 취약한 암호 알고리즘과 특허와 관련된 문제 등을 해결하기 위해서이다.

표 1 S/MIME v2와 S/MIME v3 비교

비교 항목(알고리즘)	S/MIME v2	S/MIME v3
해쉬 알고리즘	MD5	SHA-1
전자서명	RSA	DSA
공개키 암호 알고리즘	RSA	Diffie-Hellman
관용 암호 알고리즘	40 bit RC2	triple-DES

3.4 PGP/MIME

PGP의 초기 버전은 1990년대 초에 공개되어 사용되어 왔다. 이러한 PGP와 메일 메시지 표준인 MIME과 결합한 형태의 PGP/MIME은 인터넷 메일 어플리케이션 개발 업계 중에서도 특히 Qualcomm 社를 중심으로 인터넷 메일 프로토콜로 채택되어 왔다. PGP/MIME 구현은 다음 두 가지의 RFC를 기반으로 하고 있다[11][12].

- PGP Message Exchange Formats
- MIME Security with Pretty Good Privacy

PGP/MIME에 관련된 표준화 작업은 IETF의 Open PGP W/G에서 담당하고 있는데 PGP/MIME이 IETF 표준이 될 수 있도록 PGP 기반의 메일 보안 프로토콜을 정의하고 있다.

PGP를 기반으로 한 PGP/MIME과 IETF에서 PGP/MIME의 메일 표준화를 위해 정의한 OpenPGP와의 차이점을 보면 앞에서 S/MIME v2와 v3의 비교에서 기술한 바와 같이 PGP/MIME과 OpenPGP에서도 표 2에서 보는 바와 같이 사용하고 있는 암호 알고리즘이 상이한 차이가 나타나고 있다.

이와 같이 암호 알고리즘을 전체적으로 수정한 이유는 PGP/MIME에서 기반으로 하고 있는 PGP 암호 모듈은 PGP사의 소유로 특허와 관련되어 있기 때문에 이를 그대로 메일 보안 시스템으로 표준화하는데 걸림돌로 작용하기 때문이다.

표 2 PGP/MIME과 OpenPGP와 차이점 비교

비교 항목(알고리즘)	PGP/MIME	OpenPGP
해쉬 알고리즘	MD5	SHA-1
전자서명	RSA	DSA
공개키 암호 알고리즘	RSA	Elgamal
관용 암호 알고리즘	IDEA	triple-DES
압축 알고리즘	ZIP	Uncompressed

3.5 S/MIME과 OpenPGP의 분석

IETF에서 메일 표준을 위해 논의하고 있는 S/MIME v3와 OpenPGP는 MIME 메시지에 인증과 기밀성, 부인봉쇄 등을 추가한 프로토콜이다. 그러나 두 프로토콜은 많은 방식에서 차이가 있고 상호 연동되도록 설계되지 않았다. 메시지의 기밀성을 제공하기 위해 사용되는 3-DES와 같은 관용 암호 알고리즘과 SHA-1과 같은 해쉬 알고리즘 등은 두 프로토콜 모두 동일하게 이용하고 있지만 그 외의 DSA, ElGamal과 같은 전자서명용 공개키 암호 알고리즘은 서로 다른 알고리즘을 이용하고 MIME 메시지와 결합하는 과정에서 전자서명과 메시지 암호화를 위한 MIME 형식을 달리하고 있다(표 3 참조).

표 3 S/MIME V3와 OpenPGP의 비교

비교 항목	S/MIME v3	OpenPGP
메시지 형식	Binary, CMS 기반	Binary, PGP기반
인증서 형식	Binary, X.509v3 기반	Binary, PGP Certificate
관용 암호화 알고리즘	Triple-DES	Triple-DES
전자서명 알고리즘	DSA	DSA
공개키 암호 알고리즘	Diffie-Hellman	ElGamal
해쉬 알고리즘	SHA-1	SHA-1
전자서명을 위한 MIME 타입	multipart/signed 또는 CMS format	ASCII 형식의 multipart/signed
데이타 암호화를 위한 MIME 타입	application/pkcs7 -mime	multipart/encrypted

현재 S/MIME v2를 지원하는 메일 시스템으로는 마이크로소프트사의 Outlook 및 Outlook Express, Netscape Messenger, OpenSoft의 ExpressMail, Baltimore Technologies의 MailSecure, PreMail, Eudora 등이 있으며 그 외 S/MIME v2를 지원하는 제품으로는 Entrust, SSE TrustedMIME, VeriSign Digital ID, WorldTalk, NEL Mahobin, RSA S/MAIL Toolkit, Secure Messaging Toolkit 등이 있다. S/MIME v3에 대한 표준화 작업은 IETF에서 완료된 상태이나 아직까지 구현물은 없는 상태이다.

PGP/MIME의 경우 지원하는 메일 어플리케이션은 premail, Exmh, MUTT(Michael Elkins), MEW(Kazu Yamamoto), EPPI(Eudora/PGP Plug-In) 등이 있으며 그 외 제품으로 PGP/MIME Toolkit(Michael Elkins)이 나와 있는 상태이다.

지금까지 기술한 바와 같이 인터넷을 이용한 정보의 교류가 활성화되고 이 때 메일 시스템이 다양한 목적으로 활용하고 있다. 이러한 시점에서 중요한 정보를 주고받는 수단으로 이용되는 메일의 보안 문제를 해결하고

자 선진 외국을 중심으로 활발히 메일 보안 시스템을 개발하고 있으며 또한 표준화를 위해 준비중에 있다.

4. 기존 메일 기반 계좌이체 시스템 분석

4.1 기존 메일 기반 계좌이체 시스템 구조

인터넷 활용의 폭이 넓어지고 인터넷을 이용한 쇼핑, 은행 거래, 증권 거래 등 전자상거래 서비스가 활성화되고 있는 가운데 최근에는 메일을 이용한 송금 및 결제 시스템이 등장한 바 있다. 메일 기반의 계좌이체 시스템의 가장 큰 장점은 상대방의 은행 계좌번호를 몰라도 메일 주소만 알면 송금이 가능하다는 것이다. 현재 이와 같은 메일 기반의 결제 시스템은 국내에서만 5개 업체 정도에서 서비스를 제공하고 있는데 기본적인 시스템 구조는 모두 유사하다고 할 수 있다. 기존의 메일 기반 계좌이체 시스템의 구조를 분석하면 그림 2와 같다[13][14][15][16][17].

메일 기반 계좌이체 시스템은 크게 송금인, 수금인, 메일 계좌이체 서버로 구성된다. 송금인과 수금인에게는 웹 브라우저 외의 특별한 소프트웨어의 설치는 요구되지 않는다. 메일 기반 계좌이체 시스템의 동작 절차를 분석하면 다음과 같다.

① 송금인은 메일 계좌이체 서버에 회원으로 등록한다. 이 때 메일 서버로부터 사용자 신원 확인 과정을 거치며 신용카드번호 및 은행 계좌번호를 등록해야만 서비스 이용이 가능하다.

② 회원 등록이 완료되면 서비스를 이용할 수 있다. 서비스 이용을 위해서는 메일 계좌이체 서버에 로그인하는 절차를 거쳐야 하는데 이 때 일반적으로 ID와 패스워드를 이용한 사용자 인증을 거친다. 또한 서버 인증을 위해서는 SSL이 이용된다.

③ 송금인은 송금 요청 메시지를 메일 계좌이체 서버에게 전송한다. 메시지의 내용에는 수금인 실명, 수금인 메일 주소, 송금액이 반드시 포함되어야 한다. 이 메시지는 SSL에 의해서 기밀성 및 데이타 무결성을 보장받는다. 즉 이 메시지는 SSL 핸드쉐이크 과정에서 송금인과 메일 계좌이체 서버에게 공유된 암호키로 암호화되어 전송되며 해쉬함수에 의해서 데이타 무결성 서비스를 제공받는다.

④ 메일 서버는 송금인의 신원을 확인하고 수금인의 실명 및 메일 주소의 유효성을 확인한다. 이 때 송금인으로부터의 입금은 인터넷 뱅킹을 이용한 계좌 이체나 신용카드 현금 서비스 등이 사용된다. 또한 선택적으로 송금인의 계좌나 신용카드로부터 메일 서버의 계좌로 송금액 이동이 일어날 수 있다.

⑤ ④의 과정까지 종료되면 메일 서버는 메일을 이용해 수금인에게 송금 도착 사실을 알린다. 이와 같은 메일을 통한 송금 도착 통지에는 보안 메커니즘이 사용되지 않는다.

⑥ 메일을 통해 자신에게 송금된 사실을 통보 받은 수금인은 메일 계좌이체 서버에 접속한다. 이 때 비회원

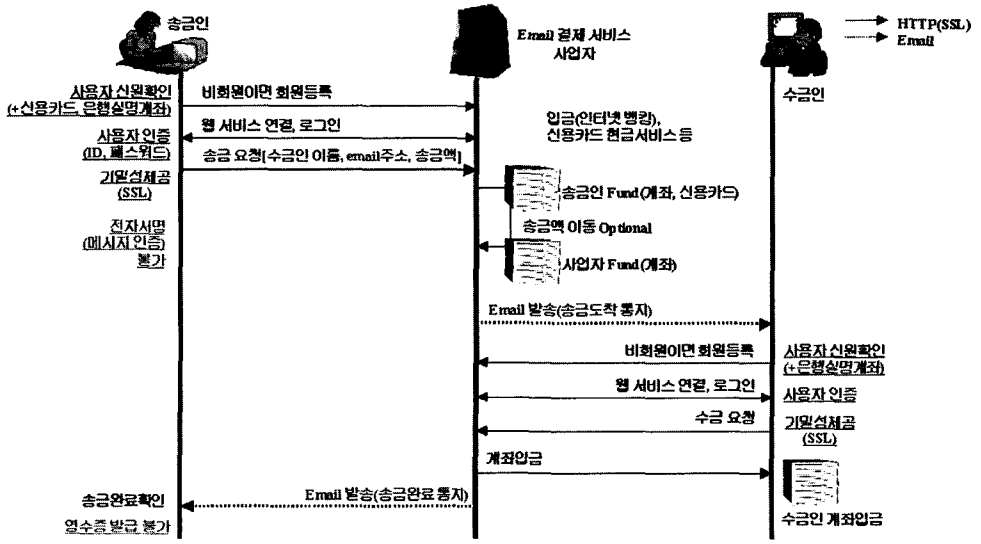

그림 2 기존의 메일 기반 계좌이체 시스템

이면 ①에서 송금인이 수행했던 회원 등록 과정을 거친다. 단 송금인의 경우에는 신용카드번호나 은행 계좌번호 가운데 하나를 등록했지만 수금인은 송금을 받을 수 있는 은행 계좌번호를 반드시 등록해야 한다. 회원 등록을 마치면 메일 계좌이체 서버에 사용자 인증 과정을 거쳐 로그인을 하고 수금 요청을 한다. 이 때 사용자 인증은 ID와 패스워드에 의한 방식이며 수금 요청은 SSL에 의해서 보호된다.

⑦ 수금인의 신원과 계좌의 유효성이 확인되면 사용자는 수금인의 계좌로 입금을 수행한다. 이 때 송금인의 계좌 또는 신용카드에서 직접 이체될 수도 있고 메일 서버의 계좌에서 이체될 수도 있다.

⑧ 수금인의 계좌로 입금이 완료되면 메일 결제 서버는 송금인에게 송금 완료를 알리는 메시지를 메일을 통해 전송한다.

4.2 기존 시스템의 기능 및 문제점

메일을 이용한 계좌이체 시스템의 가장 큰 장점은 송금인이 수금인의 메일 주소만 알면 송금이 가능하다는 것이다. 즉 기존의 결제 시스템 또는 계좌 이체 시스템에서는 수금인의 은행 계좌번호를 반드시 알아야 송금이 가능했지만 메일을 이용한 결제 시스템에서는 수금인의 계좌번호는 메일 계좌이체 서버에서 관리하며 송금인은 수금인의 메일 주소만 알면 되기 때문에 매우 편리하게 송금이 가능하다. 그러나 기존의 메일 기반 계좌이체 시스템에는 몇 가지 문제점이 있는데 이에 대해 살펴보면 다음과 같다.

- 메일이 단순히 통지용으로 사용되고 있음: 이는 이 방식의 단점이라고 할 수는 없지만 메일을 통한 실질적인 가치의 전송이 일어나지 않는다는 점을 지적할 수 있다. 즉 메일이 결제의 편리성을 향상시키는 것은 사실이지만 기존의 방식에서의 메일은 단순히 송금 도착, 송금 완료를 통지하는 용도로만 사용된다.
- SSL에 의한 보안 서비스 제공: 그림 2에서 보는 바와 같이 송금 요청 메시지나 수금 요청 메시지와 같은 중요 정보의 전송은 SSL에 의해서 보호된다. 즉 SSL 핸드쉐이크 과정에서 공유된 암호키와 MAC (Message Authentication Code) 키에 의해서 메시지에 대한 암호화 및 무결성 보장 서비스가 이루어진다. 그러나 앞에서 기술하였듯이 SSL에서는 데이타에 대한 전자서명을 제공하지 않는다. 이는 메시지를 전송한 사실에 대한 부인이 가능하다는 것을 뜻한다. 즉 송금인이 송금 요청 메시지를 전송한 사실을 부인함으로써 메일 기반의 계좌이체 시스템을 이용한 모든 거래 내용을 부인하는 것이 가능하다.
- 메일 계좌이체 서버에서 사용자들의 계좌번호를 관리: 기존의 방식에서는 송금인과 수금인의 신용카드 번호나 계좌번호를 메일 서버에게 등록을 해야만 서비스의 이용이 가능하다. 즉 메일 서버의 관리자는 사용자들의 중요 경제정보를 얼마든지 알아낼 수 있다. 이는 사용자의 사생활 보호라는 측면에서 문제가 된다. 또한 메일 서버가 외부의 공격에 노출되었을 때 사용자들의 중요 경제정보가 노출될 위험이 매우 크다.
- 영수증 발급 불가: 그림 2에서 보는 바와 같이 기존의 메일 기반 결제시스템에서는 수금인으로부터 영수증을 발급하는 절차가 없다. 따라서 수금인은 자신의 수금한 사실을 부인함으로써 전체 거래를 부인할 수 있다.

5. 시스템 설계 및 구현

5.1 시스템 설계

이 논문에서 제안하는 메일 기반 전자 지불 메커니즘은 S/MIME을 적용한 보안 웹메일 시스템을 기반으로 동작하며 전체적인 시스템 구성은 그림 3과 같다.

그림 3에서 보는 바와 같이 지불 메커니즘은 크게 사용자(송금인, 수금인), 메일 서버, 결제 서버의 3부분으로 구성되며 각각에 대하여 기술하면 다음과 같다.

- 사용자: 송금 및 수금의 당사자가 되는 사용자이다.

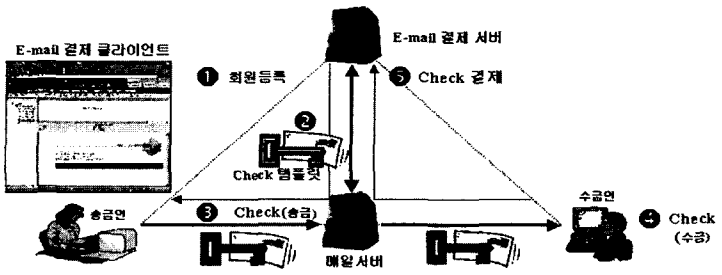

그림 3 제안 메커니즘의 시스템 구성도

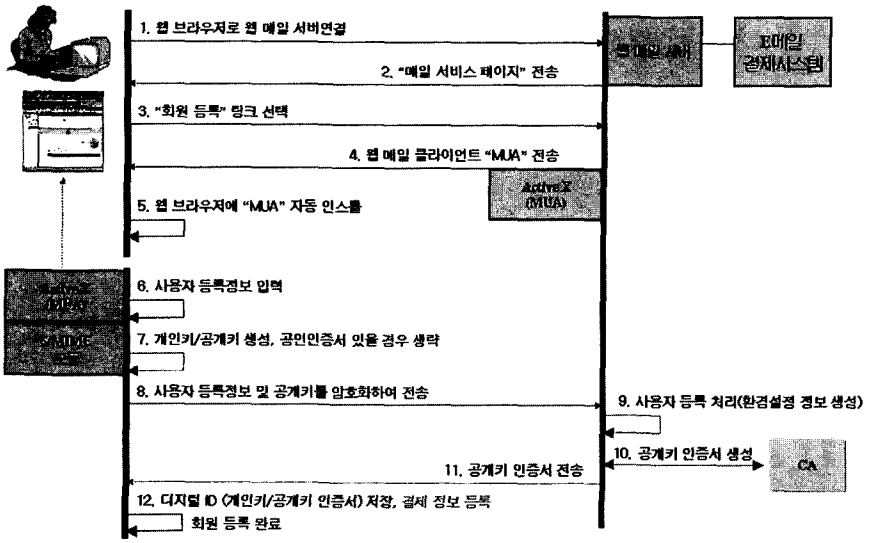

그림 4 회원 등록 과정

웹메일에 기반해서 동작하는 시스템이기 때문에 송금인과 수금인 모두 웹메일 시스템의 회원으로 등록해야 하며 시스템을 사용하기 위해서 웹 브라우저가 필요하다.

■ 메일 서버: 지불 정보는 메일 메시지 형태로 전송되어 진다. 메일 서버는 S/MIME v2를 보안 웹메일 서버로서 지불 정보가 포함된 메일 메시지를 전송하는 역할을 한다.

■ 결제 서버: 지불 수단이 되는 템플릿을 생성하고 실제 지불 처리를 수행하는 결제 서버이다.

또한 메일 지불 메커니즘의 중요한 구성요소로 "Check"란 데이타 형식이 정의된다. Check는 메일 지불 서버가 전송한 템플릿에 필요한 정보를 송금인이 기입한 정보이다. 이 데이타 형식은 메일 메시지 내에 포함되며 결제 서버는 이 데이타 형식 내의 정보를 기반으로 실질적인 지불 처리를 수행한다. Check의 내에 포함되는 필수정보는 다음과 같다.

■ 메시지 생성시각: Check 메시지가 생성된 시각

■ 수금인 실명 및 메일 주소: 수금인의 실명 및 메일 주소

■ 수금인 계좌번호: Check에 기입된 금액이 입금될 은행 계좌번호

■ 송금액: 송금할 액수

■ Check 번호: Check 발행된 순서에 따라 결정되는 일련번호

이 밖에 전화번호, 통화, 용도 등 기본적인 신상정보가 Check에 포함된다.

5.2 프로토콜 설계

메일 기반 전자 지불 메커니즘에서 이체가 이루어지는 프로토콜은 크게 회원 등록 과정, 송금 과정, 수금 과정의 3부분으로 구성되며 각각의 과정에 대해서 살펴보면 다음과 같다.

5.2.1 회원 등록 과정

회원 등록은 그림 4와 같은 과정을 통해 이루어진다. 회원 등록 과정은 일반적인 웹 메일 회원으로 등록하는 과정과 유사하다. 그러나 제안 지불 메커니즘에서의 메시지는 일반 메일을 통해 전송되는 것이 아니라 메일 보안 메커니즘인 S/MIME으로 보호된다. 회원 등록 과정에 대해서 살펴보면 다음과 같다.

① 사용자는 지불 메커니즘을 이용하기 위해서 웹 브라우저를 이용해 보안 웹 메일 서버에 접속한다.

② 웹 메일 서버로부터 사용자에게 서비스 페이지가 전송된다.

③ 사용자는 회원 등록을 위해 "회원 등록" 링크를 선택한다.

④ 웹 메일 서버로부터 클라이언트 모듈이 다운로드 된다. 이는 웹 브라우저에서 플러그인(Plug-in) 형태로 동작하며 메일 처리를 위한 MUA와 S/MIME 처리를 위한 S/MIME 모듈을 포함하고 있다.

⑤ 다운로드 된 클라이언트 모듈이 웹 브라우저에 자동으로 설치된다.

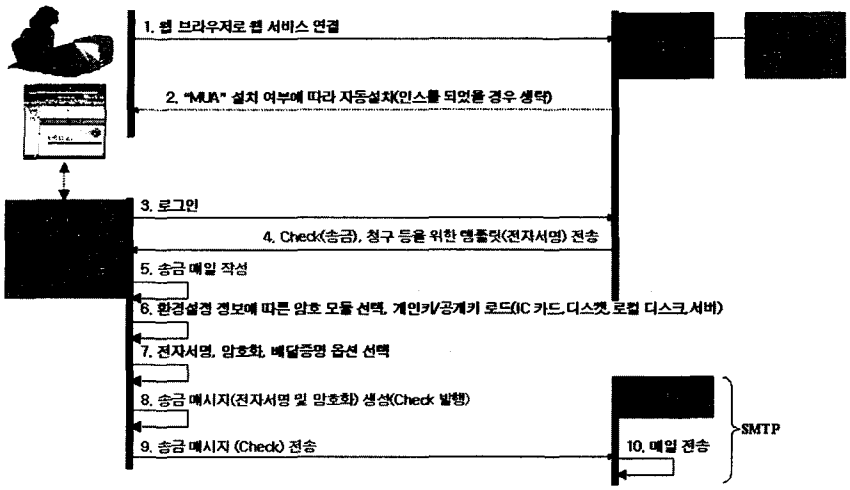

그림 5 송금 과정

⑥ 사용자는 사용자 등록 정보를 입력한다.

⑦ 입력된 사용자 등록 정보를 이용해 클라이언트 모듈은 공개키 쌍을 생성한다.

⑧ 사용자 등록정보 및 공개키가 보안 웹 메일 서버로 전송된다. 이 때 전송되는 메시지에 대해서 다음과 같이 전자서명과 암호화가 적용된다.

EKS [M || KUuser || EPassword [KRuser] || Timestamp] || EKUserver [KS]

M: 사용자 등록정보
KUuser: 사용자의 공개키
KRuser: 사용자의 비밀키
KUserver: 서버의 공개키
Password: 사용자가 입력한 패스워드
KS: 임의로 생성된 관용키(세션키)

이 때 사용자 등록정보 *M*에는 사용자가 입력한 패스워드가 포함되는데 사용자 패스워드는 보안 웹 메일 서버에서도 알지 못하도록 해야 함으로 패스워드를 그대로 전송하지 않고 패스워드의 해쉬값*(H(Password))*을 전송한다. 또한 사용자의 개인키 *KRuser* 또한 보안 웹 메일 서버가 알지 못하도록 해야하는 정보임으로 사용자만이 아는 사용자의 패스워드를 키로 사용해서 암호화한다.

⑨ 보안 웹 메일 서버는 사용자 등록 처리한다. 즉 사용자 등록 정보를 자신의 DB에 저장한다.

⑩ 보안 웹 메일 서버는 사용자로부터 수신한 공개키를 이용해 CA에게 공개키 인증서 발행을 요청하고 CA로부터 사용자의 인증서를 수신한다. 이 때 인증서 발행 요청은 PKCS#10 규격을 따른다.

⑪ 보안 웹 메일 서버는 사용자의 인증서를 사용자에게 전송한다.

⑫ 사용자는 자신의 개인키와 인증서를 저장하고 회원 등록을 완료한다.

5.2.2 송금 과정

제안 지불 메커니즘에서의 송금 처리 과정은 그림 5와 같이 이루어진다.

① 사용자는 보안 계좌이체 시스템의 이용을 위해 보안 웹 메일 서비스에 접속한다.

② 사용자가 보안 웹 메일 서버에 접속하면 클라이언트 모듈이 다운로드 되어 설치된다. 이미 클라이언트 모듈이 사용자측에 설치되어 있다면 이 과정은 생략된다.

③ 사용자는 로그인한다. 이 때 사용자 인증은 사용자 입력한 패스워드가 그대로 웹 메일 서버로 전송되어 웹 메일 서버에 저장되어 있는 패스워드와 비교하는 Basic Authentication 방식이 아닌 OTP 방식에 의해 그림 6과 같이 이루어진다.

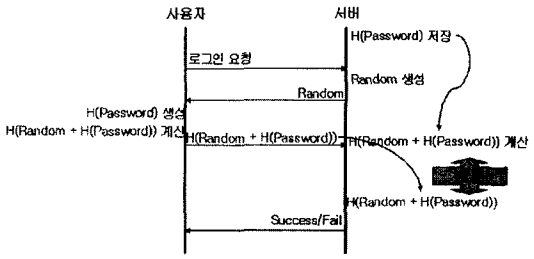

그림 6 사용자 인증 과정

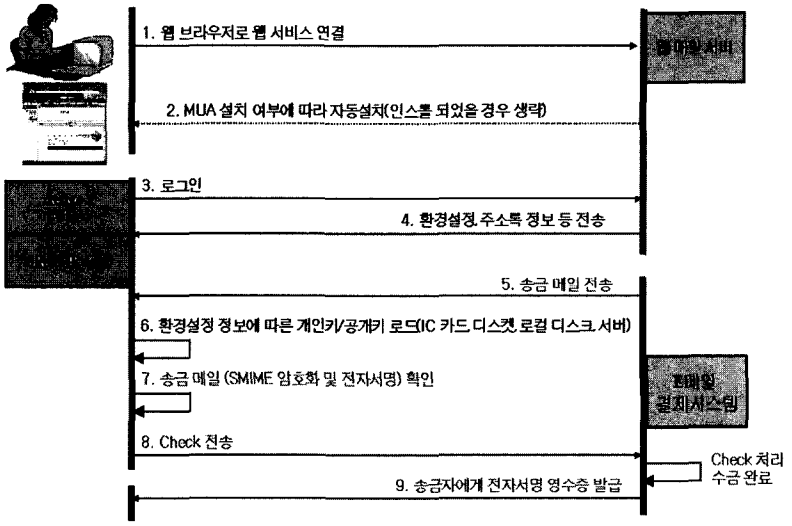

그림 7 수금 과정

• 사용자의 패스워드는 사용자의 개인키 보호를 위해 사용되는 정보이므로 웹메일 서버도 사용자의 패스워드를 알 수 없도록 보호되어야 한다. 따라서 웹메일 서버에서는 사용자 패스워드의 해쉬 결과인 *H(Password)*를 보관한다.

• 사용자가 로그인 요청을 하면 웹메일 서버는 난수 *Random*을 생성하고 이를 사용자에게 전송한다.

• 사용자는 자신의 패스워드의 해쉬 결과인 *H (Password)'*와 서버로부터 전송 받은 난수 *Random*을 합친 뒤 이에 대해 해쉬 연산을 수행하고 그 결과인 *H (Random + H (Password)'* 를 서버에게 전송한다.

• 사용자로부터 *H(Random + H (Password)')*를 전송받은 서버는 자신이 저장하고 있던 *H(Password)*를 이용하여 *H (Random + H (Password))*를 계산한 뒤 이를 사용자가 전송한 값과 비교하여 동일하면 사용자 인증에 성공한 것으로 하고 다음 단계를 진행한다.

④ 보안 웹 메일 서버로부터 송금을 위한 Check가 전송된다.

⑤ 사용자는 Check의 내용을 기입하는 것으로 송금 메일 작성을 마친다.

⑥ 사용자는 송금 메일의 환경을 설정한다. 이 때 암호 알고리즘의 종류를 결정할 수 있으며 개인키 및 인증서를 클라이언트 모듈로부터 로드한다. 개인키 및 인증서는 클라이언트 모듈 내에 저장될 수도 있고 IC카드 등의 외부 저장장치를 이용할 수도 있다.

⑦ 전자서명/암호화/배달증명 등의 선택사항을 설정한다. 송금되는 메일이 Check이기 때문에 모든 사항이 기본적으로 설정되어야만 한다.

⑧ 송금 메시지가 생성된다. 즉 Check 발행이 완료된다.

⑨ Check를 보안 웹 메일 서버로 전송한다.

⑩ Check를 수신한 보안 웹 메일 서버는 수금인에게 Check를 전송한다.

5.2.3 수금 과정

제안 지불 메커니즘에서의 수금 처리 과정은 그림 7과 같이 이루어진다.

① 사용자는 보안 계좌이체 시스템의 이용을 위해 보안 웹 메일 서비스에 접속한다.

② 사용자가 보안 웹 메일 서버에 접속하면 클라이언트 모듈이 다운로드 되어 설치된다. 이미 클라이언트 모듈이 사용자측에 설치되어 있다면 이 과정은 생략된다.

③ 사용자는 로그인한다.

④ 사용자의 환경 설정 정보, 주소록 정보 등이 전송된다.

⑤ 보안 웹 메일 서버로부터 Check가 사용자에게 전송된다.

⑥ 사용자는 Check 확인을 위해 개인키, 인증서 등 필요한 정보를 로드한다.

⑦ 사용자는 Check를 확인한다. 즉 수금인은 자신의 공개키로 암호화된 Check를 복호화한다. 복호화 한 결과는 송금인의 전자서명이 첨부된 Check이다. 수금인은 송금인의 공개키를 이용하여 Check에 첨부된 전자서명

에 대한 유효성 검사를 수행한다. 이를 통해 수금인에 대한 인증이 완료되면 계좌이체가 시작된다.

⑧ 자신에게 전송된 Check에 기입된 금액을 자신의 계좌로 옮기기 위해서 수금인은 Check를 계좌이체 서버에 전송해야 한다. 계좌이체 서버로 전송되는 Check는 송금인의 전자서명이 첨부된 Check에 대해서 다시 수금인이 자신의 개인키를 이용해 전자서명을 수행한 뒤에 전체 메시지를 암호화한 다음과 같은 형태이다. 이렇게 함으로써 Check에 대해서 기밀성, 무결성, 사용자 인증, 송신 부인 봉쇄 등의 보안 서비스가 제공되어진다. 이 메시지는 S/MIME 규격에 따라 생성된다.

EKS[EKRreceiver [EKRsender[Check] || H(Check)] || H(Check')] || EKUserver[KS]

KS: 임의로 생성한 세션키

KRreceiver: 수금인의 비밀키

KRsender: 송금인의 비밀키

KUserver: 메일 결제 서버의 공개키

Check': *EKRreceiver[EKRsender[Check] || H(Check)]*

⑨ 수금인으로부터 Check를 수신한 계좌이체 서버는 송금인과 수금인의 전자서명에 대한 유효성 검사를 수행함으로써 Check의 유효성을 확인한다. Check의 유효성에 대한 확인이 끝나면 Check에 기록된 금액만큼 수금인의 계좌로 이체하고 영수증을 발급하여 송금인에게 전송함으로써 모든 결제를 종료한다. 이 때 영수증에는 다음과 같은 정보가 기록되며 계좌이체 서버의 전자서명이 첨부된다.

- 거래 발생 시각
- 송금인 신원
- 수금인 신원
- 거래 금액

5.3 시스템 구현

이 절에서는 S/MIME을 적용한 안전한 지불 메커니즘의 구현 내용에 대해서 기술한다.

이 논문의 지불 메커니즘은 표 4와 같은 환경에서 구현되었으며, 지원 알고리즘은 다음과 같다.

표 4 구현 환경

	서버	클라이언트
운영체제	Linux	Windows95/98/ME/2000/NT
사용언어	C/C++	C/C++, Delphi, Basic
암호 라이브러리	OpenSSL 0.9.5, SFL	OpenSSL 0.9.5, SFL
지원 웹 브라우저	-	Internet Explorer 5.0/5.5/6.0

- 관용 암호 알고리즘: RC2
- 공개키 알고리즘: RSA
- 해쉬 알고리즘: MD5

5.3.1 회원 등록 과정

그림 8은 지불 메커니즘을 사용하기 위해서 회원으로 등록하는 화면이다. 이 과정에서 클라이언트 모듈은 사용자의 개인키와 공개키를 생성한다.

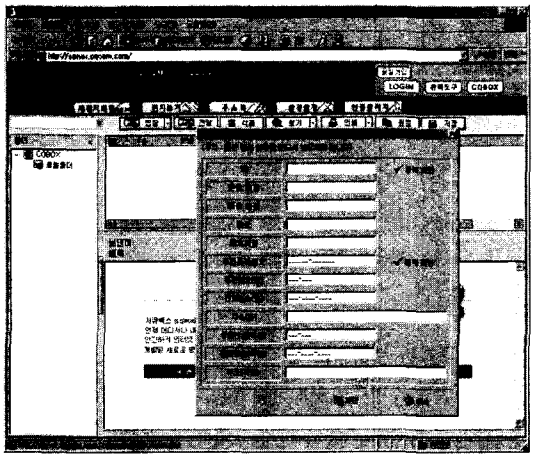

그림 8 회원 등록 화면

5.3.2 송금 과정

그림 9는 사용자가 Check를 생성하여 송금하는 화면이다. 그림 9에서 보는 바와 같이 지불 메커니즘은 보안 웹메일 시스템과 통합 운영되어 사용자는 보안 웹메일 시스템을 이용하는 것과 동일한 방법으로 지불 메커니즘을 이용할 수 있다.

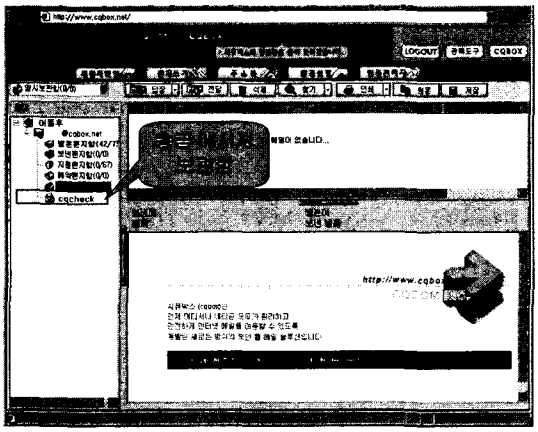

그림 9 송금 화면

5.3.3 수금 과정

그림 10은 수금인이 수신한 Check가 보관되는 모습이다. 앞에서 설명한 바와 같이 보안 웹메일 시스템 통합되어 운영되며 일반 메일 메시지와는 다른 폴더에 저장된다. 폴더에 저장된 Check에 대해서 유효성 확인이 완료되면 Check는 자동으로 메일 결제 서버로 전송된다.

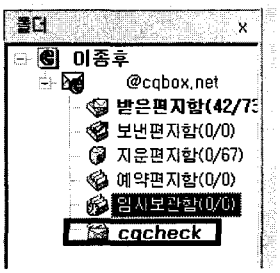

그림 10 수금 화면

5.4 성능 평가

앞에서 기존 메일 결제 시스템의 문제점으로 다음과 같은 사항들을 지적하였다.

① 메일이 단순히 통지용으로 사용되고 있음

② SSL에 의한 보안 서비스 제공

③ 메일 결제 서버에서 사용자들의 계좌번호를 관리

④ 영수증 발급 불가

이와 같은 문제점 가운데 ①, ②, ④에 대해서는 다음과 같이 해결하였다.

① 메일이 단순히 통지용으로 사용되고 있음: 이 논문에서 제안한 지불 메커니즘에서 현금 가치를 저장하여 수표처럼 사용되는 Check는 메일을 이용해 전송되어진다. 즉 메일이 실질적인 가치 전송에 사용되고 있다.

② SSL에 의한 보안 서비스 제공: 이 논문에서 제안한 지불 메커니즘에서는 메일 메시지의 보호를 위해 S/MIME을 사용하고 있으며 사용자가 웹메일 서버에 로그인 하는 과정에서는 one-time password 방식을 응용한 사용자 인증을 수행한다. 따라서 데이타에 대한 전자서명이 제공됨으로 거래 내용의 부인이 불가능하며 사용자 패스워드가 유출될 위험도 없다. 또한 웹메일 서버에서도 Check의 내용을 알 수 없도록 End-to-end 보안이 제공되어 거래의 안전성이 최대한 보장된다고 할 수 있다.

④ 영수증 발급 불가: 기존의 메일 결제 시스템에서는 영수증 발급 기능이 제공되지 않는다. 그러나 이 논문에서 제안한 지불 메커니즘에서는 S/MIME을 이용한 전자서명에 의한 영수증 발급 기능을 구현하였다.

그러나 이 논문에서 제안한 지불 메커니즘에서도 '③ 메일 결제 서버에서 사용자들의 계좌번호 관리'를 함으로써 사용자의 프라이버시가 침해될 소지가 발생하는 문제는 해결하지 못하였다. 이는 수금인의 메일 주소만으로 결제가 가능하다는 편리성을 제공하기 위해서는 수금인의 계좌 정보가 메일 결제 서버에 등록되어 있어야 하기 때문이다. 지금까지 살펴본 사항을 요약하면 표 5와 같다.

표 5 계좌이체 시스템의 비교

구분 / 기능		보안 웹 메일 시스템 기반 계좌이체 시스템	SSL 기반 계좌이체 시스템
편리성 및 이동성		우수	우수
영수증 발급		가능	불가능
보안 서비스	기밀성	제공 (S/MIME)	제공 (S/MIME)
	메시지무결성	제공 (S/MIME)	제공 (S/MIME)
	송신 부인 봉쇄	제공 (S/MIME)	제공 못함 (S/MIME)
	사용자 인증	강력 (인증서 또는 OTP 방식)	취약 (ID/Password 방식)
	키 관리	X.509	X.509

또한 기존의 메일 이체 시스템은 오직 계좌 이체의 용도만으로 사용이 가능하지만 이 논문에서 제안한 지불 메커니즘에서의 Check는 실생활에서의 수표와 유사한 기능을 제공함으로 인터넷 쇼핑몰에서의 상품 구입 등 다양한 용도로도 쉽게 확장이 가능하다.

6. 결 론

인터넷의 보편화와 함께 이제 전자상거래는 우리 생활 깊숙이 자리잡고 있다. 직접 상점까지 가지 않고 사무실이나 가정에서 손쉽게 필요한 상품을 구입할 수 있다는 장점이 있는 전자상거래는 앞으로도 더욱 활성화 될 것으로 기대된다.

이와 같은 전자상거래의 원활한 운용에 있어서 가장 중요한 요소는 안전성과 사용자 편의성이라고 할 수 있다. 즉 네트워크를 통해서 중요한 경제 정보가 전송되어지고 경우에 따라서 화폐 가치가 직접 전송되는 전자상거래에 있어서 보안기술에 의한 안전성의 확보는 전자상거래 환경 구축에 앞서 반드시 해결되어야 하는 문제이다. 또한 사용자에게 최대한 편리한 인터페이스를 제공함으로써 전자상거래 활성화에 기여할 수 있다.

이러한 면에서 볼 때 최근 등장한 메일 기반의 계좌이체 시스템은 사용자에게 매우 편리한 인터페이스를 제공한다고 할 수 있다. 즉 송금인이 수금인의 계좌번호

를 알 필요 없이 메일 주소만 알면 계좌 이체가 가능하도록 함으로써 많은 편의를 제공한다고 할 수 있다. 그러나 현재 제공되어지고 있는 메일 기반 계좌 이체 시스템은 SSL 기반으로 동작하고 있다. 이에 따라 거래 사실에 대한 부인이 가능하고 영수증 발급이 불가능하다는 문제점이 있다. 또한 메일이 실질적인 화폐 가치의 전송에 이용 된다기 보다는 단순히 송금 및 수금 사실의 통보용으로 사용되고 있다.

이에 따라 이 논문에서는 국제 표준 메일 보안 메커니즘인 S/MIME을 적용한 안전한 전자 지불 메커니즘을 설계하였다. 이 메커니즘에서는 Check라는 메시지를 통해 모든 계좌 이체 정보가 송금인과 수금인 및 메일 결제 서버 사이에서 전송되어진다. 이 메커니즘은 기존의 시스템과 마찬가지로 수금인의 메일 주소만 알면 계좌 이체가 가능한 편리성을 제공함과 동시에 Check 메시지는 S/MIME을 통해서 암호화 및 전자서명 되어지기 때문에 기밀성, 사용자 인증, 부인 봉쇄 등 필요한 보안 서비스가 모두 제공되어지고 영수증 발급도 가능하다.

메일이 단순히 메시징의 용도로 사용되는 것에서 점차 다른 여러 가지 인터넷 응용 서비스의 기반 기술로 작용하고 있는 가운데 이 논문에서 제안한 지불 메커니즘 또한 단순히 계좌 이체 서비스로만 사용되지 않고 전자지불 등 보다 복잡한 전자상거래 서비스로의 확장하는 방안에 대한 연구가 계속되어야 할 것이다. 또한 지불 메커니즘에서 사용자의 메일 주소만으로 서비스를 제공하기 위해서 메일 결제 서버 또는 메일 서버에서 사용자들의 계좌 정보를 저장하게 된다. 이는 사용자의 사생활이 침해될 수 있다는 문제점이 있기 때문에 향후 이 부분을 해결하기 위한 연구도 계속되어야 할 것이다.

참 고 문 헌

[1] Zhiqun Chen, Java Card Technology for Smart Cards, pp. 3-7, ADDISON-WESLEY, 2000.

[2] Uwe Hansmann, Martin S. Nicklous, Thomas S. Nicklous, Frank Seliger, Smart Card Application Development Using Java, pp. 13-22, Springer, 1999.

[3] http://www.digicash.com

[4] J. Galvin, S. Murphy, S. Crocker, N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted(RFC1847)", IETF, 1995. 10.

[5] Alan O. Freier, Philip Karlton, Paul C. Kocher, *"The SSL Protocol version 3.0"*, Netscape, 1996. 3.

[6] T. Dierks, C. Allen, *"The TLS Protocol version 1.0 (RFC2246)"*, IETF, 1999. 1.

[7] R. Housley, "Cryptographic Message Syntax (RFC2630)", IETF, 1999. 6.

[8] B. Ramsdell, "S/MIME Version 3 Message Specification(RFC2633)", IETF, 1999. 6.

[9] B. Ramsdell, "S/MIME Version 3 Certificate Handling(RFC2632)", IETF, 1999. 6.

[10] P. Hoffman, "Enhanced Security Services for S/MIME(RFC2634)", IETF, 1999. 6.

[11] J. Callas, L. Donnerhacks, H. Finney, R. Yhayer, "OpenPGP Message Format(RFC2440)", IETF, 1998. 11.

[12] M. Elkins, D. Del Torto, R. Levien, T. Roessler, "MIME Security with OpenPGP(RFC3156)", 2001. 8.

[13] http://www.oneclickpay.co.kr

[14] http://www.mailbanking.co.kr

[15] http://www.payletter.co.kr

[16] http://www.npaykorea.com

[17] http://www.moneymail.co.kr

전 철 우

1993년 공주영상정보대학 전산분야 강사. 1994년 한국전자통신연구원(현재 국가보안기술연구소) 근무. 2002년 충북대학교 전자계산학과 졸업(이학박사). 관심분야는 정보보호, 컴퓨터 및 네트워크 보안

이 종 후

1997년 충남대학교 컴퓨터과학과 졸업. 1999년 충남대학교 컴퓨터과학과 석사. 1999년 ~ 현재 충남대학교 컴퓨터과학과 박사과정. 2002년 ~ 현재 (주) 시큐컴 대표이사. 관심분야는 네트워크 보안

이 상 호

1976년 숭실대학교 전자계산학과 졸업(공학사). 1981년 숭실대학교 대학원 전자계산학과 졸업(공학석사). 1989년 숭실대학교 대학원 전자계산학과 졸업(공학박사). 1976년 ~ 1979년 한국전력 전자계산소. 1981년 ~ 현재 충북대학교 전기전자 및 컴퓨터공학부 교수. 2001년 ~ 현재 충북대학교 전산정보원장. 관심분야는 Protocol Engineering, Network Security, Network Management, Network Architecture