전자상거래 지불시스템을 위한 보안 프로토콜 설계

The Design of the Security Protocol for Electronic Commerce Payment System

이상덕*, 한승조*

Sang-Duck Lee* and Seung-Jo Han*

요 약

현대 사회는 인터넷의 급속한 보급과 발전으로 사회활동 전반에 걸친 변화를 주도하고 있으며, 새로운 형태의 상거래인 인터넷을 이용한 전자상거래(Electronic Commerce)가 확산발전되고 있다. 본 논문에서는 공용 키(PKI)에 기초를 두는 네트워크형 전자지불 프로토콜을 제안하고자 한다. 제안된 프로토콜은 컨텐츠 거래를 위해 개발된 NetBill 시스템의 익명성을 보장하지 못했던 단점을 보완하였다. 또한 온라인 상에서 제공된 디지털 콘텐츠에 대해 인증번호를 부여함으로써 무단 복제를 방지하고 최대한 안전성이 확보되도록 하였다.

Abstract

The Internet leads the transformation of the all-over social life with its radical diffusion and development. Moreover, it can be more focussed on the electronic commerce using the Internet - a new type of commerce, which is diffusion and developing. In the paper, we propose an electronic payment protocol with a network-type electronic-cash based on Public Key Infrastructure(PKI). The proposed protocol overcomes the problem of NetBill which deals with only contents and can't ensure anonymity. It also prevents illegal copy and distribution and insures the greatest safety by means of giving a certification number to the digital contents offered on the on-line.

Key words : Electronic Commerce, PKI, Electronic-cash, Certification

I. 서 론

현재 전자상거래에서 사용되는 지불 시스템은 지불 방식에 따라 지불브로커시스템(Payment Broker System)과 전자화폐시스템(Electronic Cash System)로 분류할수 있으나, 독립적인 신용구조를 가지고 있어서 물품 구입 시 은행이나 카드 발행사로부터 거래 승인이 필요 없는 전자화폐시스템이 현금과 유사한 개념으로써의 전자지불시스템이 지향하는 최종 목표 시스템이다.

전자상거래에 사용되는 화폐는 기능상 전자동전(Electronic Coin)[1]방식과 전자수표(Electronic Check)[2]방식으로 분류하며, 가치를 보증하기 위해 은행이 서명한 디지털 신호로 표현된 가치정보를 말

* 조선대학교 정보통신공학부(School of Information & Communication Chousn Univ.)
· 제1저자 : 이상덕(first author)
· 교신저자 : 한승조(corresponding author)
· 접수일자 : 2007년 2월 6일

한다. 따라서 인터넷을 기반으로 한 가상공간에서 사용자가 전자화폐를 서로 쉽게 주고받을 수 있도록 하여 실물화폐를 대체할 수 있는 새로운 개념의 화폐[3]에 대한 연구가 절실한 상황이다. 전자 지불 시스템의 프로토콜은 안전성 및 보안성을 위해 여러 가지 요구 사항을 고려하여야 하며[4], 이러한 시스템의 중요한 기술인 디지털 서명, 은닉 서명과 같은 인증 기능 및 보안은 공개키 기반구조(PKI)의 대표적인 RSA를 통한 암호화를 이용하여 보안기술에 기반을 둔 안전장치를 갖추는 것이 바람직할 것이다[5].

본 논문에서는 임베디드 리눅스 시스템에서 동작할 PKI 기반의 네트워크형 전자 지불 시스템을 구현함으로써 네트워크상에서 사용자의 익명성 및 호완성과 안정성을 제공하고자 한다. 제안된 프로토콜은 소프트웨어, 잡지, MP3, 비디오 타이틀 등만을 취급하는 NetBill 시스템, E-cash 및 Netcash의 문제점인 익명성이 보장되지 않는 부분을 보완하였으며, 구입과 지불을 동일 네트워크에서 처리하여 지불단계를 줄일 수 있었다. 또한 암호화 회수 및 통신회수를 감소시킴으로서 시스템의 효율성 및 안전성이 확보되도록 하였다.

본 논문의 Ⅱ장에서는 전자 지불 프코토콜을 설계하였으며, Ⅲ장에서는 전자지불시스템 구현 및 환경에 대하여 설명하고, Ⅳ장에서는 구현한 시스템의 성능 분석을 하였다. 마지막으로 Ⅴ장에서 결론 및 연구방향에 대하여 논하고자 한다.

Ⅱ. 전자지불 프로토콜의 설계

컨텐츠만을 취급하는 NetBill 시스템[6]의 경우 고객과 상점 모두 익명성이 보장되지 않는 단점을 가지고 있으며, 매 서비스마다 서버에 접속하여 확인 절차를 거치고, 거래 단계도 복잡함으로 인하여 다른 지불 프로토콜에 비해서 전자 서명이 많이 쓰이는 단점도 있다[6]. E-cash의 경우도 수취인이 은행계좌에 동전을 입금하게 되면, 은행에서는 동전의 일련번호 등을 기록하여 두 번 이상 사용될 수 없도록 하는 과정에서 수취인의 입금내역을 파악할 수 있어서 수취인의 익명성은 보증되지 않으며, Netcash의 경우도 은행이 구매자에게 화폐를 인출할 때 화폐의 일련번호를 확인하고 온라인 데이터베이스에 기록하여 익명성을 제공하지 못하는 문제점이 있다[7].

표 1. 지불 프로토콜 기호
Table. 1 Payment protocol a symbol

기호	내용
CA	인증기관
B	은행
V	판매자
C	구매자
ER	공개키 암호 알고리즘
DR	공개키 복호 알고리즘
Z	압축 알고리즘
KUA	A의 공개키
KRA	A의 개인키
E	관용키 암호 알고리즘
D	관용키 복호 알고리즘
Ks	세션키
H	Hash 알고리즘
Certificate	인증서
||	연접(Concatenation) 연산

따라서 본 논문에서 제안하는 전자 지불 프로토콜은 상품이 모두 디지털로 되어 있기 때문에 상품 제공과 지불 사이에 생기는 공백으로 인한 불신이 발생하지 않는다는 점을 감안하여, 상품 주문과 지불을 동시에 처리함으로써 익명성이 보장되고 거래 단계를 최소화 할 수 있도록 설계하였다. 본 논문에서 제안하는 프로토콜은 그림 1과 같다.

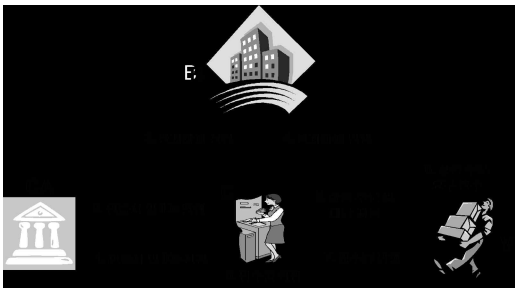

그림 2. 제안한 전자지불 프로토콜
Fig. 1. Proposal electroic payment Protocol

▶ 인증서 및 IDc 발행

ERKUca{Customer||IDc||Pswd} (1)

Certificate C (2)

▶ 전자화폐 신청 및 발행

$ERKUb\{ERKRc\{Cash||IDc||CertificateC\}\}$ (3)

$ERKUc\{ERKRb\{E\text{-}Cash||IDc||CertificateB\}\}$ (4)

▶ 상품 주문 및 대금 지불

M={IDc, 컨텐츠 번호, 전자화폐 금액, 전자 화폐 발행 번호} (5)

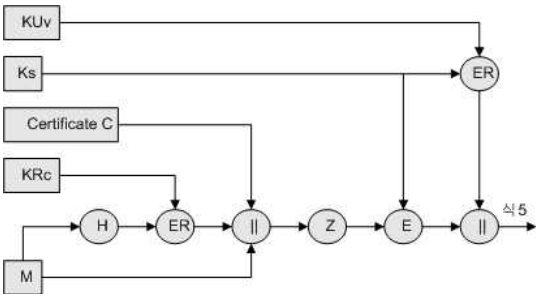

그림 2. 상품 주문 및 대금 지불
Fig. 2 Goods order and loan payment

▶ 상품 주문 요구 접수

$DRKRv\{ERKUv(Ks)\}=Ks$ (6)

$DRKUc\{ERKRc\{H(M)\}\}=H(M)$ (7)

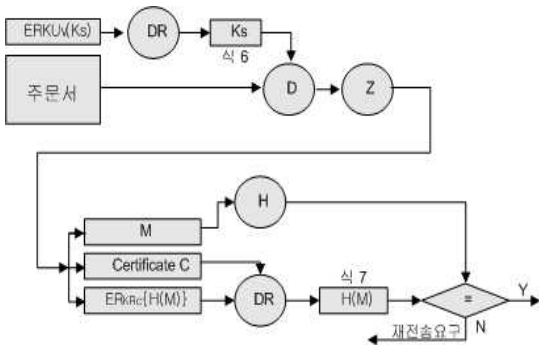

그림 3. 상품 주문서 복호화
Fig. 3 From goods order decryption

▶ 영수증 발행

$ERKRv\{H(M)||Contents\_No\}$ (8)

$ERKUc\{ERKRv\{H(M||Contents\_No)\}||Certificate V||Date/Time\}$ (9)

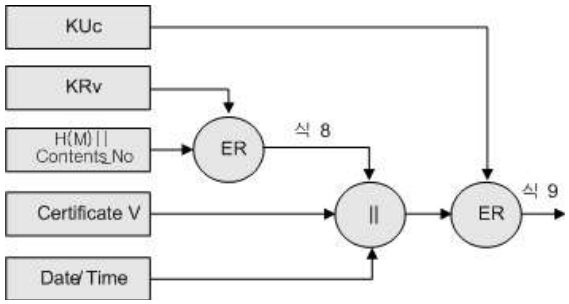

그림 4. 대금 지불에 관한 영수증 발행
Fig. 4 The receipt publication regarding a payment

Ⅲ. 전자지불시스템의 구현

3-1 개발환경

본 논문에서는 임베디드 리눅스 시스템인 HBE-EMPOSⅡ 보드를 활용하였다. 개발된 타켓보드의 CPU는 고성능 저전력 32비트 프로세서인 Inter RISC 프로세서 PXA255 Xscale을 사용하였으며, Qt/E를 활용하였다. 타겟보드에 임베디드 리눅스 시스템을 포팅하기 위하여 Redhat Linux 9.0을 설치하여 개발 환경을 설정하였다. 개발용 PC와 타겟보드는 직렬, Ethernet LAN, JTAG 등의 케이블을 통해 연결되어 있어 부트로더, 커널, 응용 프로그램 등을 전달하게 된다. 개발용 PC에서 Qt/E를 활용하여 프로그램을 개발하고 테스트하여 1차 검증하였으며, 최종적으로 타켓보드상에서 동작을 확인하였다.

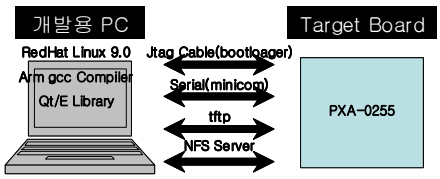

그림 5. 임베디드를 이용한 개발 환경
Fig. 5 development environment for embedded

3-2 구현범위

제안된 시스템은 은행과 연계된 이후에 전자화폐를 신청하는 부분만 처리하였고, 상품의 구입과 같은 전자화폐 사용 내역에 중점을 두고 구현하였다. SQL 데이터베이스 서버가 존재하고, 일반 사용자들이 사용할 수 있는 클라이언트용 소프트웨어를 개발

하였다. 디지털 상품과 같은 정보 상품은 컨텐츠 구입 및 결제를 위해 암호화 된 자료를 전송하고, 서버에서 복호화가 완료되면 컨텐츠에 대한 결제는 완료되어 다운로드 할 수 있도록 하였다. 개인 신상에 관한 자료로 공개키, 개인키 및 인증서를 발급 받는다. 인증서는 모든 거래에 사용되며, 증서가 사용될 때는 실명이 아닌 등록된 ID만을 사용하게 된다. 우측 하단에 사용 가능한 전자 화폐를 표시하여 잔액을 초과하는 컨텐츠는 구매가 이루지지 않도록 하였다. 본인이 그 동안 구입한 내역을 보여 주고 결제가 완료된 컨텐츠는 언제든지 다시 다운로드 할 수 있도록 하였다.암호화 및 복호화는 처리과정의 정확성을 검증하기 위하여 단계마다 암호화 및 복호화 과정을 화면에 출력하도록 하였다. 사용자는 실제 볼 수 없도록 하였다.

그림 6. 상품구매 처리
Fig. 6 Goods purchase control

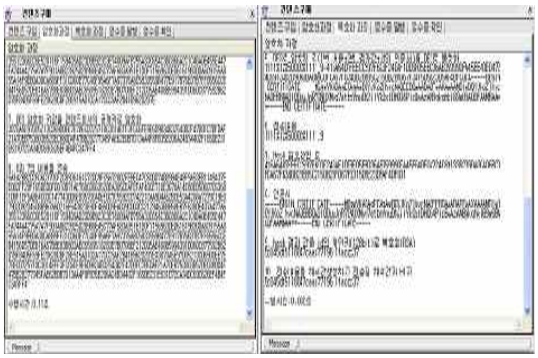

그림 7. 디지털 상품 주문을 위한 암복호화
Fig. 7 Digital goods order for Encryption / Decryption

Ⅳ. 제안한 시스템의 성능분석

제안한 시스템은 총 암호화 회수는 Hash함수를 포함하여 14회의 암호화 계산을 수행한다. 대부분의 전자지불 프로토콜이 익명성 제어를 제공하지 못하고 있으며, 제안된 프로토콜과 기존 프로토콜과의 전체적인 특성을 비교하면 표 2와 같다.

표 2. 기존 전자지불 프로토콜과의 비교
Table. 2 Comparison of existing electronic payment protocol

비교항목 / 전자화폐	이중사용방지	Vendor의 부정방지	익명성
Millicent	○	X	X
MPTP	○	X	X
Mini-pay	X	○	X
E-cash	○	○	○
Cyber-cash	-	○	X
Echeck	○	○	X
FV	-	○	X
NetCheque	○	○	X
NetBill	○	○	X
Propose System	○	○	○

제안된 시스템의 암호화 회수를 볼 때 전체적으로 보면 SET에 비해 공개키를 2회 더 추가로 필요하지만 SET에서는 영수증 발행에 대한 언급이 없는 상태이고, 제안된 시스템은 영수증 발행과정을 모두 합하였을 경우의 총 동작 회수를 나타낸 것이다. 영수증 발행과정을 제외한다면, 훨씬 적은 회수의 동작으로 거래를 처리할 수 있다. 표 4에서 나타난 것과 같이 통신 회수 또한 컨텐츠만을 취급하는 특정 프로토콜을 사용하여 상품 전달과 대금 지불이 동일 네트워크에서 이루어진다는 특성을 살려 주문과 결제를 처리할 때 2회 통신과, 영수증을 전달받을 때 1회로 하여 단 2회의 메시지 전달로 모든 거래가 종료 되도록 하였다.

표 3. 제안한 시스템과 SET의 암호화 회수 비교
Table. 3 Encryption frequency comparison of the system which it proposes and the SET

	공개키		관용키		비고
	제안한 시스템	SET	제안한 시스템	SET	
암호화 회수	9	7	2	3	영수증 포함
	4	7	1	3	영수증 제외

표 4. 제안한 시스템과 SET의 통신 회수 비교
Table. 4 Communication frequency comparison of the system which it proposes and the SET

	제안한 시스템	SET	비고
통신회수	3	12	영수증 포함
	1	12	영수증 제외

Ⅴ. 결 론

본 논문에서는 디지털 컨텐츠 거래를 위해 개발된 NetBill 시스템 등에서 익명성을 보장하지 못했던 단점을 보완하고 복잡한 지불 과정을 동일 네트워크에서 처리하여 지불단계를 간략화 하였다.

제안된 프로토콜은 영수증 발행 및 검증 절차를 수행하여 거래 당사자간에 정보의 전달 내용에 대해 부인할 수 없도록 하였으며, 전자 화폐에 대한 사용도 일련번호를 부여하고, ID로 정당한 접속이 이루어지면 접속과 동시에 사용내역을 파악하였다. 지불시스템에서 잔액을 계산함으로써 잔액 이상인 초과 금액의 사용이나 이중 사용이 불가능하도록 하였다. 거래 당사자들은 실명이 아닌 인증기관으로부터 부여받은 가상 ID만을 사용함으로써 인증기관의 개입이 없다면 완전한 익명성이 제공되도록 하였다. 컨텐츠의 제공도 인증번호를 부여하여 사용자가 인증번호를 입력하여 다운로드받을 수 있도록 하였다. 판매자가 영수증의 발급 및 검증 절차를 수행함으로써 거래의 단계가 다른 시스템에 비하여 줄어들었으며, 전자화폐의 잔액이 허락하는 금액만큼 제약 없이 사용할 수 있다. 지불 과정을 동일 네트워크에서 처리하여 지불단계를 줄일 수 있었으며, 암호화 회수 및 통신회수를 감소시킴으로서 시스템의 효율성 및 안전성이 확보되도록 하였다.

참 고 문 헌

[1] David Chaum, Amos Fiat, and Moni Naor, "Untraceable Electronic Cash", Advances in Cryptology-Crypto '88, LNCS 403, Springer Verlag, pp.319-327, 1988.

[2] David Chaum,"Online Cash Checks", Advances in Cryptology-Eurocrypto'89, LNCS 434, Springer Verlag, pp.288-293, 1989.

[3] J.Camenisch, U.Maurer, and M.Stadler, "Digital payment systems with passive anonymity-revoking trustees", In Esorics '96, Italy, 1996.

[4] Chaum, D., "Blind Signatures for Untraceable Payments," Advances in Cryptology Proceedings of Crypto '82, pp199-203, 1982.

[5] O. Toole, "The Internet Billing server Transaction Protocol Alternatives", Carnegie Mellon University Information Networking Institute, 1994.

[6] B. Cox, J. D. Tygar and M. Sirbu, "NetBill Security and Transaction Protocol", Proceeding of 1st USENIX on Electronic Commerce, 1996.

[7] William Stallings, Network and Internetwork Security, Prentice Hall, 1995

이 상 덕 (李相德)

1997년 2월 : 조선대학교 전자공학과 학사
1999년 2월 : 조선대학교 대학원 전자공학과 석사
2000년 2월 ~ 현재 : 조선대학교 대학원 전자공학과 박사과정
2005년 ~ 현재 : 조선대학교 정보통신공학과 외래교수
관심분야 : 네트워크 및 시스템보안, 임베디드 시스템, DRM

한 승 조 (韓承朝)

1980년:조선대학교 전자공학과
1982년: 조선대학교전자공학과 석사
1994년: 충북대학교 전자계산학과 박사
1986년 6월 ~ 1987년 3월: 뉴올리언스대학 객원교수
1995년 2월 ~ 1996년 1월: 텍사스대학 객원교수
2000년 12월 ~ 2002년 2월: 버클리대학 객원교수
2005년 11월 ~ 현재 조선대학교 정보전산원장
1998년 3월 현재: 조선대학교 전자정보통신공학부 정교수
관심분야 : 정보보안, 컴퓨터네트워크, DRM, S/W 불법복제방지시스템