한국산업정보학회논문지 제7권 제4호 (2002. 12)

지불시스템의 승인단계에서 보안방안
(Security Method for Approval Process of Payment System)

임 인 채*, 위장현**
(Lin-Chae Lim), (Jang-Hyeon Wi)

요 약 전자상거래의 지불시스템에서 전달되는 데이터는 무결성, 기밀성, 부인방지등이 확보되어야 한다. SET 프로토콜의 지불게이트웨이는 이러한 요구 조건을 충족시키기 위해 계산량이 많은 RSA 암호알고리즘을 과도하게 사용하고 있는데, 이로 인해 거래가 절정을 이루는 시간대에는 지불 게이트웨이에 과다한 비밀키 연산들이 집중되어 병목 현상이 발생하게 된다. 이러한 문제를 해결하기 위하여 SET 프로토콜의 지불시스템 승인단계에서 원타임패스워드를 적용하는 방안을 제안하고자 한다.

Abstract Payment systems in EC need confidentiality, integrity, non-repudiation. All transactions between cardholders and merchants must be authorized by a payment gateway in SET protocol. RSA secret key operation which requires heavy computation takes the most part of the time for payment authorization. For the reason, a heavy traffic of payment authorization requests from merchants causes the payment gateway to execute excessive RSA secret key operations, which may cause the bottleneck of the whole system. To resolve this problem, One-Time Password technique is applied to payment authorization step of the SET protocol.

1. 서 론

전자상거래에서 거래정보의 보안 수준은 거래의 내용에 따라 다양하게 요구될 수 있으나, 지불시스템 분야에서는 인증과 무결성, 기밀성, 가용성, 신뢰성 등이 보장되어야 한다. 현재 사용되어지는 지불시스템에서 보안은 주로 암호화를 통해 구현되며, 이때 사용되는 암호화 방법으로는 패스워드시스템, 공유키 방식의 암호화, 공개키 방식의 암호화 등이 활용되고 있다.

이와 같이 전자상거래에서는 모든 거래내용에 대해 다양한 방법으로 암호화를 하고 있으며, 강력한 사용자 인증과 더불어 지불에 대한 정보의 보호를 필수적으로 요구하고 있다.

이를 위해 Visa와 Master 카드사는 SET (Secure Electronic Transaction) 프로토콜이라는 신용카드 기반의 전자상거래 지불시스템을 개발하여 발표하였다[1,2]. 하지만 SET 프로토콜은 거래 절차의 단계가 복잡하여 처리시간의 지연과 시스템의 부하증가 등의 문제점을 다소 내포하고 있다.

따라서 본 연구에서는 SET 프로토콜의 거래단계를 분석하여, SET 프로토콜이 가지고 있는 문제점과 지불시스템에 있어 거래정보의 보호를 위한 요구사항을 검토한 후, 승인 단계에서의 보안 방법으로 원타임 패스워드를 적용하는 방안을 제시하여, 거래절차의 단순화와 처리시간의 단축 그리고 사용자 인증 및 암호화를 구현하고자 한다.

2. 관련연구

2.1 암호기술

(1) DES 암호화 방식

DES 암호화 방식은 대표적인 대칭적 알고리즘으로서 정보의 암호화와 해독에 64 Bits (56 Bits + 8

* 대경대학 컴퓨터통신계열 전임강사
** 두산중공업 (재무)정보운영팀

Bits의 패리티)의 동일한 키를 사용한다. 정보를 교환하는 양측이 암호화에 사용된 키를 서로 상대방에게 교환하는 방식이다. 하지만 거래의 대상이 불특정 다수일 경우에 그만큼 키를 만들어야 하므로 현실적으로 매우 비효율적인 방법이라 할 수 있다.

(2) RSA 암호화 방식

RSA 알고리즘은 개인키와 공개키를 이용한 방법으로, 제안자 이름을 따서 RSA(Rivest, Shamir, Adoleman)라고 붙여졌다. 이 알고리즘은 개인키와 공개키를 이용하는데, 공개키로 암호화 된 문장은 공개키에 대응하는 개인키를 이용하여 해독할 수 있다. 또한 개인키로 암호화 할 경우에도 대응되는 공개키를 이용하면 원문을 재생할 수 있다.

2.2 원타임패스워드

원타임패스워드는 인터넷을 포함한 네트웍 시스템에 접근하는데 있어 안전성을 보장하여 줄 수 있다. 보통의 경우 시스템에 로그인 하기위해서는 동일한 패스워드를 매번 사용하는 현재의 로그인 체계에서 불법적인 방법으로 네트웍 도청을 통하여 계정과 패스워드를 쉽게 알아낼 수 있으며, 부정사용이 언제든지 가능하다. 하지만 원타임패스워드는 시스템에 로그인 할 때마다 다른 패스워드를 사용하기 때문에 이러한 문제점을 해결할 수 있으며, 한번 사용된 패스워드는 재사용이 불가능하여 불법적인 방법으로 계정과 패스워드를 알아냈다 할지라도 시스템에 대한 접근을 허용하지 않는다[5].

원타임패스워드의 구현 방법으로는 다음과 같은 것이 있다.

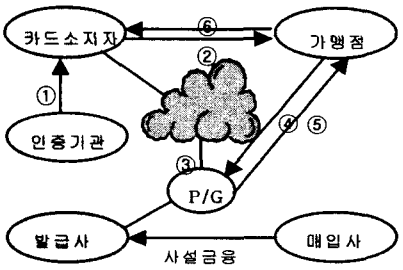
① 동기화 된 시간을 유지한 타임 스탬프 이용
② 클라이언트와 서버가 가지고 있는 임의의 패스워드리스트 위치를 동기화 하여 패스워드 사용
③ 시퀀스 생성기의 상태를 동기화 하여 임시적인 시퀀스 넘버를 사용
④ 챌린지 응답 스킴을 이용

위에서 언급된 방법 중 챌린지 응답스킴은 비교적 복잡성이 덜하고 안전성이 높으며 구현 방법이 쉽다. 챌린지 응답스킴의 인증절차는 먼저 사용자가 인증을 요구하면, 서버는 임의의 챌린지를 생성해 사용자에게 전송한다. 그리고 사용자는 PIN(Personal Identification Number)과 챌린지를 이용하여 서버에 전송할 원타임패스워드를 생성하고, 서버에게 응답 메시지를 전송한다. 그리고 서버는 동일한 챌린지와 등록된 사용자의 정보를 이용해 원타임패스워드를 생성한 후 사용자가 전송한 응답과 비교하여 사용자 인증을 해주는 방식이다.

2.3 지불시스템 승인절차

(1) SET 프로토콜 개요

SET 프로토콜은 인터넷에서 신용카드를 이용하여 대금을 지불함에 있어 개인의 정보와 재산을 보호해줄 수 있는 방안으로 규격화한 신용카드 기반의 전자상거래 프로토콜이며, 카드소지자, 가맹점, 지불게이트웨이 그리고 매입사등으로 구성된다. 먼저 카드 소지자는 가맹점의 쇼핑몰에서 상품을 검색한 후 상품을 주문하며, 가맹점은 지불게이트웨이에게 상품 주문에 대한 지불 승인을 요청하게 된다. 카드소지자와 가맹점 간의 모든 거래에 대해 지불게이트웨이는 지불승인과 지불교환 처리를 수행한다. 매입사는 가맹점과 계정을 체결하고, 카드결제와 지불을 관리하는 신뢰할 수 있는 은행 및 기관의 지불게이트웨이를 활용한다. [그림 1]에서는 SET 프로토콜의 구성 및 거래절차를 보여주고 있다[11].



① 인증서
② 주문
③ 인증 요구
④ 카드소유자 인증
⑤ 거래정산 요구
⑥ 배달

[그림 1] SET의 구성 및 거래절차

(2) 지불절차

[그림 1]의 SET 구성 및 거래절차에서 카드 소지자와 가맹점 사이에 상거래가 이루어질 경우 가맹점은 카드소지자와의 거래에 대한 지불승인 받기 위해 지불시스템에게 지불승인 요청을 하게 되며, 지불시스템은 지불승인 요청 정보를 분석하여 정당한 거래인지를 검사하고, 정당할 경우 지불승인 응답서와 캡쳐토큰을 가맹점에 보내준다. 이 과정에서 지

불시스템의 지불승인 작업은 지불승인 요청정보 검사와 지불승인 응답정보 작성의 단계로 구성 된다.

지불승인 요청정보는 가맹점이 지불게이트웨이에 보낸 지불승인 요청서와 카드소지자의 지불명령서로 이루어 진다. 카드소지자는 부인방지와 무결성 확보를 위해 지불명령서를 해쉬하여 자신의 RSA 비밀키로 서명한다. 그리고 지불 명령서에 임의의 시메트릭키(s-key #1)를 생성하여 DES로 암호화하며, 이 키는 지불게이트웨이의 RSA 공개키로 암호화 된다. 한편, 가맹점은 지불승인 요청서를 작성한 후 이를 해쉬하여 자신의 RSA 비밀키로 서명하고, 임의의 시메트릭키(s-key #2)를 생성한 다음 DES로 암호화하여 지불게이트웨이의 RSA 공개키로 암호화 한다.

지불게이트웨이는 지불승인 요청서를 검증하여, 무결성과 정상적 거래가 확인되면 지불승인 응답서와 나중에 지불교환을 위해 사용할 캡처 토큰을 작성하여 가맹점에게 보낸다. 지불게이트웨이는 지불승인 응답서와 캡쳐토큰을 해쉬하여 자신의 RSA 비밀키로 각각 서명한다. 또한 지불승인 응답서는 임의의 시메트릭키(s-key #3)를 생성하여 DES로 암호화하며, 이 키를 가맹점의 RSA 공개키로 암호화 한다. 캡쳐토큰도 임의의 시메트릭키(s-key #4)를 생성하여 DES로 암호화를 하지만, 이때 사용된 키는 자신의 공개키로 암호화 한다. 지불승인 요청정보 검사와 지불승인 응답정보 작성절차는 다음과 같다[12].

① 지불게이트웨이는 자신의 RSA 비밀키로 가맹점이 생성한 시메트릭키(s-key #2)를 복호화
② 복호화된 시메트릭키(s-key #2)를 이용하여 DES로 암호화된 지불승인 요청서를 복화화
③ 지불승인요청서를 가맹점 RSA 공개키로 검증
④ 지불게이트웨이는 자신의 RSA 비밀키로 카드소지자가 생성한 시메트릭키(s-key #1) 복호화
⑤ 복호화된 시메트릭키(s-key #1)을 가지고 DES로 암호화된 지불명령서를 복호화
⑥ 지불명령서를 카드소지자 RSA 공개키로 검증
⑦ 지불게이트웨이는 지불승인 응답서를 자신의 RSA 비밀키로 서명
⑧ 지불승인응답서를 시메트릭키(s-key #3)를 이용하여 DES로 암호화
⑨ 이 시메트릭키(s-key #3)를 가맹점의 RSA 공개키로 암호화
⑩ 지불게이트웨이는 캡쳐토큰을 자신의 RSA 비밀키로 서명
⑪ 캡쳐토큰을 시메트릭카(s-key #4)를 이용하여 DES로 암호화
⑫ 이 시메트릭키(s-key #4)를 자신의 RSA 공개키로 암호화

위의 절차에서 볼 수 있듯이 지불승인 단계(요청, 응답)를 종합해 보면, 지불승인은 크게 4번의 RSA 비밀키 연산과 4번의 RSA 공개키 연산 그리고 4번의 DES 암호연산을 수행하고 있음을 알 수 있다. 결국, 지불게이트웨이는 지불승인 작업의 대부분 시간을 RSA 비밀키 연산에 사용하고 있음을 알 수 있다. 따라서 이를 개선하기 위해 SET 프로토콜의 지불승인 단계에서 원타임패스워드를 적용할 수 있는 방안을 검토한다.

3. 지불시스템 승인단계에서의 보안방안

3.1 지불승인 단계의 문제점 및 요구사항

전자상거래의 지불시스템에서 카드소지자, 가맹점, 지불게이트웨이 사이의 모든 데이터들은 전송중 데이터 손실이나 다른 의도에 의해서 도용 또는 추가되는 경우를 방지해야 한다. 또한 가맹점은 카드소지자의 신용카드 정보 등을 변조할 수 없어야 하기 때문에 카드소지자, 가맹점, 지불게이트웨이 사이의 데이터 무결성은 반드시 확보 되어야 한다.

또한 카드소지자와 가맹점의 정보는 전송도중 노출이 되더라도 데이터의 내용이 무엇인지 알 수 없어야 하며, 가맹점은 카드소지자의 개인신상 정보를 알고 이를 도용할 수 있기 때문에 데이터의 기밀성 또한 확보되어야 한다.

SET 프로토콜에서는 위의 조건들을 보장하기 위해서 많은 RSA 알고리즘을 사용하고 있다. SET 프로토콜의 지불시스템은 모든 거래에 대하여 지불승인과 지불교환을 처리해야 하는데, 지불승인과 지불교환은 계산량이 많은 RSA 비밀키 연산이 대부분을 차지하고 있다. 그리고 상품 구입 거래가 절정을 이루는 시간대에는 지불게이트웨이에 과다한 지불승인 요청과 지불교환 요청이 발생하여, 결국 지불시스템에 과다한 RSA 비밀키 연산들이 집중됨으로써, SET 프로토콜에 병목현상이 발생하게 된다. 이러한 지불시스템의 지불승인 과정에서 과다한 RSA 비밀키 연산으로 인한 부하를 줄이기 위한 방법은 다음과 같다.

① 지불게이트웨이를 여러개 노드에 분산시키는 방법
② 지불게이트웨이를 threshold 기법을 이용하여 여러개의 노드에 분산시키는 방법
③ 서버지원 RSA 방법

먼저 지불게이트웨이를 여러개의 노드에 분산 시키는 방법은 가장 쉽게 생각할 수 있는 방법이지만, 많은 추가적인 문제를 해결해야 한다. 여러 개의 노드들에 비밀키를 분산하게 되므로, 중복된 키의 일관성, 분배, 분산된 노드들의 신뢰성 등의 많은 문제를 가지고 있다.

그리고 지불게이트웨이를 threshold 기법을 이용하여 여러개의 노드에 분산하는 방법은 RSA 비밀키를 n개의 share로 분해하고, 이들 share를 각 노드들에게 나누어 준다. 나중에 키를 알고 싶을 때는 t개 이상의 노드들이 모여야 하는 방법이다. 이 방법은 지불게이트웨이를 여러개의 노드에 분산 시키는 방법과 비교해 볼 때, 특별한 키 관리가 필요 없지만 threshold 스킴 자체의 큰 오버헤드 때문에 역시 적용이 어렵다.

서버지원 RSA 방법은 클라이언트가 비밀키 d를 알려주지 않으면서 계산보조 서버의 도움으로 RSA 비밀키 연산(M = Cd mod n)을 빨리 하도록 하는 방법이다. 그런데 이 스킴은 계산 보조 서버의 성능이 클라이언트에 비해 월등히 높은 경우에만 효과를 볼 수 있다.

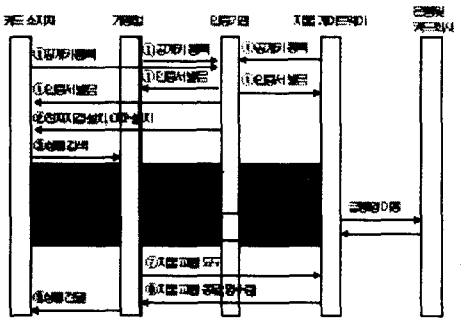
따라서 위와 같은 문제점을 해결하고 지불시스템의 요구 조건을 충족시키기 위해, 전자서명에는 RSA 암호알고리즘을 이용하고, 기밀성 확보에는 원타임 패스워드를 암호화키로 하여 DES 알고리즘을 이용함으로써, SET 프로토콜의 지불승인 과정에서 비밀키 연산 횟수를 줄이는 방안을 제시 하고자 한다.

3.2 원타임패스워드 적용방안

여기서는 앞서 살펴 보았던 카드소지자, 가맹점, 지불 게이트웨이 사이에 전송되는 데이터의 무결성과 기밀성 그리고 거래 당사자의 부인 방지를 확보하면서, SET 프로토콜의 지불승인 절차에 병목 현상을 개선 하기 위한 원타임 패스워드의 적용 방안을 제안한다.

[그림 2]는 SET 프로토콜 처리흐름 및 OTP 적용부문을 보여주고 있으며, 각 단계별 세부 내용 및 순서는 다음과 같다

① 카드소지자, 가맹점, 지불게이트웨이는 인증기관에 등록, 인증서를 발급
② 카드소지자는 전자지갑과 원타임패스워드 생성기를 설치
③ 카드소지자는 구매할 상품정보를 검색하고, 가맹점과 지불게이트웨이의 공개키 그리고 챌린지를 확보
④ 카드소지자는 주문정보와 지불명령서를 가맹점에게 전송
⑤ 가맹점은 카드소지자로부터 받은 주문 정보를 검증하고, 지불승인 요청서와 카드 소지자로부터 받은 지불 명령서를 가맹점에게 전송
⑥ 지불게이트웨이는 금융망을 통해 카드 소지자가 정당한 거래자인지를 확인하고, 지불승인 응답서와 캡처토큰을 가맹점에 전송
⑦ 가맹점은 지불게이트웨이에 정산요청
⑧ 지불게이트웨이는 정산처리를 수행
⑨ 거래가 허가되면 주문을 이행



[그림 2] SET 프로토콜 처리흐름과 OTP 적용부문

원타임패스워드의 적용을 위해 지불승인 절차를 초기설정 작업, 카드소지자의 정보전송, 가맹점의 정보처리, 그리고 지불게이트웨이의 정보처리와 지불승인 응답 등의 다섯 단계로 분류하고 지불승인과 응답절차에서의 세부 적용 방안을 제시 하고자 한다

(1) 초기작업 설정

카드소지자, 가맹점, 지불게이트웨이는 인증기관으로부터 인증서와 전자지갑, 원타임패스워드 생성기를 발급 받고 설치한다. 그리고 카드소지자는 가맹점에서 상품검색 후 거래를 위해 가맹점과 지불게이트웨이의 공개키와 원타임패스워드 생성을 위한 챌린지를 공급 받는다.

(2) 카드소지자의 정보전송

카드소지자는 상품을 구매하기 위하여 가맹점의 쇼핑몰에서 상품을 검색한 후 구매정보를 작성하여 가맹점에 보낸다. 이때 구매정보는 기밀성, 무결성, 부인방지가 확보되어야 한다. 따라서 주문정보에 대한 기밀성 확보를 위해서는 원타임패스워드를 암호화키로 하고 DES로 암호화하여 가맹점만 주문정보를 확인할 수 있게 한다. 그리고 지불명령서에 대한 기

밀성 제공을 위해 임의의 시메트릭 키를 생성하여 DES로 암호화한 후, 이 시메트릭 키를 지불게이트웨이의 공개키로 암호화하고 지불게이트웨이만이 지불명령서를 확인할 수 있게 한다. 또한 구매 정보와 지불명령서를 각각 해쉬하고 이들을 연결한 다음 다시 해쉬하여 이중서명을 함으로서 무결성을 확보한다.

(3) 가맹점의 정보처리

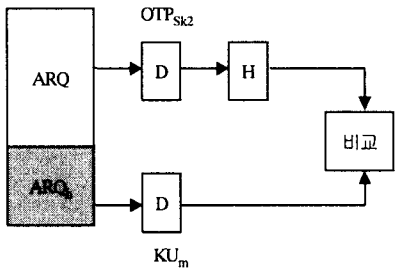
가맹점은 카드소지자로부터 전송된 주문정보에 대한 무결성을 검증한 후 가맹점에서 작성한 승인요청서와 카드소지자로부터 받은 지불명령서를 지불게이트웨이로 전송한다. 이때 가맹점은 주문정보만 접근이 가능하고 카드소지자의 개인정보나 상품에 대한 견적서 등은 위조할 수 없어야 한다. 가맹점은 인증데이터베이스에 저장된 챌린지와 카드소지자의 식별자를 이용하여 원타임패스워드를 생성하고, 이 키로서 카드소지자의 주문정보를 복호화 하여 가맹점에서 이용한다. 그리고 복호화된 주문 정보의 무결성을 검증하기 위해 주문정보의 해쉬값과 해쉬된 카드소지자의 지불명령서를 다시 해쉬하고, 카드소지자의 공개키로 이중서명 된 메시지 다이제스트와 비교한다. 주문정보의 복호화 과정에서 원타임 패스워드를 이용 함으로서 가맹점의 RSA 비밀키 연산 횟수를 1회 줄일 수 있다.

(4) 지불게이트웨이의 정보처리

지불게이트웨이는 가맹점으로부터 전달된 지불 승인요청 정보를 확인하고, 금융망을 이용하여 은행이나 신용카드 회사로부터 카드소지자의 신분을 확인한 후 지불승인 응답 메시지를 가맹점에게 발급한다. 지불게이트웨이의 정보 확인 절차는 가맹점의 지불승인 요청서(ARQ)에 대한 검증과 카드 소지자의 지불 명령서(PI)에 대한 검증의 두 단계로 구분되어 이루어 진다. 먼저 지불게이트웨이는 가맹점으로부터의 지불 승인 요청서를 검증하게 되는데, [그림 3]은 지불게이트웨이의 지불승인 요청서에 대한 무결성 검증 흐름도를 보여주고 있다.

그리고 지불승인 요청서에 대한 지불게이트웨이의 무결성 검증 절차는 다음과 같다.

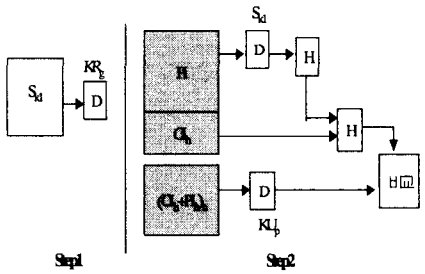
-. 지불승인 요청서에 대한 새로운 메시지 다이제스트 생성
: h(DOTPsk2[EOTPck2[ARQ]]) OTP 적용
-. 지불승인 요청서 메시지 다이제스트
복호화 : DKUm[EKRm[h(ARQ)]]
-. 위의 둘을 비교하여 무결성 검증



[그림 3] 지불승인요청서의 무결성검증 흐름

지불승인요청서 무결성 검증절차에서 지불게이트웨이는 가맹점으로부터 전달 받은 메시지의 검증을 위해 인증데이터베이스에 저장된 챌린지를 이용하여 원타임패스워드를 생성하고, 이를 복호화키로 사용하여 지불승인요청서를 복호화 한다. 또한 지불승인요청서를 해쉬한 새로운 메시지 다이제스트와 가맹점의 공개키로 복호화한 지불승인요청서의 메시지 다이제스트를 비교함으로써 전달정보가 도중에 불법적으로 수정되지 않았음을 확인한다.

가맹점과 지불게이트웨이 사이에 지불승인 요청서의 기밀성 제공을 위해 RSA 알고리즘을 사용하는 대신 원타임패스워드를 암호화키로 사용하여 DES 알고리즘을 이용함으로써 지불 게이트웨이의 RSA 비밀키 연산수행 횟수를 1회 줄일 수 있다. 또한 지불게이트웨이는 카드 소지자의 지불명령서를 검증하게 되는데, [그림 4]는 지불게이트웨이의 지불명령서 무결성 검증 흐름도를 보여주고 있다.



[그림 4] 지불명령서의 무결성검증 흐름

아울러 지불명령서에 대한 지불게이트웨이의 무결성 검증절차는 다음과 같다.

-. 시메트릭 키의 복호화 : DKRg[EKUg[Sk1]]
-. 새로운 이중서명 생성

: h(h(DSk1[E Sk1[PI]]) ‖ h(PI))

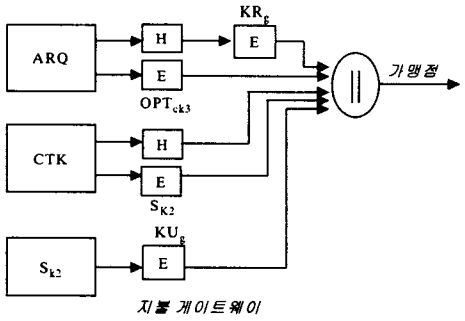
-. 이중서명 복호화 : DKUp[EKRp[h(OI h+PI h)]

-. 위의 새로 생성한 이중서명과 복호화 된 이중 서명을 비교하여 무결성 검증

지불명령서 무결성 검증절차에서, 지불게이트웨이는 카드소지자가 생성한 지불명령서를 복호화하기 위해 지불게이트웨이의 RSA 비밀키를 이용하여 지불명령서 암호화에 사용한 시메트릭키를 복호화 한다. 그리고 이 시메트릭키를 이용하여 지불명령서를 복호화하고 이 원문 메시지에 대한 해쉬값과 주문정보의 메시지 다이제스트를 연결하여 다시 해쉬한 새로운 메시지 다이제스트와 가맹점으로부터 전달 받은 이중 서명된 메시지를 카드소지자의 공개키로 복호화하여 비교함으로써 메시지의 무결성을 검증한다.

(5) 지불게이트웨이의 지불승인 응답

지불게이트웨이는 가맹점으로부터 전달 받은 지불명령서에 대한 내용 검증과 은행이나 신용카드 회사로부터 카드소지자의 신분을 확인한 후 가맹점에게 지불승인 응답 메시지와 캡쳐 토큰을 생성하여 전달한다. 지불게이트웨이의 지불승인 응답 흐름도는 [그림 5]와 같다.



[그림 5] 지불승인 응답 흐름

지불게이트웨이 정보의 기밀성, 무결성, 부인방지 확보 절차는 다음과 같다.

-. 기밀성 OTP 적용

: EOTPck3[ARP] ‖ ESk2[CTK] ‖ EKUg[Sk2]

-. 무결성 및 부인방지

: EKRg[h(ARP)] ‖ h(CKT)

위의 절차에서는 지불게이트웨이가 지불승인 응답 메시지를 해쉬하여, 이를 지불게이트웨이의 비밀키로 전자서명 하고 있음을 보여주고 있다. 그리고 지불승인 응답 메시지 원문은 원타임 패스워드를 이용하여 암호화 한다. 또한 캡쳐 토큰을 생성한 후 임의의 시메트릭키를 이용하여 암호화하고, 이 시메트릭키를 지불게이트웨이의 공개키로 암호화하여 가맹점으로 전송한다. 그리고 가맹점에서는 나중에 이 캡쳐 토큰의 정산 처리를 위해 사용하게 된다. 지불승인 응답서의 암호화 과정에서 원타임 패스워드를 암호화 키로 이용하여 DES로 암호화 함으로써 지불게이트웨이의 RSA 비밀키 연산 수행 횟수를 1회 줄일 수 있다.

4. 평 가

원타임 패스워드를 적용한 후의 SET 프로토콜에서 지불승인 요청정보 검사와 응답정보 작성 절차는 다음과 같다.

① 지불게이트웨이는 원타임패스워드를 암호화키로 사용하여, DES로 암호화된 지불승인 요청서를 복호화

② 지불승인 요청서를 가맹점의 RSA 공개키로 검증

③ 지불게이트웨이는 자신의 RSA 비밀키로 [그림 4]의 시메트릭키(s-key #1)를 복호화

④ 이 시메트릭키(s-key #1)를 가지고 DES로 암호화된 지불명령서를 복호화

⑤ 지불명령서의 메시지 다이제스트를 카드 소지자의 RSA 공개키로 검증

⑥ 지불게이트웨이는 지불승인 응답서를 자신의 RSA 비밀키로 서명

⑦ 지불승인 응답서에 원타임패스워드를 암호화키로 사용하여, DES로 암호화

⑧ 캡쳐 토큰을 [그림 5]의 시메트릭키(s-key #2)를 이용하여 DES로 암호화

⑨ 이 시메트릭키(s-key #2)를 자신의 RSA 공개키로 암호화

위의 절차에서 볼 수 있듯이 지불승인 단계(요청, 응답)를 종합해 보면, 지불승인은 크게 2번의 RSA 비밀키 연산, 3번의 RSA 공개키 연산 그리고 4번의 DES 암호연산을 수행하고 있음을 알 수 있다. [표 1]은 원타임패스워드를 적용하였을 때와 적용전의 SET 프로토콜에서 지불 게이트웨이의 지불승인 처리결과를 보여 주고 있다. 이는 원타임패스워드를 적용하였을 때 지불게이트웨이의 복호화와 서명의 RSA 비밀키 연산이 각각 2회에서 1회로 감소 하였음을 알 수 있다. 이와 같이 지불승인 과정에서 대부분의 시간(96%)을 점유하는 RSA 비밀키 연산의 수행 횟수를 줄임으로서 지불게이트웨이의 병목현상을 줄일 수 있다. 하지만 원타임패스워드를 적용함

으로써, 가맹점이나 지불 게이트웨이도 키 관리에 대한 부담을 추가로 가지게 되었다.

[표 1] 개선 전후의 성능 비교표

구 분		개선전	개선후
RSA 비밀키 연산	Decryption	2회	1회
	Signature	2회	1회
RSA 공개키 연산	Decryption	2회	1회
	Signature	2회	2회
DES 연산	Decryption	2회	2회
	Signature	2회	2회

5. 결 론

SET프로토콜은 무결성, 기밀성, 부인방지등의 확보를 위해 계산량이 많은 RSA 암호알고리즘을 과도하게 사용함으로써 거래가 절정을 이루는 시간대에는 지불게이트웨이에 과다한 비밀키 연산이 집중되어 병목현상이 발생한다.

따라서 본 연구에서는 이러한 문제점을 해결하기 위한 방안으로 SET 프로토콜의 지불승인 절차에 원타임패스워드를 적용하면 지불승인 절차의 복잡성과 처리시간의 지연, 시스템의 부하 증가 등을 해결할 수 있다는 확인하였다.

앞으로, 제안된 원타임패스워드시스템 적용방안을 NON-SET 부문의 프로토콜에 확대 적용하는 방안에 대한 연구가 필요하다.

참 고 문 헌

[1] SET Secure Electronic Transaction Specifi- cation, Book 1 : Business Description, Version 1.0, May 31, 1997.

[2] SET Secure Electronic Transaction Specifica- tion, Book 3 : Formal Protocol Definition, Version 1.0, May 31, 1997.

[3] ANSI X3.92, American National Standard for Data Encryption Algorithm, American Nation- al Stand Institute, 1981

[4] R. Rivest and A. Shamir, Adleman, A method for obtaining digital signatures and public key cryptosystem, Communications of the Associ- ation of Computer manufactures, vol.21, no.2, pp.120-126, Feb. 1978.

[5] A One-Time Password System, rfc193.

[6] 임신영, 권도균, 전자상거래 보안, 정보과학지, 제15권, 제4호, 1997년 4월.

[7] 박희운 외, 암호기술, 한국정보처리학회지, VOL. 7, NO. 1, 2000년 3월.

[8] 송용욱, 전자상거래보안과 SET, 한국과학기술원

[9] 송익진 외, 인터넷 전자상거래 지불시스템, 멀티미디어 연구소, 1998년 3월

[10] 임인채, 위장현, 원타임 패스워드 시스템을 적용한 지불시스템 모델, 한국정보처리학회지, VOL. 7, NO. 1, 2000.4.

[11] 임인채, 전자상거래를 위한 지불프로토콜의 통합모델정보처리학회 추계학술발표논문집, VOL. 6, NO. 2, 1999

[12] 위장현, SET 프로토콜에 원타임패스워드 적용방안, 2000

임 인 채 (Lim, Lin-Chae)
1993년 경남대학교 전자계산학과 (학사)
1995년 경남대학교 경영대학원 (석사)
2001년 창원대학교 대학원(석사)
2002- 전남대학교 대학원 박사과정
1994년 삼성SDS 네트웍센터
1995년 한국중공업 정보관리실
2002- 대경대학 컴퓨터통신계열 전임강사
관심분야 : 정보보안, 방화벽, 소프트웨어공학

위 장 현 (Wi, Jang-Hyeon)
1991년 조선대학교 컴퓨터공학과 (학사)
2000년 창원대학교 대학원(석사)
1991- 한국중공업(두산중공업) (재무)정보운영팀
관심분야 : 정보보안, 네트워크