카드사용자의 비밀번호 기반 이중서명을 이용한 전자 지불 프로토콜의 설계

김성열*, 이옥빈**, 배용근*

The Design of Electronic Payment Protocol Using Dual Signature based on Cardholder's Secret Number

Seong-Yeol Kim*, Ok-Bin Lee**, Yong-Geun Bae*

요 약

전자상거래는 컴퓨터 기술 분야에서 중요한 주제로서 이는 공중망에서 전자 정보를 교환함으로써 금융 거래를 수행하게 되기 때문에 다양한 종류의 위험을 내포하게 된다. 따라서 전자상거래 시스템 구축할 때는 기밀성, 무결성, 인증과 부인봉쇄와 같은 보안요소를 고려해야 한다.

본 논문에서는 이중서명 기법을 이용한 신용카드 기반의 지불프로토콜을 제시한다. 이 프로토콜은 카드사용자가 지불하는 은행에게는 지불정보를 제공하지만 구매정보는 주지 않으며, 상인에게는 구매정보를 제공하지만 카드번호를 비롯한 지불정보는 알리지 않기 때문에 카드사용자의 개인정보를 보호하게 된다. 프로토콜을 수행하기 위해서 이중서명은 사용자의 신용카드 비밀번호를 사용한 공통키와 공개키 방식을 사용함으로써 실행한다.

Abstract

The topic of electronic commerce is a hot issue in computer technology. There are many kinds of risks associated with electronic commerce which performs financial transactions by exchanging electronic information over public networks. Therefore, security factors such as confidentiality, integrity, authentication and non-repudiation should be required to construct secure electronic commerce systems.

* 조선대학교 전자계산학과

** 충북대학교 전자계산학과

접수일자 : 1999년 3월 10일

In this paper, the credit card-based payment protocol applying dual signature is presented. It provides payment information to the bank a cardholder pays to, but conceals ordering information. It also offers ordering information to a merchant, but hides payment information including the card number. Thus, cardholder's private information can be protected. In order to accomplish this, dual signature is performed employing both symmetric method utilizing cardholder's secret number as an encryption key and asymmetric method.

Ⅰ. 서 론

최근 상업적인 목적에 인터넷을 이용하려는 시도가 이루어지면서 현재의 물리적인 시장이 갖는 시공간의 제약을 뛰어넘어 새로운 이윤창출의 수단으로서 전자상거래는 점점 더 활발히 이루어질 전망이다. 또한 전자상거래를 통한 거래규모가 점차 증가할 것으로 예상되는 지금 전자상거래의 활성화[1,2]는 국가 경쟁력 강화를 위해 필수적인 요구사항이라 할 것이다. 이러한 전자상거래의 구현시에 상품의 대금을 지불하고 이를 결제하는 기술은 금전과 관련된 문제로서 안전성과 무결성이 매우 중요하다. 실거래에서 대금결재를 위해서는 현금, 수표, 신용카드 등이 주로 사용되나 인터넷과 같은 가상공간에서 신용카드번호를 노출시키는 것은 커다란 위험부담을 가지고 있다. 따라서 사용자를 보호하면서 안전한 거래를 할 수 있는 보안프로토콜과 지불프로토콜[2,3]이 필요하다. 인터넷상의 대표적인 보안프로토콜로는 SHTTP(Secure Hyper Text Transfer Protocol)[4]와 SSL(Secure Socket Layer)[5]이 있다. 그러나 이와 같은 양자간의 보안프로토콜로는 상점으로부터 사용자를 보호할 수 없으며 여러 가지 문제를 야기할 수 있다. 또한 웹, TCP/IP에 대한 기반기술 및 웹 관련 핵심기술을 보유하지 않는 한 경쟁력을 갖추기 어렵다. 따라서 전자상거래의 모든 참여자간에 발생할 수 있는 트랜잭션을 정의하고 해당 트랜잭션의 안전성을 보장하는 지불프로토콜이 요구된다. 이 지불프로토콜은 응용레벨에서 개발되기 때문에 국내 기술력으로도 경쟁력을 가질 수 있다. 현재 연구 개발되고 있는 지불관련 보안기술은 크게 암호화된 신용카드에 의한 지불방식과 전자현금을 이용한 지불방식으로 구분할 수 있다. 전자현금방식은 구매자가 전자화폐 발행자로부터 화폐를 취득하여 이를 상인에게 지불하는 방식으로서 Mondex[6], Chip[7], Ecash[8], Proton[9] 등이 대표적인 전자화폐시스템이다. 신용카드에 의한 지불방식은 구매자가 직접 지불하는 대신에 지불기관에 지불명령을 함으로써 지불이 이루어지는 방식이다. 그러나 신용카드를 이용한 전자대금 결재는 카드번호, 비밀번호, 결재계좌번호 등의 누출 가능성이 있어 그 안전성에 있어서 논란이 되고 있다. 따라서 신용카드를 이용한 전자결재를 위한 보안기술의 개발과 적용이 요구되고 있다. 신용카드사의 두 거대회사인 VISA와 Masster는 SET(Secure Electronic Transaction)[10]이라는 프로토콜을 제안하였다. 현재 SET은 신용카드 기반의 대표적인 지불프로토콜이다. 이러한 신용카드기반의 지불시스템은 일반적인 통신망 정보 보호의 요구사항인 인증(Authentication), 기밀성(Confidentiality), 무결성(Integrity), 부인봉쇄(Non-repudiation) 서비스가 필요하며 특히 다수의 소비자와 공급자, 상호간의 신분에 대한 인증 문제[11]는 신중히 고려하여야 한다. SET의 경우에는 개인정보의 보호를 위해 이중서명 기법을 적용한다. 이 기법은 카드사용자가 지불하는 은행에게는 지불정보를 제공하지만 구매정보는 주지 않으며, 상인에게는 구매정보를 제공하지만 카드번호를 비롯한 지불정보는 알리지 않음으로서 구현된다.

본 논문에서는 전자상거래의 전자지불에 있어 신용 카드를 이용한 안전한 전자상거래 프로토콜을 제시하고자 한다. 이 프로토콜은 인증, 무결성, 비밀성, 부인봉쇄, 이중서명 기능을 가지고 있으며 특히 이중서명을 통해서 사용자 정보를 보호한다. 그러나 SET과는 다르게 본 논문에서는 카드사용자와 발행처만이 알고있는 카드키로 암호화하여 전달함으로써 지불기관의 사용자 인증 트랜잭션을 줄일 수 있

음을 보인다. 이 프로토콜에 의해, 안전성을 갖춘 전자상거래 프로토콜을 설계하고, 구현시에 고려할 점과 인증서버의 과중한 부담을 줄일 수 있는 방법을 모색하게 될 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 전자지불 결재현황과 보안 고려요소를 살펴보고 3장에서는 카드사용자의 비밀번호를 기반으로한 이중서명을 포함한 전자지불 시스템을 설계 및 분석하고 제4장에서 결론 및 향후연구방향을 논한다.

Ⅱ. 전자지불 결재 현황과 보안 고려 요소

1. 전자지불 결제 기술현황

전자지불 시스템은 표 1과 같이 구분되며 크게 지불브로커 시스템(Payment Broker System)과 전자현금 시스템(Electronic Money System)의 형태로 나누어 볼 수 있다[7,8,9,11,12, 13,14].

표 3. 전자지불 프로토콜의 분류
Table 1. Electronic Payment Protocol

지 불 매 체	지 불 프 로 토 콜
전자현금기반 지불시스템	E-cash (Digicash) NetCash(NetBank) CAFE(Conditional Access For Europe) Mondex(Mondex) VisaCash(VISA)
전자수표기반 지불시스템	NetCheque(USC) NetBill(CMU) NetChex(FSTC:Financial Services Technology Consortium)
소액 전자지불 시 스 템	Millicent(DEC) PayWord, MicroMint (Rivest & Shamir) MPTP(Micro Payment Transfer Protocol : W3C)
신용카드기반 지불 시스템	iKP(internet Keyed Payment : IBM) GreenCommerce(FV : First Virtual) CyberCash(CyberCash) SmartWallet(V-One) CFWallet(Check Free) Secure Courier(Netscape) SEPP(Secure Electronic Payment Protocol : MasterCard) STT(Secure Transaction Technology : Microsoft, VISA) SET(Secure Electronic Transaction : MasterCard, VISA)
전자 자금 이체 시 스 템(EFT)	SFNB(Security First Network Bank) FDB(First Digital Bank)

지불브로커 시스템은 독립적인 신용구조를 가지고 있지 않고 신용카드나 은행 계좌 이체를 통해 네트워크 상에서 지불이 가능하도록 연결시켜주는 구조로 되어 있다. 이 시스템은 신용카드를 이용한 거래의 관행이 자리잡혀 있고 이의 응용이 용이하기 때문에 현재 많이 이용되고 있는 현실적인 전자지불 시스템이다. 구매자는 사전에 '은행 · 신용카드사'로부터 신용등급평가를 받아 신용카드를 발급받고 그림 1과 같은 지불브로커메카니즘을 통해 거래하게 된다[15].

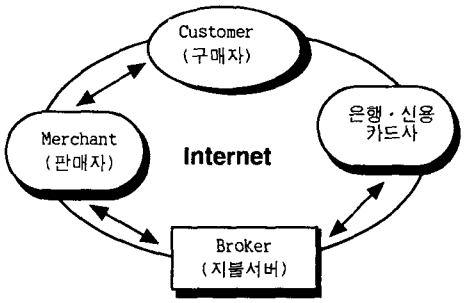


그림 1. 지불브로커 메카니즘
Fig. 1 Payment Broker Mechanism

표 1의 전자지불 프로토콜 중 신용카드 기반의 대표적인 지불 프로토콜 SET(Secure Electronic Transaction)은 상인, 은행, 카드발행처, 지불게이트웨이, 인증국(Certificate Authority) 그리고 고객을 참여자로 그림 2와 같은 절차로 수행된다. 먼저, 고객, 상인, 지불게이트웨이는 거래를 위해 인증국에 등록하고 인증서를 발부 받는다. 상품을 구매하고자 하는 고객은 상인의 웹 홈페이지에서 구매할 상품을 검색하고 선택하면 선택된 상품에 대한 구매 요구가 상인 서버로 전송된다. 이에 상인서버는 접수된 구매 요구에서 고객이 선택한 물품에 대한 가격, 선적 요금 등을 포함한 구매 형식을 고객에게 전송한다.

고객은 구매 요구형식을 확인하고 지불에 사용할 신용카드의 정보를 암호화하여 최종 구매 요구를 상인 서버로 전송하게 되는데 상인 서버는 고객이 전송한 최종 구매요구에 포함된 지불 정보를 지불게이트웨이로 전송하여 지불인가를 요청한다. 지불

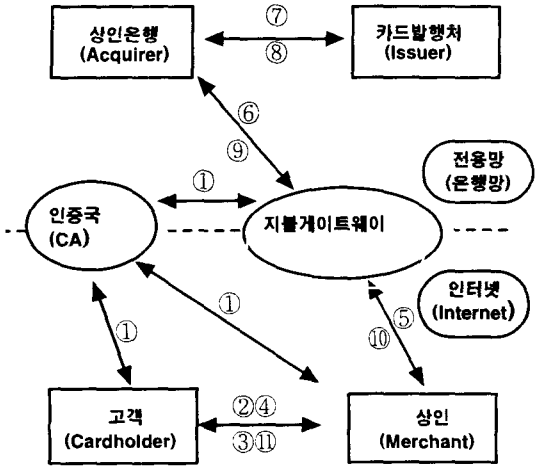


그림 2. 지불프로토콜 SET의 절차
Fig. 2 Procedure of SET

게이트웨이(payment gateway)는 지불 정보를 은행망과 연동하여 지불인가(authorization)를 요구하고 그 결과를 상인 서버로 전송하면 상인 서버는 지불인가 결과에 따라 거래가 성립되었다면 지불인가 정보를 포함한 전자 영수증에 해당하는 구매 확인서 전송하여 주고 상인 서버는 성립된 거래에 대한 서비스를 수행 또는 배달 대행 서비스에 상품 배달 의뢰하면 접수된 상품 배달 요구에 따라 해당 고객에게 상품이 배달된다. 그리고 상인서버는 지불인가와 동시에 또는 일괄처리에 의해 정기적으로 인가받은 지불에 대한 결재 요구를 지불 게이트웨이로 전송하게 된다. 마지막으로 지불 게이트웨이는 상인 서버로부터 전송된 결재 요구를 금융망과 연동하여 수행하게 된다[10,16]. 그러나 SET프로토콜이 실질적으로 서비스되기 위해서는 다음과 같은 문제들이 해결되어야 한다. 먼저 판매자와 구매자 모두가 신용카드 결재에 앞서 디지털 ID를 확보해야한다. 둘째, 신용카드 기반 전자지불 시스템이 한번의 지불 트랜잭션에 카드신용조회, 키인증, 네트워크 비용 등을 감안하여 처리절차를 최대한 단축시킴으로써 지불 트랜잭션의 비용을 감축시켜야 한다. 셋째, 신용카드 결제로 인한 개인정보 유출 등의 후유증이 해결되고 마지막으로 전자상거래 시스템을 이용하는 구매자들이 찾고자하는 물건들을 쉽게 발견할 수 있도록 전체 시스템과 결제시스템을 구성하여야 한다. 따라서 본 논문에서는 인증, 무결성, 비밀성, 부인봉쇄, 이중서명 기능을 가지고 전자상거래 메시지 전달과정에서 각 참여자간의 안전한 정보 교환 및 서로를 인증하고, 무엇보다도 카드기반 지불의 고유문제인 트랜잭션 비용의 절감을 고려하여 카드 사용자와 발행처만이 알고있는 카드키로 암호화하는 방법을 이용하여 전달거래절차를 줄여 구매자의 상품구매시 보다 편리한 환경 제공과 서비스 제공자인 상점의 효율적인 운영을 위한 전자상거래 프로토콜을 설계한다. 이 프로토콜에 의해, 안전성을 갖춘 전자상거래 프로토콜을 설계하고, 구현시에 고려할 점과 인증서버의 과중한 부담을 줄일 수 있는 방법을 모색하게 될 것이다.

2. 전자상거래 보안 고려요소

통신망을 통한 안전하고 효율적인 전자상거래가 활성화되기 위해서는 여러 가지 요구조건이 있지만 무엇보다도 정보 보안 기술이 필수 불가결한 요소로서 사용자의 익명성(Anonymity) 보장, 상대방에 대한 인증(Authentication), 그리고 사용자의 신용정보(이름, 주소) 및 신용카드 정보(카드번호, 이름, 기한)의 안정성 확보가 강구 되어야한다[17].

인터넷의 보안 취약성, 현존 인터넷 지불방식의 보안 취약성을 극복하기 위하여 전자상거래 시스템 내에 구현해야할 기본적인 정보 보호기술은 다음 표 2와 같다[18,19,20,21,22,23].

표 4. 전자상거래 정보보호 기술
Table 2. Security Technology of Economic Commerce

전자상거래 정보보호 이슈		정보 보안 기술
전자상거래 정보보호	기밀성(Confidentiality)	공통키 암호화 방식(IDEA, DES)
	인 증(Authentication)	공개키 암호화 방식(RSA)
	무결성(Integrity)	해쉬함수(MD2, MD5, SHA)
	익명성(Anonymity)	키관리(X.509)
	재전송(Resending)	사용자 인증기술(Authentication)
전자상거래 분쟁해결 기능	거래부인봉쇄 (Non-repudiation)	전자봉투(Digital envelope)
		이중서명(Dual signature)
		전자서명(Digital signature)
		블라인드 전자서명(Blind signature)

Ⅲ. 전자상거래 프로토콜 설계

본 장에서는 전자상거래 메시지 전달과정에서 각 참여자간의 안전한 정보 교환 및 서로를 인증하고 무엇보다도 카드기반 지불의 고유문제인 트랜잭션 비용의 절감을 고려하여 거래절차를 줄여 구매자의 상품구매시 보다 편리한 환경 제공과 서비스 제공자인 상점의 효율적인 운영을 위한 전자상거래 프로토콜을 설계한다.

본 논문에서 사용되는 프로토콜의 표기법은 표 3에서 표현되고 있다.

표 3. 프로토콜 표기법
Table 3. Notation of Protocol

표 기	의 미
A_{pk}	사용자 A의 공개키(pk)
A_{sk}	사용자 A의 비밀키(sk)
A_{cs}	사용자 A의 카드 비밀키
$E(A_{sk} : M)$	A의 비밀키로 M을 암호화함
A -> B : M	사용자 A가 B에게 M을 전송
ID_A	사용자 A의 식별자
H(m)	메시지m의 digest
$m_1 \| m_2$	m1과 m2의 concatenation

1. 전자상거래 시스템의 구성

본 논문에서 설계한 전자상거래 시스템의 기본 구성은 구매자, 판매자, 인증서버 그리고 은행으로 구성된다. 시스템의 구성 및 수행 절차는 그림 3과 같다

그림의 수행 절차를 자세히 살펴보면 첫 번째로 구매자가 판매자에 접속, 정보검색 및 상품 선택 후 구매자는 인증서버에게 판매자의 인증서를 요구하고 두 번째로 인증서버가 구매자에게 인증서버의 비밀키로 디지털 서명한 인증서를 전송한다. 구매자는 선택한 상품에 대해 구매 요청을 하기 위해 인증서버로부터 받은 인증서 내의 상대방의 공개키와 자신의 비밀키로 송수신되는 메시지를 암호화한 후 자신의 인증서를 판매자에게 전송한다. 다음 단계는 판매자가 구매자의 구매요청을 받고 구매 허락 메시지를 전송한다. 이에 따라 구매자는 주문상품에

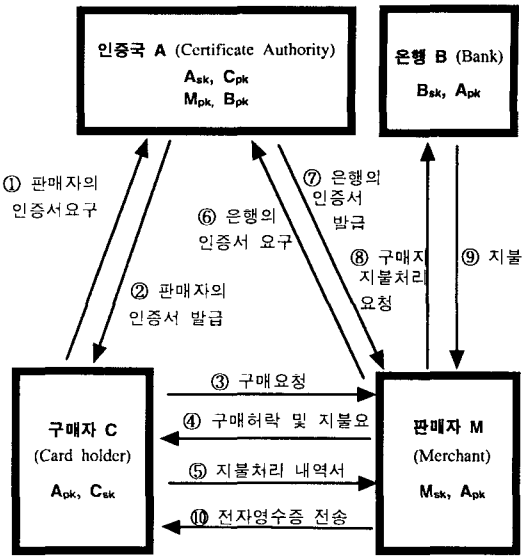


그림 3. 전자상거래 시스템의 기본구성
Fig. 3 Structure of Electronic Commerce System

대한 자신의 정보를 판매자에게 전송한다. 구매자의 정보를 가지고 판매자는 인증 서버에게 거래 은행의 인증서를 요구한다. 인증서버가 판매자에게 인증서버의 비밀키로 디지털 서명한 인증서를 전송한다. 인증이 되면 판매자는 은행에게 구매자의 구좌에 대해 지불을 요구하게 되고 은행은 판매자에게 대금을 지불한다. 마지막 단계로 판매자는 구매자에게 전자영수증을 전송함으로써 절차를 마치게 된다.

2. 프로토콜의 설계

위에서 제시된 전자상거래 시스템의 수행절차를 중심으로 보안 프로토콜을 설계한다. 본 프로토콜은 공개키 방식과 공통키 방식을 혼용하여 각자의 전자인증서를 교환하고 구매자와 판매자간의 안전한 정보교환과 각 참여자간 연동이 가능하도록 설계되었다. 여기에서 공통키는 카드사용자와 발행처만이 알고 있는 카드의 비밀키로 이는 SET에서 구매자가 은행의 공개키를 얻기 위하여 인증국에 은행의 인증서를 요구하고 발급 받는 절차를 생략할 수 있게 해 준다. 참여자는 각각 인증국 A(Certificate Authority), 카드를 소지한 구매자 C(Card holder), 인터넷에서 상점을 개설하고 카드소지자에게 상품

을 판매하는 판매자 M(Merchant), 은행 B(Bank)이며 각각은 사전에 인증국 A(Certificate Authority)에 등록하고 자신의 인증서(Certificate)를 발부 받은 상태로 가정한다. 여기서 사용자가 인증서를 발부받은 상태로 가정함으로써 판매자가 구매자의 인증서를 인증국에 요청하고 발급받는 절차를 줄일 수 있다. 인증서는 인증서버가 신청자의 공개키와 신청자의 인적사항, 인증서 발급번호, 유효기간 등을 포함하여 인증서를 만들고 이를 서버의 비밀키로 서명하여 만든 전자 인증서 형태이다. 예를 들어 사용자 C의 인증서 Auth[C]는 $E(A_{sk}: (Time, ID_C, C_{pk}))$와 같이 구성되어 사용자의 공개키가 포함되어있다. 본 프로토콜은 카드사용자, 즉 구매자가 물건을 주문하는 과정을 시작으로 은행이 판매자에게 최종 통보(지불에 관한)를 해주고 판매자는 이에 대한 전자영수증을 구매자에게 지급해주는 단계까지를 설계하였다.

(1) 프로토콜의 절차

본 논문에서 제시하고 있는 전자상거래 프로토콜은 다음과 같다.

[1 단계] C -> A : $E(C_{sk} : E(A_{pk} : (C, M)))$, C
[2 단계] A -> C : $E(C_{pk} : (C, M, Auth[M]))$
$Auth[M] = E(A_{sk}: (Time, ID_M, M_{pk}))$
[3 단계] C -> M : $E(M_{pk} : (Auth[C], Req\text{-}message, T))$
$Auth[C]=E(A_{sk}: (Time, ID_C, C_{pk}))$
[4 단계] M -> C : $E(C_{pk}:(Req\text{-}message,Ack\text{-}message))$
[5 단계] C -> M : $E(M_{pk} : (Inf\text{-}A)), E(C_{cs} : (Inf\text{-}B))$
$Inf\text{-}A = (H(OI)|H(PI)|E(C_{sk} :H(H(OI)|H(PI)), OI)$
$Inf\text{-}B = (H(OI)|H(PI)|E(C_{sk} :H(H(OI)|H(PI)), PI)$
[6 단계] M -> A : $E(M_{sk} : E(A_{pk} : (M, B)))$, M
[7 단계] A -> M : $E(M_{pk} : (M, B, Auth[B]))$
$Auth[B] = E(A_{sk}: (Time, ID_B, B_{pk}))$
[8 단계] M -> B : $E(B_{pk} : (Auth[M], Auth[C], E(C_{cs} : (Inf\text{-}B)))$
[9 단계] B -> M : $(M_{pk} : (Res\text{-}message))$
$Res\text{-}message = E(C_{cs} : (PI))$, B, Amount
[10단계] M -> C : $E(C_{pk} : E(M_{sk} : E(C_{cs} : (PI)))$, B, M, Amount)

제시된 프로토콜을 각 단계별로 살펴보면 다음과 같다.

[1단계] 구매자 C는 상품정보를 쇼핑한 후에 원하는 상품을 구매하기 위하여 판매자 M이 인증된 거래자인지를 확인한다. 자신과 판매자 M에 관한 정보를 인증국의 공개키(A_{pk})로 암호화하고 자신을 인증하기 위해 디지털 서명하여 인증국에 전송한다.

[2단계] 인증국 A는 자신의 비밀키로 $E(A_{pk}:(C,M))$을 해독하여 C, M을 획득하고 C, M이 정당한 거래자인지를 확인한 후 C, M이 정당한 사용자인 경우 M의 인증 결과를 구매자 C에게 전송하는데 구매자 C만이 정보를 얻을 수 있도록 구매자 C의 공개키로 암호화하여 보낸다. 그리고 구매자가 원하는 판매자 M이 정당한 사용자가 아니면 각 사용자에게 거래하지 못하도록 경고 메시지를 전달한다. 예를 들어 M이 정당한 사용자가 아닌 경우 C에게 $E(C_{pk}:(C, M, "경고메세지"))$를 전송한다. 인증서는 한계기간, 판매자의 식별자, 판매자의 공개키로 구성되어 디지털 서명된다.

[3단계] 2단계에서 받은 메시지에서 M의 인증서를 확인한 후 구매요청서 "Req-message"를 인증국 등록 시에 발부 받은 자신의 인증서와 함께 전송한다. 수신한 판매자 M은 인증국 A의 공개키 A_{pk}를 사용하여 C의 인증서 내에서 C의 공개키를 획득한다. 따라서 M은 C가 보낸 구매요청서를 확인하게 됨과 동시에 인증서를 통해서 C가 정당한 거래자임을 확인할 수 있다. 또한 이때 발생할 수 있는 재전송 문제를 방지하기 위하여 임시비표 T를 사용한다. T가 없다면 이 단계의 정보를 가로채서 재전송공격이 가능하게 된다.

[4단계] 판매자 M은 구매자 C의 구매요청서에 따라서 구매허락 메시지를 구매자 C의 공개키로 암호화하여 보낸다. 이에 구매자 C는 자신의 구매요청서 "Req-message" 에 대하여 M이 수락한 구매요청 승인서 "Ack-message"를 확인한다.

[5단계] 이 단계에서 구매자 C는 정보의 투명성을 기하기 위하여 주문정보(OI: Order Information)와 지불정보(PI: Payment Information)를 메시지 다이제스트와 전자서명된 정보 즉, 이중서명(Dual signature)하여 지불정보는 판매자 M이 볼 수 없도록 하는 지불정보의 투명성과 주문정보는 은행 B가 볼 수 없도록 주문정보의 투명성을 위해 각각 Inf-A, Inf-B를 구성하여 M에게 전송한다[24]. 이때 판매자에게 보낼 주문정보는 판매자의 공개키로, 은행에게 보낼 지불정보는 은행과 구매자가 신용카드 발급 시 공유하게 되는 공통키(C_{cs})로 암호화하여 별도의 키분배 절차 없이 기밀성을 유지할 수 있도록 하였다.

[6단계] 판매자 M은 구매정보(OI)로부터 C가 제시하는 상품내역 및 거래은행 B를 획득한 후 B를 확인하기 위하여 인증국 A에 은행 B의 인증을 의뢰하는데 여기에서도 자신을 인증하기 위한 자신의 비밀키와 그리고 정보의 기밀성을 위해 인증국의 공개키로 암호화한 뒤 보낸다.

[7단계] 인증국 A는 은행 B의 등록여부를 확인한 후 그 인증서 Auth[B]를 판매자 M에 전송한다. 그러나 은행 B가 인증 받지 못하는 경우 판매자 M에게 알려주어서 구매자 C에게 거래할 수 없음을 알리고 재요청을 수락하던가 거래를 중단시킨다.

[8단계] 인증국 A로부터 Auth[B]를 받은 판매자 M은 인증국 등록 시 발부 받은 자신의 인증서 Auth[M]와 구매자 C의 인증서 Auth[C], 그리고 구매자가 보내왔던 Inf-B를 은행 B에 전송한다. 은행 B는 Auth[C], Auth[M]을 획득하여 각각의 공개키를 얻고 정당한 거래자임을 인증서를 통해 확인한 후 Inf-B의 메시지를 해독하여 정보를 얻는다. 그리고 구매자 C가 정당한 거래자이고 지불에 사용될 카드의 정보(카드유효기간, 사용금액한도)등에 대하여 거래성사여부를 결정하며 판매자M에게 상품에 대한 금액 지불결정을 내린다.

[9단계] 은행 B는 구매자 C의 지불정보에 따라 지불이 가능함을 판매자 M에게 알리고 지불허락 메세지를 보낸다. 그리고 은행의 부인봉쇄를 위해 판매자 M은 은행으로부터 암호화된 지불정보를 받아 보관하게 되는데 이는 판매자가 고의로 변경할 수 없도록 은행의 비밀키로 암호화된 것이며 단지 영수증으로서 후에 판매자의 지불요구 금액과 비교하는데 사용된다.

[10단계] 판매자 M은 구매자 C에게 지불처리결과에 따른 전자영수증을 발급하는데 이는 후에 부인봉쇄를 위해서 은행 및 판매자의 비밀키로 암호화된 정보를 영수증으로 받는다.

(2) 프로토콜의 분석

본 논문에서 제시된 프로토콜은 카드지불 기반 전자상거래 시스템의 네트워크 암호화 응용시스템으로서 공개키 암호화 기술이 필수적이며 이에 키의 관리와 인증을 위해 안전한 키분배가 되어야 하고 한번의 지불 트랜잭션에 카드신용조회, 키인증, 네트워크 비용 등을 감안하여 처리절차를 최대한 단축시킴으로써 지불 트랜잭션의 비용을 감축시키고 있다.

• 안전한 전송(Secure transmission)

본 논문의 전자상거래 프로토콜에서는 메시지 기밀성을 보장하여 정보의 안전한 송수신이 가능하도록 공개키 암호화 방식과 공통키 암호화 방식을 사용하고 각 참여자간의 사용자 인증을 위해 인증 서버로부터 전자인증서를 발부 받아 정보 송수신시 서로 교환하도록 하였다.

• 인증(Authentication)

프로토콜은 메시지 인증 기술과 디지털서명 기술을 사용하고 있다. 카드사용자인 구매자의 거래절차를 좀더 단축시키기 위하여 구매요청시 구매자는 구매요청서에 자신의 전자 인증서(Auth[M] = $E(A_{sk}: (Time, ID_M, M_{pk}))$)를 첨부하여 보냄으로써 판매자는 인증서버에 구매자의 인증을 요구하는 절차를 생략하고도 거래상대자인 구매자를 인증할 수

있게 하였다. [1단계], [6단계]는 공개키 방식의 특징을 이용하여 자신을 상대가 인증할 수 있도록 하였다.

• 부인봉쇄(Non-repudiation)

거래시 각 정보는 참여자의 공개키로 암호화하여 보냄으로 전자상거래 분쟁 해결기능으로서 부인봉쇄 서비스를 하고 카드사용자인 구매자가 주문정보 및 지불정보 보안을 위해 은행과 공통키 암호화 방식을 이용한 이중서명(Dual signature)을 채택하여 정보 전송시 안전하면서도 거래 절차가 최소화하도록 하였다.

• 투명성(Transparency)

이중서명($E(M_{pk} : (Inf\text{-}A))$, $E(C_{cs} : (Inf\text{-}B))$)은 전송되는 지불정보를 중간에서 악의의 제3자가 대체할 수 없도록 하기 위해서 판매자는 지불에 관한 정보를 모르도록 보안을 유지하고 은행은 구매에 관한 정보를 모르도록 하여 판매자에 대해서는 지불정보의 투명성을 은행에 대해서는 구매정보의 투명성을 제공한다. 또한 구매자와 은행(신용카드사) 간에 카드 발급시 공유한 공통키를 이용하게 함으로써 공개키 분배를 위한 별도의 절차를 요구하지 않도록하였다.

• 메시지 재전송(Replay)

메시지 재전송에 대한 공격을 방지하기 위하여 임시비표를 첨가하는 방법을 사용하고 있다. 임시비표를 사용하는 기법은 카운터, 타임스탬프, 난수 등을 사용할 수 있다. [3단계] $E(M_{pk} : (Auth[C], Req\text{-}message, T))$에 T를 첨가함으로서 재전송 공격을 방지하게 된다.

• 트랜잭션 처리 비용의 감축

프로토콜은 안전한 거래가 이루어질 수 있도록 하면서도 처리절차를 감축하도록 제안되었다. [3단계]에서 구매자가 자신의 인증서를 전송하도록 함으로써 3, 4단계 사이에서 판매자가 인증국에 구매자의 인증서를 요청/발부 받는 절차를 줄일 수 있으며, [5단계]를 수행함에에 있어 은행과 구매자가 공유하는 공통키를 사용하게 함으로써 5단계 수행 전에 구매자가 인증국에 은행의 인증서를 요청하고 발부받는 절차를 생략하여 트랜잭션 처리 비용을 감축하고 있다.

위의 프로토콜 분석을 통하여 전자상거래에서 필요한 정보보안 서비스인 부인봉쇄 서비스, 무결성, 투명성, 기밀성 제공으로 보다 안전한 거래가 될 수 있도록 설계하였으며 전자상거래 각 참여자들의 인증국 조회 횟수 단축으로 트랜잭션 비용이 감소될 수 있도록 하였다.

Ⅳ. 결 론

전자상거래가 활성화되기 위해서는 구매자와 판매자간의 인증과 거래 내역에 대한 공증 기술과 같은 사용자 정보보호 기술이 선행되어야 가능할 것으로 전망된다. 현재 산업계와 국가간의 정보 보호 기술에 대한 연구가 많이 수행되고 있다. 본 논문에서는 전자상거래에서의 가장 많은 수요가 따를 사용자 측면에서의 보안 요구사항을 분석하고, 이에 적합한 전자거래 시스템의 사용자 보안 기능을 설계하였다. 그리고 인터넷을 기반으로 한 전자상거래 서비스를 가상하여 전자상거래 고유문제를 제시하고 그에 필요한 인증 기술 및 보안 기술을 제시하였고 이를 근거로 기존 인증 방식의 장단점의 분석 결과를 제시하였다. 그리고 전자상거래시 신용카드를 기반으로 지불을 처리할 경우, 구매자와 판매자간의 인증을 효율적으로 처리할 수 있는 방법으로 인터넷 기반의 전자 상거래의 특성을 수용함과 동시에 인증 서버의 성능을 고려한 최적 지불 프로토콜을 제시하였다.

현재까지 전자 지불은 아직 전자 상거래가 초기 단계에 있었던 관계로 최대한 구매자를 끌어 모으는 데에 주력하고 있었다. 그 결과 정보의 유출을 막고 불법적인 변조나 위조를 막는 방안을 마련하는데 많은 연구가 진행되었다. 그리고 사용자의 친숙도를 고려하여 실세계에서 사용되던 지불 방식과 형태나 사용절차가 아주 유사한 지불 방식을 따르고 있다. 그러나 앞으로 인터넷에서의 전자 지불 방식은 인터넷이라는 새로운 환경이 기존의 경제 환경과 다르다는 점에서 오는 이점을 잘 살린 처리절차를 가진 방식으로 재 설계되어야 할 것이다. 그리고 여러 가지 다른 형태의 지불 방식들이 통합되어

판매자와 구매자간에 다양한 형태의 다양한 상품 거래가 이루어질 수 있도록 지원할 수 있어야 할 것이다. 즉, 하나의 지불 시스템에서 전자 현금, 신용카드, 전자 수표, 전자 자금이체 등의 여러 가지 지불 방식을 지원하는 통합된 지불 시스템에 대한 연구가 필요하다.

참고문헌

[1] 한국전산원, 정부 EC 플랫폼 발전방안에 대한 연구, 1998.6.

[2] 김홍근, 최영철 "전자상거래 정보보호기술 현황 및 대응방안", 정보처리학회지,제6권 1호. pp.22-34,1999.1

[3] 권도균 : "WWW 보안과 전자화폐", WWW 96-1, 웹코리아 제 3회 WWW Workshop, pp.109-122, 1996.

[4] IETF, internet-draft, draft-ietf-wts-shttp-06.txt, "The Secure HyperText Transfer Protocol", 1998

[5] IETF, internet-draft, draft-freier-ssl-version3-01.txt, "The SSL Protocol Version 3.0", 1996

[6] http://www.digicash.com/cash/ecash-home.html :E-cash

[7] http://www.research.digital.com/SRC/milecent :MillicentDEC)

[8] http://www.ini.cmu.edu/netbill/home.html :NetBill(CMU)

[9] http://www.fv.com :Green Commerce(FV:First Virtual)

[10] http://www.visa.com/cgi-bin/vee/st/standard.html :SET spec v1.0

[11] http://www.digicash.com :DigiCash

[12] D.Chaum. A.Fiat. and M.Naor. Untraceable electronic cash, Advances in Cryptology-CRYPTO' 88, Springer Verlag, pp. 319-327, 1990.

[13] Steve Glassman, et al., The Millicent Protocol for Inexpensive Electronic Commerce, 4th WWW Conference, Dec. 1995

[14] http://www.zurich.ibm.com:80/Technology/security /extern/ecommerce/ikp.html:iKP(IBM)

[15] http://concert.comeng.chungnam.ac.kr/~jychang/Study/payment.html

[16] http://www.itu.ch/publications/itu-t/itux20.html :(X.509. ITUT_T Recommendation X.509: "The Directory Authentication Framwork" 1988)

[17] 박성준 : "정보보호 전문과정-전자인증", 한국정보보호센터, 1997.8

[18] Dorothy E. D., and Giovanni Maria Sacco, "Timestamps in Key Distribution Protocols", Comm. of ACM, Vol.24, No.8, pp.533-536, Aug. 1981

[19] D.Chaum, "Blind Signatures for Untraceable Payments", Advances in Cryptology-Crypto'82, Plenum Press, pp.199-203, 1983

[20] B.Pftxmann and M.Waidner, "How to Break and Repair a Provably Secure Untraceable Payment System", Advances in Cryptology, Proceedings of Crypto'91, Springer-Verleg, pp.338-350, 1991

[21] Bruce Schenier, Applied Cryptography 2nd Edition, John Wiley & Sons Inc., 1996

[22] Robin White, Public Key Authentication Framework : Tutorial, 1996. 6. http://www.ozemail.com.au/~firstpr/crypto/pkaftute.html

[23] Utah Digital Signature Act. 1996. http://www.gvnofo.state.ut.us/ccjj/digsig/dsut-act.htm

[24] 송병열, 조현규, 송유진, 이경호, 함호상"SET기반의 전자지불시스템과 보안기술",통신정보보호학회지 제7권 제3호 pp.5-21, 1997. 9.

김 성 열(Seong-Yeol Kim)

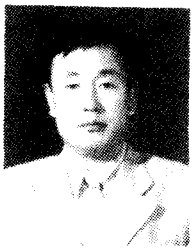
1994년 2월 조선대학교 전자계산학과(학사)

1996년 2월 조선대학교 전자계산학과(석사)

1996년 3월~현재 조선대학교 전자계산학과 박사과정

* 관심분야 : 정보보호, 네트워크, 분산시스템

이 옥 빈(Ok-Bin Lee)
1990년 2월 조선대학교 전자계산학과(학사)
1993년 2월 조선대학교 전자계산학과(석사)
1995년 3월~현재 충북대학교 전자계산학과 박사과정
* 관심분야 : 정보보호, 프로토콜 공학



배 용 근(Yong-Geun Bae)
1984년 2월 조선대학교 공과대학 컴퓨터공학과 졸업
1984년 전자계산소
현재 조선대학교 공과대학 컴퓨터공학부 조교수
* 관심분야 : 마이크로프로세서응용, 전자상거래