전자상거래 보안과 SET 프로토콜 연구

정성근*, 황종선*

*고려대학교, 컴퓨터과학기술대학원

A Study of Electronic Commerce Security and SET Protocol

Seong-keun Jeong*, Jong-sun Hwang*

*Graduate Schools of Computer Science & Technology, Korea Univ.

요 약

최근 인터넷의 급속한 발달은 개인의 생활에 많은 변화를 주었다. 새로운 환경에서 개인의 전자거래는 시장의 요구사항과 산업적 경향에 따라서 변화와 발전을 거듭하게 되었고 그 결과 전자지갑, 전자화폐, 신용카드와 같은 안전한 전자지불시스템이 필연적으로 등장하게 되었다. 하지만 국내에 도입 또는 국내에서 개발된 많은 전자지불시스템이 국산 암호알고리즘을 사용하지 않는 것이 대부분이다. 따라서, 본 논문에서는 전자지불프로토콜인 SET의 암호알고리즘 중 DES를 국내 암호알고리즘인 SEED로 대체 적용하여 실험실 모델을 설계·구현하였다.

I. 서론

인터넷 사용자의 급속한 증가는 실생활에서의 많은 변화를 가지고 왔다. 그 중에서 전자상거래에서는 사용자가 공간 및 시간 제약을 받지않고, 물건을 쉽게 구입할 수 있는 기회를 제공하였다. 또한 상거래를 위해서 필요했던 전시공간 및 관리비용을 절약하여 저렴한 구매를 가능하게 하였다. 전자상거래는 기존의 "돈"으로 표현되던 가치정보를 가상공간에서 표현해야 했고, 필연적으로 전자지불시스템이 등장하게 되었다. 최근에는 전자상거래 활성화와 발맞추어 기존 전자지불시스템의 확산 및 새로운 전자지불시스템이 등장하고 있다. 하지만, 국내에 도입 또는 국내에서 개발된 많은 전자지불시스템이 국산 암호알고리즘을 사용하지 않는 것이 대부분이다. 따라서, 본 논문에서는 기존 전자지불프로토콜인 SET의 암호알고리즘 중 DES(Data Encryption Standard)를 128-bit 키를 사용하는 국내 암호알고리즘인 SEED로 대체·적용하여 실험실 모델을 설계하고 구현하여 그 기능과 성능을 확인하였다.

본 논문의 구성은 2장에서는 기존의 전자지불 방식들을 소개하고, 간단한 특징들을 설명한다. 3장은 SET 프로토콜에 대하여 설명하고, 4장은 국내 암호알고리즘인 SEED를 적용한 실험실 모델 설계 및 구현 결과를 설명하며, 마지막으로 5장에서는 결론을 맺고 향후연구에 대하여 기술한다.

II. 관련연구

전자상거래의 발달과 더불어 많은 전자지불 시스템들이 연구되어 왔다. 또한 안전성의 향상을 위해서 많은 시스템들이 물리적 혹은 전자적인 방법들을 연구하고 있다. 특히 암호학적 연산을 이용한 시스템들이 등장하면서 많은 발전을 이룩하였다. 이러한 전자지불시스템은 가치정보의 저장 위치에 따라 전자지갑형과 네트워크형으로 크게 나뉘어 발전해 왔다. 네트워크형은 다시 전자화폐, 신용카드, 온라인 이체로 분류되어 다음과 같다.[1]

전자지갑은 사용자가 화폐가치를 가지는 정보를 은행으로부터 발급받아 개인 PC 혹은 IC

카드에 저장하는 가치 저장형으로 Mondex[2], Proton[3], Visa Cash[4] 등이 대표적인 시스템이다. 이러한 전자지급시스템은 현금을 대신하는 시스템으로 실세계의 현금을 대신한다. 장점은 익명성, 이전성, 불추적성 등이며, 단점은 사고 발생시 분쟁해결이 어렵고, 분실 및 시스템 오동작으로 가치정보를 상실할 수 있다.

전자화폐는 온라인으로 지불에 필요한 정보를 전송하여 지불을 수행하는 방식으로 eCash[5], Milicent[6]가 대표적인 시스템이다. 특징으로는 이중 사용이 방지되고 안전성이 뛰어나며 불추적성을 가진다. 발행은행의 온라인 확인과정이 필요하여 많은 시간이 소요되고 이용수수료가 비싼 것이 단점이다.

신용카드시스템은 일상생활의 신용카드를 인터넷으로 구현한 방법이며, 후불식 방식으로 SET 프로토콜[7], Cyber Cash[8], First Virtual[9]이 대표적인 시스템이다. 후불식 방식을 취하고 있어 지불에 관련된 분쟁이 발생했을 경우 분쟁해결 능력이 뛰어나고, 지불과정이 간단하여 가장 널리 사용되고 있는 지불방식이다. 단점으로는 시스템이 복잡하고 일부 시스템에서는 "이중지불"과 "신용카드 정보의 유출"로 인한 사고의 위험이 있다.

인터넷뱅킹은 금융기관과 상점이 협약을 통해 인터넷뱅킹을 이용하여 계좌이체를 수행하고 수행된 결과를 상점에 보고함으로 해서 전자지불을 수행하는 방식이다. 장점은 기존 시스템을 그대로 이용할 수 있어 수수료가 적고, 상점은 빠른 입금 확인과 현금지급이 가능하다는 점이다. 단점은 정해진 시간에만 지불이 가능하며, 현금과 같이 바로 지불되는 방식으로 분쟁이 발생하는 경우 사용자 보호에 어려움이 있다.

Ⅱ. SET 프로토콜

1. SET 개요

1996년 2월 세계적인 신용카드 회사 Visa International과 Master 카드사는 인터넷상에서 신용카드를 이용하여 대금지불을 함에 있어 개인의 정보와 재산을 보호해 줄 수 있는 안전한 방법을 찾기 위해 공동으로 연구를 시작하였고, 1997년 5월 SET1.0을 발표하였다. SET 프로토콜은 대칭적 암호화 방법인 DES와 비대칭적 암호화 방식인 RSA 및 디지털봉투를 이용하여 암호화 시간을 줄이고 해독의 가능성을 더욱 낮추었으며, 지불정보 및 주문정보에 대한 보안, 전송되는 데이터에 대한 기밀성 보장, 카드 및 카드 사용자에 대한 인증, 판매자에 대한 인증 및 각 구성요소들간의 상호 운용성을 보장해 주는 거래 프로토콜이다. 이는 전자상거래의 지불구조와 인증체계, 암호화 기술을 이용해 만들어진 종합적인 표준이다.[10, 11]

2. SET의 구조

SET의 기본적인 논리적 구조는 그림1과 같다. SET의 Entity인 구매자(Cardholder), 판매자(Merchant), 신용카드발급사(Issuer), 매입사(Acquirer) 모두가 사전에 CA로부터 공개키 인증서를 발급받아 보유하고 있어야 한다. 이 전제하에서 구매자가 판매자로부터 물품을 구입하고 전자적으로 대금을 지불하고 매입사를 통하여 처리가 이루어지게 된다.[11]

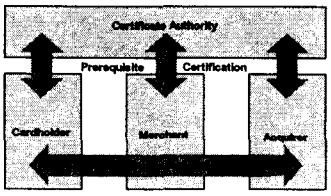

그림 1 : SET의 논리적 구성도

3. SET을 이용한 물품 구매 절차

구매자가 판매자에게서 물품을 구매할 때의 메시지 처리절차에 대해서 설명한다. 구매절차의 개략도는 그림2와 같다.[11]

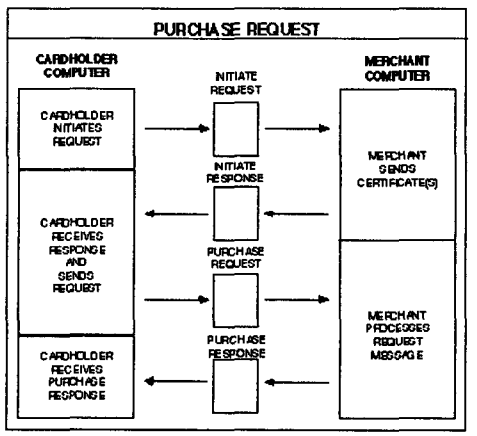

그림 2 : 구매절차 개략도

Ⅲ. 설계 및 구현

1. 실험실 모델 설계

1) 모듈별 구성

가. 실험실 모델은 구매자, 판매자, PG의 3개 모듈로 구성된다.

나. CA와 Issuer, Acquirer는 기존 SET의 규정을 그대로 준수한다.

다. 구매자, 판매자, PG는 각각 적정한 CA에 의하여, 적절한 인증서를 보유하고 있음을 전제로 한다.

2) 구매자(Cardholder) 모듈

가. 구매자 모듈은 Wallet과 Payment Process의 두 Block으로 구성되어 있다.

나. 구매자가 Wallet을 이용하여 판매자의 쇼핑몰에서 물품을 선택하고, 물품항목, 수량, 금액을 확인하여 구매처리를 선택하면 Payment Process에서 구매 관련 처리를 수행하고 그 결과를 통지한다.

다. 구매자에 대한 Class 구성은 그림3과 같다.

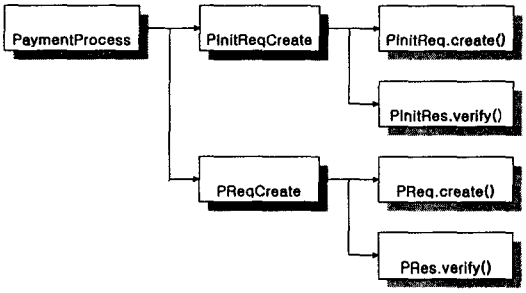

그림 3 : 구매자 Class 구성도

3) 판매자(Merchant) 모듈

가. 판매자 모듈은 Shopping Mall, Payment Process, Authenticate Process의 세 Block으로 구성되어 있다.

나. 판매자는 쇼핑몰을 운영하며, 구매자가 물품을 구입하고자 하는 경우 구매 요구 메시지를 받아 PG를 통해 구매자의 적정성 여부 파악한 후 구매완료 메시지를 구매자에게 보내고 해당 물품을 발송한다.

다. 판매자에 대한 Class 구성은 그림4와 같다.

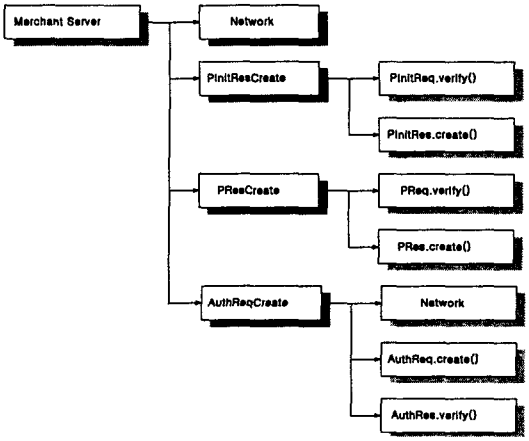

그림 4 : 판매자 Class 구성도

4) PG(Payment Gateway) 모듈

가. PG 모듈은 Network와 Authenticate Process의 두 Block으로 구성되어 있다.

나. PG는 지불브로커로서 VAN사의 기능을 수행한다. 판매자가 구매자에 대한 신용정보와 적정성 여부를 질의하면 확인후 결과를 전송하고, 판매자의 거래내역을 전송받아 Issuer와 Acquirer 간의 적절한 정산을 유도한다.

다. PG에 대한 Class 구성은 그림5와 같다.

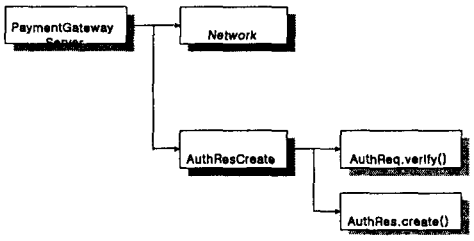

그림 5 : PG Class 구성도

2. 실험실 모델 구현

1) 시스템 개발환경

하드웨어 환경은 Windows XP 운영체제인 PentiumⅢ 555MHz, LAN Card, 256MB 메모리의 컴퓨터를 사용하였고, 소프트웨어 환경은 서비스 요청자와 서비스 제공자간의 전자지불프로토콜을 실행하기 위해서 Java가 지원되

는 운영체제와 인터넷 익스플로러6.0 이상의 인터넷 접속 소프트웨어, 서비스 요청자는 서비스 요청, 서비스 제공자는 서비스 요청을 처리하기 위해 JDK 1.3.1_01을 사용하였다.

2) 시스템 구현

가. 구매자(Cardholder) 모듈 구현

㉠쇼핑몰에서 상품의 종류와 개수를 선택하고 선택버튼을 누른다.

㉡선택한 상품의 수량과 가격을 확인한 후 SET-Initialization 파일을 다운 받아서 지정된 디렉토리에 저장한다.

㉢전자지갑을 받은 SET Initialization 파일과 함께 실행시킨다.

㉣전자지갑에서 카드에 관한 정보를 입력하고 지불 버튼을 누른다.

㉤Merchant에 필요한 정보를 전송하여 상품에 대한 지불 과정을 실행한다.

나. 판매자(Merchant) 모듈 구현

㉠MerchantServer를 실행시켜 Cardholder의 접속을 기다린다.

다. PG(Payment Gateway) 모듈 구현

㉠PaymentServer를 실행시킨후 Merchant의 접속을 기다린다.

3. 구현결과 비교분석

표 1 : 구현결과 비교

구 분		실험모델	기존 SET
구현1	지불수행시간	1,613ms	1,762ms
	메시지 길이	2,389byte	2,368byte
구현2	지불수행시간	1,672ms	1,722ms
	메시지 길이	2,389byte	2,368byte

표1에서 보는 것과 같이 기존 DES를 적용한 SET 프로토콜과 SEED를 적용한 실험모델의 구현결과를 비교한다.

먼저 지불수행시간은 SEED를 적용한 실험모델이 9.23%와 2.99%로 약간 빠르게 나타났다. 이는 테스트PC 환경이나 수행 당시 네트워크 환경에 의하여 약간의 차이가 나타난 것이지 실제로는 거의 차이가 나지 않았다.

메시지길이는 실험모델이 20byte 정도 길게 나타났다. 이는 DES를 SEED로 대체함으로써 나타난 것이다.

Ⅳ. 결론 및 향후연구

본 논문에서는 기존 전자지불 프로토콜인 SET의 암호알고리즘 중 64-bit키를 사용하는 DES를 128-bit키를 사용하는 국내 암호알고리즘인 SEED로 대체·적용하여 구현해 보았다.

기존 DES를 적용한 모델과 SEED를 적용한 실험모델은 수행속도와 메시지 길이에서 약간의 차이가 났지만, 메시지 암호화에 기존 암호학적으로 취약한 64-bit키의 DES 대신에 128-bit키인 국내 암호알고리즘인 SEED를 적용함으로써 안전성을 강화하였고, 속도상으로도 거의 차이가 없는 수준으로 설계·구현하였다.

향후에는 실험모델이 기존 SET 프로토콜의 체계속에서 움직여야 하는 단점이 있으므로 SET 프로토콜과 비슷하지만 굳이 호환될 필요가 없는 국산 전자지불 프로토콜에 대한 연구가 필요하다.

참고문헌

[1] 신종천, 박종열, 이형효, 이동익, 윤석환, "일회용 신용정보를 이용한 전자지불시스템의 설계 및 구현", 정보처리학회 논문지, 제9권 3호, 2002.6

[2] http://www.mondex.com

[3] http://www.element.be

[4] http://international.visa.com

[5] http://www.ecashtechnologies.com

[6] http://www.milicent.digital.com

[7] SET Secure Electronic Transation LLC, http://www.setco.org/setspecification.html

[8] http://www.cybercash.com

[9] http://www.fv.com/tech/greenmodel.html

[10] Visa and MasterCard, SET Secure Electronic Transation Specification, Book1 : Business Description, Version 1.0, May, 1997

[11] Visa and MasterCard, SET Secure Electronic Transation Specification, Book2 : Programmer's Guide, Version 1.0, May, 1997