Journal of the Korea Academia-Industrial cooperation Society
Vol. 17, No. 7 pp. 319-325, 2016

http://dx.doi.org/10.5762/KAIS.2016.17.7.319
ISSN 1975-4701 / eISSN 2288-4688

모바일 결제의 신뢰성 향상 방안

김철진
인하공업전문대학 컴퓨터시스템과

A Reliability Enhancement Technique of Mobile Payment

Chul-Jin Kim
Dept. of Computer Systems and Engineering, Inha Technical College

요 약 핀테크의 활성화로 모바일 결제를 위한 다양한 기반 서비스들이 개발되고 있다. 각종 결제 방식이 개발되고, 결제의 신뢰성을 향상시키기 위한 인증 방식이 개발되고 있다. 그러나, 모바일 간편 결제 서비스 시, 전화번호에 의해 인증이 이루어지므로 누출 가능성이 있어 보안이 취약하다. 따라서, 본 논문에서는 전화번호 기반의 인증과정을 개선하기 위해 모바일 디바이스의 고유한 식별자인 디바이스 ID를 활용하여 인증 과정의 신뢰성을 높이기 위한 방안을 제안한다. 핵심 연구 내용은 모바일 디바이스 ID를 기반으로 모바일 결제 인증을 위한 아키텍쳐와 인증 프로세스이다. 모바일 결제 아키텍쳐는 모바일 디바이스, 인증 서비스, 그리고 모바일 결제 어플리케이션으로 구성된다. 모바일 디바이스는 모바일 디바이스 ID와 전화번호로 구성하며, 인증 서버는 인증 모듈과 암호화 모듈로 구성된다. 모바일 결제 서비스는 사전 인증 모듈과 복호화 모듈로 구성된다. 모바일 결제 서비스의 프로세스는 모바일 디바이스, 인증 서버, 그리고 모바일 결제 어플리케이션 간에 암호화된 인증 정보(디바이스 ID, 전화번호, 인증 번호)에 의해 처리된다. 모바일 디바이스는 전화번호와 디바이스 ID를 인증 서버로 전달하며, 인증 서버는 인증 과정과 암호화 과정을 통해 사용자를 인증한다. 모바일 결제 어플리케이션은 전달받은 인증 번호에 대해 복호화를 통해 사전 인증 과정을 수행한다. 본 논문의 인증 서버의 인증 과정과 모바일 결제 서비스의 사전 인증 과정을 통해 기존 결제 서비스의 인증 번호 누출에 의한 위험을 예방할 수 있는 차별성을 제공할 것이다.

Abstract A variety of services for mobile payments by the activation of FinTech have been developed. Various payment methods were developed, and an authentication method was developed to improve the reliability of the payment. On the other hand, when mobile easy payment services are used, they have weak security because the authentication by phone number. Therefore, this paper proposes a technique for increasing the reliability of the authentication process using the unique device ID of the mobile device to improve the authentication process based on the telephone number. The core research contents are the architecture and process for the authentication of mobile payments based on the mobile device ID. The mobile payment architecture consists of a mobile device, authentication service, and mobile payment application. The mobile device consists of mobile device ID and phone number, and the authentication server consists of authentication module and encryption module. The mobile payment service consists of a pre-authentication module and decryption module. The process of mobile payment service is processed by the encrypted authentication information (device ID, phone number, and authentication number) among mobile devices, authentication server, and mobile payment application. The mobile device sends the telephone number and the device ID to the authentication server and the authentication server authenticates the user through an authentication process and encryption process. The mobile payment application performs the pre-authentication process by decrypting the received authentication number. This paper reports a difference that can prevent the risk of leakage of the authentication number in existing payment services through the authentication process of the authentication server and the pre-authentication process of the mobile payment service of this paper.

Keywords : Mobile Payment, Mobile Device ID, Pre-Authentication, Authentication Number

*Corresponding Author : Chul-Jin Kim(Inha Technical College)
Tel : +82-32-870-2338 email : cjkim@inhatc.ac.kr
Received April 25, 2016 Revised (1st May 27, 2016, 2nd June 17, 2016)
Accepted July 7, 2016 Published July 31, 2016

1. 서론

모바일 전자상거래의 활성화로 모바일 결제가 필수적인 요소가 되었으며 이에 따라 모바일 결제의 신뢰성에 대한 요구가 증가하고 있다. 그러나 모바일 결제 시 인증 과정에서 인증번호의 누출이 빈번하게 발생하고 있다. 모바일 간편 결제(Mobile Easy Payment)에서는 전화번호 관련 정보를 확인 후 인증번호를 전송하여 인증하지만, 이때 사용자의 전화번호가 누출이 되면 다른 모바일 디바이스에서 인증번호를 인터셉트 할 수 있다. 동일 전화번호를 복사한 스마트폰을 통해서 전화 통화나 문자를 도청할 수 있으며, 온라인 전자 거래 시에는 인증 번호를 복사한 스마트폰에서 모바일 결제를 진행할 수 있다.

따라서 본 논문에서는 전화번호 기반의 인증과정을 개선하기 위해 모바일 디바이스의 고유한 식별자인 디바이스 ID를 활용하여 인증 과정의 신뢰성을 높이기 위한 방안을 제안한다.

본 논문은 다음과 같이 구성한다. 2장에서는 관련연구로서 모바일 결제 시장의 주요 기술 흐름인 핀테크 서비스 기술과 현재 모바일 결제 인증 과정과 문제점을 파악한다. 또한 관련 모바일 결제의 신뢰성 관련 연구를 분석한다. 3장에서는 모바일 신뢰성 향상 기법으로 아키텍쳐와 인증 처리 프로세스를 제안한다. 4장에서는 본 논문에서 제안한 모바일 결제의 신뢰성 향상 기법을 검증하기 위해 가상의 전자 마켓을 개발하여 인증과정의 성공과 실패 과정을 실험한다. 5장에서 결론을 맺고 향후 인식 기술들과의 통합 연구를 제시한다.

2. 관련연구

2.1 핀테크 서비스

핀테크(FinTech) 서비스는 국내외에서 애플페이(Apple Pay), 삼성페이(Samsung Pay), 카카오페이(Kakao Pay), 네이버페이(Naver Pay), 안드로이드페이(Android Pay), 케이페이(K Pay) 등 다양한 모바일 결제 방식에 개발되고 있다[1]. 그러나 각 결제 방식들이 시장을 점유하기 위해 표준화되지 않은 자체적인 서비스로 개발되어 사용자들이 해당 결제 방식 모두 선택하여 사용해야하는 불편함이 발생하고 있다. 그러나 결제 기술의 발전을 위한 과정일 것이다. 각각의 결제 방식들은 보안을 위한 개인 인증과 암호화에 특화된 기술을 적용하여 기술적 차별화를 강조하고 있다[2]. 애플페이는 NFC(Near Field Communcation) 기술과 지문인식기능을 제공하며, 보안 강화를 위해 토큰화(Tokenization) 기술을 적용하고 있다[3]. 삼성페이는 MST(Magnetic Secure Transmission) 기술을 기반으로 보안 강화를 위해 토큰화 기술을 반영하였다[4]. 안드로이드페이는 NFC를 통한 결제 방식으로 사용자 인증(비밀번호, 지문인식)을 통해 잠금해제 후 결제를 한다. 애플페이와 삼성페이는 하드웨어를 기반으로 SE(Secure Element) 영역에 결제관련 정보를 암호화하여 저장하지만, 구글의 안드로이드페이는 소프트웨어 기반으로 HCE(Host Card Emulation)에 결제정보를 저장한다[5].

2.2 기존 모바일 결제 보안 인증

애플페이, 삼성페이, 안드로이드페이, 카카오페이(Kakao Pay), 케이페이(Kpay) 등의 모바일 결제에서는 사용자 보안 인증을 위해 지문인식 기술을 사용하고 있다[3,4,5,6,7]. 그러나 지문인식 또한 보안에 누출될 수 있음이 확인 되었다[8]. 이에 따라 다양한 인식 기술로 홍채, 안면, 음성, 정맥, 걸음걸이 등 다양한 생체인식 기술이 연구되고 있으며, 이러한 인식 기술들이 모바일 결제의 안정성을 향상시킬 수 있을 것이다[2].

기존 모바일 간편 결제 서비스는 Fig. 1에서와 같이 모바일 디바이스에서 결제 요청을 위해 인증번호 요청 시 전화번호가 인증서버로 전송된다. 이 경우 전화번호 누출에 의해 인증번호가 인터셉트될 수 있으며, 인터셉트된 인증번호는 악용될 수 있다.

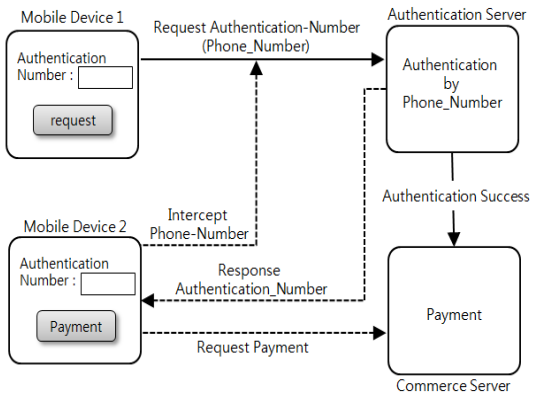


Fig. 1. Existing Mobile Payment Architecture

Fig. 1에 대한 사례를 Fig. 2에서와 같이 모바일 결제를 하려는 전화번호 '1111' 사용자는 인증번호를 요청을 인증서버로 요청하게 된다. 이 경우 전화번호 '2222' 사용자가 전화번호를 '1111'로 인식하게 한 후 인증서버로부터 인증번호 '785634'를 획득하게 된다.

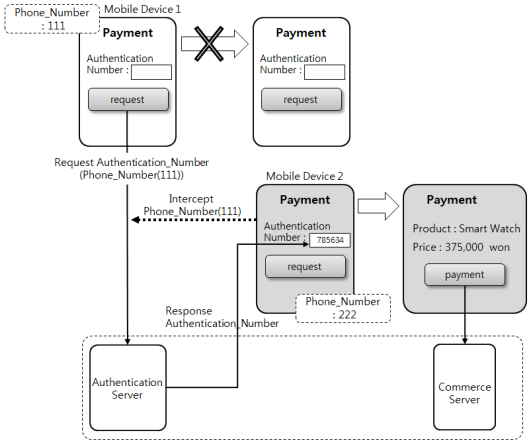


Fig. 2. Intercept Phone_Number in Existing Mobile Payment

전화번호 '1111' 사용자는 인증번호를 획득하지 못하게 되며 결제도 진행하지 못하게 된다. 인증번호를 인터셉트한 전화번호 '2222' 사용자는 결제 서비스를 진행하게 되며 커머스 서버로부터 결제 처리를 하게 된다.

2.3 모바일 간편결제의 보안과 사용의도에 관한 연구[9]

최근 금융관련 개인정보유출 사고가 빈번하므로 사용자들은 편리성 보다는 보안성을 더 고려하여 결제 서비스를 선택한다. 이에 간편 결제의 사용자 인지를 높일 수 있는 방안으로 간편 결제의 보안과 사용의도 간의 관계를 연구하였다[9]. 간편 결제의 보안과 사용의도 간의 관계를 도출하기 위해 보안성이 사용 편리성에 어떠한 영향을 미치는지 실험하여 분석하였다.

간편 결제의 보안성에 대한 사용자의 사용 인식을 검증하기 위한 연구로서 본 논문에서 제시하는 모바일 결제 시 보안성을 강화하기 위한 기술적인 방안을 제시하지는 않고 있다.

2.4 모바일 결제 서비스의 비교 및 분석[10]

모바일 결제 서비스의 비교 분석 연구에서는 모바일 결제 서비스의 종류와 국내외 모바일 결제 서비스를 비교분석 하였다[10]. 국내 모바일 결제 서비스로 신한 스마트 월렛, 삼성 월렛, 하나 N월렛, Q쇼핑 모바일 체크카드, 엠틱을 비교분석 하였으며, 국외 모바일 결제 서비스로 스퀘어(Square), 페이팔(Paypal), 베리폰(VeriFone), 저미오(Jumio), 구글 월렛(Google Wallet), 애플 아이월렛(Apple iWallet)를 비교분석 하였다. 이러한 모바일 결제 서비스를 분석을 통해 향후 모바일 결제 서비스 시장은 전자지갑 형태로 바뀔것으로 분석하였다.

모바일 결제 서비스의 비교 및 분석 연구는 본 연구에서 제안하고자 하는 모바일 결제 서비스의 보안성을 강화하기 위한 방안에 대한 기술적인 접근이 미흡하다.

3. 모바일 결제 신뢰성 향상 기법

본 연구는 기존의 모바일 간편 결제 서비스의 보안 이슈를 해결하고자 모바일 디바이스의 요소를 활용하여 모바일 결제의 신뢰성 향상 아키텍쳐 및 인증 프로세스를 제안한다.

3.1 모바일 결제 아키텍쳐

기존의 모바일 간편 결제가 전화번호 기반으로 인증번호를 요청하므로 누출의 가능성이 높아 신뢰성이 확보되지 않았다. 이에 본 연구에서는 생체인식 등 신뢰성 향상을 위한 기술들과 융합하여 사용할 수 있도록 모바일 디바이스의 식별자를 활용하는 방안을 제안한다.

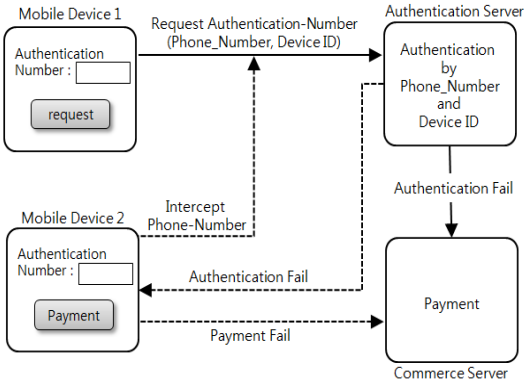


Fig. 3. Mobile Payment Architecture based on Mobile Device Identifier

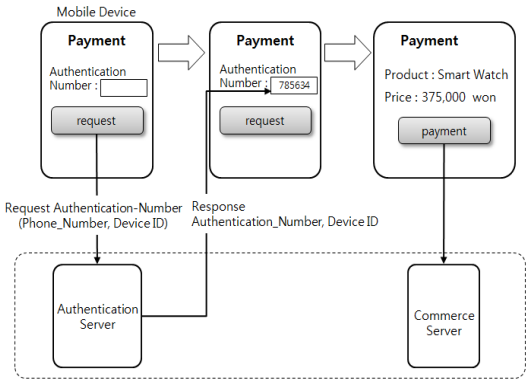


Fig. 4. Mobile Payment Architecture based on Mobile Device Identifier(Case)

모바일 디바이스는 유일한 식별자인 디바이스 ID를 보유하고 있으며, 어떠한 디바이스와도 동일하지 않은 유일한 정보이다. Fig. 3에서와 같이 해당 디바이스의 식별자 정보를 인증번호 요청 시 전화번호와 함께 요청할 수 있으며, 다른 디바이스에서 인터셉트하더라도 해당 인증번호를 받은 다른 디바이스 ID를 보유한 모바일 디바이스는 해당 인증번호를 해석할 수 없어 인증하는데 실패한다.

Fig. 4에서와 같이 인증번호를 요청하려는 모바일 결제의 디바이스는 전화번호와 디바이스 ID를 인증서버로 전송한다. 인증서버는 암호화된 인증번호와 디바이스 ID를 요청 디바이스에 전송하면 현재 디바이스의 ID와 비교를 통해 인증번호를 제공한다. 이렇게 디바이스 ID를 통해 다른 디바이스에서 인증번호를 획득하지 못하도록 할 수 있다.

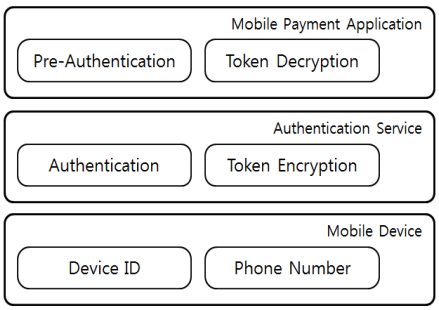


Fig. 5. Authentication Architecture of Mobile Payment

신뢰성 향상을 위한 모바일 결제의 인증 아키텍쳐는 Fig. 5와 같다. 인증번호를 요청하기 위해 모바일 디바이스에서 디바이스 ID와 전화번호를 인증 서비스에 전달하며 인증 서비스에서는 해당 디바이스 ID와 전화번호를 기반으로 인증번호를 획득할 수 있다. 인증번호는 디바이스 ID와 함께 토큰화하여 전달할 수 있도록 암호화한다. 모바일 결제 어플리케이션에서 암호화된 토큰을 복호화할 수 있도록 복호화 모듈과 인증모듈을 통해 인증번호를 획득하여 인증한다. 이 인증 과정은 사전 인증(Pre-Authentication)과정으로 인증서버에서 인증하기 위한 인증과정 전의 과정으로 인증번호에 대한 신뢰성을 확보할 수 있다.

3.2 모바일 결제 인증 프로세스

본 연구의 모바일 결제 인증은 모바일 디바이스 ID와 전화번호를 기반으로 인증서버에서 확인 후 인증번호와 디바이스 ID를 응답한다. Fig. 6에서와 같이 인증 받으려는 모바일 디바이스에서는 사전 인증(Pre-Authentication)을 수행한다. 사전 인증은 현재 디바이스의 디바이스 ID와 전송 받은 디바이스 ID를 비교하여 검증한다. 검증이 완료되면 인증 서버로 인증을 요청하여 결제를 하려는 사용자임을 확인한 후 결제처리 한다. 이러한 과정에서 모바일 디바이스 관련정보인 인증번호와 디바이스 ID는 암호화하여 전송된다.

디바이스 ID를 인증번호와 재전송하는 이유는 Fig. 7에서와 같이 본인 외의 디바이스에서 인터셉트할 경우 인증하는 과정에서 현재 디바이스의 디바이스 ID와 전송받은 디바이스 ID를 비교하여 누출된 정보 인지를 검증할 수 있다. 인터셉트 하더라도 암호화된 디바이스 ID와 현재 디바이스 ID가 일치하지 않으므로 인증이 실패한다.

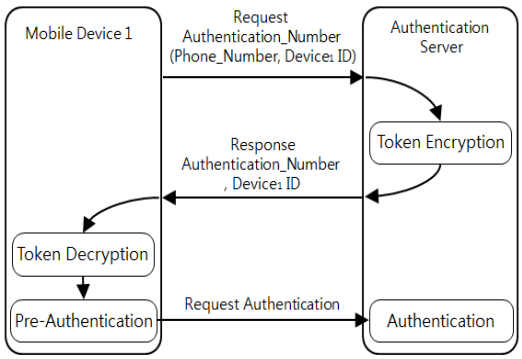


Fig. 6. Authentication Process of Mobile Payment

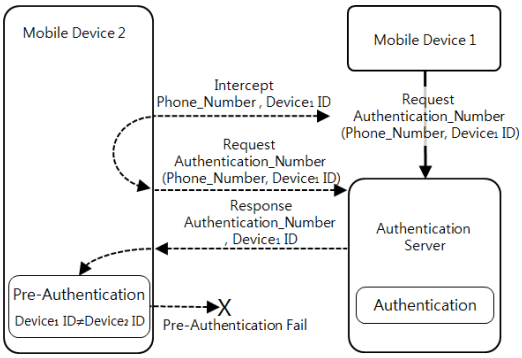


Fig. 7. Reliable Authentication by Pre-Authentication

모바일 디바이스에서 처리되는 사전 인증 알고리즘은 Fig. 8에서와 같이 구성하여 모바일 결제 어플리케이션에 내장한다.

디바이스에서 사전 인증을 위해 인증서버로부터 암호화된 디바이스 ID(Encrypted_DeviceID)와 인증번호(Encrypted_Authentication_Number)를 입력받는다.

기존의 인증번호만 받는 것과 다르게 디바이스 ID와 암호화된 인증번호를 받아 네트워크상에서의 누출로 부터 위험을 방지한다. 사전 인증 서비스에서는 디바이스 ID와 인증번호를 복호화하기 위해 2단계 복호화 과정을 수행한다. 1차 복호화에서는 암호화된 디바이스 ID를 복호화하며, 2차 복호화에서는 복호화된 디바이스 ID(Decrypted_DeviceID)를 이용하여 인증번호를 복호화한다.

```
Pre-Authentication_service ( Encrypted_DeviceID,
                             Encrypted_Authentication_Number )
{
    Decrypted_DeviceID = 1st_Decrypt(Encrypted_DeviceID);
     // Encrypted_DeviceID is only used once
    if ( Decrypted_DeviceID == DeviceID_of_Current_Device ) {
        Decrypted_Authentication_Number =
         2nd_Decrypt(Encrypted_Authentication_Number,Decrypted_DeviceID);
          // Encrypted_Authentication_Number is only used once.
     }
}
```

```
Pre-Authentication_service( ) : Authenication service by
                                Device ID and Authentication Number
1st_Decrypt( ) : 1st Decryption Service for Device ID
2nd_Decrypt( ) : 2nd Decryption Service for Authentication Number
Encrypted_DeviceID : Received Device ID from Server
Encrypted_Authentication_Number : Received Authentication Number from
Server
DeviceID_of_Current_Device : Obtained Device ID from Current Device
Decrypted_DeviceID : Decrypted Device ID by Decryption service
Decrypted_Authentication_Number : Decrypted Authentication Number by
Decryption service
```

Fig. 8. Pre-Authentication Algorithm

사전 인증의 신뢰성을 확보하기 위해 Fig. 9에서와 같이 1차 복호화 과정에서의 복호화된 디바이스 ID와 현재 모바일 디바이스로부터 추출된 디바이스 ID를 비교한다.

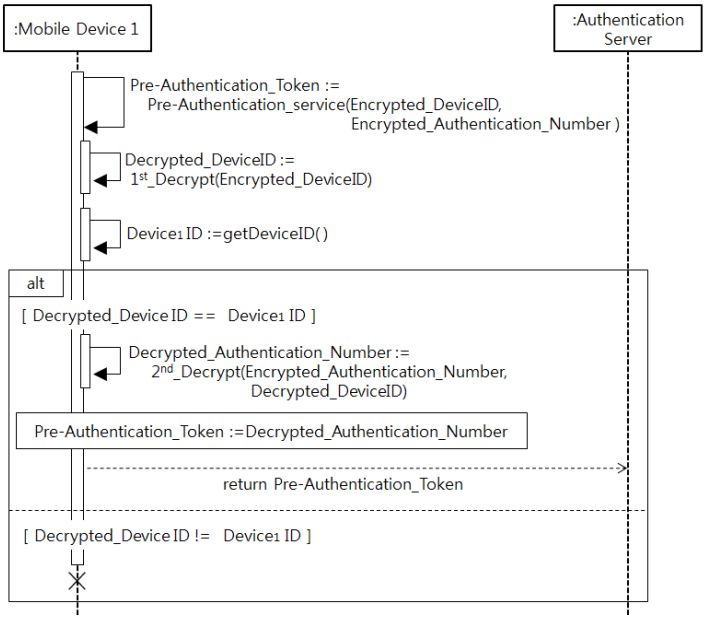


Fig. 9. Pre-Authentication Service Flow for Reliable Authentication

이 과정에 의해 다른 디바이스에서는 인증번호를 획득하더라도 복호화할 수 없다. Fig. 9의 서비스 흐름에서와 같이 다른 모바일 디바이스에서 암호화된 디바이스 ID를 획득하더라도 현재 디바이스 ID와 일치하지 않기 때문에 사전 인증이 실패하게 된다. 또한 복호화 과정에서 사용된 암호화된 디바이스 ID와 인증번호는 한번 만 사용할 수 있으므로 디바이스 비교 과정에서 실패할 경우 2차 복호화 과정을 수행할 수 없다.

Fig. 9에서와 같이 1차 복호화된 디바이스 ID(Decrypted_DeviceID)와 현재 모바일 디바이스 ID(Device1 ID)가 일치하는 경우, 2차 복호화 과정을 통해 인증번호(Decrypted_Authentiaction_Number)를 획득한다. 최종적으로 인증번호를 사전인증번호로 토큰화하여 인증서버로 전달한다.

지금까지 본 연구에서는 기존 누출 가능성이 있는 인증번호의 위험성에 대해 인증번호가 누출이 되더라도 모바일 디바이스에서 사전 인증과정을 통해 모바일 결제의 신뢰성을 높일 수 있는 방안을 제시하였다.

4. 실험 및 평가

본 사례연구에서는 온라인 쇼핑몰의 모바일 결제 시, 본 연구에서 제안한 인증 기법을 적용하여 실험한다. 인증 처리 과정에서 현재 모바일 디바이스 ID를 이용하여, 본 연구에서 제안한 인증 아키텍쳐가 적합함을 검증한다. 본 사례는 인증 과정의 적합성을 검증하는 것으로 서버에서 호출된 인증번호와 디바이스 ID를 획득하여 사전인증 처리하는 과정을 개발한다.

Fig. 10에서와 같이 모바일 인증을 요청하면, 인증 서버로부터 얻은 디바이스 ID와 인증번호를 이용하여 모바일 디바이스에 설치된 어플리케이션 내의 사전 인증 처리 과정을 통해 인증 번호를 성공적으로 얻을 수 있다.

모바일 디바이스의 사전 인증 처리는 Fig. 11과 같이 인증서버에서 호출하게 되는 콜백(Callback)함수로서 전달되는 데이터는 암호화된 디바이스 ID(encrypted_deviceId)와 인증번호(encrypted_authentication_number) 이다. 암호화 및 복호화는 AES(Advanced Encryption Standard)[11] 알고리즘을 사용한다(Fig. 12). 인증서버로부터 전달받은 디바이스 ID를 복호화한 후 인증번호를 복호화하기 전에 현재 모바일 디바이스의 사용자가 요청한 인증인지 확인하기 위해 현재 모바일 디바이스 ID를 획득한다(Fig. 13). 인증서버로부터 전달받은 디바이스 ID와 현재 모바일 디바이스 ID를 비교하여 일치하면 Fig. 10과 인증번호를 복호화하여 표시한다.

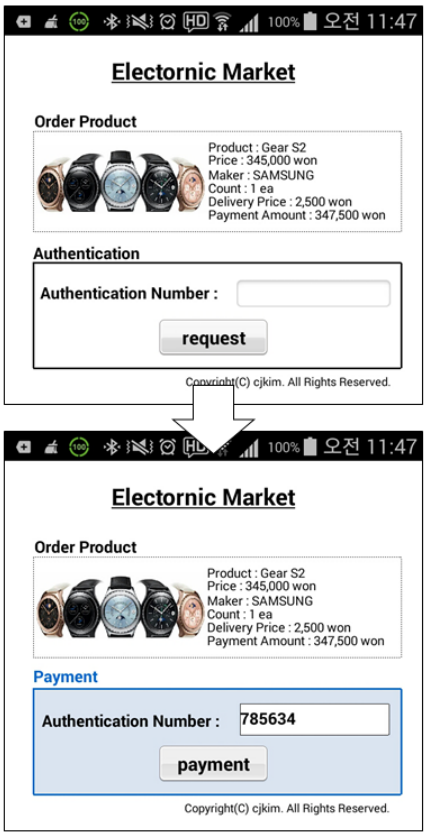


Fig. 10. Pre-Authentication Success

```
import javax.crypto.Cipher;
import javax.crypto.SecretKey;
import android.telephony.TelephonyManager;
...
public String preAuthenticationService ( byte[] encrypted_deviceId,
                                         byte[] encrypted_authentication_number,
                                         SecretKey key ) {
    byte[] decrypted_deviceId = decrypt(encrypted_deviceId, key);
     // encrypted_deviceId is only used once

    byte[] decrypted_authentication_number = null;
    byte[] deviceId_of_current_device = this.getCurrentDeviceId();
    if ( decrypted_deviceId == deviceId_of_current_device ) {
        decrypted_authentication_number =
            decrypt(encrypted_authentication_number, key);
            // encrypted_authentication_number is only used once.
        return decrypted_authentication_number.toString();
    } else {
        encrypted_authentication_number = null;
        // encrypted_authentication_number extinction
        return "Pre-Authentication Fail !!";
    }
}
```

Fig. 11. Pre-Authentication Code

```
public byte[] decrypt(byte[] encrypted_deviceId, SecretKey key) {
      Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
      cipher.init(Cipher.DECRYPT_MODE, key);
      byte[] decrypted_deviceId = cipher.doFinal(encrypted_deviceId);
      return decrypted_deviceId;
}
```

Fig. 12. Decryption Code[12]

```
public byte[] getCurrentDeviceId(){
      String deviceId = ((TelephonyManager)context.
                        getSystemService( Context.TELEPHONY_SERVICE )).
                        getDeviceId();
      return deviceId.getBytes();
}
```

Fig. 13. Code for Getting Current Device ID[13]

인증서버로부터 전달받은 디바이스 ID와 현재 모바일 디바이스 ID가 일치할 경우에는 인증번호를 얻을 수 있지만, 만약 해킹에 의해 다른 디바이스에서 인증번호를 인터셉트할 경우에는 Fig. 11과 같이 모바일 디바이스 ID가 일치하지 않으면, 인증번호를 소멸시키고 Fig. 14와 같이 에러 메시지를 표시한다.

Fig. 14. Pre-Authentication Fail

본 사례연구에서와 같이 모바일 디바이스 ID를 통해 인증관련 정보가 누출되더라도 기존 방식보다 안정적이며 모바일 결제의 신뢰성이 향상될 것이다.

5. 결론

본 연구에서는 모바일 간편 결제 시 전화번호 누출로 인한 인증 보안의 신뢰성을 향상시키기 위해 모바일 디바이스 ID 기반으로 사전 인증 처리 과정을 제안하였다. 사전 인증을 위해 모바일 디바이스에서는 현재 디바이스 ID와 인증 서버로부터 전달받은 디바이스 ID를 비교하여 현재 모바일 디바이스가 인증을 요청한 것인지 확인할 수 있다. 이러한 사전 인증 알고리즘을 통하면 정보가 누출되더라도 인증이 실패하여 결제를 진행할 수 없다. 향후에는 이러한 모바일 인증 처리 과정과 여러 생체 인식 기법과 결합하여 모바일 결제의 신뢰성을 더욱 향상시킬 수 있는 방안을 연구한다.

References

[1] Sung-Tae Moon, Gi-Nam Kim, "FinTech Technology and Security Trend Analysis", Review of Korean Society for Internet Information, p23-32, 2015.

[2] Connectinglab, Mobile Trend 2016, Miraebook Publishing Co., 2016.

[3] Apple Pay, http://www.apple.com/apple-pay.

[4] Samsung Pay, http://www.samsung.com/samsung-pay.

[5] Android Pay, https://developers.google.com/android-pay.

[6] Kakao Pay, http://www.kakao.com/kakaopay.

[7] K-Pay, http://www.inicis.com/kpay.

[8] Researchers find a shockingly simple way to hack Samsung's fingerprint scanners, http://bgr.com/2016/03/08/samsung-galaxy-s7-galaxy-s6-fingerprint-scanner-hack.

[9] Eun Oh, Tae-Sung Kim, "A Study on Security and Use Intention of Easy-to-use Mobile Payment", Proceedings of Symposium of the Korean Institute Of Communication Sciences, p54-55, 2015.

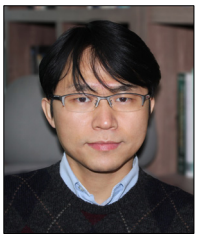
[10] Phil-Joo Moon, "The Comparison and Analysis of Mobile Payment Service", Proceedings of the Korea Institute of Electronic Communication Sciences, p485-489, 2013.

[11] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard(AES)," FIPS PUB 197, Nov. 2001.

[12] Cryptographic Cipher for encryption and decryption, https://docs.oracle.com/javase/7/docs/api/javax/crypto/Cipher.html.

[13] TelephonyManager for telephony services on the device, http://developer.android.com/reference/android/telephony/TelephonyManager.html.

김 철 진(Chul-Jin Kim) **[종신회원]**



- 2004년 2월 : 숭실대학교 대학원 컴퓨터학과 (공학박사)
- 2004년 3월 ~ 2009년 2월 : 삼성전자 책임연구원
- 2009년 3월 ~ 현재 : 인하공전 컴퓨터시스템과 부교수

<관심분야>
컴포넌트 기반 개발 방법론, 컴포넌트 커스터마이제이션, 모바일 서비스, 클라우드 컴퓨팅