전자화폐 충전기능의 취약점 분석[1)]

김일곤[0*], 문영주*, 강인혜**, 이지연*, 한근희*, 최진영*

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

**서울시립대학교 기계정보공학과
inhye@uos.ac.kr

Vulnerability Anaysis of E-cash Load Transaction

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

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

요약

CEPS(Common Electronic Purse Specification) 전자지갑 규제 표준을 기반으로 한 전자상거래 서비스의 요구사항 및 시장성이 점차 큰 비중을 차지하고 있다. 전자지갑의 전자화폐 충전기능은 물품기능 만큼 매우 중요한 안전 필수 요구사항이다. CEPS에서는 LSAM (Load Secure Application Module) 기능을 통해, 전자금액 충전기능을 담당하도록 정의하고 있다. 전자지갑 본 논문에서는 전자지갑의 전자금액 충전기능을 설명하였다. 그리고 정형기법을 이용하여 CEPS 전자지갑 표준에서 정의한 전자금액 충전기능을 정형명세 및 정형검증 하여, 전자상거래시 발생할 수 있는 취약점을 확인하고 분석하였다.

1. 서론

초고속 통신망 및 이동통신 단말기의 보급으로 인해, 유.무선 네트워크를 기반으로 한 전자상거래 서비스 산업이 널리 확산되고 있다. 이와 더불어 기존의 동전이나 지폐와 같은 화폐개념에서 벗어 나, 전자금액을 이용한 지불 시스템이 도입되게 되었으며, 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]. CEPS 표준에서 정의한 전자지갑의 주요 요구사항은 전자금액 충전, 물품 구매, 거래 취소 및 환불 기능 등이다.

전자상거래 프로토콜을 비롯한 다양한 통신 프로토콜이 비정화된 설계 및 구현 과정을 통해, 설계자 및 개발자들이 예기치 못한 문제점들을 야기시키게 되었다. 이에 따라 정형화된 설계방법을 통해 통신 프로토콜을 디자인하고 안전성을 분석하기 위한 정형기법이 활용되고 있다. 이에 따라, 전자상거래 시스템의 행위를 정형적으로 명세하고 검증하기 위한 연구가 진행되어오고 있다.

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

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]. Jan J?rjens는 UML을 이용하여 처음으로 CEPS 전자지갑 시스템의 기능을 명세하는 연구를 진행하였다[4]. 그리고 [5] 논문에서는 CEPS 표준의 물품구매 기능의 보안성을 정형명세하고 분석하였다.

본 논문에서는 Casper 도구를 이용하여 CEPS 기반 전자금액 프로토콜의 행위를 정형명세하고 FDR 모델체킹 도구를 이용하여 보안 취약점을 분석하였다.

본 논문의 나머지 부분은 다음과 같이 구성되어 있다. 제 2장에서는 CEPS 표준 및 전자화폐 충전과정에 대해 소개하고, 제 3장에서는 프로토콜을 명세하고 검증하기 위한 Casper 및 FDR 모델체킹 도구에 대해 간략히 소개하고, 취약점 분석 결과를 언급하고자 한다. 마지막으로 제 4장에서는 결론 및 향후 연구 방향을 제시하고자 한다.

2. CEPS(Common Electronic Purse Specification)

전자지갑의 상호운용성 보장 프레임워크 표준규격이라 할 수 있으며, 1999년에 설립되었다. CEPS의 목적은 국제적으로 사용 가능한 전자지갑프로그램이 되기 위해 특정 조직이 요구

하는 모든 필요한 요소를 정의하는 것이다. 스마트 카드를 기반으로 한 전자지갑은 일반적으로 다음과 같은 행위가 이루어진다; 물품 구매, 전자화폐 충전, 구매 취소, 환불, 통화교환. 스마트 카드를 기반으로 전자지갑은 크게 전자화폐를 충전하는 LSAM(Load Secure Application Module)과 카드를 이용하여 제품 구매를 처리하는 PSAM(Purse Security Application Module) 모듈로 구성되어 있다. 본 논문에서는 전자화폐 충전기능을 담당하는 LSAM 기능의 취약점에 중점을 두어 언급하고자 한다. 그림 1은 CEPS 기반 전자화폐 충전 과정을 보여주고 있다. 그림 1에 명시된 기호 및 의미는 표 1을 참조하도록 한다.

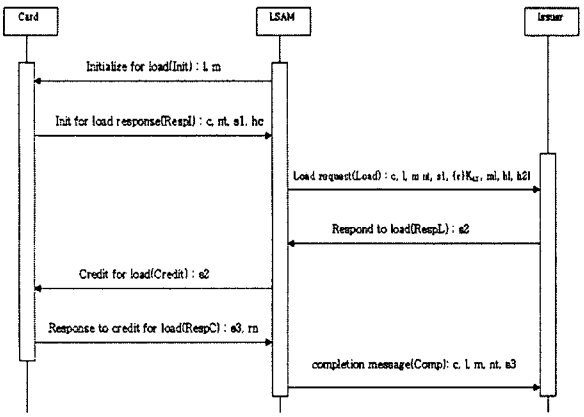

그림1. CEPS 기반 전자화폐 충전 프로토콜

표 1. 기호 및 의미

기호	의미
l	LSAM의 식별자
m	전자화폐 충전금액
i	카드 발행자(issuer)의 식별자
c	전자지갑 카드(card)의 식별자
nt	거래 번호
hc	l, c, nt 와 R_{CI} 에 대한 해쉬값
hl	c, l, m, nt에 대한 해쉬값
h2l	L, c, nt, rl에 대한 해쉬값
R_{CI}	카드와 카드 발행자 사이의 임의난수 세션키
s1	$S1=\{c, i, l, m, nt\}K_{CI}$
K_{CI}	카드와 카드 발행자와의 공유키
rn	LSAM에서 생성한 임의 난수
rl	LSAM에서 생성한 임의 난수
K_{LI}	LSAM과 카드 발행자와의 공유키
ml	ml={i, c, nt, l, m, s1}r
s2	$s2=\{c, nt, s1\}K_{CI}$
s3	$s3=\{c, i, nt, l, m, nt\}K_{CI}$

그림 1에서 보는 바와 같이, CEPS에서 정의한 전자화폐 충전 프로토콜은 카드(Card), 전자화폐 충전 시스템에 내장된 LSAM 및 카드 발행자(Issuer)로 구성되어 있다. 위에서 언급한 프로토콜이 동작하기 이전에, 카드 소지자는 자신이 소지한 현금화폐를 LSAM 기능을 내장하고 있는 시스템에 투입하는 시나리오를 가정해 볼 수 있다.

1 단계 : LSAM은 카드에게 Init 메시지를 보내서, 카드 소지자가 투입한 전자화폐 금액을 알리게 된다.
2 단계 : Card는 RespI 메시지를 보내서 nt, sl 및 hc 정보를 송신한다. hc 데이터는 R_{CI}에 대한 해쉬값을 포함하고 있다.
3 단계 : LSAM은 카드 발행자에게 LOAD 메시지를 보내서 전자화폐 충전금액에 대한 확인과정을 요청한다.
4 단계 : 카드 발행자는 3단계에서 보낸 메시지에 대해 정상적인 거래인지 확인해 준다.
5 단계 : 정상적인 거래인 경우, 카드 발행자는 LSAM에게 RespI 메시지를 보낸다.
6 단계 : LSAM은 Card에게 충전된 전자화폐 금액의 승인결과를 화면에 보여준다.
7 단계 : Card는 RespC 메시지를 LSAM에게 보내서, 거래가 정상적으로 이루어졌음을 알려준다.
8 단계 : LSAM은 Compl 메시지를 통해 거래의 종료의 통보한다.

3. Casper 명세 및 FDR 검증 결과

3.1 Casper 및 FDR 도구

Casper[6]를 이용하여 보안 프로토콜의 행위와 검증하고자 하는 속성을 명세한 후, Casper 컴파일 기능을 이용하여 자동으로 프로세스 대수형태의 CSP 언어로 변환할 수 있다. 마지막으로 자동 생성된 CSP[7] 모델을 FDR 도구[8]에 입력한 후, 비밀성, 인증 등과 같은 보안속성을 만족하는지 검사하게 된다. 만일 해당 보안속성을 위반하는 이벤트를 CSP 모델에서 찾게 되면, 반례를 보여주기 때문에 보안 취약점을 분석하고 개선하는데 도움을 준다. 논문의 페이지 제한상, 보다 상세한 내용은 [6][7][8]를 참조하기 바란다.

3.2 Casper를 이용한 전자화폐 충전기능 명세 및 검증

Casper 도구를 이용하여 전자상거래 프로토콜의 보안 행위를 명세하고 검증하기 위해서는 일반적으로 8개의 헤더섹션이 요구된다. 본 논문에서는 페이지 사정상, 중요한 몇 가지 헤더 섹션만을 명시하고자 한다.

그림 2는 CEPS 기반 전자화폐 충전 프로토콜에 대한 #Free variable과 #Protocol description와 헤더 섹션을 보여주고 있다. #Free variable은 프로토콜에서 사용되는 호스트의 타입 및 암호화 복호화 키를 정의한다. 예를 들어, c와 l은 각각 카드와 LSAM의 식별자를 나타내며, kli는 LSAM과 카드 발행자와의 세션키를 의미한다.

#Protocol description은 프로토콜의 통신 행위절차를 선언하고 있다. 예를 들어, 메시지 앞의 일련번호는 통신 순서를 의미하고 있다. 그리고 % 표시는 메시지의 전달기능을 표현할 때 사용된다. 즉, 2번 메시지에서 카드는 LSAM에게 kci 키로 암호화된 c, i, l 및 m 데이터를 포함하는 s1 메시지를 보내면, 3번 메시지에서 LSAM은 카드 발행자에게 s1 메시지를 전달하고 있음을 의미한다

```
#Free variables
c, l : Agent
i : Server
m, rn : Nonce
r, kli, kci : SessionKey
InverseKeys = (r, r), (kli, kli), (kci, kci)


#Protocol description
0.   -> l : c
1.  l -> c : m
2.  c -> l : i, c, {c, i, l, m}{kci} % s1
3a. l -> i : m, rn, s1 % {c, i, l, m}{kci}
3b. l -> i : {r}{kli}, {m, s1 % {c, i, l, m}{kci}}{r}
4.  i -> l : rn, {c, i, l, m}{kci} % s2
5.  l -> c : s2  % {c, i, l, m}{kci}
6.  c -> l : {c, i, l, m}{kci} % s3
7.  l -> i : m, s3 % {c, i, l, m}{kci}
```

3.3 명세 및 분석 결과

본 논문에서는 CEPS 기반 전자화폐 충전과정에서 발생할 수 있는 보안 취약점을 분석하기 위해, Casper 도구를 이용하여 보안 속성을 정의하고 보안 취약여부를 분석하였다.

Casper 도구에서는 #Specification 섹션 헤더를 통해 보안속성을 정의할 수 있다. 본 논문에서는 비밀성 및 인증 속성을 정의하고 분석하였다. 다음 코드는 #Specification 섹션 헤더를 이용하여 정의한 비밀성 및 인증 속성이다.

```
Secret(l, m, [i])
Agreement(l, i, [r, kli])
Agreement(i, l, [r, kli])
```

위 코드에서 'Secret'는 비밀성을 나타내며, 'Agreement'는 인증 속성을 나타내는데 사용된다. 예를 들어, 첫번째 줄은 "LSAM과 카드 발행자는 거래충전 금액(m) 이 악의적인 공격자에게 노출되지 않는다고 믿는다" 의미를 내포하고 있다. 그리고 두번째 줄은 "LSAM은 카드 발행자에게 r과 kli 데이터를 통해 인증을 받는다"는 의미이다.

전자상거래와 같은 보안 프로토콜의 취약점을 정형적으로 분석하기 위해서는 무엇보다 공격자 모델에 대한 가정이 중요시 된다. 본 논문에서는 공격자는 메시지 도청, 메시지 변조 및 정상적인 사용자로 위장하는 공격행위를 갖고 있으며, 공격자의 호스트 이름은 Mallory 라고 가정하였다. 또한 공격자는 모든 호스트의 공개키 정보 및 자신의 개인키 정보를 알고 있다고 설정하였다.

FDR 도구를 이용하여 CEPS 전자화폐 충전 프로토콜의 보안성을 분석한 결과 위에서 언급한 비밀성 및 인증속성을 만족하지 않는다는 사실을 확인하였다.

첫째, 전자화폐 충전거래 금액 m은 암호화 되지 않은 상태로 전달되는 영역이 존재하기 때문에 메시지 비밀성을 위배하고 있다.

둘째, 그림 1에서 언급한 Load 메시지상에서, LSAM은 ml 정보에서 r키를 이용하여 I, c, nt, l, m, s1 정보를 암호화하여 카드 발행자에게 송신하고 있다(ml={i, c, nt, l, m, s1}r). 그리고 r 암호화 키는 K_U 키로 암호화하여 카드 발행자에게 전달된다. 이 경우, 카드 발행자는 LSAM이 보낸 충전거래 금액 m을 보다 큰 금액 m' 로 변경할 수 있다. 이렇게 되면, 만일 카드를 소지한 고객이 10,000원 금액을 전자화폐 충전 장치에 투입하였을 경우, 카드 발행자는 100,000으로 거래금액을 변경하여 화폐충전기 매입자(load acquirer)로 하여금 보다 많은 금액을 카드 발행자에게 납부하도록 요구할 수 있다. 만일 대형 카드 발행자가 악의적인 목적으로 법적인 소송을 걸게 되면, 소규모 매입자들은 큰 피해를 당할 수 있게 된다.

4. 결론 및 향후 연구 방향

유·무선 네트워크의 발전과 더불어 스마트 카드의 확산은 전자화폐를 이용한 전자 상거래 서비스의 활성화를 가속화 시키고 있다. 또한 CEPS의 국제화 표준 준수 영역의 중요성이 증대되고 있다. 전자 상거래시 전자화폐에 대한 보안성 보장은 안전한 거래 질서를 확립하기 위한 중요 요구사항이다. 본 논문에서는 보안 프로토콜 검증 도구로 알려져 있는 Casper 및 FDR 검증 도구를 통해, CEPS 기반 전자화폐 충전 프로토콜의 비밀성 및 인증속성을 분석하였다. 그 결과 LSAM과 카드 발행자 사이에 보안 취약점이 존재함을 확인 할 수 있었다.

향후 연구방향으로는 충전화폐의 보안성을 유지시킬 수 있는 개선방안에 대해 연구하고자 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. Jrjens and G. Wimmel, "Security Modelling for Electronic Commerce: The Common Electronic Purse Specifications," 2001, pp. 489-506, 2001.

[5] 김일곤, 문영주, 방기석, 강인혜, 최진영, "CEPS(Common Electronic Purse Specification)의 정형 명세 및 보안성 분석," 정보과학회 춘계학술대회, 제31권, 제2호, pp.124-126, 2005.

[6] G.Lowe. "Casper: A compiler for the analysis of security protocols. 10th IEEE Computer Security Foundations Workshop, 1997.

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

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