M-Commerce에서 OTP를 이용하여 사용자 익명성을 보장하는 소액 결제 시스템

신동규° 정기원, 천준호, 전문석
숭실대학교 대학원 컴퓨터학과
nicesdg@empal.com, jels@cherry.ssu.ac.kr,
choun@ssu.ac.kr, mjun@computing.ssu.ac.kr

Design of Micropayment System Using anonymous OTP for M-commerce

Dong-Gyu Shin° , Ki-Won Jung, Jun-ho Choun, Moon-Seog Jun
Dept of Computer Science, Soong-sil University

요 약

인터넷을 통한 전자상거래의 급격한 발전으로 현재는 사용자가 이동하는 상황에서도 전자상거래가 이루어지고 있다. 즉 M-Commerce의 발전방향은 기존의 고가의 물품에 대해서가 아니라 문서, 음악 파일, 동영상과 같은 소액에 대한 상거래가 급격히 발전할 것이다. 이로 인해 현재 소액결제시스템이 발전하고 보급되어있는 상태이다. 하지만 기존의 소액결제 시스템의 문제점인 사용자 익명성에 관한 부분에 대하여 본 논문에서는 OTP형식의 소액결제시스템에서의 새로운 프로토콜을 제안하였다. 거래가 이루어지기전에 이미 서로의 인증이 되는 고객과 이동통신업체에 중점을 두어 고객이 직접 인터넷 콘텐츠 공급업체에 개인정보를 입력하지 않아도 인증을 할 수 있도록 설계하였다.

1. 서론

최근 인터넷 전자 상거래가 활성화되고 있어 거래비용의 감소와 거래의 신속성을 높이는 효과를 가져오고 있다. 이런 전자 상거래 중에서 기존의 고가의 물품뿐만 아니라 문서, 음악 파일, 동영상이나 그림 등의 정보 상품에 대해서도 매매가 이루어지고 있다. 위와 같은 상품들은 비교적 낮은 가격으로 거래되어지고 있기 때문에 기존의 인터넷 상에서 거래되던 높은 가격의 상품들의 지불 시스템을 그대로 사용 할 경우 필요 이상의 수수료 등의 불합리한 점이 발생하게 된다. 지불 대상이 소액인 만큼 수수료나 결제방법이 차별화 되어 좀 더 간편하고 저렴하게 이용할 수 있는 소액 결제시스템(Micropayment System) 이 도입되기 시작했다.

소액결제시스템은 사용자에게 이동성을 부여하고, 경제성, 시간적 제약성과 효율성을 높여주는데 탁월한 면을 보이고 있다. 이로 인해 M-Commerce[1], 즉 모바일 결제에 적용하여 유용하게 쓰이고 있다.

현재 우리가 사용하고 있는 소액결제시스템은 기존의 고액결제시스템에서 사용한 공개키 방식과는 다르게 좀 더 작은 시스템인 One Time Password(OTP)[2]를 사용하고 있다. OTP인증방식을 적용함으로서 통신상에서 혹 비밀번호가 유출되었다 하더라도 한번 사용된 번호는 폐기되므로 안전하게 결제와 거래를 할 수 있다는 장점을 가지고 있다.

하지만 개인정보 유출 및 훼손이라는 부작용도 동반하고 있는 실정이다.

본 논문에서는 OTP를 이용한 소액결제 시스템에서의 발생할 수 있는 문제점을 지적하고 그에 대한 해결방안 제시와 발전 가능성에 대해 말하기 위해 다음과 같은 구성으로 짜여있다. 2절에서는 관련연구로서 OTP와 결제시스템에 대해 알아보면서 기존의 OTP를 이용한 소액결제에 대해서 분석하고, 3절에서 본 논문에서 제안한 시스템을 설명한다. 그리고 4절에서 결론을 맺는다.

2. 관련연구

2.1 One Time Password(OTP) 시스템

OTP 시스템이란 말 그대로 한번 쓰고 password를 버리는 일회용 password이므로 기존의 password가 sniffing 등으로 가로채여도 새로 생성된 password를 사용하므로 안전할 수 있다. OTP는 이러한 password를 MD4, MD5 해싱 알고리즘을 이용하여 만들어 낸다.

OTP는 다음과 같이 3가지가 있다.

첫 번째는 S/Key 인증 시스템은 passive attack에 대해 사용자의 패스워드를 보호하기 위한 간단한 scheme으로 password 정보를 저장하지 않고 쉽고 빠르게 설치 할 수 있다.

두 번째는 Challenge-Response 방식으로 사용자가 login하면, server는 challenge message를 보낸다. 사용자는 Personal Identification Number(PIN)와 challenge를 이용하여, OTP를 생성하여 response를 한다. 서버는 동일한 challenge와 등록된 사용자의 정보를 이용해 OTP를 생성한 후 사용자의 response와 비교하여 사용

자 인증을 해주는 방식이다.

세 번째는 Time-Synchronous 방식 이다.이 방식은 난수생성 알고리즘은 관리가가 정한 시간(t)마다 64bit의 비밀키가 생성되어 진다. 각각의 사용자에게는 특정키가 할당되어지고, 지능형 토큰과 인증서버 데이터베이스에 이것들이 저장되어진다. 사용자가 login을 할 때 PIN과 6개의 숫자로 된 난수를 전달하면, (이 난수는 토큰으로 생성되어 짐) 난수는 토큰 안에 저장되어 있던 비밀키와 t를 초기값으로 하여 토큰안의 알고리즘을 통해 만들어 진다. 이렇게 만들어진 10개의 숫자가 서버로 가면 서버는 PIN을 인덱스로 하여 해당 비밀키를 찾고, 생성된 6개의 랜덤 숫자들을 수신 것과 일치하는 지를 확인한다.

2.2 M-Commerce에서의 결제 시스템의 종류

M-Commerce의 결제 시스템은 온라인과 오프라인 상에서 이루어지는 서비스와 재화 구매 시 무선기기를 이용하여 대금을 지불하는 결제 서비스이다.

M-Commerce의 결제 시스템의 종류는 3가지로 크게 구분하는데 스마트카드(IC칩)내장, 무선 네트워크 이용여부, 이동통신 업체의 참여정도로 구분한다.

스마트카드(IC칩)내장은 다시 두 가지로 구분되는데 하나는 카드기반(H/W방식)으로 스마트카드(칩)에 결제정보를 담아 인증 및 결제서비스를 하는 것으로 싱글슬롯, 듀얼슬롯, 듀얼칩, 원칩(통신칩, 신용카드 칩)등이 있다. 그리고 다른 하나는 비카드기반(S/W방식)으로 무선네트워크를 통하여 실시간 인증 및 대금결제(폰빌방식)와 휴대폰 메모리에 결제정보를 저장하는 Mobile Wallet 방식(클라이언트형, 서버형)그리고 바코드 방식이 이에 속한다.

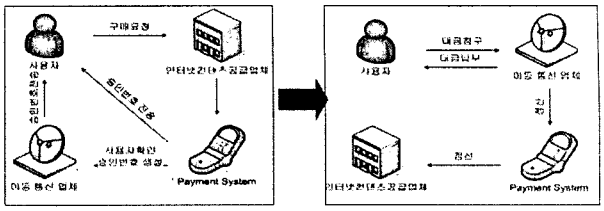
무선 네트워크 이용여부에 따른 구분은 On-line방식과 Off-line방식으로 나뉘게 되는데 On-line방식은 무선인터넷에 접속하여 모바일 뱅킹 또는 무선 Payment Gateway(PG)를 이용한 온라인 쇼핑몰 등에서의 대금 지급결제 하는 방식이고, Off-line방식은 휴대폰과 POS단말기, ATM등간에 근거리 통신 기술(RF, IrFM, 블루투스, 2D바코드 등)을 이용하여 대금 지급결제를 하는 것으로 통화요금 부담하지 않는 장점이 있다.

이동통신업체의 참여정도는 직접결제방식과 간접결제방식으로 나뉘게 된다. 직접결제방식은 이동통신업체가 직접 결제서비스를 제공하는 것으로 지급결제과정 전반을 이동통신업체가관리하고 책임을 부담하게 된다. 폰빌(휴대폰통화과금), SKT의 네모서비스등이 이에 속한다. 간접결제방식은 금융기관과 제휴하여 간접적으로 서비스를 제공하는데 선불, 직불, 신용카드, 계좌이체 등이 이에 속한다.

2.3. 기존의 M-Commerce에서의 소액 결제 시스템

앞에서 알아봤던 결제 시스템 중 OTP를 사용한 결제시스템은 이동통신업체의 참여정도부분에 해당하는 직접결제방식을 사용하고 있다.

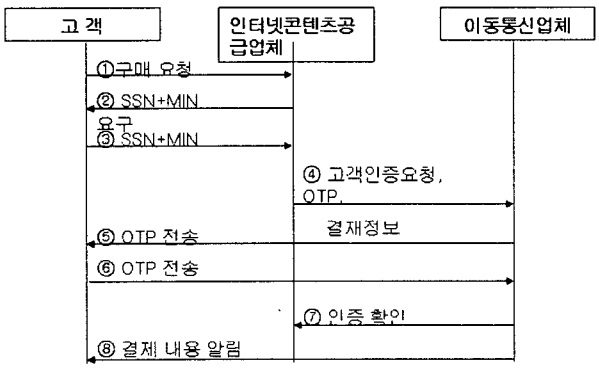
M-Commerce 소액결제시스템의 큰 구조를 보면 아래의 그림과 같다.



[그림 1] M-Commerce 소액결제시스템 구조

온라인상에서 안전하게 거래가 이루어지기 위해서는 결제를 이용자가 본인임을 확인할 수 있도록 인증기관에서 관리하고 있는 주민등록번호와 통신업체에 등록된 Mobile 결제 업체에서는 OTP를 생성하여 요청하는 사람의 Mobile에 SMS로 송신하여 일치할 경우에만 거래가 이루어질 수 있도록 승인 한다.

OTP를 이용한 Mobile번호로 사용자에게 후과금방식으로 결제하는 시스템의 프로토콜은 다음과 같다.



- SSN : Social Security Number(주민등록번호)
- MIN : Mobile Identification Number
- OTP : One Time Password

[그림 2] 기존의 OTP를 이용한 소액결제시스템 프로토콜

이동통신에서 참여하여 직접결제하는 방식은 고객이 인터넷콘텐츠공급업체(Internet Contents Provider:ICP)에게 구매요청을 하게 되면 ICP는 SSN과 MIN을 요구하게 된다. 그 후 고객은 SSN과 MIN정보를 입력하게 되고 ICP는 그 정보를 이동통신업체에게 고객인증요청과 OTP를 보내게 되고 이동통신업체는 ICP에게서 받은 OTP를 SMS를 통해서 고객에게 보내게 되고 OTP를 받은 고객은 OTP를 이동통신업체에게 보내고 OTP를 확인하여 고객의 신뢰성을 보장하게 되어 ICP에게 고객인증에 대한 메시지를 보내게 되면 ICP는 고객에게 Contents를 제공하게 된다.

본 논문에서는 위와 같은 과정 중에서의 문제점을 제기하고 그에 대한 해결책을 제안하였다.

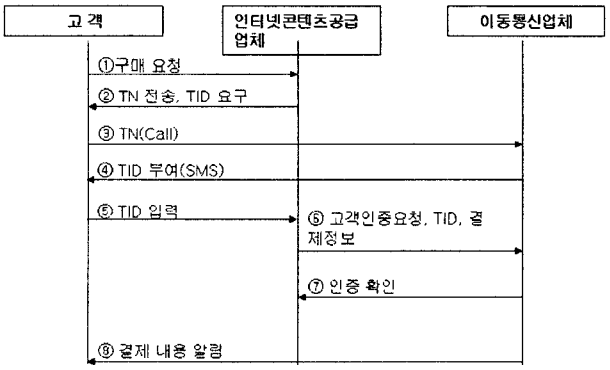
고객과 ICP와의 통신에서 ICP가 고객에게 SSN과 MIN

을 요청하게 되는데 이 부분에서 SSN이나 MIN과 같은 개인정보가 ICP측에 자연스럽게 유출이 되고 있는 것이다. 만약에 ICP업체가 이런 개인정보를 악용을 하게 된다면 그에 대한 대책은 상당히 어려운 과제이다. 고객이 자신의 개인정보를 직접 입력하고 그 ICP업체를 믿는다는 전제하에 이런 개인정보의 유출은 자연스럽게 이루어지고 있는 실정이다.

3. 제안하는 OTP를 이용한 사용자 익명성을 보장하는 소액결제 시스템

본 논문에서 Ticket Number와 Ticket ID라는 새로운 개념으로 기존의 OTP를 이용한 소액결제시스템의 문제점인 ICP에게 개인정보가 유출되는 부분을 고객의 익명성을 고려하여서 사전에 개인정보를 통해 인증이 되어있는 이동통신업체와 통신으로 OTP와 같은 형식의 새로운 password를 사용함으로서 고객이 ICP에게 개인정보를 입력하지 않아도 된다.

3.1 제안 프로토콜



- TN : Ticket Number(ICP가 제공하는 임의의 전화번호 형식의 일련번호)
- TID : Ticket ID(이동통신업체가 고객의 인증을 확인하고 부여하는 임의의 ID)

[그림 3]사용자 익명성을 보장하는 소액결제시스템 프로토콜

3.2 익명성이 강조된 인증 단계

① 구매요청
고객이 ICP에게 콘텐츠의 구매요청을 한다.

② TN전송, TID요구
ICP는 고객에게 TN(Ticket Number)를 부여하고 TID(Ticket ID)를 요구하게 된다. 여기서 TN은 ICP가 고객에 부여하는 전화번호 형식의 일련번호이다.

③ TN(Call)
고객이 이동통신업체에게 TN을 이용하여 전화를 하게 되면 이동통신업체는 이미 고객의 개인정보로 인증을 한다. 고객과 이동통신업체 사이에는 별다른 개인정보를 입력할 필요가 없다.

④ TID부여(SMS)
이동통신업체가 고객에게 SMS로 OTP와 같은 형식의 TID를 부여하게 된다.

⑤ TID입력
고객은 그 TID만을 ICP에 입력하게 된다. ICP에게는 고객의 그 어떤 개인정보도 제공하지 않는다.

⑥ 고객인증요청, TID, 결제정보
ICP는 이동통신업체에게 고객인증요청과 TID, 결제정보를 보낸다.

⑦ 인증 확인
이동통신업체로부터 TID에 대한 인증을 받는다.

⑧ 결제 내용 알림
이동통신업체는 결제정보를 받아서 결제 내용을 고객에게 전송하게 된다.

4. 결론

제안한 시스템은 기존의 OTP를 응용한 것으로 현재 사용하고 있는 소액결제시스템의 형태에서 크게 벗어나지 않으면서도 사용자 익명성에 대해서 보안적 측면을 강화하였다.

앞으로도 소액 결제 시스템은 널리 사용하고 보급될 가능성이 많기 때문에 기존의 유선의 네트워크상에서의 보안정적인면을 그대로 가져올 수는 없지만 사용자가 안심하고 소액결제시스템을 사용할 수 있도록 더 많은 부분에서 시도해봐야 할 것이다. 후에는 M-Commerce의 소액결제시스템의 보안성이 강화되어 소액에만 사용되지 않고 고액부분에서도 좀 더 편리하게 결제시스템을 이용할 수 있게 되어야 한다.

참고문헌

[1] 김국진, "T-Commerce와 M-Commerce의 현황과 정책방향," 정보통신정책 제14권 1호 통권 293호, 2002.

[2] "A One Time Password System RFC", http://www.ietf.cnri.reston.va.us/html.charters/otp-charter.html.

[3] 이현주, 김선신, 이충세 "모바일 전자상거래를 위한 ID기반 지불 프로토콜", 2004.

[4] 윤종호, "네트워크 보안 프로토콜," 교학사, 2004.

[5] Andrew Dahl & Leslie Lesnick, "Internet Commerce", New Riders, 1996.