NFC 모바일 결제 환경을 위한 Hash Chain기반의 Time-Stamping Proxy 서명 기술

박성욱*, 이임영*
*순천향대학교 컴퓨터소프트웨어공학과
e-mail:swpark@sch.ac.kr, imylee@sch.ac.kr

Hash Chain based Time-Stamping Proxy Signature Scheme for NFC Mobile Payment Environment

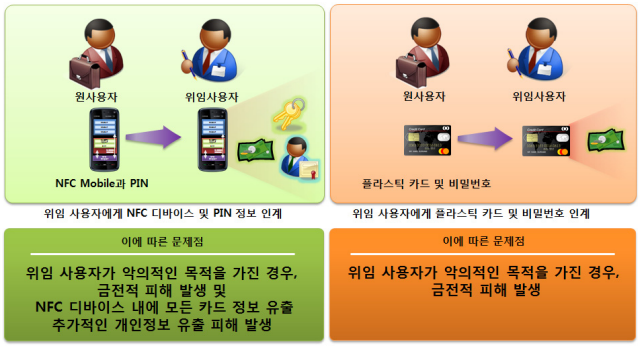
Sung-Wook Park*, Im-Yeong Lee*
*Dept of Computer Software Engineering, Soonchunhyang University

요 약

최근 스마트 기기는 결제, 할인쿠폰 등 각종 기능을 제공하는 수단으로 진화되면서 통신과 금융이 융합된 모바일 NFC 서비스의 시장이 급성장할 것으로 전망되고 있다. 특히 모바일 NFC 결제 서비스 시장의 활성화가 예상됨에 따라 모바일 NFC 결제 서비스는 국내·외적으로 널리 주목받고 있다. 하지만 이를 주도할 수 있는 보안 관련 기술력이 부족한 상태이며 NFC 모바일 결제 환경에서 적용이 가능한 NFC 결제 관련 기술 연구도 미흡한 실정이다. 이에 따라 기존 방식과는 전혀 다른 결제 환경과 결제 방식에 의해 도출될 수 있는 다양한 응용서비스에 대한 새로운 법·제도의 정비와 새로운 결제 환경에 맞는 보안기술이 필요할 것으로 예상된다. 본 논문에서는 기존의 물리적인 플라스틱 신용카드의 권한 위임 문제와 NFC 모바일 신용카드를 비교하여 NFC 모바일 기반 결제 서비스 상에서의 위협을 분석하고 NFC 결제환경에서 안전한 결제 권한 위임이 가능한 Hash Chain기반의 Time-Stamping Proxy 서명 기술을 제안하였다.

1. 서론

현재 논의되고 있는 NFC 적용 서비스 분야는 크게 모바일 결제서비스와 그 이외 응용 서비스 분야로 나눌 수 있다. 우선 누구든지 모바일 카드를 발급받아 해당 정보를 NFC 기능이 있는 단말기에 내려 받으면, 결제기에 단말기를 태깅(Tagging)하는 것만으로 결제가 가능하다. 이는 기존 신용카드 결제방식과 유사하다. 하지만 NFC 기반의 결제 서비스에서는 기존 신용카드 기반 서비스에서 제공할 수 없는 다양한 형태의 응용서비스가 가능하다. 예를 들어 기존 IC기반 신용카드의 경우 자체 연산능력을 가지고 있지만 RF 반송파 신호에 의한 연산에 불과하며 카드 자체가 임의의 연산을 수행하는 것이 불가능하기 때문에 사용하는데 있어 활용 범위에 대한 많은 제약 사항이 따른다. 가령, 사내 법인카드 사용 문제 또는 신용카드 대리결제와 같은 신용카드의 사용권한을 타인에게 일시적으로 위임해야 하는 특수한 상황에서 권한을 위임받은 대리 결제자에 의한 금전적인 피해가 발생할 수 있으나 기술적인 조치로 해결이 불가능하며 이와 같은 특징 때문에 신용카드는 원사용자가 관리할 권한만 가지게 되고 양도 또는 질권 설정을 할 수 없도록 법적으로 관리·조치되고 있다. 하지만 이는 원천적인 문제의 해결책은 되지 못해 유사시 신용카드 사용에 있어 권한 위임이 물리적인 형태로 이루어지고 있는 실정이다. 이러한 물리적인 형태의 권한 위임이 NFC 기반 모바일카드에서 이루어질 경우 많은 문제점을 내포하게 된다. 기존 신용카드의 경우 금전적인 피해만 발생한다면 NFC 기반 모바일카드에서는 금전적인 피해와 더불어 NFC 디바이스 내에 있는 개인정보부분까지 위협을 받을 수 있다. 그러나 NFC 기반 서비스의 경우 모바일과의 연동을 통해 자체적인 연산 수행이 가능하며 물리적인 형태의 위임이 아닌 전자적인 형태의 데이터 전송을 통한 권한 위임이 가능하기 때문에 다양한 형태의 응용서비스를 안전하게 수행하는 것이 가능하다. NFC 결제환경에서는 개인의 금융 결제 정보를 다루기 때문에 다양한



(그림 1) 결제 권한 위임에 관한 문제

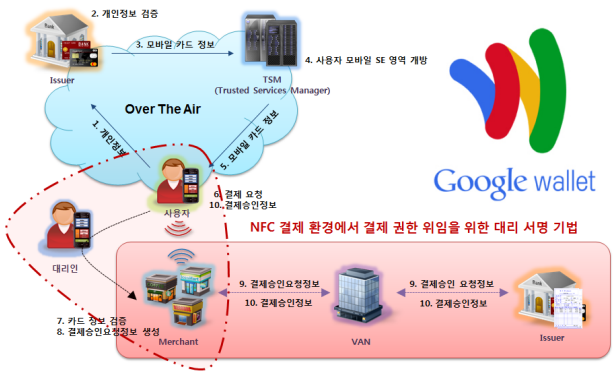
측면에서의 안전성을 제공해야 하는데 권한 위임을 위해 기존의 다수 제안된 대리 서명 기법을 그대로 적용할 경우 보안상 여러 가지 문제점이 발생할 수 있다. 따라서 본 논문에서는 NFC 결제환경에서 안전한 결제 권한 위임이 가능한 Hash Chain기반의 Time-Stamping Proxy 서명 기술을 제안하였다. 본 논문의 구성은 다음과 같다. 2장에서는 기존 NFC 기반 근거리 결제 방식과 일반적인 위임 서명에 대하여 분석하며, 3장에서는 기존연구를 기반으로 NFC 모바일 결제에 대한 보안요구사항에 대하여 분석한다. 4장에서는 보안요구사항을 만족하는 제안방식을 기술하며, 5장에서는 보안요구사항에 의한 제안방식을 분석한다. 마지막으로 6장에서 결론을 맺는다.

2. 관련연구

본 장에서는 최근 국외에서 상용화된 Google wallet 서비스에 대해 설명하고, 기존의 위임 서명 방식 분석과 이를 NFC 결제 환경에 적용했을 경우 발생할 수 있는 취약점을 분석한다.

2.1 Google Wallet

Google Wallet 서비스[4]는 Google 사에서 제공하는 NFC 스마트폰 기반의 결제 서비스로 현재 미국 일부지역, 일부 상점에서 시범 서비스가 진행 중이다. 삼성의 '넥서스S'를 시작으로 서비스 이용 가능 단말은 추후 지원 기종 및 통신사가 확대 될 예정이며, 결제 흐름도는 (그림 2)과 같다. 결제에 관련하여 Citi Bank가 참여하고 사용자에 대한 다양한 개인정보를 각 금융·카드사, 이통사, 상점 등에서 수집을 수행한다. Google사 측에서 모든 신용카드 정보가 NFC 통신 결제 규격인 M/Chip 4(Mobile MasterCard(R) PayPass™ M/Chip 4)[5]에 의해 암호화되고 이중 삼중의 보안 절차를 거치므로 물리적인 지갑보다 안전하다고 주장하고 있으나 검증된바 없으며 최근 '탈옥'하지 않은 정상적인 기기에서도 개인정보가 새나가는 문제가 수차례 발견됨에 따라 서비스의 일시적인 중단>패치>재개를 반복하고 있는 실정이다. 현재 Google Wallet 서비스에 적용된 PayPass의 표준 기술은 신용카드를 위한 표준 기술로서 NFC기반의 모바일 결제 흐름과 기존



(그림 2) Google Wallet 결제 흐름도 및 제안방식 범위

신용카드 결제 흐름 자체가 유사하다. 하지만 NFC와 모바일이 융합된 NFC기반 결제환경에서는 기존의 신용카드 기반 서비스에서 제공할 수 없는 다양한 형태의 서비스 제공이 가능하므로 그 특성에 맞는 새로운 형태의 보안 기술들이 부가적으로 필요할 것으로 예상된다.

2.2 대리서명

일반적으로 대리 서명의 위임 방식은 완전 위임, 부분 위임, 위임장에 의한 위임 그리고 위임장에 의한 부분 위임 방식으로 나누어진다. 본 논문에서 제안하는 환경은 개인의 주요 금융 데이터를 다루므로 대리 서명자의 서명 능력 남용을 제한할 수 없는 완전 위임 방식과 부분 위임 방식은 배제하며 위임장에 의한 위임 방식과 위임장에 의한 부분 위임 방식을 중심으로 설명한다.

위임장에 기반한 위임 방식은 대리 위임장이 대리 서명자에게 주어지며 위임장은 원 서명자와 대리 서명자의 식별자, 위임 기간, 그리고 대리 서명자가 서명할 수 있는 메시지의 종류 등이 기재되어 있어 대리 서명자의 서명 권한을 제한하고 통제할 수 있다. 그리고 부분 위임 방식의 약점을 보완하기 위해 위 두 가지 위임 방식을 혼합하여 위임장에 기반한 부분 위임 방식[1]이 고안되어 현재 많은 대리 서명 방식들이 제안되고 있다.

2.3 Sun의 방식[2]

위임장에 기반한 부분 위임 방식 또한 몇가지 한계를 가지고 있다. 검증자는 대리 서명자가 언제 서명을 생성했는지 정확한 시점을 알 수 없기 때문에 위임장에 기재된 위임 기간이 사실상 쓸모가 없어질 수 있다. Sun의 대리 서명 방법은 Time-Stamp를 통해 대리 서명자가 위임 기간 동안만 서명을 생성할 수 있도록 설계되었다. 하지만 정확한 시간 정보를 생성하고 이를 검증하는 메커니즘이 없으며, 매 서명마다 연결정보를 생성하여 인증된 저장 공간에 공고해야 하기 때문에 주요 파라미터가 시간 구간 수에 종속적이라는 문제점을 가진다.

2.4 Wang의 방식[3]

Wang은 두-참가자 Schnorr 서명방식에 기반을 둔 안전성 증명 가능한 대리서명을 제안하였다. 이 방식은 서명 권한을 위임할 수 있는 기능을 가지며 서명 권한의 높은 유연성을 제공한다. 반면에 위조 증명 기능이 없기 때문에 서명의 위조가 발생 시 서명자를 보호할 수 있는 방법이 없다는 문제점이 존재한다.

3. 보안요구사항

NFC 모바일 환경 특성을 고려하여 대리서명기법이 기본적으로 만족해야할 안전성과 더불어 기존 방식의 문제점인 효율성을 제공해야 한다. 따라서 NFC 위임 결제 기술에서의 보안요구사항은 다음과 같다.

· 강력한 위조 불가성 : 원 서명자에 의해 지정된 대리 서명자만이 대리 서명을 생성할 수 있어야 하고 원 서명자를 포함한 어떤 제3자도 대리 서명자를 가장한 서명을 생성할 수 없어야 한다.
· 검증성 : 검증자는 대리 서명으로부터 원 서명자의 위임 동의를 확인할 수 있어야 한다.
· 강력한 신원 확인성 : 누구나 대리 서명으로부터 대리 서명자의 신원을 확인할 수 있어야 한다.
· 오용방지 : 대리 서명자는 원 서명자로부터 위임받은 권한 이외에 목적으로 대리 서명키를 사용할 수 없어야 하며, 대리 서명키 오용 발생 시 대리 서명자의 책임이 명시적으로 드러나야 한다.
· 효율성 : 주요 파라미터가 시간 구간의 수에 독립적이며 부가적인 저장 공간을 필요로 하지 않아야 한다.
· 안전성 : 대리 서명자는 원 서명자가 설정한 위임 기간 동안만 타당한 대리 서명을 생성할 수 있어야 하며 현재 시간 구간의 서명키로부터 과거 시간 구간의 서명키를 유도할 수 없어야 한다. 또한 위임기간이 만료된 대리 서명자는 수신자가 공모하여 서명을 생성할 수 없어야 한다.

4. 제안방식

이 장에서는 3장의 보안요구사항을 만족하는 NFC 모바일 결제 환경을 위한 Hash Chain기반의 Time-Stamping Proxy 서명 기술을 제안한다. 본 제안방식은 위임 정보 생성 단계, 위임 정보 검증 단계, 대리 서명키 생성 및 갱신 단계, 대리 서명 생성 단계, 대리 서명 검증 단계로 구분되며, 각 단계의 수행절차는 다음과 같다.

4.1 시스템 계수

본 제안방식에서는 다음과 같은 시스템계수를 사용하여 프로토콜을 설계한다.

· $*$: 개체 (A : 원 서명자, B :대리 서명자 S : 검증서버(Bank))
· g : 위수가 q인 Z_p상의 서브 그룹 생성자
· p, q : $q|p-1$을 만족하는 큰 소수
· m_w : 대리 서명 위임장, 대리 서명자가 서명 가능한 서명의 종류, 위임 기간, 원 서명자와 대리 서명자의 식별자 등이 기재됨
· X_*, Y_*: 각 개체의 비밀 키, 공개 키
· $H()$: 공개된 암호학적 해시함수
· T, U : 대리 서명키 갱신 횟수 및 갱신 주기
· $S(), V()$: 이산 대수 문제의 어려움에 기반한 서명 생성 및 검증 알고리즘

4.2 위임 정보 생성단계

원 서명자는 대리 서명자에게 위임 정보를 제공하기 위해 위임 정보 생성단계를 거친다.

Step1 : 보증정보 m_w는 원 서명자가 지정한 임의의 값 T, U 정보를 포함하며 해쉬 체인의 초기값 A를 T만큼 해쉬를 취한 E를 생성한다.

$$A: m_w = (T, U)$$
$$A: A \in_R Z_q^*$$
$$A: H^T(A) = E$$

Step2 : 원 서명자는 임의의 수 $K_A \in_R Z_q^*$를 선택하고 아래와 같이 계산한다. K_A는 임의의 난수로서 원 서명자만이 알고 있는 비밀 값이다. 계산된 r_A는 비밀 값 K_A에 대한 공개 값이며 C는 그것에 대한 해쉬 값이다. 계산 수행 후 원 서명자는 C를 대리 서명자에게 전송한다.

$$A: K_A \in_R Z_q^*$$
$$A: r_A = g^{K_A} \bmod p$$
$$A: C = H(r_A)$$
$$A \rightarrow B: C$$

Step3 : 대리 서명자도 임의의 수 $K_B \in_R Z_q^*$를 선택하고 아래와 같이 계산한다. 이후 원 서명자에게 (C, r_B)를 전송한다.

$$B: K_B \in_R Z_q^*$$
$$A: r_B = g^{K_B} \bmod p$$
$$A \rightarrow B: (C, r_B)$$

Step4 : 원 서명자는 (C, r_B)를 받으면 아래와 같이 계산 후 (r_A, S_A, m_W, A, E)를 대리 서명자에게 전송한다.

$$A: r_P = r_A \cdot r_B \bmod p$$
$$A: S_A = X_A \cdot H(m_W, r_P, E) + K_A$$
$$A \rightarrow B: (r_A, S_A, m_W, A, E)$$

4.3 위임 정보 검증단계

대리 서명자는 원 서명자로부터 위임 정보를 수신한 후 대리 서명키 생성에 필요한 S_A를 검증하기 위해 다음과 같은 단계를 수행한다.

Step1 : 대리 서명자는 (r_A, S, m_W, A, E)를 수신한 후, 아래와 같이 계산을 통해 원 서명자로부터 받은 S_A를 검증한다.

$$B: C = H(r_A)$$
$$B: r_P = r_A \cdot r_B \bmod p$$
$$B: g^{S_A} = Y_A^{H(m_W, r_P)} \cdot r_A \bmod p$$

4.4 대리 서명키 생성 및 갱신단계

매 시간 구간 $t (1 \le t \le T)$마다 서명키 갱신 및 생성을 위해 다음과 같은 단계를 수행한다.

Step1 : $H^t(A) = H(H^{t-1}(A))$를 계산하여 시간 구간을 갱신한다.

$$B: H^t(A) = H(H^{t-1}(A))$$

Step2 : 대리 서명키 생성 요청 시 시간 구간 t동안 사용할 대리 서명키 X_P를 생성한다.

$$B: S_B = X_B \bullet H(m_W, r_P, H^t(A)) + K_B \bmod q$$
$$B: X_P = S_A \bullet S_B$$

4.5 대리 서명 생성단계

대리 서명자는 메시지 m에 대한 대리 서명을 생성하기 위해 다음과 같은 단계를 수행한다.

Step1 : 보증 정보 m_w를 통해 메시지 m이 서명 위임된 사항인지 확인한 후 현재 시간 구간 t의 대리 서명키 X_P로 메시지 m에 대한 서명 $\sigma = S(X_P, m)$을 생성한다.

$$B: \sigma = S(X_P, m)$$

Step2 : $\sigma = S(X_P, m)$를 메시지 m에 대한 서명으로 삼고 검증서버에 $(m, m_W, r_P, \sigma, E, t, H^t(A))$를 전송한다.

$$B \rightarrow A: (m, m_W, r_P, \sigma, E, t, H^t(A))$$

4.6 대리 서명 검증단계

검증서버는 메시지 m에 대한 대리 서명을 검증하기 위해 다음과 같은 단계를 수행한다.

Step1 : $H^{T-t}(H^t(A)) = E$를 확인하여 위임 권한의 유효 기간을 검증한다.

$$S: H^{T-t}(H^t(A)) = E$$

Step2 : 메시지 m이 위임장 m_w의 기재사항(각 서명자 확인)에 따르는지 확인 후 아래와 같이 계산하여 대리 공개 키를 구한다.

$$S: Y_P = Y_A^{H(m_W, r_P, E)} \bullet Y_B^{H(m_W, r_P, H^t(A))} \bullet r_P \bmod p$$

Step3 : 대리 서명자의 대리 서명 공개키 Y_P를 통해 $V(Y_P, m, \sigma) = true$인지 검증한다.

$$S: V(Y_P, m, \sigma) = true$$

5. 제안방식분석

본 제안방식은 3장에서 도출된 보안요구사항을 다음과 같이 만족한다.

· 강력한 위조 불가능성 : 대리서명 검증키 Y_P로부터 X_P를 알아내는 문제는 이산 대수 문제의 어려움에 기반하므로 계산상 위조가 불가능하다.

· 검증성 : 검증서버가 대리 서명을 검증할 경우 원 서명자의 공개키를 사용하므로 원 서명자의 위임 동의가 검증된다.

· 강력한 신원확인성 : 검증서버가 대리 서명을 검증하기 위해서 대리 서명 검증키를 계산할 경우 대리 서명자의 공개키를 통해 대리 서명자의 신원이 확인된다.

· 오용방지 : 보증 정보에 명시되지 않은 악의적인 목적으로 대리 서명키를 사용할 경우 위조 불가능성에 의해 대리 서명자의 책임이 명시적으로 드러난다.

· 효율성 : 검증서버가 대리 서명 검증 시 해쉬 함수 연산을 제외하고 대리 서명키 생성의 계산량이 대리 서명키 갱신 횟수 T에 독립적이며 부가적인 저장 공간이 필요하지 않다.

· 안전성 : 위임 서명의 위임 기간 만료 시, 검증서버는 시간 구간에 관련된 정보를 통해 위임 권한의 유효 기간을 검증이 가능하며 대리 서명자는 위임 서명에 포함된 서명 생성 시간 정보를 통해 자신의 대리 서명에 대한 정당성을 증명할 수 있다.

6. 결론

본 논문에서는 NFC 결제 환경에서 타인에게 금융결제 권한을 위임해야하는 특수한 상황에서 일시적으로 권한 위임이 가능하며 사후 검증이 가능한 Hash Chain기반의 Time-Stamping 대리 서명 기술을 제안하였다. 본 방식은 일반적인 신용카드 환경에서는 수행할 수 없는 NFC 결제 환경에 특화된 성격을 띄고 있으며 NFC 결제 환경의 특성에 맞는 법적인 규제가 제정되어 있지 않은 현 시점에서 여신전문금융업법 상에 제정되어 있는 법규에 상충되는 문제점을 가지고 있지만 향후 NFC 결제환경을 위한 전자금융거래와 정보보호법이 제정된다면 금융결제 권한을 대리인에게 임시적으로 위임하는 서명기술 연구 자료로 활용될 것으로 예상된다. 향후 연구로는 NFC 결제 서비스 환경에서 사용자의 개인정보보호를 위해 부분적인 익명성을 제공하는 서명기법에 관한 연구가 필요할 것으로 사료된다.

참고문헌

[1] B. Lee, H. Kim and K. Kim "Strong Proxy Signature and its Applications", Proc. of SCIS 2001, 2001

[2] H. M. Sun, "Design of Time-Stamped Proxy Signature with Traceable Receivers," Proc. of IEE Computers and Digital Techniques, Vol. 147, No. 6, 2000.

[3] G. Wang, "Designated-Verifier Proxy Signature Schemes", Security and Privacy in the Age of Ubiquitous Computing, Vol. 181, pp. 409-423, 2005.

[4] "Google Wallet: Security", Google, 2011

[5] "MasterCard PayPass", MasterCard, 2011