인증 기능이 강화된 온라인 전자 화폐 모형과 시뮬레이션

이 성 렬°, 주 재 훈
부산대학교 전자계산학과, 동국대학교 정보산업학과

An On-line Electronic Coin Model Enhanced the Authentication and its Simulation

Sung-Yeol Lee°, Jae-Hun Joo
Computer Science of Pusan National University, Department of Information Systems Dongguk University

요 약

본 연구에서는 인터넷 기반의 전자 상거래에서 극소액 지불을 지원하고, 원격지에서의 계정 개설과 관리 등을 용이하게 할 수 있도록 지불인과 수취인을 쉽게 인증할 수 있는 인증 기능이 강화된 전자 현금 모형의 지불 프로토콜을 개발하고, 프로토타입을 통해 그 효과성을 실험하였다. 또한 본 연구에서 개발하고자 하는 온라인 전자 현금인 OnCash 에서는 기존의 전자 현금인 Ecash 나 NetCash 와 마찬가지로 공개키 암호방식과 비밀키 암호방식을 이용하여 메시지 기밀성을 유지하고 전자 화폐의 이중사용을 방지하고, 적정한 수준의 익명성을 유지할 수 있도록 하였다.

I. 서 론

전자 상거래는 판매자와 제품 등에 대한 정보 검색 및 주문, 지불, 제화와 서비스의 인도 과정을 통해 이루어진다. 전자 상거래에서 지불 과정을 지원하기 위한 다양한 전자 지불 시스템이 개발되어 운영되고 있다. 국내에서는 DACOM 의 매직링크, 매타랜드의 SET(Secure Electronic Transaction) 기반 지불 시스템, 이니텍의 신용 카드 기반의 전자 지갑이 개발되어 있다. 그러나 국내에서 개발된 대부분의 전자 지불 시스템은 SET 기반의 신용카드 모형의 전자 지불 시스템으로서 Pay-Per View 와 같은 극소액 거래를 지원하는데 한계점이 있다.

본 연구에서는 인터넷 기반의 전자 상거래에서 극소액 지불을 지원하고, 원격지에서의 계정 개설과 관리 등을 용이하게 할 수 있도록 지불인(payer)과 수취인(payee)을 쉽게 인증할 수 있는 인증(authentication) 기능이 강화된 전자 현금 모형의 지불 프로토콜을 개발하고, 프로토타입을 통해 그 효과성을 실험하고자 한다. 또한 본 연구에서 개발하고자 하는 온라인 전자 현금인 OnCash 에서는 기존의 전자 현금인 Ecash 나 NetCash 와 마찬가지로 공개키 암호 방식과 비밀키 암호 방식을 이용하여 메시지 기밀성을 유지하고 전자 화폐의 이중 사용을 방지하고, 적정한 수준의 익명성(anonymity)을 유지할 수 있도록 한다.

II. 기존의 전자 화폐와 OnCash 의 설계목표

1. 기존의 전자 화폐

오늘날 인터넷과 같은 개방 통신망에서의 전자 상거래를 지원하는 다양한 유형의 전자 지불 시스템 또는 전자 화폐 시스템이 개발되어 있고, 그 종류도 다양하다. 그 대표적인 예로는 CyberCash 와 SET 표준에 기반을 둔 신용 카드 모형, FSTC(Financial Service Technology consortium) 와 NetCheque 및 NetBill 과 같은 전자수표 모형, Smart Card 를 이용한 Mondex 와 Ecash 및 NetCash 와 같은 전자 현금 모형이 있다.

본 연구에서 개발하고자 하는 전자 지불 시스템 OnCash 는 Ecash 나 NetCash 와 유사한 온라인 전자 현금 모형의 진지 화폐이다. Ecash 의 장점은 지불인의 익명성을 보장하면서 RSA 공개키 암호 방식을 이용하여 강력한 보안 서비스를 제공한다는 점이다. Ecash 의 지불인(payer)은 무색 전자 서명(blind digital signature)을 통해 추적 불가능한 수준에서 익명성을 유지할 수 있다. 그러나 Ecash 는 일정기간 동안 한 번 사용된 동전의 일련 번호를 데이터베이스에 저장해야 하기 때문에 확장성(scalability)의 문제를 야기시킬 수 있다. NetCash 는 Ecash 와 같은 수준의 익명성을 유지할 수는 없지만 다수의 분산된 통화 서버(currency server)를 이용한 확장성이 높은 온라인 전자 화폐이다. 그러나 NetCash 는 다수의 공개 세션키(public session key)를 사용함으로써 시스템의 성능이 저하될 수 있다.

2. OnCash 의 설계 목표

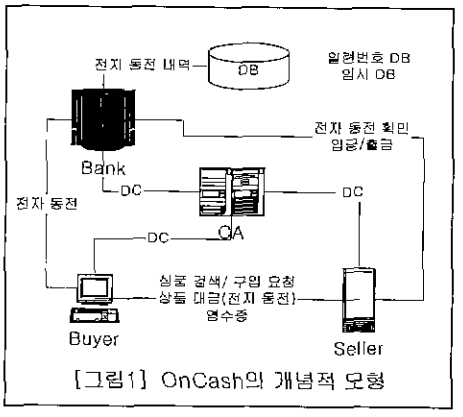
본 연구에서 개발하고자 하는 전자 지불 시스템인 OnCash 는 Ecash 와 NetCash 의 장점인 익명성을 적정 수준에서 유지하면서 시스템의 성능을 저하시키지 않고 확장성을 높일 수 있고, 인증 서버(Certificate Server)를 연동함으로써 은행과 같은 전자 화폐 발행 기관에서 원격지에서도 고객 계좌 관리를 편리하게 할 수 있는 인증 기능이 강화된 전자 현금 시스템이다. 따라서 OnCash 의 설계 목표는 다음과 같다.

- 원격지에서의 계정 관리를 지원할 수 있는 편리성과 인증 서버를 통한 인증의 강화
- 메시지 도청 방지(eavesdropping prevention) 및 무결성(integrity)을 확보를 위한 강력한 보안 서비스
- 적정수준의 익명성 보장
- 이중 지불(double spending)과 같은 전자 동전의 부정 사용 방지
- 전자 상거래에서의 거래 사실에 대한 부인방지(non-repudiation)
- 사용자 수의 증가에 따른 시스템 확장성(scalability)의 제고

III. 모형 및 거래 프로토콜

1. OnCash 모형

OnCash 시스템은 인증 기관(또는 인증서버), 은행, 판매지, 구매자로 구성되며, 그 개념적 모형은 [그림 1]과 같다



[그림1] OnCash의 개념적 모형

(1) 인증 기관(Certification Authority CA, or Certification Server) : 은행에 계정 개설을 청구하는 주체의 신원을 확인하여 전자 인증서(digital certificate)를 발행하고 관리하며, 공개키(public key)를 관리한다.

(2) 은행 또는 발행기관 : 전자 동전을 발행하고, 그 이중 지불을 방지하기 위해 데이터베이스에 발행한 동전의 일련 번호를 저장하고 관리한다 은행에서는 일련 번호 DB 와 거래(Transaction) DB 라는 두 개의 데이터베이스를 유지 관리한다

(3) 판매자. 쇼핑몰(shopping mall) 또는 수취인(payee) : 소비자에게 상품 정보를 제공하며, 제품 판매 대금을 수령하는 전자 동전의 수취인 또는 판매자는 수령한 전자 동전의 유효성을 확인하고, 자신의 은행 계좌에 입금할 수도 있고, 새로운 전자 동전의 발행을 요청할 수도 있다.

(4) 구매지 또는 지불인 : 전자 동전을 발행하는 은행에 계좌를 개설하고, 판매자로부터 상품을 구입하고 전지 동전을 지불하는 지불인 또는 구매자는 은행에서 전자 동전을 인출하여 개인 간 가치 교환으로 이를 이용할 수도 있다

2. 전자 인증서(DC: digital certificate)

Version
Subject Name
Public Key
Issuer Name
Serial Number
Validity
Period
KeyUsage
AltNames

[그림 2] 전자 인증서의 양식

위의 그림에서 Subject Name 은 각 개체(entity)의 식별 가능한 이름(Distinguished Name DN)으로 성명(Common Name CN), 기관(Organization Unit,OU), 조직(Organization O) 국적(Country:C)으로 구성되며, Issuer Name 은 인증서를 발급하는 기관이다 그리고 Serial Number 는 다른 인증서와 구별되는 일련 번호이다. 그 외에 X 509 v3 에서 확장된 키의 용도(KeyUsage)와 AltNames 은 DNS name, Email address, IP address 로 구성되어 있다

계정개설과 관리, 입출금 등에 전자 인증서가 이용되며, 익명의 거래를 요구하지 않을 때 구매지와 판매지 간 신원 확인에도 이용된다

3. 전자 동전의 발행 과정

3.1 기호 정의

SK_{sender} 송신자가 산출한 세션키(session-key)

$K^{private}_{sender}$ 송신자의 비밀키

$K^{public}_{receiver}$ 수신자의 공개키

$Trans\_ID$ 판매지별로 고유한 거래번호

3.2 전자동전의 발행과정

(1) 구매자는 전자 인증서(DC), 계좌 번호(Acc_No), 출금액(Amount) 비밀번호(passwd)를 전자 서명(digital signature)하여 은행의 공개키로 암호화한 메시지를 은행에 전송하여 자신의 계좌에서 전자 동전을 인출한다

Buyer→Bank $\{\{DC, Acc\_No, Amount, Passwd\} K^{private}_{Buyer}\} K^{public}_{Bank}$

(2) 은행은 구매자가 보낸 메시지를 비밀키로 해독한 후 전자 서명을 확인한 다음 구매자의 계좌에서 일정 금액을 공제하고 전지 동전을 발행한다

Bank→Buyer

$\{\{Bank\_Name, Bank\_Addr, Exp\_Date, Seri\_No, Coin\_Val\} K^{private}_{Bank}\} K^{public}_{Buyer}$

4. 거래 프로토콜

(1) 구매지는 쇼핑몰에서 상품을 검색한 후 임의의 세션키(session key)를 산출하고, 구매 요청을 판매자에게 판매자의 공개키로 암호화하여 전송한다

Buyer → Seller $\{Buy\ Request, SK_{buyer}\} K^{public}_{Seller}$

(2) 판매자는 구매자의 구매 요청에 대한 응답(예. 재고가 없는 경우에는 판매 거절 또는 상품 가격)을 구매자에게 전송한다 판매지의 응답 메시지, 금액, 거래 번호(Trans_ID), 거래 날짜를 판매지의 비밀키로 전자 서명을 하고 이를 구매자의 세션 키로 암호화하여 구매자에게 전송한다

Seller → Buyer

$\{\{Sell\ Response\ or\ Good\ Price, Trans\_ID, Date\} K^{private}_{Seller}\} SK_{buyer}$

(3) 구매자는 지불(거절) 메시지 또는 지불할 금액을 전자 지갑에서 인출하여 판매자의 공개키로 암호화하여 판매지에게 전송한다

Buyer → Seller $\{Payment(Refusal)\ Response\ or\ Coins\} K^{public}_{Seller}$

(4) 전지 동전을 수령한 판매자는 은행에서 동전의 유효성을 확인하고, 은행 계좌에 입금 또는 새로운 동전을 발급받는다 이 때 판매자는 전자 동전과 거래 번호에 자신의 비밀키로 전지 서명을 첨부하고, 이 메시지를 은행의 공개키로 암호화하여 전송한다

Seller → Bank $\{\{Trans\_Id, Coins\} K^{private}_{Seller}\} K^{public}_{Bank}$

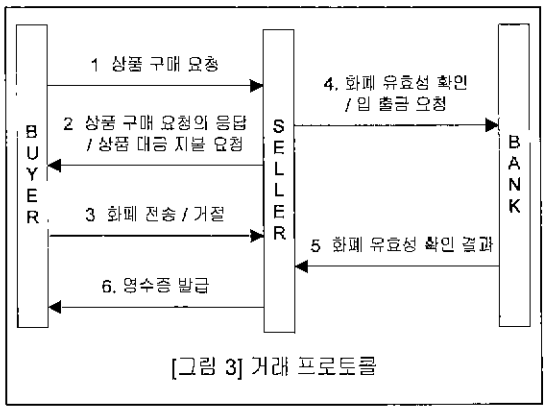
(5) 은행에서는 발행한 전자 동전의 일련 번호를 DB에 저장하고 있다. 수취인이 전자동전의 타당성을 확인하고 새로운 동전으로 교환할 수도 있고, 자신의 계좌에 입금할 수도 있다. 일단 한 번 사용된 동전의 일련 번호는 일련 번호 DB에서 삭제된다. 이때 거래 코드(Trans_ID)와 거래 금액(amount)은 은행의 거래 DB에 저장된다.

Bank → Seller $\{\{New\_Coins\}K_{Bank}^{private}\}K_{Seller}^{public}$

(6) 판매자는 은행으로부터 전자 동전의 유효성이 확인되면, 상품 지불 금액, 거래 번호, 거래 날짜를 영수증에 자신의 비밀키로 전자 서명을 첨부하고, 임의의 세션키로 암호화하여 구매자에게 전송한다

Seller → Buyer $\{\{Good\_Price, Trans\_Id, Date\}K_{Seller}^{private}\}SK_{buyer}$

지금까지 전자 인증서는 계정 개설과 전자 동전의 발행에만 사용되었다. 그러나 익명의 거래를 원하지 않는 경우 구매자는 판매자에게 전자 인증서를 제시하고 거래할 수 있다. 이 경우에는 거래 프로토콜이 익명성을 요구할 때보다 간단하다



[그림 3] 거래 프로토콜

IV. 구현 및 실험 결과

1. 구현

OnCash 모형은 구매자의 전자 지갑 프로그램을 제외하고는 SUN 워크스테이션의 C/UNIX 환경에서 구현하였다. 데이터 전송 시 암호화는 RSA 공개키 암호화 알고리즘을 이용하였고 판매자와 구매자 간의 세션키는 DES 를 이용하였다

인증 서버는 고객의 요청에 따른 공개키 등록과 등록된 공개키의 확인 및 변경 부분으로 구성되어 있다 그리고 거래의 안전을 위해 공개키의 크기는 512 바이트로 이루어져 있고, 각각의 공개키는 유일성을 보장하기 위해 저장 시 항상 다른 공개키와 비교하여 중복되지 않도록 했다

은행 서버는 전자 동전의 발행과 고객의 계좌에서 진짜동전의 입금 및 출금, 판매자의 거래 부인을 막기위한 거래 코드 및 동전의 일련 번호 저장 부분으로 구성되어 있다

구매자의 전자 지갑 프로그램은 Windows NT4.0 에서 Visual C++ 5.0 을 사용하여 구현하였으며, 프로그램 구성은 공개키의 생성 및 저장 부분과 전자 지갑의 입출금 그리고 상점과의 거래 시 영수증 관리 부분으로 구성되어 있다.

2. 실험 결과

전자 지불 시스템(OnCash) 모형을 시뮬레이션한 결과 원격지에서 은행의 계정 관리를 지원하는 편리함과 인증 기능을 통한 상호 거래의 안전성을 높일 수 있으며, 공개키 비밀키 암호화와 디지털 서명을 통해 메시지의 도청 방지와 메시지의 무결성을 확보할 수 있었다

은행에 저장된 일련 번호를 통해 이중 지불과 전자 동전의 불법 사용을 막을 수 있고, 상품 거래 시 발생하는 거래 구매자와 판매자의 거래 부인은 상점과 고객 사이의 거래 코드를 은행 데이터베이스에 보관함으로써 해결했다

전자 동전의 발행 기관인 은행 시스템에서 발생하는 데이터베이스의 확장성 문제는 거래가 끝난 후 데이터베이스에서 거래 내역을 삭제함으로써 해결하였으며, 이로 인해 계속적으로 증가하는 사용자를 수용할 수 있었다.

인증기관에서 발행하는 전자 인증서를 통해 거래 상호간의 신뢰성과 인증 기능을 강화할 수 있었다 그리고 전자 동전의 인출 과정에서만 전자 인증서를 사용하여 거래 상호간의 적절한 익명성을 보장하였다.

실험 과정에서 인증 기관에 등록할 공개키 생성 시 약간의 시간 지연이 있었다 그리고 거래 상대편이 인증 기관에서 공개키를 확인하는 과정에서 공개키의 크기와 사용자가 증가로 인한 데이터베이스 검색 시 시간 지연이 있었다

개인간의 가치 교환 시 익명성은 은행에서 새로운 전자 동전을 발급함으로써 적절한 수준의 익명성을 보장할 수 있었다. 그리고 별도의 하드웨어 없이 소프트웨어만으로 극소액 거래가 가능하다는 결과를 얻었다

V. 결론

OnCash 에서는 Ecash 와는 달리 발행한 동전의 일련 번호를 DB에 저장함으로써 시스템의 사용에 따른 DB 저장량을 감소시킬 수 있다. 그리고 한 번 사용된 동전의 일련번호가 DB에서 삭제되었을 때, 판매자가 구매자에게 영수증을 전송하지 않는 것을 방지하기 위해 일정 기간 동안 판매자의 거래 코드(Trans_ID)와 거래 금액을 은행의 거래 DB에 저장하여 둔다 그러면 판매자로부터 지불 영수증을 수령하지 못한 구매자는 거래 코드를 은행에 제시하여 판매자의 계좌에서 거래 금액을 공제하여 지불에 대한 보증을 받을 수 있다.

구매자와 판매자간의 거래 시에 전자 인증서(DC)를 제시하지 않으면 상호간의 신원을 알 수 없으므로 익명성이 유지된다 그리고 은행에서는 구매자가 거래 코드를 제시하지 않으면, 구매자의 거래 내역을 알 수 없다. 은행은 판매자의 거래 코드와 거래 금액만으로 거래의 상세한 내역을 알 수 없으므로 구매자는 거래에 대한 익명성이 보장된다.

수취인이 사용한 전자 동전을 은행에서 새로운 전자 동전으로 교환하여 동전의 유통 과정을 추적하기는 어려우며, 단지 은행에서는 전자 동전을 교환하는 수취인의 네트워크 주소만을 추적할 수 있다

참고 문헌

[1] 주재훈, '인터넷 결제시스템의 비교연구", 경영학연구, 제 27 권 제 1 호, p25 -65, (1998)

[2] D Chaum, "Security without Identification Transaction Systems to Make Big Brother Obsolete", Communications of ACM, Vol 28, No 10 p1030-1044, (1985)

[3] Gennady Medvinsky and B Clifford Neuman "NetCash A design for practical electronic currency on the Internet" In Proceedings of 1st the ACM Conference on Computer and Communication Security November, (1993)

[4] Michael Peirce Donal O'Mahony. 'Scaleable, Secure Cash Payment for WWW Resource with the PayMe Protocol Set', 4th International World Wide Web Conference, (1995)