Journal of the Korea Academia-Industrial cooperation Society
Vol. 14, No. 7 pp. 3487-3494, 2013

http://dx.doi.org/10.5762/KAIS.2013.14.7.3487

NFC를 이용한 안전한 모바일 지급결제 시스템

이요람[1], 오수현[2*]
[1](주)이베이코리아 정보보안팀, [2]호서대학교 정보보호학과

A Secure Mobile Payment System for Near Field Communication System

Yo-Ram Lee[1] and Soo-Hyun Oh[2*]
[1]**ebayKorea, Information Security Team**
[2]**Dept. of Information Security, Hoseo University**

요 약 최근 NFC 기술을 탑재한 스마트 기기를 이용하여 모바일 지급결제, 출입통제, 스마트 포스터와 같이 정보 제공 또는 광고에 관련된 응용 서비스가 제공되고 있다. 이에 따라 NFC 기술과 더불어 스마트 기기 시장은 더욱더 성장할 것으로 전망된다. 특히, 모바일 지급결제 서비스가 국내·외에서 더 활성화될 것으로 예상되고 있으며, 2012년 3월에는 모바일 지급결제를 위한 표준인 KS X 6928이 제정되었다. 모바일 지급결제 시스템은 사용자에게 편의성을 제공하지만 거래 정보를 전송하는 과정에서 데이터가 노출되는 등 다양한 보안 위협이 발생할 수 있기 때문에 인가되지 않은 제 3자에게 전송되는 데이터가 노출되지 않도록 암호화를 수행하는 것이 반드시 요구된다. 따라서 본 논문에서는 KS X 6928의 대면 거래와 비대면 거래에서 데이터를 암호화하는데 사용하는 세션키 생성 방식의 문제점을 분석하고 안전성을 향상시킬 수 있는 안전한 모바일 지급결제 시스템을 제안한다.

Abstract Diverse application service such as mobile payment, access control or smart poster have been provided by using smart devices with built-in Near Field Communication technology. Especially, a mobile payment system can provide convenience to its users, but it also can poses including data disclosure while transmitting. There are vulnerabilities while generating session keys used to encrypt data in transaction processes as proposed in KS X 6928, the standard for mobile payment system. Therefore, in this thesis, I analyzed weaknesses of session keys used to encrypt transaction data and proposed a more secure mobile payment system based on NFC to enhance security. The proposed system will provide security functionalities such as key freshness, mutual authentication and key confirmation.

Key Words : Mobile Payment System, NFC(Near Field Communication), Session key

1. 서론

최근 NFC(Near Field Communication) 기술을 탑재한 스마트 기기 등을 이용하여 모바일 지급결제, 출입통제, 스마트 포스터와 같이 정보 제공 또는 광고와 관련된 응용 서비스가 제공되고 있다. 다양한 응용 서비스 중에서도 모바일 지급결제 서비스가 국내·외에서 널리 주목받음에 따라 더욱 활성화 될 것으로 예상되고 있으며, 2013년 3월 지식경제부 기술표준원에서는 모바일 지급결제를 위한 표준으로 KS X 6928을 제정하였다[1-3]. 모바일 지급결제는 모바일 기기에 저장된 모바일 신용카드를 이용하여 결제를 수행하는 것으로, 대면거래와 비대면 거래로 나눌 수 있다.

그러나 KS X 6928에서 정의한 대면 거래에서는 세션키(Session Key)를 생성하는 과정에서 카드사의 비밀키인 MK(Master Key)가 노출될 경우, 거래에 사용되는 모

"이 논문은 2012년도 호서대학교의 재원으로 학술연구비 지원을 받아 수행된 연구임"(2012-0315)
*Corresponding Author : Soo-Hyun Oh(Hoseo Univ.)
Tel: +82-41-540-5716 email: shoh@hoseo.edu
Received April 30, 2013 Revised June 3, 2013 Accepted July 11, 2013

든 키를 알아낼 수 있다. 또한, 비대면 거래에서는 세션키를 누구나 알 수 있는 정보인 TS(Time Stamp)를 기반으로 생성하기 때문에 키의 안전성이 보장되지 않는다.

본 논문에서는 KS X 6928에서의 대면 거래 및 비대면 거래에 각각 사용되는 세션키에 대한 문제점을 분석하고 안전성을 향상시킬 수 있는 안전한 모바일 지급결제 시스템을 제안한다. 제안하는 방식의 대면 거래의 경우 MK가 노출되어도 세션키를 생성할 수 없도록 모바일 단말기와 카드사 서버 사이에 사전에 공유한 비밀키인 PSK(Pre-Shared Key)를 이용한다. 또한, 비대면 거래의 경우 모바일 단말기에서 생성한 비밀 랜덤수와 PSK를 이용하여 키의 안전성을 향상시켰다. 본 논문의 구성은 다음과 같다. 먼저 2장에서는 NFC와 KS X 6928을 설명한다. 그리고 3장에서는 KS X 6928에서 사용된 세션키의 취약점을 분석하고 이를 개선한 안전한 모바일 지급결제 시스템을 제안한다. 4장에서는 제안한 방식의 안전성을 분석하고 5장에서 결론을 맺는다.

2. 관련연구

2.1 NFC(Near Field Communication)

NFC는 13.56MHz 주파수 대역을 이용하여 10cm 이내의 거리에서 데이터 전송이 가능한 비접촉식 근거리 무선통신 기술이다. NFC는 단방향 통신과 더불어 두 디바이스가 통신할 수 있는 양방향 통신을 지원하며, NFC가 제공하는 운영모드는 Fig. 1과 같다[4].

[Fig. 1] Three operation modes of NFC

- Card mode: NFC 디바이스가 스마트카드처럼 동작하는 모드
- R/W mode: NFC 디바이스가 수동적인 응답기처럼 동작하는 모드
- P2P mode: 두 개의 NFC 디바이스에서 양방향 연결을 수립하는 모드

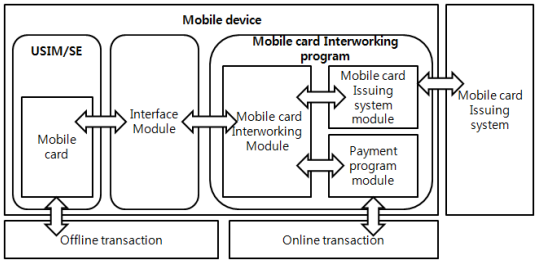
NFC에 관련된 표준화는 2002년 12월 ECMA International에서 발표한 ECMA-340을 시작으로, 2003년 12월에는 국제표준규격인 ISO/IEC 18092가 제정되었다[5,6]. 이후에는 NFC 포럼(Forum)의 설립을 통하여 세부 규격 개발, 기기와 서비스 간의 호환성 확보 및 NFC 응용 서비스 분야의 확대 등을 활발히 진행하고 있다. 특히, 2008년 12월에는 ECMA International과 NFC 포럼에서 ECMA-385(NFC -SEC)를 발표하여 보안 서비스를 제공하고 있다[7,8].

NFC 기술이 스마트 기기에 탑재됨에 따라 다양한 분야에서 응용 서비스를 제공하고 있으며, 그 범위를 점차 늘려갈 것으로 예상된다. 국내에서는 교통카드 및 전자지갑 서비스를 통해 활성화되고 있으며, 앞으로는 스마트키, 음식 주문, 스마트 명함과 같은 응용 서비스를 도입할 것으로 보인다. 현재 NFC가 활용되고 있는 분야를 Fig. 2와 같다[9].

[Fig. 2] Application services using NFC

2.2 모바일 지급결제 시스템

2012년 3월, 지식경제부 기술표준원에서는 모바일 지급결제를 위한 국가표준으로 KS X 6928을 제정하였다. KS X 6928은 총 3부로 구성되며, 1부는 결제 절차를 수행하기 위한 일반적인 사항을 규정한다. 그리고 2부와 3부는 각각 대면 거래와 비대면 거래의 결제 절차를 규정한다. Fig. 3은 대면 거래 및 비대면 거래의 개념을 간략하게 나타낸 것이다.



[Fig. 3] Mobile payment system

2.2.1 발급 단계

발급 단계에서 모바일 단말기에 모바일 카드를 설치하고 모바일 신용카드를 발급받는 절차를 규정한다. 사용자는 모바일 카드를 선택함으로써 발급 요청 및 안전한 채널을 열기 위한 상호 인증, 데이터 저장 과정을 수행한다.

2.2.2 대면 거래

대면 거래는 모바일 카드가 저장된 모바일 단말기에서 결제 단말기로 NFC를 이용하여 결제 정보를 전송하고 온라인으로 결제 승인을 처리하는 모바일 지급결제 방식이다.

[대면 거래 절차]

1) 사용자는 결제 단말기를 통해 거래 금액을 확인하고 NFC가 탑재된 모바일 단말기를 결제 단말기의 리더기에 근접시킨다.
2) 모바일 단말기에 저장된 모바일 카드와 모바일 신용카드 정보를 NFC를 이용해 결제 단말기로 전송한다. 이때, 카드사를 식별하기 위한 값과 파생키 DK를 생성하기 위한 Chip ID 및 세션키 SK를 생성하기 위한 거래 계수기가 전송된다.
3) 결제 단말기는 모바일 단말기로부터 전송된 데이터를 세션키를 생성하여 암호화 한 후, 승인 서버로 전송하여 승인 요청을 한다.
4) 승인 서버는 전송된 데이터를 확인한 후, 결제 단말기로 결과를 전송하여 결제를 종료한다.

대면 거래에서 데이터를 암호화하는데 사용하는 세션키의 생성 과정은 다음과 같다.

- 모바일 단말기는 SELECT FILE 및 GET PROCESSING OPTIONS 명령을 통해 Chip ID와 거래 계수기, 주 계좌 번호를 결제 단말기로 전송한다.
- 결제 단말기는 주 계좌 번호를 이용하여 카드사 A의 비밀키인 MK_A를 식별한다.
- 결제 단말기는 카드사 A의 MK_A와 모바일 단말기가 응답한 Chip ID를 CBC 연산을 통해 파생키 DK를 생성한 후, DK와 거래 계수기를 ECB 연산을 통해 세션키 SK를 생성한다.
- 모바일 단말기 또한 동일한 과정을 통해 동일한 세션키 SK를 생성한다.

2.2.3 비대면 거래

비대면 거래는 온라인 가맹점에서 상품을 선택한 다음, 모바일 카드 결제 프로그램을 이용하여 결제 정보를 전송하고 온라인으로 결제 승인을 처리하는 모바일 지급결제 방식이다.

[비대면 거래 절차]

1) 사용자는 온라인 가맹점에서 상품 및 결제 방식 등과 같은 데이터를 선택한다.
2) 가맹점은 모바일 카드 결제 서버로 거래 정보 및 사용자 정보, 가맹점 정보를 전송한다.
3) 사용자는 모바일 결제 프로그램을 실행한 후, 모바일 카드 결제 서버에서 TS를 기반으로 생성한 세션키로 암호화한 거래 정보를 수신한다.
4) 수신된 거래 정보를 확인하여 모바일 카드 및 모바일 신용카드의 데이터를 모바일 카드 결제 프로그램을 통해 모바일 카드 결제 서버로 전송한다.
5) 카드사는 전송된 데이터를 확인한 후, 모바일 카드 결제 프로그램으로 승인 결과를 전송한다.
6) 사용자가 승인 결과를 확인하면 카드사는 가맹점으로 승인 결과를 전송하여 결제를 종료한다.

비대면 거래에서 데이터를 암호화하는데 사용하는 세션키의 생성 과정은 다음과 같다.

- 모바일 카드 결제 서버와 모바일 카드 결제 프로그램은 TS를 Unique Key로 하여 세션키 SK를 생성한다.

3. 제안하는 모바일 지급결제 시스템

본 장에서는 기존의 모바일 지급 결제 시스템이 갖고 있는 문제점을 제시한 후, 이에 대한 해결책인 보다 안전한 방식의 결제 프로토콜을 제안한다. 기존의 모바일 지급 결제 시스템의 문제점은 다음과 같이 요약할 수 있다.

- 대면 거래의 문제점: 파생키 DK와 세션키 SK를 생성하는데 각각 사용되는 Chip ID와 거래 계수기는 모두 평문 형태로 결제 단말기에 전송된다. 결과적으로 모든 키의 안전성은 MK에 의존한다고 할 수 있다. 따라서 카드사의 비밀키인 MK가 노출될 경우, 누구나 파생키 DK와 세션키 SK를 생성할 수 있기 때문에 데이터를 암호화하는데 사용하는 세션키의 안전성을 보장할 수 없다.
- 비대면 거래의 문제점: 대면 거래와는 달리, 서로 사전에 공유하는 값이 없다. 그렇기 때문에 거래 시간 정보인 TS를 Unique Key로 이용하여 세션키 SK를 생성한다. 그러나 TS는 누구나 알 수 있는 정보이기 때문에 데이터를 암호화하는데 사용하는 세션키의 안전성이 보장되지 않는다.

제안하는 프로토콜에서 사용하는 기호 및 의미는 Table 1과 같다.

[Table 1] Notations

Symbol	Definition
AID	mobile card's identifier in mobile device
$Chip\ ID$	Mobile card's chip identifier
$Counter$	transaction counter
TS	time stamp
$Cert_{T/S}$	payment device 가 Mobile card payment server's certificate
$PK_{T/S}$	payment device 가 Mobile card payment server's public key
$SK_{T/S}$	payment device 가 Mobile card payment server's private key
MK_i	Card company i's secret key
DK	Derivation Key
SK	Session Key
PSK	Pre-Shared Key between mobile device and card company i
$Nonce$	random number
$E_*()/D_*()$	Encryption/Decryption using key *
$PRF()$	Pseudorandom Function

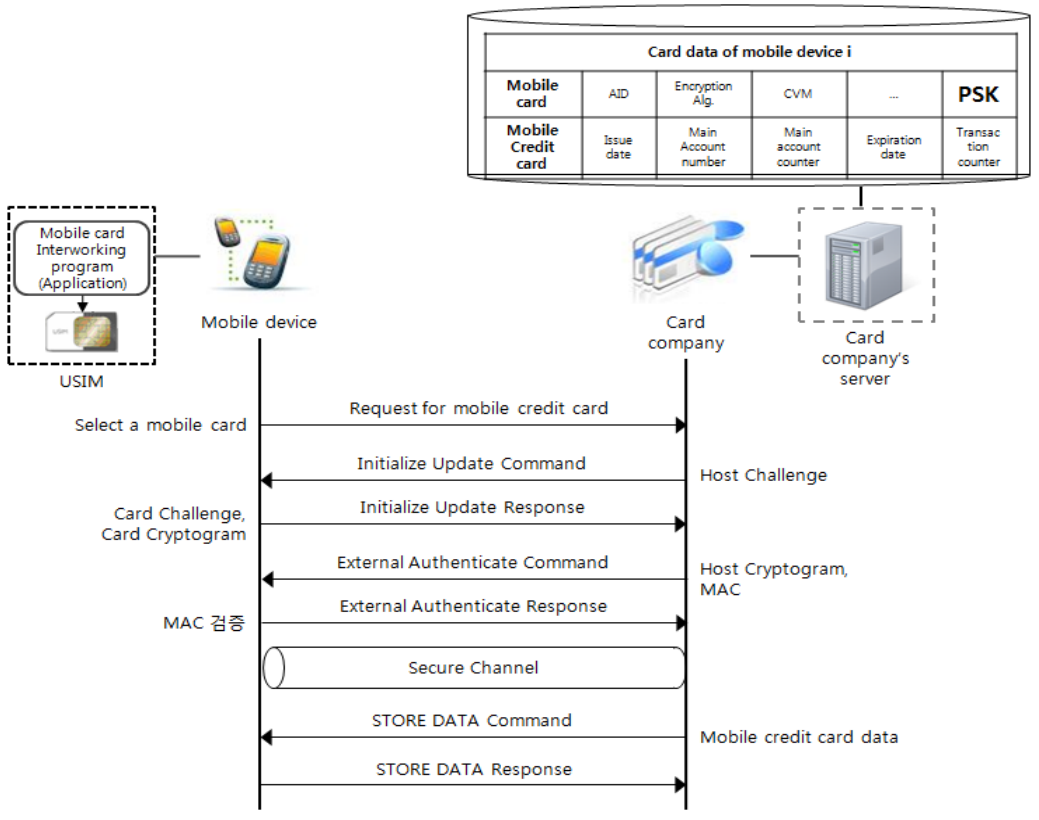
3.1 발급 단계

제안하는 모바일 지급결제 시스템의 발급 단계는 사전에 공유한 비밀키인 PSK를 안전하게 설정하는 과정을 추가로 수행하며 발급 과정은 Fig. 4와 같다.

3.2 대면 거래

대면 거래는 모바일 단말기와 결제 단말기가 상호 인증을 수행하고 거래 데이터를 암호화하는데 사용하기 위한 세션키 SK를 수립한다. 대면 거래에서의 가정 사항은 다음과 같다.

○ 비밀키 공유: 모바일 단말기는 카드사와 사전에 공유한 비밀값 PSK를 공유한다.
○ 공개키 인증서 사용: 카드사 서버는 인증서에 수납된 공개키를 이용하여 PSK를 암호화하여 결제 단말기로 전송한다.



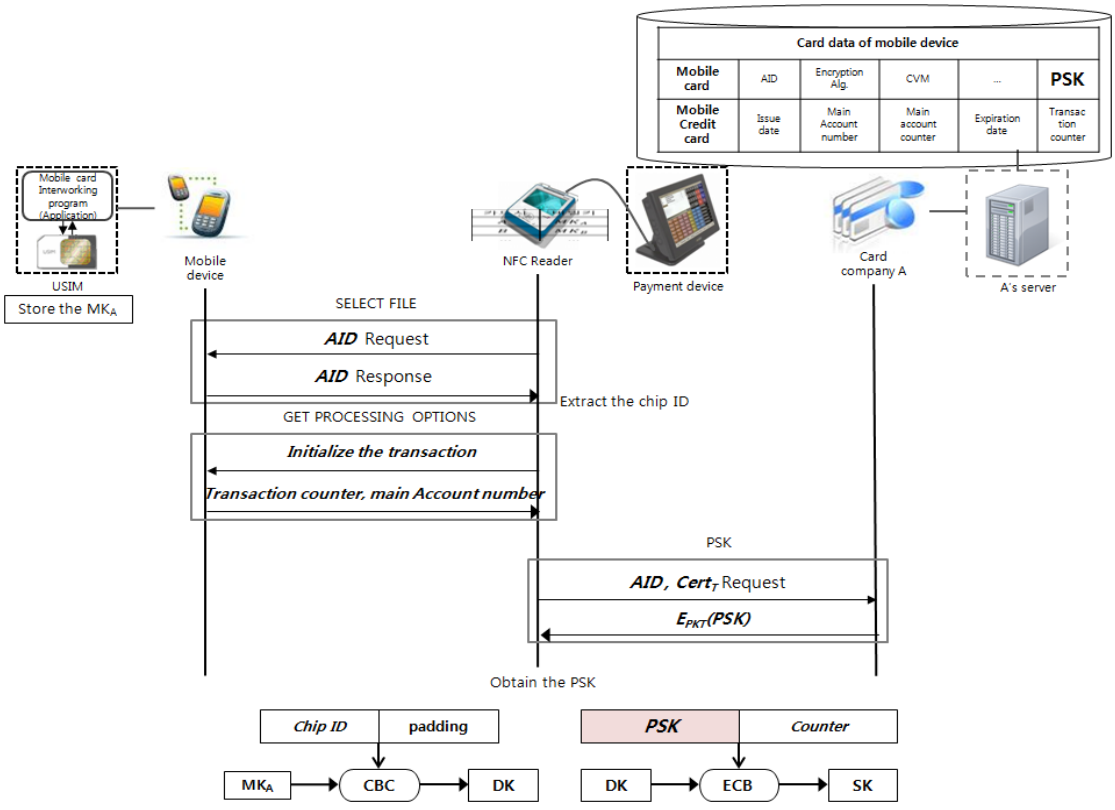
[Fig. 4] The proposed issuing phase in Offline transaction

[대면 거래 절차]

1) 사용자는 결제 단말기를 통해 거래 금액을 확인하고 NFC가 탑재된 모바일 단말기를 결제 단말기의 리더기에 근접시킨다.
2) 모바일 단말기는 대면 거래에 사용되는 모바일 카드를 식별하기 위한 데이터 요소를 결제 단말기로 전송한다. 이때 포함되는 데이터는 카드사를 식별하기 위한 값, 파생키 DK 생성에 사용하는 Chip ID, 세션키 SK 생성에 사용하는 거래 계수기이다.
3) 결제 단말기는 전송된 데이터로 카드사를 식별하고 해당 카드사로 사용자의 PSK를 요청한다.
4) 카드사 서버는 결제 단말기의 인증서 $Cert_T$에 포함된 공개키 PK_T로 PSK를 암호화하여 전달한다. 그러면 결제 단말기는 암호화된 PSK를 비밀키 SK_T로 복호화하여 PSK를 획득한다.
5) 결제 단말기는 모바일 단말기로부터 전송된 데이터와 PSK를 이용하여 세션키 SK를 생성한 다. 그리고 모바일 단말기가 전송한 암호문을 세션키로 복호화하여 데이터를 안전하게 획득한다.
6) 결제 단말기는 획득한 데이터를 승인받기 위해 카드사 서버로 전송한다.
7) 카드사 서버는 전송된 데이터를 확인한 후, 결제 단말기로 결과를 전송하여 결제를 종료한다.

제안하는 대면 거래에서 데이터를 암호화하는데 사용하는 세션키 SK의 생성 과정은 [Fig. 5]와 같다.

- 모바일 단말기는 SELECT FILE 및 GET PROCESSING OPTIONS 명령을 통해 Chip ID와 거래 계수기, 주 계좌 번호를 결제 단말기로 전송한다.
- 결제 단말기는 주 계좌 번호를 이용하여 카드사 A를 식별하고 Chip ID에 해당하는 PSK를 요청한다.
- 카드사 서버는 PSK를 결제 단말기의 인증서 $Cert_T$에 포함된 공개키 PK_T로 암호화하여 전송하면, 결제 단말기는 SK_T로 복호화하여 PSK를 획득한다.
- 결제 단말기는 카드사 A의 비밀키 MK_A와 Chip ID에 대해 CBC 연산을 수행하여 파생키 DK를 생성한 후, DK와 거래 계수기에 대해 ECB 연산을 수행하여



[Fig. 5] The proposed session key generation in Offline transaction

세션키 SK를 생성한다.

· 모바일 단말기는 결제 단말기와 동일한 과정을 수행하여 세션키 SK를 생성한다.

3.3 비대면 거래

비대면 거래는 모바일 카드 결제 프로그램과 모바일 카드 결제 서버 간에 상호 인증을 수행하고 거래 데이터를 암호화하는데 사용하기 위한 세션키 SK를 수립한다. 비대면 거래에서의 가정 사항은 다음과 같다.

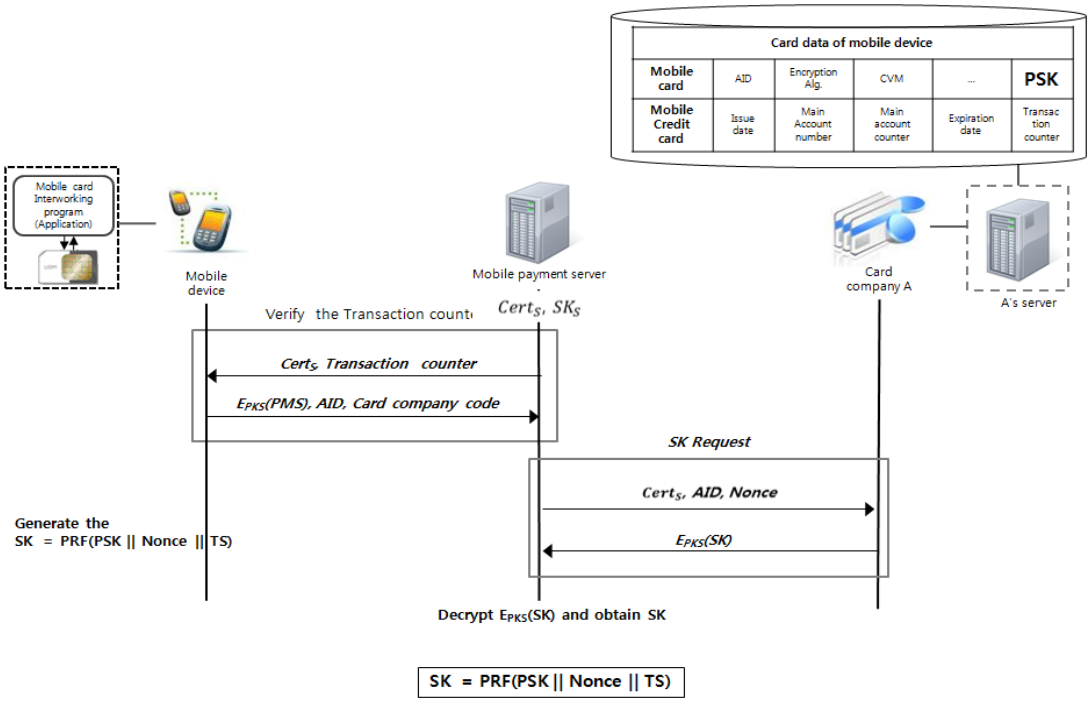
○ 비밀키 공유: 모바일 단말기는 카드사와 사전에 공유한 비밀값 PSK를 공유한다.

○ 공개키 인증서 사용: 카드사 서버는 모바일 카드 결제 서버의 인증서에 수납된 공개키를 이용하여 세션키 SK를 암호화하여 모바일 카드 결제 서버로 전송한다.

[비대면 거래 절차]

1) 사용자는 온라인 가맹점에서 상품 및 결제 방식 등과 같은 데이터를 선택한다.
2) 가맹점은 모바일 카드 결제 서버로 거래 정보 및 사용자 정보, 가맹점 정보를 전송한다.
3) 모바일 카드 결제 서버가 모바일 카드 결제 프로그램으로 Nonce를 요청하면 인증서 $Cert_S$에 포함된 공개키 PK_S로 Nonce를 암호화하여 전송한다.
4) 모바일 카드 결제 서버는 비밀키 SK_S로 복호화하여 Nonce를 획득하고 카드사를 식별한 다음, 카드사 서버에 세션키 SK를 요청한다.
5) 카드사 서버는 세션키 생성 방식을 통해 생성된 세션키 SK를 모바일 카드 결제 서버의 공개키로 암호화하여 전송한다.
6) 모바일 카드 결제 서버는 공개키 SK_S로 세션키 SK를 복호화하여 획득하고 거래 정보를 암호화하여 모바일 카드 결제 프로그램으로 전송한다.
7) 수신된 거래 정보를 확인하여 모바일 카드 및 모바일 신용카드의 데이터를 모바일 카드 결제 프로그램을 통해 모바일 카드 결제 서버로 전송한다.
8) 모바일 카드 결제 서버는 전송된 거래 데이터를 확인한 후, 승인 결과를 모바일 카드 결제 프로그램으로 전송한다.
9) 사용자가 결과를 확인하고 승인하면 카드사는 가맹점으로 승인 결과를 전송하여 결제를 종료한다.

제안하는 비대면 거래에서 데이터를 암호화하는데 사용하는 세션키 SK의 생성 과정은 Fig. 6과 같다.



[Fig. 6] The proposed session key generation

· 모바일 카드 결제 서버는 모바일 카드 결제 프로그램으로 거래 일련번호와 인증서를 전송하여 정당한 구동 요청인지 확인하고, 모바일 카드 결제 프로그램은 전송된 인증서를 검증하여 공개키를 추출한 후, Nonce를 암호화하여 전송한다.
· 모바일 카드 결제 서버는 전송된 $E_{PK_S}(Nonce)$를 비밀키 SK_S로 복호화하여 Nonce를 획득한 다음, 카드사 식별 코드를 이용하여 카드사를 식별하여 카드사 서버로 인증서를 전송한다.
· 카드사 서버는 전달받은 인증서를 검증한 다음 공개키를 추출한다. 해당하는 PSK를 이용하여 세션키 SK를 생성한 후에 공개키로 암호화하여 전송한다.
· 모바일 카드 결제 서버는 비밀키 SK_S로 복호화하여 SK를 획득하고 데이터를 암호화한다.

4. 안전성 분석

본 장에서는 제안하는 모바일 지급결제 시스템의 대면 거래 및 비대면 거래에서 생성한 세션키 SK의 안전성을 분석한다.

4.1 대면 거래

· 전방향 안전성: 제안하는 방식에서는 모바일 단말기와 카드사 간의 공유 비밀키인 PSK를 사용하기 때문에 MK가 노출되더라도 실제 데이터를 암호화하는데 사용하는 세션키 SK를 생성할 수 없기 때문에 세션키에 대한 전방향 안전성을 제공한다.
· 키 신규성: 매번 거래할 때마다 모바일 단말기의 거래 계수기인 Counter를 이용하여 생성한다. 이 거래 계수기는 매번 바뀌기 때문에 세션키 SK 또한 이전과는 다른 값을 갖게 되어 신규성을 유지할 수 있다.
· 상호 인증 및 키 확인: 공개키에 대응하는 비밀키를 소유한 정당한 단말기만이 암호화된 데이터를 복호화할 수 있기 때문에 묵시적인 상호 인증 및 키 확인을 제공한다.

4.2 비대면 거래

· 세션키 안전성: 제안하는 방식은 모바일 단말기에서 선택한 비밀 랜덤 수 Nonce와 사전에 공유한 비밀키 PSK, 거래 시간 정보 TS를 이용해서 세션키를 생성하고 공개키로 암호화해서 안전하게 전송하기 때문에 기존의 방식에 비해 안전성을 강화하였다.
· 키 신규성: 매번 거래할 때마다 모바일 단말기가 선택한 비밀 랜덤 수 Nonce를 이용해 생성한다. Nonce는 매번 바뀌는 값이기 때문에 세션키 SK 또한 이전과는 다른 값을 갖게 되어 키 신규성을 유지할 수 있다.
· 상호 인증 및 키 확인: 공개키에 대응하는 비밀키를 소유한 정당한 단말기만이 암호화된 데이터를 복호화할 수 있기 때문에 묵시적인 상호 인증 및 키 확인을 제공한다.
· 효율성: 모바일 카드 결제 서버만이 인증서를 사용하는 방식으로, 모바일 단말기에는 별도의 인증서를 발급받고 관리하는 절차가 요구되지 않는다. 따라서 모바일 단말기에 인증서 발급 및 관리를 위한 별도의 오버헤드가 요구되지 않으며, 양방향에서 인증서를 사용하는 방식에 비해 효율적이다.

5. 결론

NFC를 이용한 모바일 결제 시스템이 활성화됨에 따라, 2012년 3월 28일 지식경제부 기술표준원에서는 모바일 지급결제를 위한 표준으로서 KS X 6928을 제정하였다. 표준은 NFC 기술을 탑재하여 대면 거래 및 비대면 거래를 규정하였지만. 거래 데이터를 전송하는 과정에서 암호화하는데 사용하는 세션키에 취약점이 존재하며, 안전성이 보장되지 않는다. 따라서 본 논문에서는 세션키의 안전성을 향상시키기 위한 키 생성 방식을 제안하였다.

본 논문에서 제안하는 대면 거래의 경우, 카드사의 고유값인 MK가 외부로 노출되더라도 공격자는 거래 데이터를 암호화하는데 사용하는 세션키를 생성할 수 없도록 모바일 단말기와 카드사 서버 간에 공유 비밀키인 PSK를 이용한다. 따라서 전방향 안전성, 키 신규성, 상호 인증 및 키 확인을 제공한다. 또한, 비대면 거래의 경우, 모바일 단말기가 생성한 비밀 랜덤 수와 PSK를 이용하여 세션키의 안전성을 향상시켰다. 따라서 키 신규성, 상호 인증 및 키 확인, 효율성 등을 제공한다. 제안하는 모바일 지급결제 시스템을 적용함으로써 보다 안전한 결제 시스템을 제공할 수 있을 것으로 기대한다.

References

[1] KS X 6928-1 “Mobile payment - Mobile card - Part 1 : General", 2012.
[2] KS X 6928-2 “Mobile payment - Mobile card - Part 2 : Offline transaction, 2012.

[3] KS X 6928-3 “Mobile payment - Mobile card - Part 2 : Online transaction, 2012.
[4] http://www.nfc-forum.org/
[5] ECMA International, Standard ECMA-340 “Near Field Communication Interface and Protocol-1(NFCIP-1)”, 1st edition, December. 2002.
[6] ECMA International, Standard ECMA-352 “Near Field Communication Interface and Protocol-2(NFCIP-2)”, 1st edition, December. 2003.
[7] ECMA International, Standard ECMA-385 “NFC-SEC: NFCIP-1 Security Services and Protocol”, June. 2010.
[8] ECMA International, Standard ECMA-386 “NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES”, June. 2010.
[9] http://www.koreanfc.org/

이 요 람(Yo-Ram Lee) **[정회원]**

- 2013년 2월 : 호서대학교 정보보호학과 대학원 졸업 (공학학석사)
- 2013년 3월 ~ 현재 : (주)이베이코리아

<관심분야>
NFC 보안, 네트워크 보안

오 수 현(Soo-Hyun Oh) **[정회원]**

- 1998년 2월 : 성균관대학교 전기전자 및 컴퓨터공학부 대학원 졸업 (공학석사)
- 2003년 8월 : 성균관대학교 전기전자 및 컴퓨터공학부 대학원 졸업 (공학박사)
- 2004년 3월 ~ 현재 : 호서대학교 정보보호학과 교수

<관심분야>
암호학, 네트워크 보안, 정보보호 제품 평가 및 인증