안전한 결제 환경을 위한 NFC 기반 모바일 결제 시스템

김대석, 박성욱, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail:[dskim8708, swpark, imylee]@sch.ac.kr

Mobile payment system based on NFC for secure payment environment

Dae-Suk Kim, Sung-Wook Park, Im-Yeong Lee
Dept. of Computer Software Engineering, Soonchunhyang University

요 약

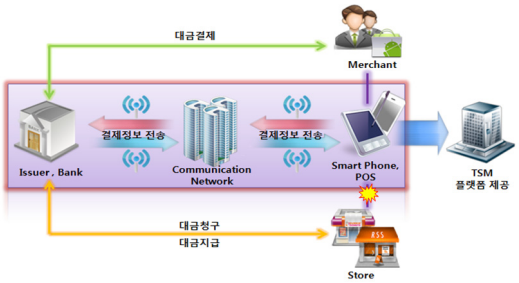
NFC 기능을 탑재한 스마트폰의 보급이 증가하고 점차적으로 NFC를 활성화하여 고객에게 편리함을 주려는 기업들이 늘어나고 있다. 하지만 기존의 NFC 기반 Payment System의 경우 사용자의 개인정보를 부분적으로 암호화하지 않은 것과 내부 및 제 3자의 개인정보 유출, 그리고 개인정보를 무단활용을 대표적인 문제점으로 나타낼 수 있다. 뿐만 아니라 도난 및 분실의 위험으로 인한 피해가 있을 수 있다. 이러한 문제점들로 인하여 본 연구에서는 자체적인 NFC 보안에 사용자 어플리케이션 실행 시 한 번의 개인정보 입력에 따른 암호화로써 NFC 단말기 간의 정보를 주고 받을 때 암호화를 할 수 있도록 구현하고자 한다. 이렇게 함으로써 NFC를 이용하여 결제를 하였을 시에 암호화 된 개인정보이기 때문에 외부의 공격자로부터 보안에 대한 위협을 줄일 수 있으며, 도난과 분실에도 개인정보가 식별되지 않기 때문에 보다 안정성을 높일 수 있다.

1. 서론

NFC(Near Field Communication)는 13.56MHz대역의 비접촉식 근거리 무선 통신 기술로 작동 방법이 간편하여 사용자 측면에서 쉽게 그 기능을 이용할 수 있으며, 사업자 측면에서도 기존 서비스 및 다른 단말기들과 쉽게 융합이 가능해 다양한 서비스를 제공할 수가 있다. 현재 NFC는 스마트폰에서 NFC 기능을 지원하고 있어서 스마트폰을 이용한 정보의 송·수신을 위한 매개체로 활용하여 결제, 의료, 개인인증 등 다양한 분야에서 융·복합된 형태의 서비스로 NFC 서비스가 전개 될 전망이다. 이렇듯 NFC의 도입으로 인해 NFC를 기반으로 한 모바일 결제(Mobile Payment) 시장에 대한 관심이 고조되고 있다. 특히 구글, 애플 등 기존의 플랫폼 사업자가 이동통신 사업자들을 중심으로 모바일 결제시장을 선점하기 위한 노력들이 활발히 전개되고 있다. 하지만 이러한 NFC서비스는 NFC 사업자가 서비스 제공 시 다양한 개인정보의 수집, 이용, 제공, 보관, 파기 등과 같은 개인정보 취급이 발생할 것으로 예상된다. 특히 이용자의 개인정보 및 성향 등을 분석하여 각 이용자에 특화된 형태의 맞춤형 서비스로 그 서비스가 제공될 경우, 개인정보의 수집, 이용, 제공, 보관, 파기 등과 같은 개인정보의 취급이 과도하게 발생할 수 있다. 본 논문에서는 기존의 결제 시스템에서의 개인정보가 많이 기입이 됨에 따라서 암호 알고리즘을 이용하여 사용자인증에 대한 정보를 최소화하여 도난이나 분실 시에 정보를 취득할 수 없도록 하는 결제 보안 솔루션을 설계 및 구현하였다. 본 논문의 구성은 2장에서 기존의 사용되고 있는 Google의 Payment System에 대한 방식과 NFC구조 및 기능을 기술하고 3장에서는 결제 보안 솔루션의 보안요구사항을 기술한다. 4장에서는 이를 만족하는 제안방식에 대하여 기술하고, 5장에서는 제안방식의 구현에 대하여 기술하며, 마지막으로 6장에서 결론을 맺는다.

2. 관련 연구

본 장에서는 기존 Google의 Payment System에 대해 분석하고, 본 논문에서 사용할 NFC의 구조 및 기능을 기술한다.



(그림 1) Google Wallet Payment System 구조

<표 1> NFC 기능

mode	특 징
Peer to Peer	- 장치 간의 논리적인 링크 수준의 제어 프로토콜 - NFC 호환 단말기 간의 콘텐츠 또는 프로그램의 송수신 가능
Read & Write	- Card Reader와 같이 Tag등의 데이터를 읽고 쓰는 기능 - 비 접촉식 통신 API 지원
Card Emulation	- 스마트카드와 같은 기능 - 비 접촉식 통신 API 지원

2.1 Google의 payment system 분석

NFC를 이용한 Google Wallet Payment System에서 볼 때 사용자가 NFC 단말기를 통하여 결제를 요청하게 되면 소매점의 POS(Point of sales) 단말을 통해 개인정보가 은행으로 전달되게 되며 매입 및 결제사가 개인정보와 결제 계좌를 대조하여 결제를 승인하고 통신사가 중간에서 데이터를 전송하게 해주는 방식을 취하고 있으며, 현재 이러한 방식을 Master카드와 사업적 관계를 구축하여 사용하고 있지만, 스마트폰과 상점의 단말기간의 명확하고 신뢰할만한 암호화 작업이 없으므로 사용자의 개인정보가 노출이 될 수 있다는 점을 볼 수 있다(그림 1 참조).

2.2 NFC 구조 및 기능

NFC의 동작 방식은 크게 카드 에뮬레이터, 리더 및 라이터, P2P의 3가지 모드로 작동한다. 이러한 기능들로 NFC는 RFID태그를 이용자의 단말기로 읽어 들일 수도 있으며, 스마트폰에 탑재함으로써 암호화 기술이 적용되어 개인정보를 활용한 무선통신 서비스 이용에 대한 소비자의 부담과 이용절차를 간소화 할 수 있다(표 1 참조).

3. 보안 요구사항

본 장에서는 본 기존 Payment System에서 암호 알고리즘을 적용하여 진행하는 제안방식에 대한 보안 요구사항을 알아본다.

3.1 보안 요구사항

본 연구는 기밀성, 무결성, 사용자 인증에 대하여 다음과 같은 보안 요구사항을 가진다.

(그림 2) 시나리오

- 기밀성: 거래정보와 결제정보를 요청 시에 사용자의 정보가 노출이 되어서는 안된다. 거래정보와 개인정보를 암호화하여 제 3자가 취득하더라도 알아볼 수가 없어야 한다.
- 무결성: Issuer가 가지고 있는 사용자의 개인정보와 사용자가 전송한 개인정보의 내용이 일치해야 한다. 따라서 Issuer의 데이터베이스에 있는 사용자 정보를 전송하는 과정에서의 데이터의 내용에 대한 위·변조 및 삭제 등과 같이 변경이 없어야 한다.
- 사용자 인증: Issuer에서 관리하는 데이터베이스의 정보를 이용하여 사용자의 정보를 확인하는 것으로 사용자인증을 진행할 때 암호화된 데이터를 복호화 하여 사용자의 신원과 개인정보를 확인할 수 있어야 한다.

4. 제안방식

본 논문에서 제안하는 방식은 기존에 많은 정보를 기입하고 안전하지 못한 NFC 결제 시스템을 암호 알고리즘을 이용하여 인증하는 방식으로 사용자의 단말기 식별번호를 이용한 사용자인증을 제공함과 동시에 사용자 인증 과정을 줄일 수 있도록 설계하였다. 이 장에서는 클라이언트와 및 Issuer 서버간의 사용자 등록 및 발급 과정, 스마트 폰과 Store, Issuer서버 간의 결제정보 전송 및 승인과정으로 이루어져 있다

4.1 시나리오

본 연구에서 제안하는 시나리오는 NFC가 탑재 된 스마트폰을 이용하여 사용자가 손쉽게 거래 및 결제를 할 수 있는 방식이다. 사용자는 최소한의 개인정보를 기입하고 암호화하게 된다. 이후 Issuer와 Store에 결제를 위해 개인정보 및 결제에 대한 요청을 하게 되고 이러한 값들과 데이터베이스에 있는 값들을 비교하여 결제를 승인시키는 방식이다. 여기서 TSM과 다른 개체간의 정보전송은 신뢰된 기관에서 이루어지므로 생략하도록 한다.(그림 2참조).

Step 1. 사용자는 NFC를 탑재한 Smart Phone에 App을 통하여 개인정보를 입력한다.

Step 2. 스마트폰 Issuer에게 개인정보 및 Key를 전송하여 사용여부를 확인요청을 보낸다.

Step 3. Issuer는 사용자에 관리에 대하여 DataBase에 개인정보를 저장한다.

Step 4. 활성화된 NFC App에 개인정보가 식별할 수 없도록 Issuer에게 보낸 Key를 통해 암호화 하여 Store에 결제를 신청한다.

Step 5. store는 Issuer에게 암호화된 개인정보를 전송한다.

Step 6. Issuer는 Smart Phone에게서 받은 Key를 이용하여 복호화하여 인증 후 승인한다.

Step 7. Store는 Smart Phone에 결제성공 확인 전송한다.

본 프로토콜에 사용 되는 시스템 계수는 다음과 같다.
- * : 참여 객체(U : 사용자, IS : 신뢰된 은행 기관
ST : 판매자)

본 프로토콜에 사용 되는 시스템 계수는 다음과 같다.
- UIS : U의 개인정보 [ID||PW||IM||nonce||Request]
- CIS : U의 카드정보 E_{Ks}[CN||CVN||CCN||Ks]
- Request : 세션키 요청 메시지
- K* : *만 볼수 있는 마스터 키
- nonce : 임시비표
- PU* : *의 공개 키
- PC* : *의 개인 키
- ID : 아이디
- PW : 비밀번호
- IM : 단말기 식별번호
- CN : 카드 명
- CVN : 신용카드 CVC 번호
- CCN : 신용카드 번호
- md : 주문 품목
- price : 주문가격
- Ks : 세션 키
- Nonce : 임시비표
- POK : 결제 완료 메시지

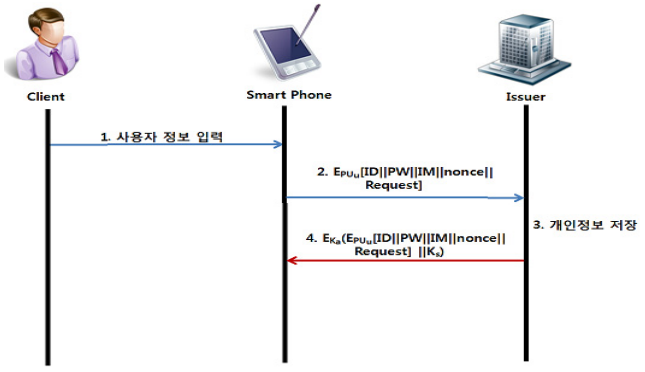
4.2 사용자 등록 및 발급 과정

사용자는 결제를 하기 전에 자신을 인증할 수 있도록 신뢰된 인증기관인 은행에게 자신의 개인정보와 세션키를 요청하여 발급받아야 한다. 발급 순서는 다음과 같다(그림 3참조).

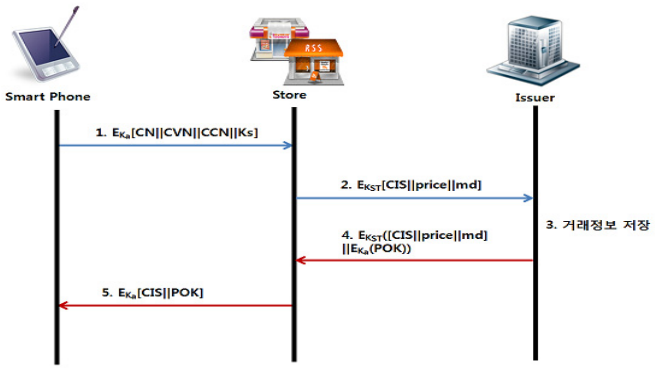
Step 1. 클라이언트는 스마트 폰에 자신이 사용 할 아이디, 패스워드, 단말기 식별번호, 사용할 카드, 신용카드번호, 신용카드 CVC번호를 기입한다.

Step 2. 클라이언트는 공개키와 개인키 쌍을 생성하고 기입한 정보 중에서 아이디, 패스워드, 단말기 식별번호, 임시비표, 그리고 일정기간동안에 사용할 세션 키를 사용자의 개인키로 암호화하여 요청한다.

Step 3. Issuer서버는 클라이언트의 공개키를 이용하여 데이터를 복호화하고 데이터베이스에 저장한다.



(그림 3) 사용 등록 및 발급



(그림 4) 결제 요청 및 결제 승인

Step 4. Issuer서버는 전송받은 암호문에 세션 키를 연결하고 클라이언트만 확인 할 수 있도록 서로 알고 있는 마스터 키를 이용하여 암호화한다. 클라이언트는 자신이 보낸 메시지임을 마스터 키로 복호화하여 확인 할 수 있다.

4.3 결제정보 전송 및 승인과정

사용자는 개인정보를 Store서버에 전송하여 결제를 요청하고 Store서버는 Issuer서버에게 결제정보를 전송한다. Issuer서버는 올바른 사용자인지를 확인하여 Store서버의 승인여부를 관리하도록 한다. 정보 전송 및 승인 순서는 다음과 같다(그림 4).

Step 1. 클라이언트가 기입 정보 중 사용할 카드, 신용카드번호, 신용카드 CVC번호를 Issuer서버에서 받은 마스터 키를 이용하여 암호화하고 Store서버에 Tag하여 데이터를 전송한다.

Step 2. Store서버는 Issuer와 공유 된 마스터키를 사용하여 결제정보와 주문 품목 및 주문가격을 암호화하여 Issuer에게 전송한다.

Step 3. Issuer서버는 Store서버에게 전달 받은 정보를 복호화하여 결제정보를 저장하고 이미 데이터베이스에 저장된 데이터와 연산한다.

Step 4. Issuer서버는 Store서버에게 전달 받은 정보에 결제 완료 메시지를 클라이언트가 볼 수 있도록 암호화 한 뒤 Store서버에 전송한다.

Step 5. Store서버는 결제 완료 메시지를 클라이언트인 스마트폰에 전송한다.

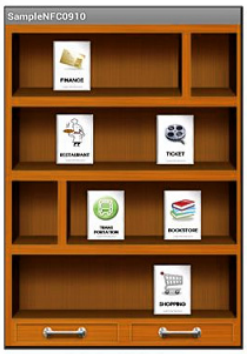
5. 제안방식 구현

4장에서 설계한 내용을 기반으로 인증방식을 사용한 NFC기반의 Payment System을 구현하였다.

5.1 클라이언트 구현

클라이언트가 쉽게 사용 하도록 간편하게 구현하였다. (a)는 사용자가 개인정보를 기입한 뒤 암호화 되어 Issuer서버의 데이터베이스에 저장한다. (b)는 NFC 기능의 많은 활용도에 따른 콘텐츠 구성 화면이며 (c)는 사용자가 가지

(a)로그인화면



(b)메인화면

(c)카드등록

(d)태깅화면

(그림 5) 클라이언트 데모 구현

고 있는 카드를 선택한 뒤 카드를 선택해 그 카드에 맞는 카드번호 및 CVC번호를 암호화하여 Issuer서버에 전송하고 Issuer서버의 데이터베이스에 저장한다. 그리고 (d)는 NFC를 Tag하라는 명령화면으로 결제정보를 Store서버에 요청한다. 이러한 클라이언트들이 전송하는 개인정보들을 암호화함으로써 보다 안정성을 향상 시킬 수 있다.

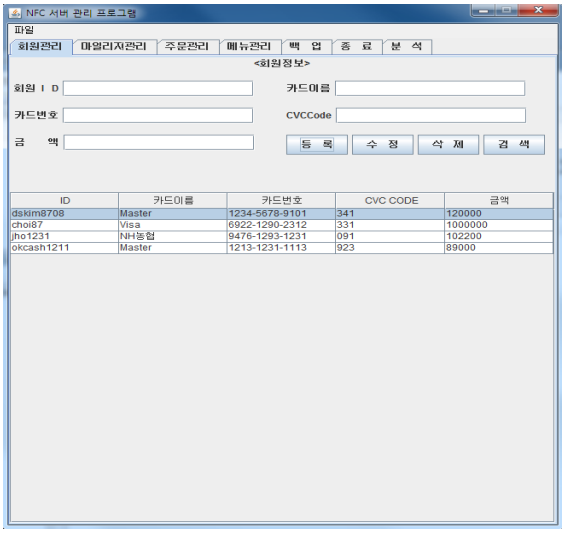
5.2 Store서버 구현

Store서버는 클라이언트가 결제 할 정보들에 대한 인증과정을 가지며 Issuer서버와 데이터베이스가 연결이 된다. (a)는 Store의 초기화면으로 상품을 업로드 및 데이터베이스에 저장 할 수 있고 (b)는 사용자가 보낸 개인정보를 이용하여 Issuer 서버와 통신하여 결제한 정보를 나타낸다. 또한 Issuer에게 거래가 승인 될 시에 사용자에게 거래 승인정보를 전송 보낼 수 있다.

(a) 초기화면

(b) 등록 및 결제화면

(그림 6) Store 서버 구현



(그림 7) Issuer 서버 데모 구현

5.3 Issuer서버 구현

클라이언트와 Store서버에 대하여 각각의 통신을 하는 Isuuer서버는 사용자가 보낸 암호화 된 개인정보를 Issuer서버에서 복호화하여 데이터베이스의 값을 갱신하고 올바른 데이터 값일 경우 Store서버에게 거래승인을 보내어 기밀성, 무결성, 부인방지를 예방 할 수 있다.

6. 결론

본 논문에서는 NFC 기능을 활용한 NFC Tag 방식으로 금액을 사용할 수 있고, 또한 스마트 폰을 이용하여 금액에 대한 정보를 실시간 검색함으로써 결제하는 방식을 구현하였다. 보안 문제에 있어 카드정보와 개인정보 노출로 통해 항상 금융 사고의 위험성을 안고 있지만 본 논문에서 제시한 프로토콜을 통하여 카드정보와 개인정보가 암호화가 되어 결제 시에 안전성, 편의성을 극대화하여 사용자와 판매자 간의 정보에 대한 신뢰성을 높였다.

앞으로 스마트폰을 통한 전자결제시스템에 대하여 강력한 보안성에 대한 연구와 발전이 필요하다.

참고문헌

[1] 최용락, 소우영, 이재광, 이임영, “컴퓨터 통신보안 3rd Edition”, 도서출판 그린, 2005. 8. 20

[2] 구철회, “무인화 마켓을 구현하기 위한 모바일 NFC결제시스템”, 한국산업기술대학교, 2011

[3] 공영일, “NFC 기반 모바일 결제시장의 이해관계 분석과 시사점”, 정보통신정책연구원, 2011

[4] 김경태, “KT NFC Service”, KT 단말연구센터, 2011

[5] 전문석, “NFC_개인정보보호_대책_최종보고서”, 한국인터넷진흥원, 2011

[6] 이상호, “USIM_탑재_스마트폰_기반_모바일_신용카드_결제_프로토콜의_안전성_향상”, 이화여자대학교, 2010