USIM 탑재 스마트폰 기반 모바일 신용카드 결제 프로토콜의 안전성 향상 방안 연구*

지은화O 김애영 이상호
이화여자대학교 공과대학 컴퓨터공학과
jhee0411@ewhain.net, kay@ewhain.net, shlee@ewha.ac.kr

A Study on the Security Improvement of Mobile Credit Card Payment Protocol for USIM-based Smart Phone

Eun-Wha JheeO Ae-Young Kim and Sang-Ho Lee
Dept. of Computer Science and Engineering, Ewha Womans University

1. 서론

스마트폰 사용자가 급증하면서 인터넷의 전자상거래 활성화가 모바일 환경에서 그대로 재현되고 있다. 특히 어플리케이션을 실행할 수 있는 스마트폰의 특성을 기반으로 신용카드를 이용한 모바일 결제의 사용이 빠르고 편리함을 장점으로 내세워 증가하고 있다. 그러나 결제 시 통일 되지 않은 각 결제 시스템에서의 입력 카드 정보의 상이성 및 암호화 되지 않은 결제 정보 입력으로 애플리케이션 단에서의 정보 노출 및 금융 사고의 위험성이 있다. 본 논문에서는 이러한 취약점을 고려해 신용카드 정보의 비밀성을 유지 할 수 있는 USIM 기반의 스마트폰에서의 안전한 모바일 신용카드 등록 및 결제를 위한 E2E 암호화 적용 결제 프로토콜을 설계하고 분석한다.

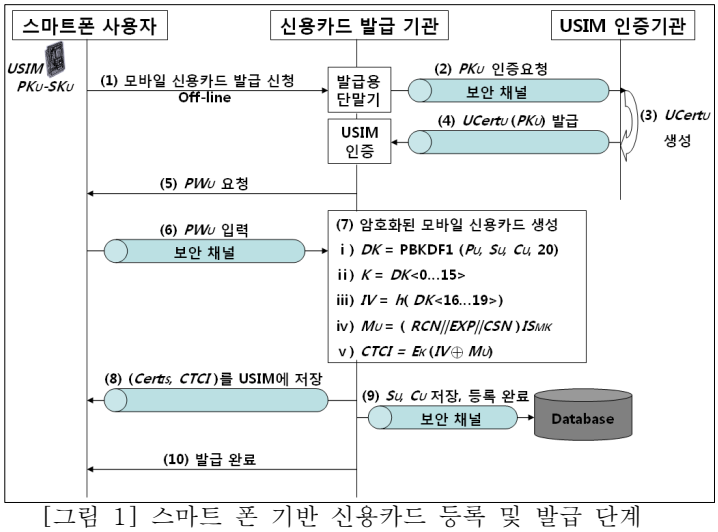
2. 본론

본 논문의 제안 모델은 스마트폰에서의 신용카드를 통한 전자상거래의 결제 시 필요한 카드 정보를 그대로 입력하는 기존의 방법과는 달리 암호화된 카드정보를 입력하여 카드 사용 정보의 비밀성을 높인다. 이를 위하여 PKCS#5(Public Key Cryptography Standards #5)에서 정의한 PBES1(Password Based Encryption Scheme 1, 패스워드 기반의 키 암호화 기법)을 바탕으로 카드 사용자의 패스워드 암호화 기법을 응용한다. [그림 1]과 같은 단계로 스마트폰에 탑재된 USIM에 모바일 신용카드를 발급받아 등록하는 프로토콜을 제안한다.

(1) 스마트폰 사용자 U는 오프라인을 통하여 카드 발급 기관 IS에게 스마트폰에 탑재된 USIM를 통한 신용카드 발급을 요청한다.
(2) IS는 U의 신원 확인 후 안전한 통신 채널을 통하여 USIM 등록 인증 기관에 U의 USIM 공개키 PK_U에 대하여 인증 요청을 한다.
(3) USIM 인증 기관은 U의 신원 및 USIM 등록 확인 후, U의 USIM 등록 인증서 $UCert_U$를 생성한다.
(4) IS는 USIM 인증 기관으로부터 받은 $UCert_U$(PK_U)에 의하여 U의 USIM 등록을 인증한다.
(5) IS는 U의 모바일 신용카드를 발급하기 위해 U에게 카드 비밀번호 PW_U 4자리를 요청한다.
(6) U는 안전한 통신 채널을 통하여 PW_U를 입력한다.
(7) IS는 U로부터 받은 PW_U를 기반으로 암호화 된 모바일 신용카드를 생성한다.

i) U가 PW_U를 입력하면 IS는 U를 위한 난수 S_U와 계산 반복 횟수 C_U를 생성한다. PBES1에서 사용하는 키 추출 함수인 PBKDF1는 PW_U, S_U, C_U와 함께 SHA-1 해쉬함수 사용으로 20바이트 추출키 DK를 생성한다.
ii) 생성된 DK에서 처음 16바이트를 암호화된 비밀키 K로 한다.
iii) IV는 DK에서 나머지 4바이트에 대한 일방향 해쉬 함수에서 계산한 16바이트를 사용한다.

* 이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 대학중점연구소 지원 사업으로 수행된 연구임(2009-0093827)



[그림 1] 스마트 폰 기반 신용카드 등록 및 발급 단계

iv) 실제카드번호 *RCN*과 유효기간 *EXP* 및 3자리 보안번호 *CSN*에 대하여 카드 발급 기관의 마스터키 IS_{MK}로 대칭키 암호화에 의하여 암호화된 중간 암호문 M_U을 생성한다.

v) 생성된 M_U에 대하여 *IV* 와 비밀키 *K*를 사용하여 SEED 블록 암호화 알고리즘에 의해 개인 신용카드 정보 암호문 *CTCI*를 생성한다.

(8) 카드 발급 기관은 통합인증기관 CA에게 자신이 발급한 것임을 인증하는 인증서 $Cert_{IS}$를 요청하여 *CTCI* 정보와 함께 카드 사용자의 스마트폰 USIM 내에 안전하게 저장시킨다.

(9) 카드 발급 기관은 차후 *U*의 카드 사용시 검증을 위하여 S_U, C_U만을 카드 발급 기관의 안전한 저장장치에 저장 후 모든 과정의 데이터는 삭제한다.
(10) *IS*는 *U*의 USIM을 기반으로 암호화된 모바일 신용카드 발급 및 등록을 완료한다.

제안한 모바일 신용카드 등록 프로토콜에 의하여 생성된 암호화된 모바일 신용카드를 이용하여 E2E 암호화 적용 결제 프로토콜을 설계한다. 본 결제프로토콜은 S. Fourati의 3-D secure 기법을 사용하여 X. Wang 등이 제안한 모바일 결제 프로토콜을 기반으로 한다[1,2]. 3-D secure 기법은 메시지 복구 서명과 공개키 기반 암호 기법을 적용하고, 신뢰할 수 있는 제 3자를 참여시킨 결제 기법이다. Wang의 모델은 참여객체인 구매자와 카드 발행기관 사이에 발생하는 직접적인 통신이 이루어질 필요가 없도록 개선된 것이다. 이를 응용한 제안 결제프로토콜은 E2E 암호화를 통해 스마트폰 내부에서부터 모바일 네트워크 및 결제 서버까지의 모든 경로에서 사용자의 카드정보에 대한 비밀성을 효과적으로 제공한다. 즉, 패스워드 기반 암호화에 따라 암호화 된 신용카드의 직접적인 정보 획득은 패스워드를 아는 카드 사용자의 입력에 따른 복호화 없이는 불가능하다. 또한 모바일 전자상거래상의 카드 사용을 원하는 구매자와 카드 결제 승인 여부를 판단하는 발급 기관은 신용카드 등록 단계에서 발급 된 공개키를 기반으로 결제 관련의 생성 메시지에 대하여 제 3자 접근을 불가하게 한다. 따라서 오프라인 및 온라인 상에서 어떠한 카드 정보도 노출되지 않아 카드 사용에 있어 기밀성을 보장한다.

3. 결론

본 논문에서는 신용카드 정보의 비밀성을 유지 할 수 있는 USIM 기반의 스마트폰에서의 안전한 모바일 신용카드 등록 및 결제를 위한 E2E 암호화 적용 결제 프로토콜을 제안하였다. 스마트폰을 이용한 전자상거래에서의 카드 결제 시 오프라인 및 애플리케이션 단에서 나타날 수 있는 카드 정보 노출의 취약점을 고려하였다. 제안한 신용카드 등록 프로토콜을 사용한 모바일 신용카드는 USIM 안에 카드의 정보들이 모두 암호화 된 하나의 암호문 형태로 저장되어 있다. 따라서 사용자의 카드 결제를 위한 패스워드 입력 외의 신용카드의 많은 정보 입력을 원클릭 형태로 대신함으로써 데이터 입력에서의 사용자 편의성을 증가 시켰다. 또한 함께 제안한 결제 프로토콜은 공개키 기반 암호 기법 및 결제 구간 별 세션키 사용으로 모바일 전자상거래에 사용하는 신용카드에 대하여 사용 입력에서 결제 완료까지의 비밀성 등 데이터 안전성을 확보한다. 앞으로 스마트폰을 통한 전자결제시스템에서의 강력하고 경량이며 종단간의 보안상 안전한 암호 프로토콜 및 스마트 전자결제시스템의 보안 표준화 연구가 더욱 필요하다.

참고 문헌

[1] S. Fourati, "Protocol Specification Core Functions of Visa International 3-D Security Protocol," *Wireless Communications, Issue7, 353-360, 2002.*
[2] X. Wang, N. Cui, "Research of Security Mobile Payment Protocol in Communication Restrictions Scenarios," *Computational Intelligence and Security, 2009.*