NFC 기반 시스템의 안전한 인증 메커니즘에 관한 연구

류선영*, 김강석*, 홍만표*
*아주대학교 대학원 지식정보공학과
e-mail : syra@ajou.ac.kr

A Study on Secure Authentication Mechanism in NFC based System

Seonyoung Ryu*, Kangseok Kim*, Manpyo Hong*
*Dept. of Knowledge Information Engineering, Graduate School of Ajou University

요 약

NFC(Near Field Communication) 기술은 스마트 폰과 같은 모바일 기기에 적용되어 정보의 송수신을 위한 매체로 활용될 뿐만 아니라 결제, 개인인증 등 다양한 분야에서 활용되고 있다. 따라서 이러한 NFC 기술을 이용해 개인정보를 활용한 다양한 맞춤형 서비스들이 등장하고 있으며 이에 따른 개인정보위협의 부작용도 발생되고 있는 실정이다. 그러나 현재 NFC 서비스에서 발생할 보안 위협 요소에 대한 분석과 해결책에 대한 연구는 매우 미비하다. 본 논문에서는 NFC 서비스에 대한 보안 취약점과 NFC 기반 시스템에서 발생할 수 있는 공격들에 대해 분석하고, 이를 해결하기 위해 NFC 기반 시스템의 인증 메커니즘을 제안한다.

1. 서론

NFC 기술은 일본 SONY와 NXP가 공동 개발하였고, RFID(Radio Frequency Identification) 표준인 ISO/IEC 14443 Proximity-card Standard를 확장한 방식이다. 또한 13.56MHz 주파수 대역을 사용하는 10cm이내의 단거리에서 106kbps 최대 424kbps의 속도로 양방향 통신이 가능한 비접촉식 근거리 무선통신 기술을 말한다[1].

최근 스마트 폰 시장의 급격한 증가로 스마트 폰은 우리 실생활에서 없어서는 안 될 생활필수품이 되었다. 사용자들의 스마트 폰을 실생활에서 좀 더 효율적으로 사용하고자 하는 사회적 요구가 증가함에 따라 NFC 기술을 활용한 서비스가 국내외적으로 널리 주목 받고 있으며, 기존 단방향 통신만 가능한 RFID기술을 이용했던 서비스가 점차 NFC 기술로 활발히 전환하고 있다. 대표적인 예로 모바일 전자결제, 출입문 통제, 스마트 워크, 모바일 정보공유 등이 있다. 이처럼 다양한 분야에서 NFC 서비스 관련 시장의 활성화가 이루어지고 있음에도 불구하고 아직 NFC 서비스 보안 위협과 관련된 연구는 미비한 실정이다.

NFC 기술은 비영리 유럽 표준화 기구 ECMA의 NFCIP-1에 의해 사전에 인증 절차 없이 무선 통신이 연결된 후 보안 서비스를 수행하게 된다[2]. 이러한 무선 통신구간에서 안전한 통신 채널을 확보하지 않을 경우 서버와의 별도 인증과정이 없이 공격자는 이를 악용할 소지가 매우 크다. NFC 기기 간 통신이 이루어 질 때 RF 신호를 통해 RF 통신 구간에서 데이터가 송수신 된다. 이 같은 경우 공격자는 RF 통신 구간에 접근해 데이터 도청이 가능하고 Tag 데이터를 가로채 위조, 변조가 발생할 수 있음을 의미한다. 이러한 보안 위협은 프라이버시 침해, 재산 손실 등과 같은 피해를 가져올 수 있다.

본 논문에서는 NFC 서비스 보안의 취약점과 발생 가능한 보안 위협에 대해 분석하고, 이를 해결하기 위한 NFC 인증 메커니즘을 제안하여 보다 안전한 NFC 서비스가 이루어 질 수 있도록 한다.

본 논문의 구성은 다음과 같다. 2장 관련연구에서는 NFC 기술에 대해 알아보고 NFC 서비스 이용 중에서 발생할 수 있는 공격기법에 대해서 연구해본다. 그리고 3장에서는 NFC 데이터에 대한 기밀성 및 무결성을 제공하는 인증 메커니즘에 대해 제안한다. 마지막으로 4장에서는 결론 및 향후 연구에 대해 설명한다.

2. 관련연구

2.1. NFC 공격 유형

NFC 공격 유형은 물리적 공격 유형과 논리적 공격 유형 이렇게 두 가지 유형으로 나눌 수 있다. 물리적 공격 유형에는 데이터 도청, 데이터 삽입, 데이터 위조, 데이터 변조 등이 있다. 논리적 공격 유형은 Relay attack,

※ 본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정 지원 사업"의 연구결과로 수행되었음

Replay attack, MITM(Man-in-the-middle) attack 등이 있다.

2.2. NFC 보안 위협에 대한 기존연구

2.2.1. 악성 Code Injection Worm

Code Injection공격은 공격자가 타깃 프로세스에 독립 실행 코드를 삽입 한 후 실행 시키는 기법이다. Code Injection은 해당 메모리에 흔적을 남기지 않는 특징 때문에 악성 코드를 제작 할 때 Code Injection을 많이 사용한다. 이러한 특징을 이용해 NFC공격자는 수동 NFC Tag를 악의적인 목적으로 사용해 버퍼 오버플로우, SQL Injection 등과 같은 문제점을 발생시킨다[4]. 하지만 수동 Tag를 이용한 공격은 제한적이다. 수동 Tag는 자체 전원이 내장되어 있지 않아 리더기로부터 전자유도나 전파로 전력을 받아야 Tag를 판독하고, 저장되어 있는 데이터 분석이 가능하기 때문이다.

2.2.2. NKMM(NFC Key Management Mechanism)

NKMM 방법은 NFC Tag와 서버 간에 공유해 사용하는 비밀 키에 대한 정보를 안전하게 관리하기 위해 비밀키를 서버에 저장함으로써 NFC Tag 는 비밀키가 필요할 때마다 NFC 디바이스를 통해 서버에 요청하는 키 관리 메커니즘이다. NKMM은 NFC 디바이스에 대한 인증 절차가 없이 NFC Tag 데이터에 접근이 가능하다. 이러한 문제점을 악용해 공격자는 정당하지 않은 NFC 디바이스를 사용 할 경우 NFC Tag 데이터에 접근이 가능해진다[5].

3. 제안방식

본 장에서는 Replay 공격 과 NFC 물리적 공격에 안전하고 암호화, 해쉬를 통해 NFC Tag 정보에 대한 기밀성 및 무결성을 보장하는 NFC 기반 시스템의 인증 메커니즘을 제안한다. 제안하는 인증 메커니즘은 NFC 디바이스를 통해 서버에 어플리케이션을 등록 하는 등록절차와 NFC 서비스 이용을 위해 사용자에 대한 인증절차로 구성된다. 등록절차는 인증을 위해 사용자 정보를 서버에 등록하게 된다. 인증절차에서는 등록한 사용자 정보와 NFC 디바이스 그리고 NFC 리더를 통해 서버로부터 인증 절차를 수행하게 된다.

3.1. 등록절차

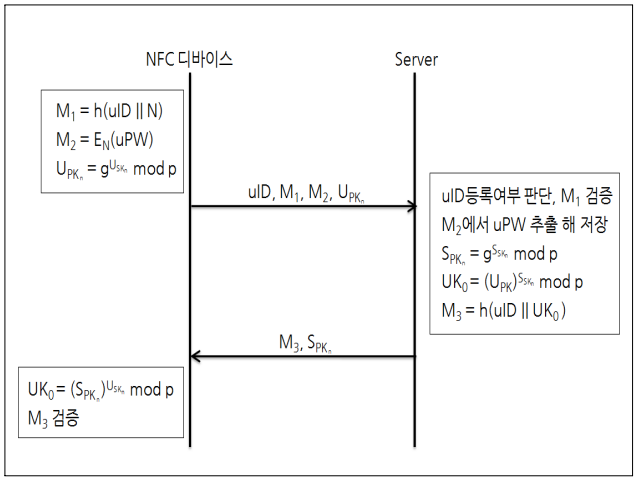
NFC 디바이스에 어플리케이션 설치 후 최초 실행 시 등록 절차를 수행하게 된다. 먼저 등록 전 웹페이지 회원가입을 통해 사용자 식별자(uID)와 인증번호(N)를 부여받게 됨으로써 서버와 사전 공유되어 있다.

<표 1> 은 제안하는 인증 메커니즘에서 사용되는 표기를 나타낸 것이다.

<표 1> 제안하는 메커니즘에서 사용되는 표기

표기	설명
U	사용자 (User)
R	NFC 리더기(NFC Reader)
S	서버(Server)
N	랜덤 난수(Nonce)
uID	사용자 식별자(User Identifier)
rID	NFC 리더기 식별자(Reader Identifier)
uPW	사용자가 NFC 어플리케이션에서 사용할 NFC 패스워드(User Password)
g	곱셉 군 Z_p^*의 생성자
p	매우 큰 소수
A_{PK}	A의 공개키
A_{SK}	A의 개인키
UK_n	n번째 세션에서 NFC 디바이스와 서버 간에 Diffie-Hellman 키 교환을 통해 생성된 비밀키
RK_n	n번째 세션에서 NFC 리더와 서버 간에 Diffie-Hellman 키 교환을 통해 생성된 비밀키
$E_K(\bullet)$	K를 이용해 암호화
$h(\bullet)$	일 방향 해쉬함수
$A \rightarrow B: C$	A가 B로 C를 전송

(그림 1)은 등록 절차를 나타낸 것이다. 새로운 사용자가 최초 어플리케이션 실행 시 등록절차가 이루어지게 된다. 등록절차를 통해 인증 시 필요한 사용자 정보를 안전하게 서버에 등록하게 된다.



(그림 1) 등록 절차

1) 사용자는 어플리케이션을 최초 실행 시 웹페이지 회원가입을 통해 발급받은 사용자 식별자(uID), 인증번호(N) 그리고 어플리케이션에서 사용할 NFC 패스워드 (uPW)를 입력하게 된다.

2) NFC 디바이스는 입력받은 정보를 이용해 M_1, M_2, U_{PK_n}를 생성해 서버에 사용자 등록 요청을 하게 된다.

$$M_1 = h(uID \| N)$$

$$M_2 = E_N(uPW)$$

$$U_{PK_n} = g^{U_{SK_n}} \bmod p$$

3) 서버는 사용자 식별자(uID)가 기존에 등록되지 않은 uID인지 정당한 인증번호(N)가 맞는지 검증하게 된다. 검증 완료 후 M_2에서 uPW를 추출해 서버의 데이터베이스에 NFC 패스워드 (uPW)를 저장한다.

4) 저장이 완료되면 서버는 S_{SK_n}와 S_{PK_n}를 생성하게 된다. 전송받은 U_{PK_n}와 S_{SK_n}를 통해 UK_0를 연산하다. 그리고 M_3를 계산해 사용자 식별자(uID)와 함께 사용자 등록 응답 메시지를 NFC 디바이스로 전송하게 된다.

$$S_{PK_n} = g^{S_{SK_n}} \bmod p$$

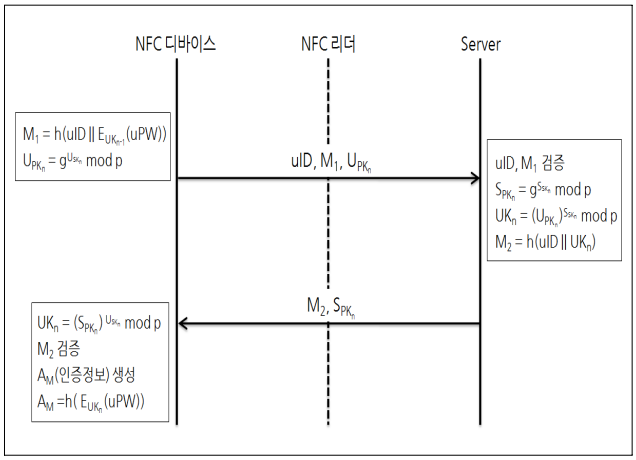
$$UK_0 = (U_{PK_n})^{S_{SK_n}} \bmod p$$

$$M_3 = h(uID \| UK_0)$$

5) NFC 디바이스는 서버로부터 발급받은 S_{PK_n}를 이용해 UK_0를 계산하게 된다. UK_0를 계산 후 M_3에 대한 무결성을 검증하게 된다.

3.2. 인증 절차

사용자는 NFC 서비스를 이용하기 위해 어플리케이션 실행 시 각 세션마다 NFC 디바이스와 서버 간 Diffie-Hellman 키 교환을 통해 UK_n을 생성한다. 생성한 UK_n로 암호화한 인증정보(A_M)를 생성해 NFC 리더로 전송한다. NFC 리더 또한 Diffie-Hellman 키 교환을 통해 RK_n을 생성하여 암호화한 정보를 서버로 전송한다. 서버는 전송받은 정보를 통해 검증된 사용자가 맞는지 인증하게 된다.



(그림 2) NFC 디바이스를 통한 인증 절차

인증 절차는 NFC 디바이스 인증과 NFC 리더를 통한 인증 순으로 진행된다.

(그림 2)는 NFC 디바이스 인증에 대한 절차는 사용자가 어플리케이션을 실행 시 서버로부터 NFC 디바이스 사용자 정보를 검증 받게 된다. 각 단계별 세부내용은 다음과 같다.

1) 사용자가 어플리케이션을 실행 시 NFC 디바이스 어플리케이션 데이터베이스에 저장된 정보를 통해 M_1, U_{PK_n}를 생성하게 된다.

$$M_1 = h(uID \| E_{UK_{n-1}}(uPW))$$

$$U_{PK_n} = g^{U_{SK_n}} \bmod p$$

2) NFC 디바이스는 인증 사용자 정보 검증 요청을 위해 서버에 uID와 함께 생성된 M_1, U_{PK_n}를 전송하게 된다.

3) 서버는 인증 사용자 정보인지 검증하기 위해 서버 데이터베이스에 저장되어 있는 정보와 수신된 uID를 비교한다. 만약 등록되어 있는 uID가 아닐 경우 서버는 현재 세션을 종료하게 된다.

4) 등록되어 있는 uID일 경우 uID와 서버의 UK_{n-1}을 통해 M_1을 검증하게 된다. 검증이 완료되면 서버의 S_{SK_n}와 S_{PK_n}를 생성하게 된다. 그리고 전송받은 U_{PK_n}와 서버의 S_{SK_n}를 이용해 UK_n을 연산한다. 그리고 M_2를 생성해 S_{PK_n}와 함께 NFC 디바이스로 전송하게 된다.

$$S_{PK_n} = g^{S_{SK_n}} \bmod p$$

$$UK_n = (U_{PK_n})^{S_{SK_n}} \bmod p$$

$$M_2 = h(uID \| UK_n)$$

5) NFC 디바이스는 전송받은 S_{PK_n}와 자신의 U_{SK_n}를 이용해 UK_n를 연산한다. 연산한 UK_n와 자신의 식별자인 uID를 해쉬하여 전송받은 M_2에 대한 무결성을 검증한다.

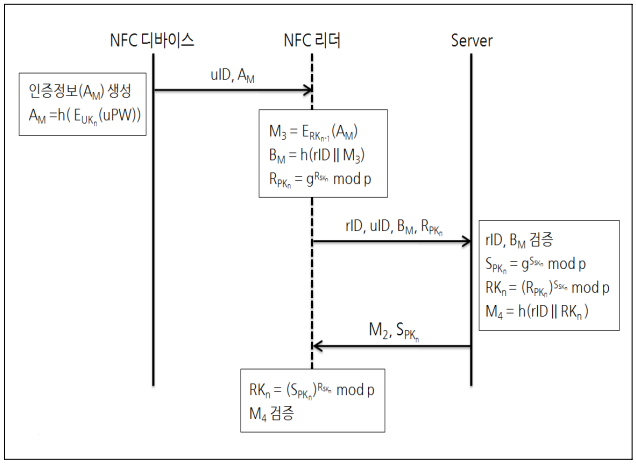
$$UK_n = (S_{PK_n})^{U_{SK_n}} \bmod p$$

6) 검증이 완료되면 NFC 리더를 통한 인증절차를 위해 인증정보(A_M)를 생성하게 된다.

$$A_M = h(E_{UK_n}(uPW))$$

다음은 NFC 리더를 통한 인증 절차이다.

(그림 3)은 NFC 리더를 통한 인증에 대한 절차로 NFC 리더는 인증 정보(A_M)를 전송 받아 서버로부터 인증 사용자 정보를 검증 받게 된다. 각 단계별 세부 내용은 다음과 같다.



(그림 3) NFC 리더를 통한 인증 절차

1) NFC 디바이스는 NFC 리더에 접촉 시 인증정보(A_M)와 자신의 식별자(uID)을 NFC 리더로 전송한다.
2) NFC 리더는 전송 받은 A_M을 이용해 M_1을 생성하고, NFC 리더 식별자(rID)와 M_1을 이용해 B_M을 생성한다. 인증 정보 검증 요청을 위해 rID, uID, B_M, R_{PK}를 서버에게 전송한다.

$$M_1 = E_{RK_{n-1}}(uID \| A_M)$$

$$B_M = h(rID \| M_1)$$

$$R_{PK} = g^{R_{SK}} \bmod p$$

3) 서버는 인증 정보 검증을 위해 등록된 rID와 uID가 맞는지 확인 후 M_1을 연산해 B_M에 대한 무결성을 검증하게 된다.
4) 검증이 완료되면 서버의 S_{SK_n}와 S_{PK_n}를 생성하고, 전송받은 R_{PK_n}와 S_{SK_n}를 이용해 RK_n를 연산하게 된다. 연산한 RK_n와 NFC 리더의 식별자인 rID를 해쉬하여 M_2를 연산하게 된다.

$$S_{PK_n} = g^{S_{SK_n}} \bmod p$$

$$RK_n = (R_{PK_n})^{S_{SK_n}} \bmod p$$

$$M_2 = h(rID \| RK_n)$$

5) 서버는 NFC 리더에게 인증 정보 검증 요청에 대해 응답값으로 rID, M_2, S_{PK_n}를 전송하게 된다.
7) NFC 리더는 전송받은 S_{PK_n}와 자신의 R_{SK_n}를 이용해 RK_n를 연산한다. 연산한 RK_n와 자신의 식별자인 rID를 해쉬하여 전송받은 M_2에 대한 무결성을 검증한다. 만약 검증이 완료 되지 않을 경우 현재 세션을 종료한다.

$$RK_n = (S_{PK_n})^{R_{SK_n}} \bmod p$$

4. 결론 및 향후 연구과제

NFC 서비스가 본격적으로 도입되면 NFC 서비스에 대한 보안 기술 역시 가시화 될 것이다. 현재 다양한 분야에서 NFC 서비스가 각광을 받고 있음에도 불구하고 아직 NFC 서비스 보안 위협에 대한 대책 연구는 미비한 실정이다.

본 논문에서는 NFC Tag 데이터에 대한 기밀성을 보장하고 Replay 공격과 데이터 도청, 삽입, 위조, 변조 될 수 있는 NFC 서비스 보안상의 문제점을 해결하고자 NFC 기반 시스템의 인증 메커니즘을 제시하였다. 제안 방식은 악의적인 목적을 가진 공격자가 Tag 데이터를 획득하더라도 Tag 데이터에 대한 확인이 불가능해 프라이버시 침해에 안전할 것이다. 그리고 세션마다 키 교환을 하므로 매번 다른 비밀키 사용이 가능함으로써 Replay 공격에도 안전할 것이다. 또한 NFC Tag 데이터에 대한 보안성을 높이는 효과를 가져 올 수 있고, 다양한 NFC 환경에 적용이 가능할 것이다.

향후 연구 계획으로는 제안하는 인증 메커니즘을 NFC 모바일 환경에 적합하도록 개선하고, 이를 구현함으로써 기존 인증 메커니즘과의 안전성과 성능을 비교분석 하고자 한다.

참고문헌

[1] 김연우, 문일영, “NFC의 기술 동향 분석 및 활용 사례”, 한국해양정보통신학회, pp.519-521, 2011.
[2] NFC Forum, “NFCIP-1 Security Service and Protocol (Cryptography Standard using ECDH and AES)”, ECMA International, 2008.
[3] 임선희, 전재우, 정임진, 이옥연, “NFC 보안 기술 분석 및 UICC 적용 효과 연구”, 한국통신학회논문지. pp.29-36, 01. 2011.
[4] R. Verdult, F. Kooman, “Practical attacks on NFC enabled cell phones”, in Proceedings of the Third International Workshop on Near Field Communication (NFC), Hagenberg, Austria, pp.77 - 82, Feb. 2011.
[5] H.C Cheng, W.W Liao, T.Y Chi, S.Y Wei, “A Secure and Practical Key Management Mechanism for NFC Read-Write Mode”, The 13th International Conference on Advanced Communication Technology (ICACT), Seoul, Korea, pp.1095 - 1100, Feb. 2011.
[6] NFC Forum, “NFC Data Exchange Format (NDEF)”, http://www.nfc-forum.org/, 2006.
[7] C. Mulliner, “Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones”, in Proceedings of the 1st International Workshop on Sensor Security (IWSS) at ARES, Fukuoka, Japan, pp. 695 - 700, Mar. 2009.