추적 가능한 Off-line 전자지불 프로토콜의 제안

강혁, 김태윤
고려대학교 컴퓨터학과
e-mail:paranblue@netlab.korea.ac.kr

A Proposal of traceable off-line Electronic Payment Protocol

Hyeok kang, Tai-Yun Kim
Dept of Computer Science & Engineering , Korea University

요약

최근 정보통신기술의 발달과 인터넷 이용의 폭발적인 성장에 따라 인터넷을 통한 전자 상거래가 새로운 경제 활동으로 등장과 동시에 off-line을 기반으로 하는 전자 상거래 시장이 급속한 성장을 하고 있다. 이에 따라 기존의 on-line 상의 전자 지불 방식을 보다 실용적인 off-line 상의 전자 지불 방식이 요구되고 있다. 전자 지불 방식의 하나인 전자 화폐는 효과적인 응용을 위해 실물 화폐와 유사한 여러 가지 성질을 갖고 있기는 하지만, 이러한 성질 중에서 사용자의 프라이버시를 보장하는 경우 발생하는 부정적인 문제 즉 돈 세탁, 약탈, 그리고 자금의 해외 유출의 용의 등을 문제점을 해결하기 위해 익명성 제어, 익명성 취소 등의 다양한 프로토콜의 개발이 연구되고 있다.

이에 따라 본 논문에서는 off-line 상에서 전자상거래를 할 때 부정 사용자에 대한 사용자 추적, 즉 익명성 제어가 가능한 프로토콜을 제안한다. 제안한 프로토콜의 특징은 기존의 on-line 상의 시스템 구현의 효율성을 고려하여 RSA와 Hash 함수만을 사용하여 사용자 은닉이 가능하도록 하였으며, 또한 익명성 제어가 가능하지만 어느 기관 단독이 아는 은행과 인증기관이 협조 할 경우에만 추적이 가능하다.

1. 서 론

최근 off-line 상에서 이루어지는 거래는 주문과 지불에 이루는 모든 상거래 과정이 인터넷이라는 가상의 공간에서 이루어지며, 특히 디지털 상품(S/W, 게임, 전자서적, 콘텐츠 등)의 경우 제품 자체도 인터넷을 통해 인도되기 때문에 off-line 상에서의 새로운 전자 거래의 기능을 하게 된다. 그리고 일상생활에서 적용되고 있는 금융, 재화의 구매, 언론, 광고, 교육, 관광 등 사회 전 분야에서 실행되고 있는 전자상거래는 가상공간에서 실시간에 사용할 수 있도록 하고 있다. 이에 따라 인터넷 중심의 전자상거래는 기업과 기업, 개인과 기업, 개인과 개인의 형태로 IT 사업자들의 진출을 급속도로 증가시키고 있다. 이는 무선 인터넷상에서 통신을 이용하여 화상으로 제품 정보를 제공함과 아울러 고객들에게 상품 선택의 자유를 주어 원하는 물건을 쉽고 빠르게 화면상에서 열람 , 주문 그리고 배달까지 일관 전자 거래 방식의 특성을 가지고 운영되고 있기 때문이다. 본 연구에서는 기존의 오프-라인 전자 지불 시스템에 대한 고찰을 기반으로 인증 단계 및 전자 화폐 생성 및 지불 단계를 개선하여, 전자 화폐의 불법적인 사용, 즉 돈 세탁, 자금의 해외 불법 유출 등의 문제점을 해결하기 위해서는 추적 가능성이 전자 화폐의 기능에 포함시켜 사용자 개인의 익명성을 보호하기 위해 조건부 추적 가능성이 요구되는 시스템을 제안한다.[1]

2. 오프-라인 전자 지불 기법

기존의 Brands의 오프-라인 전자 지불 시스템은 스마트 카드와 같은 추가적인 장치를 사용하여 전자 지불을 수행할 수 있는 체계를 제시하였다.

기존의 시스템인 경우 각 엔티티에 대한 인증 단계가 비효율적이고, 전자 화폐 자체에 대한

은닉 서명 단계 없이 인증서에 의한 지불이 수행되므로 개선할 필요가 있다. 지불 단계를 수행하기 이전에 공개키에 대한 인증서 발급 단계를 수행한다. 인증서를 기반으로 카운터 기반 전자 화폐에 대한 이중 지불 방지 기능을 제공하지만, 은닉성 및 공정성 제공 측면에서는 취약점이 있다.[2,3]

2.1 Brands의 오프-라인 전자 지불 시스템

Brands 시스템은 스마트 카드와 같은 추가적인 보안 장치를 사용하여 전자 지불 기법에 접목하였다. 이중 지불이 수행되지 않는다면 개인의 프라이버시에 대한 보호 기능을 제공하는 오프-라인 전자 지불 시스템이다. Brands의 일반적인 지불 시스템인 경우 은행으로부터 전자 화폐를 인출하고자 할 경우 제한적 은닉 서명 기법을 적용하여 은행이 수행한 은닉 서명에 대해서 이중 지불에 대해 검출할 수 있는 기능을 제공한다. Schnorr의 인증 기법을 사용하고 사용자와 판매자는 은닉 서명된 전자 화폐에 대해 오프-라인 방식으로 지불 단계를 수행한다. 그러나 Brands의 일반적인 전자 지불 방식은 동일한 크기의 전자 화폐만 사용할 수 있기 때문에 소액 지불 방식에 적용하고자 할 경우에는 전체 트랜젝션 비용 측면에서 비효율적이다. 인터넷에 기반한 분산 이동 컴퓨팅 환경에서 발생하는 빈번한 소단위 전자 지불을 만족하기 위해서는 지급 금액에 대한 자유로운 설정이 가능한 방식이 필요하다. 따라서 Brands는 스마트 카드에 전자 화폐 금액을 관리하는 변수를 두고 카운터 방식에 의해 필요로 하는 만큼의 전자 화폐를 지불하는 방식이다. 스마트 카드를 사용한 카운터 방식의 오프-라인 전자 지불 방식은 지불하고자 하는 금액에 대한 인출 과정을 수행한 후에 스마트 카드에 금액을 예치한다. 사용자는 서비스 제공자에게 전자 화폐를 지불하고자 할 경우 사전에 은행으로부터 전자 지불에 사용할 공개키에 대한 인증서를 발급 받는다. 인증서를 기반으로 임의의 전자 화폐 금액에 대해 지불하고 은행은 최종적으로 검증 단계를 수행한다. 본 연구에서는 Brands의 카운터 기반 오프-라인 전자 지불 방식에 대해 고찰해 보고 개선된 방식을 제시하고자 한다.[8]

3. 제안한 오프-라인 전자 지불 기법

3.1 스마트 카드 기반 전자 지불

본 연구에서 제안하는 오프-라인 전자 지불 기법은 Brands의 카운터 기반 전자 지불 방식에 전자 화폐의 일련번호라는 요소를 첨가하여 불법 사용자가 이중으로 사용하지 못하도록 개선한 기법이다

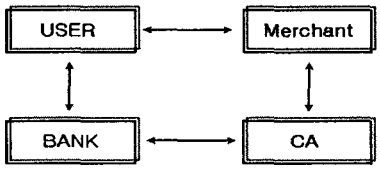

그림 1. 전자 지불 시스템의 기본 모델

3.2 제안한 전자 지불 프로토콜의 흐름

① 사용자(U)는 인증기관(CA)와의 사전등록을 수행하는데 우선 사용자 U는 임의적인 수 p, q, r, x를 와 자신의 ID_U를 CA의 공개키로 암호화하여 CA에게 보낸다.

② CA는 ID_U를 확인하고 인증 비밀키를 이용하여 p 와 q를 서명한 후 U에게 전송한다.

③ 사용자 U는 자신의 데이터와 인증 받은 데이터를 이용하여 전자 화폐 발생을 요구한다.

④ 인증기관에 등록을 거친 사용자와 판매자(M)는 전자 지불을 위해 초기 설정 단계를 시행한다. 우선 사용자는 인증기관에서 서명에 필요한 요소들로부터 자신의 서명에 필요한 요소들을 생성한다. 판매자는 인증기관에서 생성하여 보낸 값과 동일한지 비교하고 자신만의 비밀 난수를 생성, 사용자에게 전달한다.

⑤ 사용자는 판매자가 보낸 비밀 난수를 검증과정을

통하여 올바른 경우이면 받아들인다.

⑥ 이처럼 초기 설정 과정을 수행한 후 사용자와 판매자는 인증 단계를 수행하는데 보다 실제적으로 구현이 가능하도록 RSA 알고리즘과 이산 대수 문제 및 hash 함수를 기반으로 하였다.

⑦ 사용자가 은행의 구좌를 개설하기 위해 비밀키 u_1 를 생성하고, 판매자는 사용자에 해당하는 정보들을 데이터베이스에 저장하고, 사용자를 위한 비밀키 o_1 를 생성한다. 그리고 스마트 카드에 대한 식별 공개키 h_0 를 계산하고 사용자/스마트 카드에 대한 식별 공개키 I 를 생성한다.

⑧ 판매자는 h_0 와 I 를 자신의 데이터베이스에 저장하고 h_0 를 사용자에게 보낸다.

⑨ 따라서 사용자는 h_0 , I 를 h_u , u_1 과 함께 자신의 소프트웨어 내에 저장한다. 사용자는 o_1 을 모르기 때문에 서명을 위조할 수 없다. 따라서 사용자 측면에서의 이중 지불 방지 기능을 제공한다.

⑩ 은행은 먼저 인증기관을 통하여 정당한 사용자에 대해 인증을 받은 후 인증기관으로부터 전송된 사용자가 요청한 화폐 요청 요소들을 사용자에게 보낸다.

⑪ 사용자는 은행으로부터 받은 화폐 요청 요소들을 자신의 것과 비교하여 같으면 바르게 서명되었다고 알게 되고 화폐를 사용하게 된다. 사용자는 위의 모든 단계를 정당히 끝마친 후 전자화폐를 지불한다.

⑫ 은행은 판매자를 통하여 들어온 전자화폐를 검증한다.

⑬ 은행으로부터 화폐에 대한 확인을 요청 받은 인증기관은 먼저 사용자의 지불 요소를 찾아 그 사용자의 데이터베이스에 저장되어진 발행 화폐와 비교하여 정당한 화폐인지를 검사 후 결과를 은행에 전송한다.[8]

3,3 사용자 추정과정

은행은 판매자를 통하여 들어온 전자화폐의 일련번호를 검색하여, 사용한 적이 있는 경우 이미 은행 자신의 데이터 베이스에 저장되어져서 화폐의 이중 사용을 검출할 수 있다. 이때 판매자로부터 전송된 데이터 값 중 사용자의 전자화폐 지불시 인증용으로 사용된 값(p)을 인증기관에 전송하면 인증기관은 그 값을 사용하는 사용자를 검사하여 사용자의 신원을 검출 할 수 있다.

4. 결 론

최근 On-Line 상에서의 전자 상거래가 많이 이루어지고 있다. 이에 따라 Off-Line에 해당되는 무선 인터넷을 통한 전자 상거래도 점차 증가하는 추세이다. 상거래 시 익명성 제어 또는 익명성 취소에 관한 연구가 활발히 진행되고 있다. 본 논문에서는 이러한 연구의 일환으로 무선 인터넷 환경에서 보다 효율적으로 적용될 수 있는 RSA와 hash 함수만을 응용하여 익명성 제어 방법의 하나인 조건부 추적성을 전자 화폐에 부여한 프로토콜을 제안하였다. 또한 제안된 프로토콜은 RSA와 hash 함수만을 사용함으로 해서 계산 능력이 열악한 PC 환경에서도 효율적인 실제 구현을 가능케 하고 있으며 시스템 구성 요소간의 정보의 주고받음을 경감시킬 수 있도록 하였다. 제안된 프로토콜을 이용할 경우 어느 기관이든 단독으로 사용자 추적을 할 수 없고 반드시 은행과 신뢰기관이 서로 협조해야만 사용자의 신원을 확인할 수 있다. 향후 보다 정확한 추적성과 보안성을 유지하면서 전자 화폐를 분할 할 수 있는 방안에 대한 연구가 필요하다.

6. 참고 문헌

[1] D . Chaum, " Blind Signature for Untraceable Payments", Proceeding of Crypto'82 pp.199-223 (1982)

[2] T. Okamoto and K. Ohta, " Universal Electronic Cash ", Advance in Crytology-crypto'91 Lecture Notes in CS, Springer- Verlag, pp32-27, (1992)

[3] 김해만, 이임영, "분할성과 부분적인 추적이 가능한 효율적인 전자 시스템에 관한 연구" (1999) http://www.multimedia.or.kr/multimedia/nonmoon/

[4] S. Band ; "Untraceable Off-line Cash in Wallets with Observe", Proceedings of Crypto'93 LNCS 773,

Springer Verleg, pp.302-318

[5] J.Camenish, J.M Pirveteau, M. Stadler: "Efficient Payment System Protesting Privacy of ESORICS '94, Lecture Note in Computer Science 875, Springer Verlag, pp.27-215

[6] R.L.Rivest, A.shamor and L.Adleman, "A method of Obtaining Digital Signatures and Public-key Cryptosystem" ACM, V0l21 no2, pp.120-126(1997)

[7] R.L.Rrivest, "The MD5 message-digest algorithm", Request for Comments(RFC) 1320, Internet Activities Board, Internet Privacy Task Force, April (1992)

[8] 이형우, 김태윤 "분산 이동 컴퓨팅 환경에서의 오프-라인 전자 지불" 고려대학교 (1998)