SKP기반 SET프로토콜의 Petri Nets를 이용한 분석

송 유 진[†] · 서 미 경[††] · 이 종 근[†††]

요 약

SET은 전자상거래에 있어서 가장 많이 사용되고 있는 결재 시스템 규약 중의 하나이다. 그러나 전자상거래에서 실질적인 배달이나 배달 확인과정에 대해서는 SET은 고려하고 있지 않다. 따라서 본 논문에서는 배달이나 배달 확인에 의한 지불에 대한 보안성을 좀 더 높여주는 SKP(Secure Key Protocol)를 제안한다. 그리고 Petri Nets 모델링 방법을 이용하여, SKP를 적용한 SET 모델의 적합성 여부를 증명한다.

Analysis Using Petri Nets for SKP-based SET Protocol

Yu-Jin, Song[†] · Mi-Kyoung, Seo[††] · Jong-Kun, Lee[†††]

ABSTRACT

SET is one of the useful protocol for credit payment in the Electronic market. Since, the delivery problem is conformed to delivery cooperation not payment problem, the classic SET protocol didn't consider about the certification of delivery. But the environment of electronic market be changed to manage the sold, delivery and payment etc.. In this paper, based on this consider, we propose a new SET protocol which has an function to verify the delivery based on SKP and verify it after analyzed by Petri nets. Specially, we consider SKP between Customer, Merchant, and Acquirer for improve the verify function.

키워드 : SET, SKP(Secure Key Protocol), Petri Nets, 전자상거래, 프로토콜

1. 서 론

컴퓨터와 네트워크가 등장하고 발전함에 따라, 인간의 생활상에는 단기간에 많은 변화를 가져오고 있다. 이러한 변화에서 근래에 대두되고 있는 것이 전자상거래 시스템의 등장 및 발전 양상이다. 대부분의 변화 요소가 그러하듯이 전자상거래 시스템의 등장 또한 단순한 컴퓨터와 네트워크의 발전에 기인한 결과물은 아니다. 전자상거래 시스템의 등장은 다각적인 요소가 복합적으로 작용하여 이루어진 결과물이다. 전자상거래에 대해 가장 일반적인 해석은 북미의 AIAG(Automotive Industry Action Group)에서 언급한 것으로, 거래 당사자간 비즈니스 관계의 효과성 증진을 위하여 진보된 정보기술의 지원을 받아 비즈니스 비전을 가능하게 하는 것이라고 정의하고 있다[1, 2]. 이러한 전자상거래를 위해 Visa와 Master 카드사에서는 신용카드 기반의 전자상거래 프로토콜 SET(Secure Electronic Transition)을 개발 발표하였다[3,4]. 개방형 통신망에서 가장 안전하고 효율적인 신용카드 기반의 전자지불 프로토콜인 SET은 정보의 기밀성, 결제정보의 무결성, 카드 및 카드소지자, 상점에 대한 인증, 구성요소들 간의 상호운용성(Interoperability)을 보장해 준다. 하지만, SET은 전자상거래 과정 중 실질적인 배달과 배달 확인에 의한 지불과정이 포함되어 있지 않다. 그래서 가맹점이 돈만 받고 구매자에게 상품을 배달하지 않아도 이에 대한 확인이나 재재 조치가 없어, SET프로토콜의 큰 단점으로 지적되고 있다. 단지, SET은 카드나 회원정보에 대한 인증, 또는 구매와 지불에 대한 정보를 전송하는데 보안성을 가지고 수행해주는 프로토콜이다.

따라서 본 연구에서는 이러한 배달과정이나 지불에 대해 좀 더 보안성을 가지고 수행할 수 있도록 새로운 SKP(Secure Key Protocol) 기반의 SET프로토콜을 제안하고자 한다. 그리고 이러한 SKP 기반의 SET프로토콜의 흐름을 Petri Nets 모델을 이용해 분석하여, 모델의 적합성 여부를 증명하고자 한다.

2. Petri Nets

패트리 네트는 다양한 시스템에 적용할 수 있는 수학적인 도구며, 그래프를 이용하여 그 흐름 활동을 표현하고 분석하는데 효과적인 모델링 도구이다. 또한, 패트리 네트

† 준 회 원 : 창원대학교 교수
†† 정 회 원 : 창원대학교 산업대학원 컴퓨터공학과
††† 종신회원 : 창원대학교 컴퓨터공학과 교수
논문접수 : 2001년 2월 28일, 심사완료 : 2001년 7월 19일

는 시스템에서의 비동기적이고 불확실한 이산적인 사건을 모델링하고, 모니터하며 분석하는데 매우 유용하므로, 병렬 시스템이나 통신 프로토콜, 유연 생산 시스템과 같이 병행적으로 일어나는 시스템을 모델링하고 분석하는데 사용될 수 있다.

일반적인 시스템의 모델링에 쓰이는 패트리 네트는 마크트 패트리 네트(Marked Petri Nets : MPN)이며 다음과 같이 정의한다[5, 6].

MPN = (P, T, I, O, M_0)

여기에서

P = p1, p2, ···, pn : 플레이스의 유한 집합 (n ≥ 0)
T = t1, t2, ···, tm : 트랜지션의 유한 집합 (m ≥ 0)
I(tj∈T → I(tj)∈P) : 트랜지션의 입력 함수
O(tj∈T → O(tj)∈P) : 트랜지션의 출력 함수
M_0 : P→0, 1, 2, 3,··· : 초기 마킹

이때 플레이스(place)는 시스템의 상태(state) 혹은 조건(condition)을 나타내며 원으로 표시한다. 트랜지션(transition)은 시스템의 상태를 변화시키는 동작(event)을 나타내며 선으로 표시한다. 아크(arc)는 흐름으로서 화살표로 표시하고, 토큰(token)은 플레이스의 조건의 진위 또는 시스템의 가용 자원을 나타낸다. 따라서, 토큰은 시스템의 동적이며 병행적인 동작의 특성을 나타내기 위해 사용되며, 동작이 일어나도록 하는데 필요한 조건을 만족할 경우 플래이스에 토큰을 위치시킴으로써 표현한다. 트랜지션은 자신에게로 입력되는 모든 플레이스가 토큰을 보유하고 있어야 점화(fire)될 수 있고, 트랜지션이 점화되면 자신의 각 입력 플레이스로부터 토큰을 하나씩 제거하고 각 출력 플레이스에 토큰을 하나씩 첨가한다. 따라서 토큰의 수와 위치는 패트리 네트를 실행하는 동안 바뀌게 된다.

이러한 마크트 패트리 네트는 다음과 같은 기본적인 성질을 가진다[7].

1) 안전성 (Safeness)

플레이스에서 토큰의 수가 1개를 초과하지 않으면, 패트리 네트의 플레이스는 안전하다. 트랜지션은 모든 출력 플레이스가 비어 있지 않으면 점화할 수 없으므로 패트리 네트는 안전하며, 또한 네트의 모든 플레이스들이 안전하면 패트리 네트는 안전하다.

2) 유한성 (Boundedness)

플레이스에서 토큰의 수가 k개를 초과하지 않으면 플레이스는 k-유한하다. 패트리 네트가 유한하거나 안전하면 어떤 점화 순서를 선택하여도 버퍼나 레지스터에서 오버플로우가 발생하지 않는다는 것이 증명된다.

3) 보존성 (Conservation)

패트리 네트에서 항상 일정한 수의 토큰이 흐르면 보존하다고 한다.

4) 생동성 (Liveness)

생동성의 개념은 운영체제에서 교착상태가 발생하지 않는다는 것과 밀접한 관계가 있다. 초기 마킹 M_0로부터 어떤 점화 순서에 따라 계속 트랜지션을 점화하는 것이 가능하면 패트리 네트는 생동적이라고 한다. 생동적인 패트리 네트는 어떤 점화 순서를 선택하여도 교착상태가 발생하지 않는 연산을 수행한다.

5) 도달가능성 (Reachability)

도달가능성은 시스템의 동적 특성을 연구하는 기본이다. M_0로부터 Mn으로 전환하는 점화순서가 존재한다면 마킹 Mn은 M_0로부터 도달 가능하다고 한다.

6) 가역성 (Reversibility)

각각의 마킹 M에 대하여, M_0가 M으로부터 도달 가능하면 가역적이라고 한다. 가역적인 패트리 네트는 항상 초기 마킹이나 상태로 돌아갈 수 있다.

3. SET(Secured Electronic Transaction) 프로토콜

1996년 2월 전세계적으로 가장 큰 신용카드 회사인 VISA International과 Master 카드사는 인터넷 상에서 신용카드를 이용하여 대금지불을 함에 있어 개인의 정보와 재산을 보호해 줄 수 있는 안전한 방법을 찾기 위해 공동으로 연구를 시작하였고, 97년 5월 SET 1.0을 발표하였다. SET 프로토콜은 대칭적 암호화 방법인 DES와 비 대칭적 암호화 방식인 RSA 및 디지털 봉투를 이용하여 암호화에 걸리는 시간을 줄이고 해독의 가능성을 더욱 낮추었으며, 지불 정보 및 주문 정보에 대한 보안, 전송되는 데이터에 대한 기밀성 보장, 카드 및 카드 사용자에 대한 인증, 판매자에 대한 인증 및 각 구성 요소들간의 상호 운용성을 보장해주는 거래 프로토콜이다. 이는 단순히 SSL[8]과 같은 암호화 기법이 아닌 전자상거래의 지불구조와 인증체계, 암호화 기술을 이용해 만들어진 종합적인 표준이다[3, 4].

다시 말해서, SET은 정보의 기밀성, 지불정보의 무결성, 가맹점과 카드소지자 상호간의 인증[9]이라는 세 가지 형태의 보안서비스 제공을 목적으로 하고 있으며, 이러한 목적을 달성하기 위해 암호화 알고리즘, 전자서명 및 해쉬 함수[10, 11], 전자 인증서와 같은 기술요소를 이용하고 있다.

3.1 SET 구성요소

SET 프로토콜은 크게 카드소지자(Cardholder), 가맹점(Merchant), 지불 게이트웨이(Payment Gateway) 그리고 인증기관(Certification Authority)으로 이루어져 있다[4].

1) 카드소지자(구매자) : 카드사에 의해서 카드를 발급 받은 구매자로서 인증기관을 통해서 거래 승인을 득한 사람을 의미한다.

2) 가맹점(서비스 제공자) : 유형의 상품을 판매하거나 또는 특정 정보(예, 주식거래, 논문 정보 등) 및 특정 서비스(예, 온라인 컨설팅, VOD 서비스 등)등을 일정 금액의 대가를 받고 판매 또는 제공하는 업체를 의미한다.

   2)-1 상품 검색 시스템 : 구매자가 보다 쉽게 웹브라우저를 통해 상품 정보를 검색할 수 있도록 도와주며, VRML 브라우저를 통해 3차원 상품 형상 정보를 가시화 할 수 있도록 하는 시스템이다. 이러한 정보를 바탕으로 구매자는 특정 상품 정보를 구매의뢰하고, 배달 받게 된다.

   2)-2 회원 관리 시스템 : 구매자의 인적 정보 등을 관리하고 있으며, 구매의뢰 발생 시에는 구매자에 대한 인증을 수행하고, 구매자가 거래하는 금융기관에게 구매자에 대한 인증을 수행하고, 인증된 결과에 따라 검색 시스템으로 하여금 배달하도록 의뢰하는 기능을 한다.

3) 발행은행(Issuer) : 개개의 카드소지자에게 카드를 발급해 주는 기관을 의미한다. 우리 나라의 경우 삼성, LG, 국민, Visa, Master 등이 있다. 본 논문에서는 카드발급기관으로 용어를 통일한다.

4) 취득은행(acquire) : 상점으로 유입되는 구매관련 지불정보를 취합하여 처리해 주는 금융기관으로, 본 논문에서는 은행으로 용어를 통일한다.

5) 지불 게이트웨이(Payment Gateway) : 지불 게이트웨이는 취득은행에 의해 운영되는 전문 지불처리 시스템으로, 카드소지자로부터의 지불지시를 포함한 가맹점의 지불요청 메시지를 처리한다. 국내에서는 BC, 국민, LG, 삼성, 외환 등 5개 카드사에 의해 설립된 KCP가 지불 게이트웨이로서의 역할을 수행하고 있다. 이는 가맹점과 카드발급기관 중간에서 지불관련 서비스를 중계하는 회사이다.

6) CA(인증기관) : 하나의 신용카드회사나 복수의 신용카드회사에 대해서 각각의 카드소지자, 가맹점 및 지불 게이트웨이에 대한 인증을 생성하고 분배해 주어 SET 기반 지불처리에 참여하는 각 참여자 모두가 신뢰할 수 있음을 보장해 주는 관리기관을 말한다. SET은 인증기관 인증을 통해 인증성을 보장하고 있다.

3.2 전자지불 프로세스

전자상거래에서의 거래 절차를 아래와 같이 구체적인 12개의 프로세스로 나뉘어 살펴보면 다음과 같다.

1) 상품검색 : 본 단계는 카드소지자가 검색 시스템을 이용하여 상품 검색을 수행하는 단계이다. 이는 인터넷을 통한 전자상거래에서 일반적으로 생각해 볼 수 있는 것처럼 웹브라우저를 통해서 수행하기도 하며, VRML 브라우저를 통해 3차원 상품 형상 정보를 확인할 수도 있다. 기존의 MOTO(Mail Order/Telephone Order)시스템에서와 마찬가지로 CD-ROM 형태로 주어지는 상품정보 등을 통해서 검색하는 것도 가능하다.

2) 구매할 상품 선택 : 앞 단계의 검색을 통해 자신이 구매할 상품 정보를 선택하거나 또는 장바구니와 같은 개념을 통해 자신이 구매할 상품 정보의 군을 형성하는 과정이다.

3) 구매 요청 : 구매할 상품 정보의 목록 및 단위 가격과 전체 가격, 세금 등을 모두 포함한 주문서를 제시한다.

4) 지불방식 선택 : 구매 요청에 대한 지불방식을 선택한다. SET 프로토콜은 지불방식으로 구매자가 신용카드를 선택했을 경우에 적용된다.

5) 회원정보에 대한 인증 : 검색 시스템은 상기의 모든 구매 정보를 회원관리 시스템에 인증 의뢰를 하고, 회원관리 시스템은 구매자에 대한 인증을 수행한다.

6) 회원관리 시스템에게 구매와 지불에 대한 정보 전송 : 구매요청과 지불 정보가 구매자에 의해 회원관리 시스템에게 전송된다. 구매 및 지불정보는 모두 인증을 취득한 구매자에 의해 전자서명이 되어서 전달된다.

7) 카드에 대한 인증 : 구매자로부터 넘겨받은 정보를 바탕으로 회원관리 시스템은 구매자가 거래하는 금융기관에게 구매자에 대한 인증을 수행한다.

8) 구매 요청 승인 : 위의 인증 결과를 바탕으로 하여서 회원관리 시스템은 구매자에게 상품정보의 구매에 대한 확인을 해준다.

9) 배달 의뢰 : 회원관리 시스템은 구매 의뢰자의 의뢰에 대한 결과를 검색 시스템에 보내고, 상품 정보를 배달하거나 또는 서비스를 제공하도록 의뢰한다.

10) 상품 정보의 배달(다운로드) : 검색 시스템은 위에서 확인된 결과에 따라 구매자에게 해당하는 상품 정보를 배달하거나 또는 서비스를 제공해 준다.

11) 배달(다운로드)의 완료 : 구매자는 웹브라우저를 통해 해당 상품 정보의 구매 완료에 대한 확인을 해 준다.

12) 수금 : 회원관리 시스템은 구매자가 거래하는 금융기관을 통해서 상품 대금을 수금한다.

상기와 같은 일반적인 전자상거래의 프로세스 중 SET은 구매자가 지불수단으로 신용카드를 선택하였을 경우 6), 7), 8), 9)의 프로세스에 대해서만 관여한다. 따라서, SET프로토콜

중 10), 11), 12)의 프로세스에서는 어떠한 프로토콜이나 보완책을 제시하지 못하고 있다. 그러므로 본 논문에서는 상품의 배달과 수금 과정에 필요한 프로토콜을 제시하고자 한다.

4. iKP에 기반한 새로운 지불 프로토콜 SKP(Secure Key Protocol)

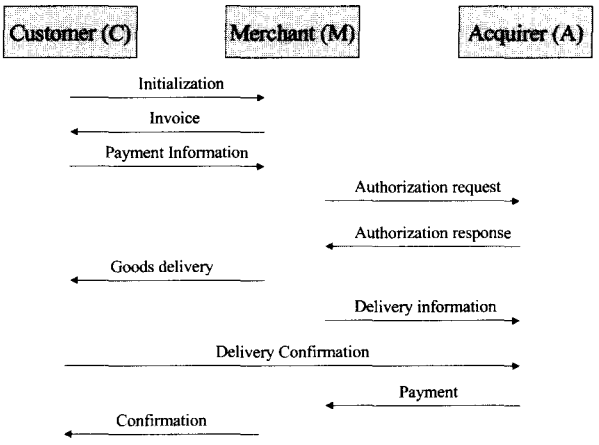
iKP(i-Key-Protocol)[12, 13, 14]는 IBM에서 기존 신용카드 인프라를 이용하여 개발한 지불 프로토콜이다. SET설계에 아주 큰 영향을 끼친 iKP는 인터넷상의 3자 이상이 관련된 거래에서 보안성을 가지고 결제를 보장해주는 구조물이다. 이러한 iKP는 공개키 암호화 알고리즘[15]과 디지털 서명 알고리즘을 채용하고 있으며, 인터넷이나 금융전산망을 통해 이루어지는 지불 과정에 쓰이는 프로토콜이다.

그러나 iKP프로토콜에서도 SET프로토콜과 마찬가지로 "상품 배달의 확인절차"가 고려되지 않고 있다. 따라서 가맹점에게 대금이 지불된 뒤의 상품배달에 관한 사항은 완전히 가맹점만의 수행과정으로 되어 있고, 만약 대금을 받고, 상품을 배달하지 않았더라도 그 부분에 대한 제재 사항은 전무한 상황이다.

따라서 본 논문에서는 이러한 SET의 단점을 보완하고자 기존의 iKP 프로토콜을 기반으로 새로운 지불절차 프로토콜을 제시하며, 이를 SET에 적용하고자 한다.

4.1 SKP 프로토콜의 기본 절차

SKP프로토콜은 3자가 관련되어 거래가 이루어진다. 여기에서 customer는 SET프로토콜에서의 구매자를 뜻하며, merchant는 가맹점, 그리고 acquirer는 보안성을 가지고, 지불을 처리하고자 할 때 있어야 할 모든 요소, 즉 지불 게이트웨이, 인증기관, 고객은행, 카드발급기관등을 통칭하여 가리키는 용어이다. 따라서 SKP 프로토콜에서의 구성요소는 Customer(C), Merchant(M), Acquirer(A)이다. SKP의 구성요소와 각각의 거래 과정을 (그림 1)에 도식화하였다.



(그림 1) SKP 구성요소와 거래과정

4.2 SKP 거래 과정

4.2.1 Initialization

Customer가 Merchant에게 거래를 하자고 한다.

4.2.2 Invoice

Merchant가 Customer에게 하는 답변으로서 Merchant의 서명과 거래자료(수량, 물건 설명등)가 첨부되기도 한다.

4.2.3 Payment information

Customer의 답변으로서 Merchant에게 지불창구(Acquirer)의 공개키(public key)로 암호화한 자신의 계좌번호와 신분확인번호(Personal Identification Number, PIN)가 기재된 지불확인서(payment slip)를 보낸다. Customer는 이 때 거래 자료에 자신의 서명을 기재하기도 한다.

4.2.4 Authorization request

Merchant가 Acquire에게 암호화된 지불확인서(payment slip)를 보낸다.

4.2.5 Authorization response

Acquirer가 Merchant에게 Acquirer의 서명과 함께 거래 자료를 넘긴다.

4.2.6 Goods delivery

Merchant가 임의로 발생시킨 난수로 구성된 상품코드와 함께 주문된 상품을 Customer에게 보낸다.

4.2.7 Delivery information

Merchant가 Customer에게 상품을 배달했다는 메시지를 Acquirer에게 보낸다.

4.2.8 Delivery confirmation

Customer가 Merchant로부터 주문된 상품을 받았다는 메시지를 Acquirer에게 보낸다.

4.2.9 Payment

Acquirer는 Customer와 Merchant로부터 온 배달 완료 메시지를 비교하여 승인되면 Merchant에게 지불한다.

4.2.10 Confirmation

Merchant는 Acquirer로부터 지불을 받은 후 Customer에게 확인메시지를 보낸다.

4.3 SKP 프로토콜에서 사용되는 요소들

요 소	요소에 대한 설명
PK_X	Party X의 공개키 (여기서 X는 CA(Certification Authority), C(Customer), M(Merchant), A(Acquirer)등이 된다.)
SK_X	Party X의 공개키
$CERT_X$	CA에 의해 발행된 party X의 공개키 인증서
H( )	단방향 해쉬 함수
$H_K(K,)$	단방향 해쉬 함수, 여기서 K는 random 하게 선택된 요소.

ϵ_X	PK_X를 이용한 공개키 암호화, confidentiality와 message integrity를 검사하는데 사용.
$S_X(\ )$	SK_X 를 이용해 계산된 서명
$SALT_M$	Merchant에 의해 생성되는 random number
AUTHPRICE	금액
DATE	Merchant의 date, time stamp. Replay 공격으로부터의 보호를 위해 사용된다.
$NONCE_M$	Merchant의 random number. Replay 공격으로부터의 보호를 위해 사용된다.
ID_M	Merchant의 ID. acquirer가 merchant를 구분하는데 사용된다.
TID_M	Transaction ID. 유일한 문서임을 구분하는 merchant에 의해 선택된 구분자.
DESC	구입상품, 전달주소의 설명.
BAN	Customer의 account number(예 : credit card number)
EXPIRATION	Customer의 account number와 관련된 만료일자.
R_C	Customer에 의해 선택된 random number
ID_C	$ID_C = H_K(R_C, BAN)$
RESPCODE	YES/NO 혹은 인증코드
PIN	Customer의 PIN
$SALT_C$	Customer의 인증서에 account number를 감추는 데 사용되는 random number
V	Merchant에 의해 생성되는 random number. merchant가 지불을 받았다는 증거로서 사용된다.
VC	Merchant에 의해 생성되는 random number. seller가 지불을 받지 않았다는 증거로서 사용된다.
$DATE_M$	Merchant가 customer에게 상품을 배달할 때의 날짜와 시간
$DATE_C$	Customer가 acquirer에게 상품이 배달되었음을 알릴 때의 날짜와 시간
GOODS	Merchant가 customer에게 상품을 배달할 때, random하게 선택된 상품코드

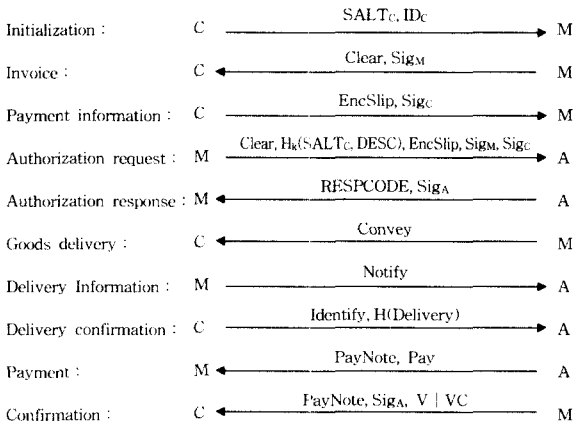
4.4 SKP 프로토콜에서 사용되는 합성된 요소들

합성된 요소	구 성 요 소
Common	AUTHPRICE, ID_M, TID_M, DATE, $NONCE_M$, ID_C, $H_k(SALT_C, DESC)$, H(V), H(VC)
Clear	ID_M, TID_M, DATE, $NONCE_M$, H(Common), H(V), H(VC)
SLIP	AUTHPRICE, H(Common), BAN, R_C, PIN | $SALT_C$, EXPIRATION
EncSlip	ϵ_A(SLIP)
Sig_A	S_A(RESPCODE, H(Common))
Sig_M	S_M(H(Common))
Sig_C	S_C(EncSlip, H(Common))
Delivery	ID_M, ID_C, GOODS, $DATE_M$, TID_M, RESPCODE
Confirm	ID_M, ID_C, GOODS, $DATE_C$, TID_M, DESC
Convey	S_M(GOODS, H(Delivery))
Notify	S_M(GOODS, $DATE_M$, H(Delivery))
Identify	S_C(GOODS, $DATE_C$, H(Confirm))
PayNote	S_A(GOODS, H(Delivery))

4.5 각 부분의 시작 정보

Customer	DESC, AUTHPRICE, BAN, EXPIRATION, PK_{CA}, PIN, SK_C, $CERT_C$, $SALT_C$, PK_M, PK_A,
Merchant	DESC, AUTHPRICE, PK_{CA}, $CERT_A$, SK_M, $CERT_M$, PK_A, , PK_C
Acquirer	PK_{CA}, SK_A, $CERT_A$, PK_M, , PK_C ,

4.6 SKP 프로토콜의 흐름



4.6.1 Initialization

Customer가 random number R_C를 생성하여 $ID_C = H_k$ (R_C, BAN)를 계산하여 만든다. Customer는 또 다른 random number $SALT_C$를 생성하여 $SALT_C$와 ID_C를 merchant에게 보낸다.

4.6.2 Invoice

Merchant가 customer로부터 $SALT_C$와 ID_C를 받고, DATE와 random number $NONCE_M$를 생성하는데, 여기서 DATE와 $NONCE_M$는 나중에 acquirer로부터 이 지불이 유일함을 구별할 때 사용된다. Merchant는 또한 이 문서가 유일함을 나타내는 transaction ID인 TID를 선택하고, random value V와 VC를 선택하여, Clear에 H(V)와 H(VC)를 첨가한다. 그리고 Merchant는 $H_k(SALT_C, DESC)$를 계산하고, 위에 정의한 사항들로 계산한 값 H(Common)과, H(Common)에 서명한 $Sig_S = S_S(H(Common))$를 Invoice에 포함하여, 이 메시지를 customer에게 보낸다. Merchant는 이 메시지에 $CERT_A$를 붙여 보낼 수도 있고 나중에 confirm 메시지와 함께 보낼 수도 있다.

4.6.3 Payment information

Customer는 invoice과정에서 받은 Clear로부터 DATE를 얻고, $H_k(SALT_C, DESC)$와 H(Common)을 계산하여, 받은 H(Common)과 customer가 계산한 H(Common)이 같은지 비교한다. 그 다음 customer는 SLIP을 계산하여 acquirer의 public key로 암호화되는 EncSlip을 merchant에게 보낸다.

4.6.4 Authorization request

Merchant가 acquirer 에게 지불에 대한 인증을 요구하는 과정으로서, merchant는 EncSlip 과 함께 Clear 와 $H_k(SALT_C, DESC)$를 acquirer에게 보낸다. 또한 Merchant는 acquirer에게 customer에게 보냈던 $Sig_M = S_M(H(Common))$를 포함하여 보낸다.

4.6.5 Authorization response

Acquirer는 Authentication request 단계에서 Clear, EncSlip, $H_k(SALT_C, DESC)$를 뽑아 낸다. Clear로부터 추출되는 ID_M, TID_M, DATE, $NONCE_M$ 로부터 replay 검사가 가능하며, 또한 EncSlip을 복호화 할 때, 만약 복호화에 실패하면 acquirer는 seller나 그 외의 다른 상대방에게 EncSlip이 바뀌어졌다고 가정한다. 그렇지 않으면 acquirer는 SLIP을 얻는다. 그리고, h1과 h2를 체크 함으로써 acquirer은 merchant와 customer가 주문 정보에 동의함을 보증한다. acquirer은 다시 Common을 구성하고, 지불에 대한 온라인 인증을 얻어 merchant에게 Authentication Response를 보낸다.

4.6.6 Goods delivery

Merchant가 customer에게 상품을 배달할 때 merchant가 임의로 발생시킨 상품코드 GOODS와 함께 보낸다. 이는 Merchant가 customer에게 상품을 제대로 배달했음을 나중에 customer에게 온 메시지와 merchant에게 온 메시지를 비교하여 acquirer가 알 수 있도록 하기 위함이다. Merchant는 또한 H(Delivery)를 만들어 Merchant의 비밀키로 GOODS와 H(Delivery)를 암호화하여 customer에게 보낸다.

4.6.7 Delivery information

Merchant는 customer에게 보낸 메시지를 acquirer에게도 보낸다. 단, 이 과정에서는 merchant는 acquirer에게 보낼 때의 날짜와 시간 값을 $DATE_M$의 형태로 생성하여, merchant의 비밀키로 GOODS, $DATE_M$, H(Delivery), 를 암호화하여 보낸다. Acquirer는 merchant의 공개키를 알고 있으므로 공개키를 사용하여 GOODS와 $DATE_M$, H(Delivery)의 값을 알아낼 수 있다.

4.6.8 Delivery confirmation

Customer는 acquirer에게 메시지를 보낼 때의 날짜와 시간 값을 $DATE_C$ 의 형태로 생성하고, H(Confirm)과 $DATE_C$ 를 customer의 비밀키로 암호화한 Identify와 H(Delivery)를 acquirer에게 보낸다. Delivery information 과정에서와 마찬가지로 Acquirer는 customer의 공개키를 알고 있으므로 customer의 공개키를 사용하여 GOODS와 $DATE_C$, H(Confirm)의 값을 알아낼 수 있다. 이때 acquirer은 자신이 가지고 있는 정보로 H(Delivery)와 H(Confirm)의 값을 만들 수 있으며, 이 값들과 merchant와 customer로부터 받은 H(Delivery)와 H(Confirm)을 비교하여 이 지불과정을 수행하고 있는 merchant와 customer가 맞다는 사실을 알 수 있다. 또한 acquirer는 Delivery information 과정에서 얻은 $DATE_M$과 Delivery confirmation에서 얻은 $DATE_C$ 의 값으로 merchant와 customer에서 메시지를 보낸 시점의 시간차를 계산할 수 있다. 이러한 시간차를 이용하여 delay를 검사할 수 있으며, 이 시간 차이 값이 하루 이상이거나 어느 한 곳에서 메시지를 보내지 않았을 경우 이 지불 과정은 무시된다.

만약 customer가 Delivery confirmation메시지를 acquire에게 보내지 않았을 경우, Delivery information 과정에서 customer 정보를 추출하여 해당되는 customer를 black list에 올림으로써 이후에 상거래를 할 수 없도록 처리한다.

4.6.9 Payment

Acquirer가 배달을 확인한 후 merchant에게 PayNote메시지와 함께 상품값에 해당하는 값(Pay)을 customer의 구좌에서 빼 내어 merchant에게 지불한다.

4.6.10 Confirmation

Merchant는 customer에게 PayNote 메시지와 함께 V(success)나 VC(failure)의 값을 포함하여 보낸다. Customer는 H(V)나 H(VC)를 계산하고, 이를 Invoice에서 보냈던 값과 비교한다.

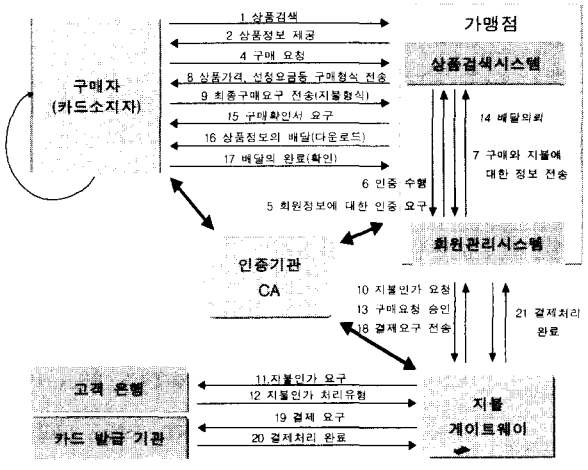
5. 전자지불 프로세스의 Petri Nets 모델링

위 4장에서 기술한 SKP프로토콜을 SET프로토콜 프로세스에 적용시킨다면, SET에서 고려되지 못했던 상품의 배달과 수금과정에 관해 보안성을 가지고 수행함으로써, 신용카드를 이용한 거래과정에서 기존의 SET프로토콜보다 더 안정적인 전자지불 처리가 가능하다.

따라서, 이번 장에서는 이러한 수행과정을 Petri Nets를 이용하여 모델링하고, 이를 Petri Nets분석 도구인 Visual Object Net ++[16] 을 이용하여, 모델의 보존성, 생동성, 도달가능성, 가역성 등의 성질을 분석함으로써 모델의 적합성 여부를 제시한다.

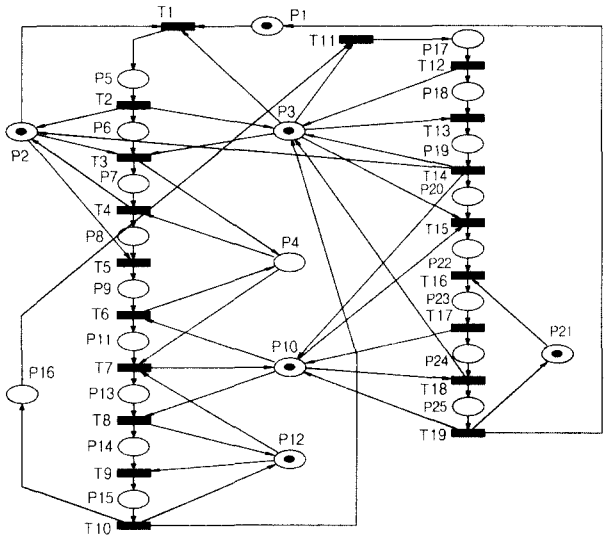
5.1 SKP 기반 SET 프로토콜 모델

다음 (그림 2)는 SKP 프로토콜을 적용한 SET프로세스 모델을 도식화하여 표현한 것이다.



(그림 2) SKP 프로토콜을 적용한 SET기반 전자 지불 프로세스

(그림 2)의 SET 기반 전자 지불 모델을 MPN으로 나타내면 (그림 3)과 같고, 각각의 플레이스와 트랜지션의 집합은 <표 1>과 같다. 따라서, MPN을 통해 모델링하고 이를 분석함으로써 안정적인 모델임을 보여준다.



(그림 3) SKP를 적용한 SET 기반 전자 지불의 MPN 모델

〈표 1〉 (그림 3)의 MPN 모델에 대한 플레이스와 트랜지션의 집합

플레이스	설 명	트랜지션	설 명
P1	전자지불 시스템 시작	T1	상품 검색, 선택
P2	구매자 준비됨	T2	구매 요청
P3	가맹점 준비됨	T3	구매자 인증 요청
P4	인증기관 준비됨	T4	구매자에게 구매형식 전송
P5	구매 요청 메시지	T5	가맹점에게 최종 구매요구 전송
P6	구매자 및 가맹점 인증	T6	지불 게이트웨이의 인증 요청
P7	인증 수행 대기	T7	지불인가 메시지 전송
P8	최종 구매 요구 형식	T8	카드발급기관 지불인가 처리 승인
P9	최종 구매 요구	T9	지불 게이트웨이에 구매요청 승인
P10	지불 게이트웨이 준비됨	T10	가맹점에 전송
P11	인증 수행 대기	T11	배달 의뢰
P12	카드발급기관 준비됨	T12	구매자에게 구매 확인서 요구
P13	지불인가 요구 메시지	T13	구매자에게 상품 정보 배달
P14	지불인가 처리 결과 메시지	T14	배달 확인
P15	지불인가 결과	T15	지불 게이트웨이에 결제요구 전송
P16	대기 상태	T16	은행에 결제요구
P17	구매 확인서	T17	지불게이트웨이에 결제처리 완료전송
P18	상품(정보)	T18	가맹점에게 결제처리 완료 전송
P19	가맹점 배달 완료 메시지	T19	전자지불 시스템 완료 전송
P20	결제 요구 메시지		
P21	은행 준비됨		
P22	결제 요구 메시지		
P23	결제 처리 완료 메시지		
P24	결제 완료 메시지		
P25	결제 완료		

(그림 3)을 MPN의 분석도구인 Visual Object Net ++[16]을 이용하여 분석한 결과, 보존적이고, 생동적이며, 도달가능하며, 가역적이라는 것이 증명되었다. 이는 전자지불 시스템에 영향을 주는 최악의 경우는 발생하지 않으며, 시스템이 어떤 한 상태에서 다른 상태로 진행될 수 있으며, 요구되는 최종상태에 도달할 수 있음을 보여준다.

5.2 비교분석

기존의 SET프로토콜과 SKP 기반의 SET 프로토콜과의 차이점은 다음과 같다.

〈표 2〉 SET프로토콜과 SKP 기반의 SET 프로토콜과의 비교분석

기 능	기존의 SET 프로토콜	SKP 기반의 SET 프로토콜
지 불 방 식	신용 카드	신용 카드
카드나 회원정보에 대한 인증	○	○
구매와 지불에 대한 정보전송	○	○
배달 의뢰	○	○
상품정보의 배달	×	○
배달의 완료 확인	×	○
지불 시점	배달의뢰의 시점	배달의 완료 확인 시점

위의 <표 2>에서와 같이 기존의 SET프로토콜과 SKP 기반의 SET프로토콜과는 배달 과정에 대한 차이점을 가지고 있다.

제안된 SKP 기반의 SET프로토콜은 배달 증명을 통해 중도의 물품 도난을 방지할 수 있을 뿐만 아니라 Merchant와 Customer가 보내는 $DATE_M$과 $DATE_C$의 데이터들을 통해 거래 취소의 원인을 제공하는 당사자들에 대한 블랙리스트의 작성이 가능하므로 이러한 목록들의 데이터베이스화를 통한 좀 더 투명한 전자상거래로의 진입을 가능하게 한다. 그러나 배달 증명 후에 결재를 하게 함으로 해서 결재일이 늦어지게 된다. 이러한 점의 보완을 위해 SKP 기반의 SET 프로토콜에서는 $DATE_M$과 $DATE_C$의 응답기간 차이를 하루라는 일정 수준으로 의무 규정함으로써 결재일이 늦어지게 되는 단점을 보완할 수 있다.

6. 결 론

전자상거래 시스템이 보급되기 위해서는 안전성의 확보가 중요하다. 국내에서 인터넷을 통한 전자상거래가 활발해지기 위해서는 신뢰할 수 있는 인터넷 보안 기술을 발전시키고, 전자상거래 정보보호기술의 국가경쟁력 확보가 필요하다. 현재 가장 안전한 전자지불 시스템의 표준으로 인정받고 있는 Visa사와 Master카드사의 주도하에 성립된 SET은 메시지의 암호화, 개인을 인증(Authentication)할 수 있는 전자증명서, 그리고 디지털 서명(Digital Signature) 등을 통해 개방환경에서 가장 우려가 되는 보안적인 요소를 보완한 가장 안전한 신용카드 전자지불 시스템으로 자리잡고 있다. 하지만, 프로토콜로서 지니고 있는 한계점은 여전히 가지고 있다.

따라서 본 논문에서는 SET이 지니고 있는 단점, 즉 SET에서 아직 고려하지 못하고 있는 배달과 배달 확인에 의한 지불에 요구되는 프로토콜 및 방식을 제안하고 그 모델에 관한 적합성 여부를 Petri Nets를 이용해 알아보았다. 앞으로는 여기에서 더 나아가 신용카드를 제외한 방식의 지불방식이나, 구매자, 상점, 지불게이트웨이 등의 시스템에 저장되는 정보에 대한 보호 등의 관점에서 보안성을 가지는 지불방식에 대해 연구하여야 할 것이다.

참 고 문 헌

[1] Daniel C. Lynch, and Leslie Lundquist, Digital Money, John Wiley and Sons, 1996.

[2] Peter Wayner, Digital Cash 2nd Edition, AP Professional, 1997.

[3] VISA and MasterCard, SET Secure Electronic Transition Specification, Book 1 : Business Description, Version 1.0, May, 1997.

[4] VISA and MasterCard, SET Secure Electronic Transaction Specification, Book 2 : Programmer's Guide, Version 1.0, May, 1997.

[5] Kim M. H., Lee J. K., "Schedules of Multi-Robot Interconnection Systems using Time Petri Nets," Proceedings of ITC-CSCC '97 Okinawa, Japan, pp.1095-1098, July, 1997.

[6] J. L. Peterson, "Petri Net Theory and Modeling of System," Prentice-Hall, NJ, 1981.

[7] Tadao Murata, "Petri Nets : Properties, Analysis and Applications," Proceedings of the IEEE, Vol.77, No.4, pp.541-580, April, 1989.

[8] Alan O.Freier, Philip Kariton, and Paul C. Kocher, "The SSL protocol : Version 3.0", Tech. Rep., Internet Draft, 1996.

[9] ISO/IEC, "Information Technology open systems interconnection the directory : Authentication framework," June, 1994.

[10] Mihir Bellare, Ran Canetti and Hugo Krawczyk, "Keying hash functions for message authentication," in Advances in Cryptology CRYPTO '96, 1996.

[11] NIST National Institute of Standards and Technology (Computer Systems Laboratory), "Secure Hash Standard," Federal Information Processing Standards Publication FIPS PUB 1801, Apr. 1992.

[12] Mihir Bellare, Juan A.Garay, "Design, Implementation and Deployment of the iKP Secure Electronic Payment System," IEEE Journal of Selected Areas in Communications, Vol.18, No.4, April 2000.

[13] N.Asokan, Phil Janson, Michael Steiner, and Michael Waidner, "State of the art in electronic payment systems," IEEE Computer, Vol.30, No.9, pp.28-35, Sept. 1997.

[14] Steen Larsen, Zurich iKP Prototype (ZiP) : iKP Transaction Layer Functional Specification, IBM Zurich Research Laboratory, May. 1996.

[15] Shai Halevi and Hugo Krawczyk, "Public-key cryptography and password protocols," ACM Transactions on Information and System Security, Vol.2, No.3, pp.25-60, 1999.

[16] Visual Object Net++, Visual Object oriented Petri Net based Engineering Tool Evaluation Version 1.44.2, Rainer Drath, http : //www.systemtechnik.tu-ilmenau.de/~drath

송 유 진

e-mail : syj@sarim.changwon.ac.kr

1992년 창원대학교 컴퓨터공학과 졸업 (학사)

1995년 창원대학교 대학원 컴퓨터공학과 졸업(석사)

1999년 현재 창원대학교 대학원 컴퓨터공학과(박사과정)

1995년~현재 창원대학교 강사

관심분야 : 페트리 넷, 성능분석, 정보보호, 스케쥴링연구

서 미 경

e-mail : meteor3@hitel.net

1997년 숙명여자대학교 경제학과 졸업

2001년 창원대학교 산업대학원 컴퓨터공학과졸업

관심분야 : 패트리 넷, 정보보호

이 종 근

e-mail : jklee@sarim.changwon.ac.kr

1974년 숭실대학교 전산과 졸업 동 대학원 수료

1977년 고려대학교 경영대학원 경영학과 수료

1990년 Univ. de Montpellier II 전산과 박사 수료

1983년~현재 창원대학교 컴퓨터공학과 교수, 창원대학교 전산소장, 자연대 부학장역임

관심분야 : 패트리 넷, 성능분석, 정보보호, 스케쥴링연구