CEPS(Common Electronic Purse Specification)의 정형명세 및 보안성 분석[1)]

김일곤[0*], 문영주*, 방기석**,강인혜***, 최진영*

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

**한림대학교 정보통신공학부
kbang@formal.korea.ac.kr

***서울시립대학교 기계정보공학과
inhye@uos.ac.kr

Formal Specification and Security Analyis of CEPS(Common Electronic Purse Specification)

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

Ki-Seok Bang**
**Division of Information Engineering and Telecommunication
Hallym University

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

요약

초고속 통신망 및 이동통신 단말기의 보급을 통해 전자상거래 서비스가 널리 확산되고 있으며, 이로 인해 유.무선 기반의 다양한 전자지불 시스템 및 표준들이 제안되고 있다. 그 중에서도 스마트 카드를 이용한 CESP 전자 상거래 표준이 많이 사용되고 있다. 본 논문에서는 Casper 및 FDR 도구를 사용하여, CEPS 표준 중에서 전자화폐를 이용한 물품 구입 프로토콜을 정형적으로 명세하고, 보안 취약점을 분석해 보았다.

1. 서론

초고속 통신망 및 이동통신 단말기의 보급을 통해 전자상거래 서비스가 널리 확산되고 있으며, 이로 인해 유.무선 기반의 다양한 전자지불 시스템 및 표준들이 제안되고 있다. 그 중에서도 CEPS(Common Electronic Purse Specification)는 전자지갑의 상호 운용성 보장 표준규격으로, 국제적으로 사용 가능한 전자지갑의 필요요소를 정의하고 있다[1]. 최근 스마트 카드의 발전과 더불어 대부분의 제품들이 CEPS 표준을 기반으로 한 전자지불 시스템들을 개발하고 있는 추세이다. 전자지불시스템의 보안성 유지는 상거래의 안전성을 보장하기 위한 가장 핵심적인 고려 사항이라 하겠다.

새로운 보안프로토콜의 제안과 더불어, 보안 프로토콜 설계상의 안전성을 분석하기 위한 다양한 연구가 진행되어 오고 있다.

그 중에서도 Casper 및 FDR을 이용한 정형명세 및 검증 방법은 보안 프로토콜의 취약점을 분석하는데 매우 효율적인 것으로 알려져 있다[2].

전자지갑의 기능을 정형적으로 명세하고 검증하고자 하는 연구는 Susan Stepney에 의해 처음 시도되었으며, 그는 Z 정형명세 언어를 이용하여 일반적인 전자지갑의 기능을 명세하고 증명하는 연구를 하였다[3]. Jan Jürjens는 UML을 이용하여 CEPS 전자지갑 시스템의 기능을 명세하는 연구를 진행하였다. 하지만, 그의 연구는 검증 측면 보다는 UML을 이용한 보안 시스템 명세 측면에 중점을 두고 있다[4].

본 논문에서는 Casper를 이용하여 CEPS의 전자화폐 구입(Purchase) 프로토콜을 정형적으로 명세하였으며, FDR 자동화 검증 도구를 이용하여 보안 취약점을 분석하였다.

본 논문의 나머지 부분은 다음과 같이 구성되어 있다. 제 2장에서는 CEPS 표준에 대해 간략히 소개하고, 제 3장에서는 프로토콜을 명세하고 검증하기 위한 Casper 언어와 FDR 도구를 이용한 보안 프로토콜 취약성 분석 방법에 대해 소개하고, 제 4장에서는 PSAM(Purchase

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

Security Application Module)의 구입 프로토콜 명세 및 검증 결과를 보여주고, 마지막으로 제 5장에서는 결론 및 향후 연구 방향을 제시하고자 한다.

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. 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 전자화폐를 이용한 물품 구매를 담당하게 된다. 본 논문에서는 PSAM 기능의 행위 및 보안 취약점에 대해서만 언급하고자 한다.

2.1 구입(Purchase) 기능

CEPS에서 정의한 전자화폐를 이용한 구입 기능은 그림 1과 같은 메시지 순서로도 나타낼 수 있다.

1. Card → PSAM : Ccert(ID_C, PK(C), {ID_C, PK(C)}SK(CA))
2. PSAM → Card : Pcert(ID_P, PK(P), {ID_P, PK(P)}SK(CA))
3. PSAM → Card : Debit(NT, {M, K_{CP}, {M, K_{CP}, ID_P, ID_C, NT}SK(P)}PK(C))
4. Card -> PSAM : Purchase({ID_C, ID_P, M, NT}K_{CP}, {M, {ID_C, ID_P, M, NT}K_{CP}}SK(C)))

그림 1. CEPS의 구입 프로토콜 메시지 순서도

표1. CEPS 구입 프로토콜 기호 및 의미

기호	의미
Card	스마트 카드
PSAM	POS 단말기에 내장된 PSAM
CA	제3의 인증기관
Ccert	인증기관에서 발행한 Card의 인증서
Pcert	인증기관에서 발행한 PSAM의 인증서
PK(X)	X의 공개키
SK(X)	X의 개인키
ID_C	Card의 식별자
ID_P	PSAM의 식별자
NT	거래번호
M	거래금액
K_{CP}	Card와 PSAM의 세션키
Debit	차입 메시지
Purchase	구입 메시지
{M}K	메시지 M을 K 키로 암호화

표 1은 그림1에서 사용된 기호 및 의미를 나타내고 있다. 스마트 카드를 이용하여 물품을 구매한 카드 소지자는 거래상인에게 구매 결제를 요청하게 되며, 카드는 POS에 내장된 PSAM과 통신을 시작하게 된다. 그림 1에 나타나 있듯이, 1번과 2번 메시지를 통해 Card와 PSAM은 CA가 발행한 서로의 인증서를 교환하게 되며, 3번 메시지에서 PSAM은 Card에게 Debit 메시지를 보내, 거래 금액을 확인하고 세션키를 교환하게 된다. 그리고 마지막으로 4번 Purchase 메시지를 통해 구입 절차를 끝내게 된다.

4. CEPS 구입 기능 정형명세 및 검증

4.1. Casper 및 FDR

Casper[5]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[6] 모델을 FDR 도구[7]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 [5][6][7]를 참조하기 바란다.

4.2 Casper 명세

제2장에서 기술한 CEPS의 구입 기능 메시지 순서도를 바탕으로, Casper를 이용하여 프로토콜의 행위 및 보안요구사항을 명세하였다.

```
#Protocol description
0.   -> c : p
1a. s -> c : {c, pkc}{SSK(s)} % digC
1b. s -> p : {p, pkp}{SSK(s)} % digP
2.   c -> p : c, pkc, digC % {c, pkc}{SSK(s)}
3a. p -> c : p, pkp, digP % {p, pkp}{SSK(s)}
3b. p -> c : {m, sk, {m, sk, p, c}{skp}}{pkc}
4.   c -> p : {c, p, m}{sk}, {m, {c, p, m}{sk}}{skc}

#Specification
Secret(c, sk, [p])
Secret(p, sk, [c])

#Intruder Information
Intruder = Mallory
IntruderKnowledge = {CARD, PSAM, CA, Mallory,
MM, PKc, PKp, PKm, SKm, SPK(CA)}
```

그림 2. Casper를 이용한 CEPS 구입 기능 명세

본 논문에서는 추가적으로 인증기관 S의 행위도 Casper 모델에 추가하였다. Casper 모델은 기본적으로 8개의 헤더로 나누어 지지만, 본 논문에서는 페이지 사정상 #Protocol description, #Specification 및 #Intruder Information 섹션 부분에 대해서만 기술하도록 하겠다. 그림 2는 CEPS의 구입기능에 대한 Casper 명세를 보여주고 있다. 그리고 본 논문에서는 암호 알고리즘은 안전하기 때문에 공격자가 암호키를 알지 못한 상태에서 암호문을 통해 암호키와 평문을 알아내는 것은 불가능하다고 가정하고 있다.

#Protocol description 섹션 헤더는 보안 프로토콜상의 메시지 전송을 표현하기 위해 사용된다. s는 인증기관, c는 전자지갑 카드 이고 p는 POS에 내장된 PSAM 장치를 의미한다. 0번 메시지에서는 명시적으로 카드 c가 PSAM p와 통신을 해야 한다는 사실을 알려주고 있다. pkc와 skc는 c의 공개키와 개인키 쌍을 의미하며, pkp와 skp는 p의 공개키와 개인키 쌍을 나타낸다. SSK(s)는 s 인증기관의 개인키를 나타내게 되며, {c, pkc}{SSK(s)}는 인증기관 s의 개인키로

서명된 인증서 Ccert를 의미하게 된다. 이와 마찬가지로, {p, pkp}{SSK(s)}도 인증기관 s의 개인키로 서명된 p의 인증서 Pcert를 표현하고 있다. Casper 기호 중, {data} % v의 표현은 data를 v 변수에 저장한다는 의미이며, v % {data}의 표현은 v 변수는 data의 내용을 담고 있음을 나타내기 위해 사용된다. 예를 들어, 1a 메시지에서 s는 인증서 Ccert를 digC 변수를 통해 c에게 전송하게 되며, 2번 메시지에서 c는 digC 변수를 통해 p에게 Ccert를 전달하고 있음을 의미하고 있다. #Specification 섹션 헤더는 검증하고자 하는 보안속성을 표현하는데 사용된다. Secret 기호는 비밀성(confidentiality)을 나타내며 다음과 같이 정의된다.

정의 4.1. 비밀성

만일 신뢰할 수 있는 호스트 A가 갖고 있는 중요정보 $x_1,\ldots,x_n$이 존재하고, 호스트 B 하고만 통신 할 경우, 다른 호스트 M은 중요정보를 가로채지 못한다는 의미이다. 즉, $M \not\ni \{x_1,\ldots,x_n\}$라고 표현할 수 있다.

따라서, 'Secret(c, sk, [p])' 표현식은 "c는 p하고만 중요정보 sk를 공유하고 있다고 믿는다"는 비밀성을 가리키고 있다. 이와 마찬가지로 'Secret(p, sk, [c])' 표현식은 "p는 c하고만 중요정보 sk를 공유하고 있다고 믿는다"는 비밀성을 나타낸다.

#Intruder Information은 공격자의 사전지식을 표현하기 위해 사용된다. 공격자의 사전지식을 어떻게 구성하느냐에 따라, 보안 취약점 탐지 유무가 결정된다. 본 논문에서 악의적인 공격자의 이름은 Mallory 이며, 그는 모든 호스트의 공개키를 알고 있다고 가정했다. SPK(CA)는 인증기관의 공개키를 나타낸다.

4.2 FDR 검증 결과

FDR 모델체커 도구를 이용해서 CEPS의 구입 프로토콜이 비밀성 속성을 만족하는지 검증하였다. 그 결과 Secret(c, sk, [p]) 와 Secret(c, sk, [p]) 속성을 만족하지 않는다는 것을 확인하였고, 다음과 같은 공격 시나리오를 발견하였다.

공격 시나리오

1.Card -> I_PSAM : Ccert(ID_C, PK(C), {ID_C, PK(C)}SK(CA))
2. I_PSAM -> PSAM' : Ccert(ID_C, PK(C), {ID_C, PK(C)}SK(CA))
3 PSAM' -> I_PSAM : Pcert(ID_P, PK(P), {ID_P, PK(P)}SK(CA))
4. I_PSAM -> Card : Pcert(ID_P, PK(P), {ID_P, PK(P)}SK(CA))
5. PSAM -> I_PSAM : Debit(NT, {M, K_{CP}, {M, K_{CP}, ID_P, ID_C, NT}SK(P)}PK(C))
6. I_PSAM -> Card : Debit(NT, {M, K_{CP}, {M, K_{CP}, ID_P, ID_C, NT}SK(P)}PK(C))
7. Card -> I_PSAM : Purchase({ID_C, ID_P, M, NT}K_{CP}, {M, {ID_C, ID_P, M, NT}K_{CP}}SK(C)))
8. I_PSAM -> PSAM' : Purchase({ID_C, ID_P, M, NT}K_{CP}, {M, {ID_C, ID_P, M, NT}K_{CP}}SK(C)))

위의 보안 취약점은 CEPS의 표준에 따라, 공격자 I는 POS단말기의 조작을 통해, 인터넷을 통해 다른 PSAM' 장치에 접속할 수 있다고 가정을 바탕으로 생성되었다. 전자화폐 구매를 위한 POS 장치를 소유한 거래상인의 직원으로 일하는 종업원이 공격자(I)인 경우, 그는 카드로부터 전송된 메시지를 인터넷을 통해 다른 PSAM' 장치로 전송 시킬 수 있도록 조작할 수 있게 된다. 이 경우 카드 소지자인 고객 또한 악의적인 공격자와 미리 공모하였을 경우, 고객은 물품을 구매한 후, 거래 금액을 전송하고 금액이 정상적으로 POS의 디스플레이 화면에 출력된 것을 거래상인에게 확인시켜 주고 정상적인 거래가 이루어진 것 처럼 조작할 수 있다. 하지만, 추후 거래상인은 월말 결산이 이루어 질 때쯤 거래금액이 총합계가 부족함을 확인하게 된다. 위 보안 취약점은 처음 [4]에 의해 발견되었으며, 보안 취약점을 해결하기 위한 방안으로 POS내의 PSAM과 DISPLAY 장치의 통신 채널을 구분하지 않고 하나로 통합하여, 다른 PSAM'을 통해 DISPLAY 장치에 거짓 정보가 출력되지 않도록 제안하고 있다.

5. 결론 및 향후 연구 방향

스마트 카드의 보급 확산 및 유,무선 네트워크의 활성화와 더불어 CEPS 표준을 기반으로 한 전자상거래 시스템 큰 비중을 차지하게 되었다. 전자상거래 시스템의 경우, 보안성 확보는 고객과 기업간의 안전한 상거래 정착을 위한 가장 중요한 고려 사항이라 하겠다. 본 논문에서는 CEPS의 구매기능을 보안 프로토콜 관점에서, Casper 도구를 이용하여 정형적으로 명세하고 FDR 자동화 검증도구를 이용하여 보안 취약점을 분석해 보았다. 그 결과, 정형화된 모델로부터 CEPS 구매 기능의 보안 취약점을 확인할 수 있었다.

향후 연구방향으로는 CEPS의 전자화폐 충전기능의 보안성을 검증해보고자 한다. 또한, CEPS의 보안 프로토콜상에서 중요키 정보의 노출관점에서 분석하지 않고, 안전한 상거래를 통해 고객의 거래 금액이 통신 도중 손실되거나 증가되지 않는다는 accountability 속성을 검증해 보고자 한다.

참고문헌

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

[2] P. Ryan and S. Schneider, Modelling and Analysis of Security Protocols, Addison Wesley, 2001.

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

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

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

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

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