스마트 카드 기반 전자상거래 프로토콜 정형분석[1)]

김일곤[0*], 문영주*, 김현석*, 강인혜**, 최진영*

*고려대학교 컴퓨터학과
{igkim[0], yjmoon, hskim, choi}@formal.korea.ac.kr,

**서울시립대학교 기계정보공학과
inhye@uos.ac.kr

Formal Analysis of E-Commerce Protocols based on Smart Cards

Il-Gon Kim[0*], Young-Joo Moon*, Hyun-Seok Kim*, Jin-Young Choi*
*Dept of Computer Science & Engineering, Korea University

Inhye Kang**
**Dept of Mechanical and Information Engineering, University of Seoul

요약

스마트 카드 보급의 확산과 더불어 CEPS(Common Electronic Purse Specification) 전자지갑 규제 표준을 기반으로 한 전자상거래 서비스의 개발이 활성화 되고 있다. 전자상거래 프로토콜은 그 특성상, 소비자와 상인간의 정확한 물품 거래가 이루어져야 할 뿐만 아니라, 문제 발생시 상호간의 원인규명을 판단하기 위한 기준이 마련되어 있어야 한다. 본 논문에서는 CSP 언어를 이용하여 CEPS 기반 전자상거래 프로토콜의 행위를 정형 명세하였고, FDR 도구를 이용하여 전자상거래 관점에서 문제점을 분석해 보았다.

1. 서론

스마트 카드 보급의 확산과 더불어 CEPS(Common Electronic Purse Specification) 전자지갑 규제 표준을 기반으로 한 전자상거래 서비스의 개발이 활성화 되고 있다. CEPS는 전자지갑의 상호 운용성 보장 표준규격으로, 국제적으로 사용 가능한 전자지갑의 필요요소를 정의하고 있다[1]. 전자상거래 과정에서 "소비자는 거래 금액에 맞는 물품을 구입해야 하고, 거래 과정에서 서비스의 오동작으로 인해 전자화폐 액수가 증가되거나 감소되어서는 안 된다"는 요구사항을 반드시 만족시켜야 한다. 또한 스마트 카드 개발시 고등급의 제품 인허가 등급을 받기 위해서는 정형적으로 시스템의 행위를 명세하고 안전성을 검증하기 위한 절차가 요구된다. 이에 따라, 전자상거래 시스템의 행위를 정형적으로 명세하고 검증하기 위한 연구가 진행되어오고 있다. 그 중에서도 전자지갑의 기능을 정형적으로 명세하고 검증하고자 하는 연구는 Susan Stepney에 의해 처음 시도되었으며, 그는 Z 정형명세 언어를 이용하여 일반적인 전자지갑의 기능을 증명하였다[2]. Nevin Heintze는 CSP 및 FDR 도구를 이용하여 NetBill 프로토콜의 안전성 분석하는 연구를 수행하였다[3]. 그리고 Jan Jürjens는 UML을 이용하여 처음으로 CEPS 전자지갑 시스템의 기능을 명세하는 연구를 진행하였다. 하지만, 그의 연구는 보안 프로토콜 관점에서 CEPS 기반 전자상거래 프로토콜의 암호화 메시지 순서도를 기술하고, 키 노출에 의한 보안 취약점을 지적하는데 중점을 두었다[4].

본 논문에서는 CSP 프로세스 알제브라 언어를 이용하여, 암호화 키 관점이 아닌, 전자상거래 측면에서 CEPS 기반 프로토콜의 행위를 정형명세하고 FDR 모델체킹 도구를 이용하여 상거래 보존성(accountability) 만족여부를 분석하였다.

본 논문의 나머지 부분은 다음과 같이 구성되어 있다. 제 2장에서는 CEPS 표준에 대해 간략히 소개하고, 제 3장에서는 프로토콜을 명세하고 검증하기 위한 CSP 정형명세 언어와 FDR 모델체킹 도구에 대해 간략히 소개하고, 제 4장에서는 전자상거래 시스템의 중요한 요구사항인 기록 보존성(accountability) 원칙에 대해 설명하고 CEPS의 PSAM(Purchase Security Application Module)을 이용한 구입 프로토콜 명세 및 검증 결과를 보여주고, 마지막으로 제 5장에서는 결론 및 향후 연구 방향을 제시하고자 한다.

[1)] 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성지원사업의 연구결과로 수행되었음

2. CEPS(Common Electronic Purse Specification)

CEPS는 전자지갑의 상호 운용성 보장 국제표준으로 1999년에 제정되었다. CEPS의 목적은 국제적으로 사용 가능한 전자지갑 프로그램이 되기 위한 필수 기능 및 요구사항을 정의하는 것이다[1]. CEPS에 정의된 전자지갑의 주요 기능은 물품을 구매하거나 전자화폐를 충전하는 과정으로 구분된다. 예를 들어, CEPS 표준에 따라 전자화폐 기능을 지원하는 스마트 카드를 소지한 소비자는 POS(Point-Of-Sale) 단말기를 통해 전자상거래 서비스를 이용하게 된다. PSAM은 POS 단말기내에 부착되어 전자화폐를 이용한 물품 구매를 담당하게 된다. 예를 들어, 소비자가 거래 상인으로부터 물품을 구입하고 나면, 거래상인은 소비자의 스마트카드를 이용하여 POS 단말기를 통해 소비자의 카드 발행사 또는 거래은행에 거래금액에 대한 승인을 요청하게 되며, 거래가 정상적으로 완료되게 되면 전자화폐금액을 거래은행으로부터 지불 받게 된다. 본 논문에서는 CEPS 기반 구입 프로토콜에만 초점을 맞추고 있다.

1. PSAM -> CARD : debit
2. CARD -> PSAM : purchase
3. PSAM -> BANK : endorsed signed EPO
4. BANK -> PSAM : signed receipt
5. PSAM -> CARD : OK

그림1. CEPS 기반 전자화폐 지불 과정

2.1 PSAM을 이용한 구입 프로토콜

CEPS에서 정의된 PSAM을 통해 물품거래에 대한 전자화폐 금액을 지불하는 과정은 그림 1과 같이 표현할 수 있다.
그림 1에서 보는 바와 같이, 전자화폐를 지불하기 위해서 소비자의 스마트 카드 CARD, 거래상인의 POS 단말기에 내장된 PSAM, 그리고 거래은행 BANK 사이의 메시지 전달 순서를 보여주고 있다. 소비자의 카드가 POS 단말기를 통해 통신을 시작하게 되면, PSAM은 CARD에게 지불요청(debit) 메시지를 보내고, 그런 다음 CARD는 구입 금액 및 개인 서명이 포함된 메시지(purchase)를 PSAM에게 보내게 된다. 이제 PSAM은 거래 정보 메시지(endorsed signed EPO)를 BANK에게 보내어 거래의 정상적인 처리여부를 확인한다. 거래가 정상적으로 이루어졌을 경우, BANK는 PSAM에게 거래의 정상적인 승인결과(signed receipt)를 알려주고, CARD는 PSAM으로부터 거래의 승인(OK) 확인 받게 된다. CEPS 기반 구입 프로토콜의 상세한 지불 및 승인 절차에 대해서는 [1]을 참조하기 바란다.

3. CSP 명세 및 FDR 검증 결과

3.1. CSP

CSP는 프로세스 알제브라 언어로서, 병렬성을 갖는 통신 프로토콜의 동작을 효율적으로 명세하기 위해 제작되어졌다[4]. 처음에는 일반적인 통신 프로토콜과 제어 시스템을 명세하기 위해 사용되어졌지만, 점차 보안 프로토콜을 명세하기 위한 영역으로도 확대되어 오고 있다. CSP에서 제공하는 pure synchronization(|||)과 Interleaving parallelism(||) 개념을 사용하여 분산 시스템 환경에서 동작하는 클라이언트 서버, 공격자 모델을 정형적으로 표현할 수 있다는 장점을 갖고 있다. 예를 들면, 분산시스템 환경에서 동작하는 전자상거래 시스템은 다음과 같이 간략히 표현될 수 있다.

SYSTEM = CARD ||| PSAM||| BANK

3.2 FDR

FDR은 유한상태 모델체킹 도구로서, CSP 언어로 구현된 구현모델과 속성모델의 포함관계를 분석해서, 구현모델이 안전성, 교착상태 등과 같은 속성들을 만족시켜주는지 검증하는 도구이다[5]. 예를 들어, 전자상거래 시스템의 상세 구현모델이 SYSTEM이고 요구사항 모델이 SPEC인 경우 다음과 같이 표현함으로써 모델체킹을 수행하게 된다.

assert SPEC [FD= SYSTEM

3.3 보존성(accountability)

전자상거래 시스템에서 가장 중요한 요구사항은 소비자와 거래상인이 거래를 마치고 난 후, 소비자 및 거래상인의 거래금액이 정상적으로 처리되어 거래금액의 보존성이 보장되어야 한다는 점이다. 예를 들어, 소비자가 100,000원의 전자화폐를 충전한 후, 거래상인에게 50,000원의 금액을 지불한 경우, 소비자의 총잔액은 50,000원이 되어야 하며, 시스템의 오작동으로 인해 금액이 임의대로 차감되거나 증가되어서는 안 된다. 이와 마찬가지로, 거래상인의 금액도 비정상적으로 차감되거나 증가되어서는 안 된다. 소비자 고객의 총금액이 'C(total balance), 지불금액이 'C(coin)' 이고 거래상인의 총금액이 'M(total balance)' 이면 다음과 같은 관계가 항상 성립해야 한다.

C(total balance') = C(total balance) – C(coin)
M(total balance') = M(total balance) + C(coin)

3.4 명세 및 분석 결과

본 논문에서는 CEPS 기반 전자화폐 지불과정에서 보존성 원칙을 만족시키고 있는지 확인하기 위해 다음과 같은 요구사항을 SPEC 모델로 작성하였다. 아래 모델은 거래상인 입장에서 보존성 원칙이 준수되고 있는지 표현하고 있다.

SPEC = STOP |~| (mGets_epoToken -> ((creditM ->
STOP) |~| (mGetsRefundSlip -> STOP)))

즉, 거래상인은 소비자로부터 거래금액을 받게 되면 거래상인의 총금액을 증가시키거나 또는 잘못된 거래에 소비자에게 금액을 반환하게 된다. 예를 들어서 CARD가 PSAM에게 거래금액 epo_TokenA을 전송 한 후, 통신상의 이유로 제대로 전달이 되었는지 여부가 확실치 않아서, 다시 한번 epo_TokenB를 전달한 경우, CARD 입장에서는 두번 epo_Token이 전달되었는지 확신하지 못하게 된다. 이런 경우, CARD는 BANK의 데이터베이스에 저장되어 있는 거래 내역을 통해 거래 내역을 확인하게 된다. BANK는 거래 내역에 대한 조회를 통해, PSAM을 통해 CARD에게 epo_TokenB에 대한 거래취소 메시지(mGetsRefundSlip)를 보내주게 된다.

```
-- The customer process
CARD = cinp?x -> DEBIT_CARD(x)
DEBIT_CARD(x) = if (x==correctDebitA) then
                  (coutp!epo_TokenA-> EPO_TOKEN_SENT)
                  else if (x==correctDebitB) then
                  (coutp!epo_TokenB -> EPO_TOKEN_SENT)
                  else RETURN_TOKEN

RETURN_TOKEN = coutb!paymentAlready -> cinb?x ->
                (if (x==refundSlip) then REFUND_RECEIVED
                else if (x==depositSlip) then
                        epo_tokenSpent -> ARBITRATION
                else ERROR_DEBIT)

-- The PSAM process
PSAM = STOP |~| REPEATED_DEBIT_REQUEST(none)
REPEATED_DEBIT_REQUEST(previousDebitRequest) =
if (previousDebitRequest == none) then (SEND_DEBIT_A []
SEND_DEBIT_B)
else if (previousDebitRequest == correctDebitA) then
SEND_DEBIT_B
else SEND_DEBIT_A

-- The BANK process
BANK = WAIT_ENDORSED_EPO
WAIT_ENDORSED_EPO = RECORD_LOG(0,0,0)
RECORD_LOG(Flag, A, B) =
binc?x -> (if (x==paymentAlready) then
          (if (Flag==0) then depositC -> boutc!refundSlip ->
           RECORD_LOG(1,0,0))
          else if (A==1 or B==1) then
          (arbitration -> boutc!depositSlip ->
             RECORD_LOG(Flag, A, B))
          else RECORD_LOG(Flag, A, B))
             else RECORD_LOG(Flag, A, B)) []
binp?x ->
          (if (x==epo_TokenA) then
          (if (Flag==0) then
         (debitC -> creditM -> boutp!depositSlip ->
             RECORD_LOG(1,1, B))
          else if (A==1) then
          (boutp!alreadyDeposited -> mFraud ->
              RECORD_LOG(Flag, A, B))
          else if (B==1) then
          (debitC -> creditM -> boutp!depositSlip ->
```

그림 2. CSP 명세

그림 2는 CEPS 기반 전자화폐 지불과정을 CSP 언어로 명세한 일부 코드를 보여주고 있으며, 논문에 페이지 사정상 상세한 설명을 생략하도록 하며, 전체 명세 코드는 [7]을 참조하기 바란다. 위 CSP 명세가 앞에서 언급한 보존성 원칙을 준수하고 있는지 FDR을 통해 검증해 보았다. 그 결과 다음과 같은 2가지 분석내용을 파악할 수 있었다.

첫째, PSAM이 CARD로부터 epo_TokenA 정보를 수신 한 후, BANK에 전달하여 거래를 정상적으로 끝내고 creditM 이벤트를 통해 자신의 계좌 금액을 증가시키게 된다. 그런 다음 거래상인은 스마트 카드를 소비자에게 전달하고 거래의 정상적인 완료를 확인시켜준다. 그러나, 악의적인 목적을 가진 거래상인이 epo_TokenA 정보를 담은 카드를 복사하거나 재사용하여 다시금 BANK에게 거래 승인 요청을 의뢰하게 되면, 소비자 입장에서는 한번의 물품 구입에 대해 2번 지불하는 결과를 초래할 수도 있게 된다. 하지만, BANK는 RECORD_LOG(Flag, A, B)와 같은 거래내역을 기록하는 데이터베이스가 존재하여, 거래상인에게 mFraud 이벤트를 보내주어, 비정상적인 거래임을 알려주게 됨으로써 소비자와 거래상인간의 거래금액에 대한 보존성을 유지시켜주는 것을 확인하였다.

두 번째로, CARD로부터 PSAM에게 epo_TokenA가 전송되고 난 후, 전송상의 문제로 제대로 거래금액이 전달되었는지 확신할 수 없는 경우에도, BANK의 거래내역 조회를 통해 거래금액의 보존성을 보장될 수 있음을 확인하였다.

4. 결론 및 향후 연구 방향

스마트 카드의 보급 확산과 더불어 CEPS의 국제화 표준 준수 영역의 중요성이 증대되고 있다. 또한, 전자상거래 시스템의 경우, 소비자와 거래상인과의 거래금액에 대한 보존성 보장을 통한 안전한 상거래 보장은 매우 중요한 요구사항이다. 본 논문에서는 CSP 언어 및 FDR 검증 도구를 통해, CEPS 기반 전자상거래 프로토콜을 설계하는 단계에서 거래금액의 보존성 관점에서 발생할 수 있는 확인할 수 있었다.

향후 연구방향으로는 CEPS의 LSAM(Load Security Application Module)을 이용하여 전자화폐를 충전하는 프로토콜을 정형명세하고 보안 취약점을 검증하고 분석해 보고자 한다.

참고문헌

[1] CEPSCO, Common Electronic Purse Specification, version 2.3, available from http://www.cepsco.com, 2001.

[2] S. Stepney, D. Cooper, and J. Woodcock, "An Electronic Purse : Specification, Refinement, and Proof," Technical Report PRG-126, 2000.

[3] N. Heintze, J. D. Tygar, J. Wing, H. C. Wong, "Model Checking Electronic Commerce Protocols", Proceedings of the 2nd USENIX Workshop on Electronic Commerce, pp147-164, 1996.

[4] J. Jürjens and G. Wimmel, "Security Modelling for Electronic Commerce: The Common Electronic Purse Specificatio," I3E 2001, pp. 489-506, 2001.

[5] C.A.R. Hoare, *Communicating Sequential Processes*, Prentice-Hall, 1985.

[6] Formal Systems(Europe) Ltd. Failure Divergence Refinement-FDR2 User Manual, Aug. 1999.

[7] CSP source code for CEPS, available from http://formal.korea.ac.kr/~igkim/ceps_psam.csp, 2005.