論文
7-3-9

안전한 모바일 전자상거래를 위한 분석 연구 (A Study on Analysis for Secure M-Commerce Transaction)

이지연 (Lee Ji Yeon) [1)]

요 약

지금까지의 많은 모바일 전자상거래 프로토콜들은 비정형화된 설계 및 검증 방법을 통해 개발되었다. 그 결과 유.무선 네트워크 분야에서 보안상 안전하다고 여겨왔던 많은 프로토콜들의 보안 취약점들이 하나둘씩 발견되어오고 있다. 현재, 스마트 카드의 확산과 더불어 CEPS 전자상거래 표준을 이용한 모바일 전자상거래 영역이 큰 각광을 받고 있다. 본 논문에서는 정형적 검증 방법을 이용한 전자상거래 프로토콜의 보안성 분석을 위한 방법에 대해 기술하고, CEPS에서 정의한 구매 프로토콜의 보안 취약점을 분석한다. 마지막으로 구매 프로토콜의 보안 취약점을 해결하기 위한 방안에 대해 언급한다.

Abstract

M-commerce protocols have usually been developed using informal design and verification techniques. However, many security protocols thought to be secure was found to be vulnerable later. With the rise of smart card's usage, mobile e-commerce services with CEPS which is one of e-commerce transaction standards has been increased. In this paper, we describe a methodology to analyze the security of e-commece protocols and identify the security vulnerability of the CEPS based good purchase and e-money load protocols using formal verification technique. Finally, we discuss a countermeasure against the vulnerability in the purchase transaction protocol.

논문접수 : 2006. 5. 11.
심사완료 : 2006. 5. 30.

1) 정회원 : 동남보건대학 e-비즈니스과 조교수

** 이 논문은 2005년도 동남보건대학 연구비 지원에 의하여 수행된 것임

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. 전자 지불시스템의 보안성 유지는 상거래의 안전성을 보장하기위한 가장 핵심적인 고려 사항이라 하겠다.

지금까지의 모바일 프로토콜의 대부분은 비정형화된 설계 및 검증 방법을 통해 개발되었다. 그 결과 유.무선 네트워크 분야에서 보안상 안전하다고 여겨왔던 많은 모바일 전자상거래 프로토콜들의 보안 취약점들이 하나둘씩 발견되어오고 있다[2]. 이에 따라, 설계단계에서 보안 프로토콜의 보안성, 인증 및 무결성과 같은 보안 속성들을 검증하기 위해 정형기법이 활용되어 왔다. 특히, Casper 및 FDR 도구를 이용한 정형적 설계 및 검증 방법은 많은 보안 프로토콜의 취약점을 밝혀낼 수 있었다[2].

기존의 정형적 설계 및 분석 방법론은 대부분 유선 네트워크 상에서 동작하는 보안프로토콜의 보안성을 분석하는데 중점을 두었다. 현재 무선 네트워크의 활성화와 더불어 다양한 모바일 프로토콜들이 등장하고 있다. 그리고 모바일 디바이스를 이용한 소프트웨어 다운로드 및 전자상거래와 같은 유료화 서비스가 각광을 받고 있다. 이에 따라, 모바일 사용자 및 서비스 제공자간의 안전한 통신 및 서비스 보장을 위해 모바일 프로토콜이 제안되고 있으며, 보안프로토콜의 안전성 보장은 중요한 연구과제로 부각되고 있다.

본 논문에서는 Casper/FDR 도구를 이용한 정형적 설계 및 검증방법을 사용하여, CEPS 전자상거래 표준에서 정의한 스마트카드를 이용한 물품 구매 프로토콜의 보안 취약점을 분석한다. 본 논문의 구성은 다음과 같다. 제2장에서는 정형기법을 이용하여 보안프로토콜의 취약점을 분석하는 관련연구를 소개하고, 제3장에서는 Casper 및 FDR 도구를 이용한 보안프로토콜 정형적 설계 및 검증 방법론에 대해 간략히 설명한다. 제4장에서는 CEPS 전자상거래 표준에 대해서 간략히 소개한다. 제5장에서는 CEPS 기반 물품 구매 프로토콜의 보안속성을 정의하고 검증결과를 보여준다. 마지막으로 제6장에서 결론을 맺고자 한다.

2. 관련연구

보안 프로토콜의 안전성을 검증하기 위한 방법은 크게 모델체킹과 정리증명 방법으로 나누어진다. 모델체킹의 장점은 자동화 검증도구가 지원된다는 사실이다. 즉, 사용자가 시스템의 모델을 입력하고 요구 사항 명세를 나타내는 속성들을 입력하면 도구는 자동적으로 모델의 상태를 검사하여, 속성을 만족하지 못하는 경우, 반례를 보여주어 모델의 어느 부분이 잘못되었는지를 쉽게 알 수 있게 해 준다는 것이다. 반면에 정리증명 방식은 증명과정에 사람의 개입이 필요하기 때문에, 보안 프로토콜을 논리적으로 증명하기에 앞서 가정을 세우고, 논리 추론 규칙에 따라 보안 취약점을 추론해 내기가 쉽지 않다.

Roscoe와 Goldsmith는 CSP 언어를 이용하고 FDR 모델체킹 도구를 이용하여 보안 프로토콜의 안전성을 검증하는 연구의 기반을 마련하였다[3]. 대부분의 보안 프로토콜 검증 연구는 유선 네트워크상에서 사용되는 프로토콜의 취약점을 검증하는데 중점을 두어 왔으며, 상대적으로 모바일 프로토콜의 보안 취약점을 검증한 논문은 그다지 많지 않다.

Coffey와 Dojen은 정리증명 방법에 기반을 둔 GNY 로직을 이용하여, BCY 모바일 프로토콜의 보안 취약점을 지적하고 새로운 CDF-BCY 프로토콜을 제안하였다[4]. 하지만, GNY 로직

을 이용한 정리증명 방법의 경우 수학적 논리 전문가가 아니면, 보안 취약점을 분석해 내기가 어렵다는 단점을 보여주고 있다.

전자지갑의 기능을 정형적으로 명세하고 검증하고자 하는 연구는 Susan Stepney에 의해 처음 시도되었으며, 그는 Z 정형명세 언어를 이용하여 일반적인전자지갑의 기능을 명세하고 증명하는 연구를 하였다[5]. Jan Jűrjens는 UML을 이용하여 CEPS 전자지갑 시스템의 기능을 명세하는 연구를 진행하였다. 하지만, 그의 연구는 검증 측면 보다는 UML을 이용한 보안 시스템 명세 측면에 중점을 두고 있다[6].

3. Casper와 FDR 도구

3.1 Casper(A Compiler for the Analysis of Security Protocols)

CSP[7] 언어를 이용하여 보안프로토콜 행위를 명세하고 FDR[5] 정형검증 도구를 이용하여 보안속성을 검증하는 연구가 진행되었다. 하지만, CSP 언어를 이용한 정형명세과정은 정형적 설계 방법에 익숙치 않은 보안프로토콜 설계자에게는 매우 복잡한 명세언어라는 단점을 갖고 있었다. 이에 따라, 보안프로토콜의 행위를 간략히 명세할 수 있도록 Casper 도구가 개발되었다[8]. Casper 도구로 보안프로토콜의 행위와 검증속성을 명세하게 되며, 자동변환기능을 이용해 CSP 명세코드를 생성할 수 있다. 결국, 자동 생성된 CSP 명세코드를 FDR 정형검증도구에 입력하여 보안프로토콜을 검증하게 된다. 다음은 Casper 명세에서 사용되는 기본적인 7개의 섹션헤더와 의미를 간략히 보여주고 있다.

•#Free variables : 변수의 타입 및 함수 선언
•#Process : 통신 에이전트의 초기 상태 표현
•#Protocol description : 통신 에이전트간의 메시지 교환 표현
•#Specification : 검증하고자 하는 보안속성 선언
•#Actual variable : 통신 에이전트가 사용하는 실제 데이터 타입 및 이름 선언
•#Function : 프로토콜에서 사용하는 함수선언
•#System : 통신 에이전트의 초기 상태정보 표현
•#Intruder information : 공격자의초기상태정보 표현

3.2 FDR(Failure Divergence Refinement)

FDR 도구는 CSP 명세언어를 입력으로 받아들이는 모델체킹 도구로서 옥스포드 대학에서 개발되었다[9]. 이 도구는 CSP 명세언어로 기술된 보안프로토콜 모델이 보안성 및 인증속성과 같은 보안속성들을 만족하는지 검증하게 되며, 만일 만족하지 않을 경우에는 CSP 이벤트로 기술된 반례(counterexample)을 보여주어 보안상 취약점 분석을 도와준다.

FDR 도구는 3가지의 검증방법을 지원하고 있다.

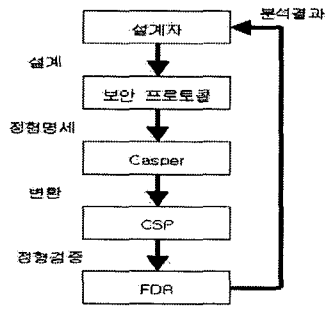
- **Trace refinement : 안전성(safety) 검증**
- **Failures refinement : 교착상태(deadlock) 검증**
- **Failures - Divergence : 라이브락(livelock) 검증**

[그림 1] 은 Casper 및 FDR 도구를 이용하여, 보안프로토콜을 정형적으로 설계하고 검증하는 과정을 보여주고 있다.

첫째, 검증하고자 하는 보안프로토콜을 Casper 도구로 명세한다.

둘째, Casper의 자동변환기능을 이용해 CSP 명세코드를 생성한다.

셋째, FDR 도구에 CSP 명세코드를 입력한다.



[그림 1] Casper 및 FDR 도구를 이용한 보안프로토콜 설계 및 검증

[Fig. 1] Security protocol specificatio and varification with Casper and FDR

넷째, FDR 도구의 검증결과를 분석한다.

마지막으로 보안프로토콜의 취약점이 밝혀지면, 문제점을 수정하여 동일한 설계 및 검증절차를

반복 수행한다.

4. CEPS(Common Electronic Purse Specifications)

CEPS는 전자지갑의 상호 운용성 보장 국제표준으로 1999년에 제정되었다[1]. CEPS의 목적은 국제적으로사용 가능한 전자지갑 프로그램이 되기 위한 필수 기능 및 요구사항을 정의하는 것이다. CEPS에 정의된 전자지갑의 주요 기능은 물품을 구매하거나 전자화폐를충전하는 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.

4.1 구입(Purchase) 프로토콜

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 27] CEPS의 구입 프로토콜 메시지 순서

CEPS에서 정의한 전자화폐를 이용한 구입 기능은 그림 2와 같은 메시지 순서로도 나타낼 수 있다.

[Fig. 2] Purchase protocol message sequences of CEPS

<표 1>은 [그림2]에서 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 교환하게되며, 3번 메시지에서

PSAM은 Card에게 Debit 메시지를 보내, 거래금액을 확인하고 세션키를 교환하게 된다. 그리고 마지막으로 4번 Purchase 메시지를 통해 구입 절차를 끝내게 된다.

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
IDC	Card의 식별자
IDP	PSAM의 식별자
NT	거래번호
M	거래금액
KCP	Card와 PSAM의 세션키
Debit	차입 메시지
Purchase	구입 메시지
{M}K	메시지 M을 K 키로 암호화

<표 1> CEPS 구입 프로토콜 기호 및 의미

<Table 1> Symbols and meaning of CEPS purchase protocol

5. CEPS 구입 기능 정형명세 및 검증

5.1. Casper 및 FDR

Casper[7]를 이용하여 보안 프로토콜의 행위와 검증하고자 하는 속성을 명세한 후, Casper 컴파일 기능을 이용하여 자동으로 프로세스 대수 형태의 CSP 언어로 변환할 수 있다. 마지막으로 자동 생성된 CSP[8] 모델을 FDR 도구[9]에 입력한 후, 비밀성, 인증 등과 같은 보안속성을 만족하는지검사하게 된다. 만일 해당 보안속성을 위반하는 이벤트를 CSP 모델에서 찾게 되면, 반례를 보여주기 때문에 보안 취약점을 분석하고 개선하는데 도움을 준다.

5.2 Casper 명세

제2장에서 기술한 CEPS의 구입 기능 메시지

순서도를 바탕으로, Casper를 이용하여 프로토콜의 행위 및 보안요구사항을 명세하였다.

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 c가PSAM 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.

비밀성 : 만일 신뢰할 수 있는 호스트 A가 갖고 있는 중요정보 $x_1,...,x_n$이 존재하고, 호스트 B 하고만 통신할 경우, 다른 호스트 M은 중요정보를 가로채지 못한다는 의미이다. 즉, M은 $\{x_1,...,x_n\}$의 원소들을 포함할 수 없다.

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.

5.3 FDR 검증 결과

FDR 모델체커 도구를 이용해서 CEPS의 구입 프로토콜이 비밀성속성을 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(IDC, PK(C), {IDC, PK(C)}SK(CA))
2. I_PSAM -> PSAM' : Ccert(IDC, PK(C), {IDC, PK(C)}SK(CA))
3 PSAM'-> I_PSAM : Pcert(IDP, PK(P), {IDP, PK(P)}SK(CA))
4. I_PSAM -> Card : Pcert(IDP, PK(P), {IDP, PK(P)}SK(CA))
5. PSAM -> I_PSAM : Debit(NT, {M, KCP, {M, KCP, IDP, IDC, NT}SK(P)}PK(C))
6. I_PSAM -> Card : Debit(NT, {M, KCP, {M, KCP, IDP, IDC, NT}SK(P)}PK(C))
7. Card -> I_PSAM : Purchase({IDC, IDP, M, NT}KCP, {M, {IDC, IDP, M, NT}KCP}SK(C)))
8. I_PSAM -> PSAM': Purchase({IDC, IDP, M, NT}KCP, {M, {IDC, IDP, M, NT}KCP}SK(C)))

위의 보안 취약점은 CEPS의 표준에 따라, 공격

자 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 [6]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.

6. 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 중요 키 정보의 노출관점에서 분석하지 않고, 안전한 상거래를 통해 고객의 거래 금액이 통신 도중 손실되거나 증가되지 않는다는 accountability 속성을 검증해 보고자 한다.

참 고 문 헌

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

[2] G. Lowe, "Breaking and Fixing the Needham-Schroeder Public-Key Protocol," TACAS 96, pp.147-166, 1996.

[3] A. Roscoe and M. Goldsmith , "The Perfect Spy for Model-Checking Cryptoprotocols," Proceedings of the 1997 DIMACS Workshop on Design and Formal Verification of Security Protocols, 1997.

[4] T. Coffey and R. Dojen, "Analysis of a mobile communication security protocol," Proceeding of the 1st international symposium on Information and communication technologies, pp. 322- 328, 2003.

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

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

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

[8] G. Lowe, "Casper: A Compiler for the Analysis of Security Protocols," 10th IEEE Computer Security Foundations Workshop, 1997.

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