향상된 S/Key 방식을 이용한 RFID 인증 방안에 관한 연구

강수영, 이임영
순천향대학교 컴퓨터학과
e-mail : bbang814, imylee@sch.ac.kr

A Study on RFID Authentication Scheme using Improved S/Key Scheme

Soo-Young Kang, Im-Yeong Lee
Division of Computer, Soonchunhyang University

요 약

유비쿼터스 환경에 적합한 기술로써 RFID가 많은 관심을 받고 있다. RFID는 바코드를 대체하기 위한 무선 주파수 인식 기술로 유비쿼터스를 실현하기 위한 핵심 기술이다. 하지만 무선 기술을 사용하며 비접촉으로 인식할 수 있기 때문에 악의적인 사용자가 불법적인 목적으로 사용자가 소지한 태그의 내용을 몰래 획득하여 사용자 프라이버시 침해 문제가 발생하고 있다. 이를 해결하기 위하여 RFID 보안에 관한 연구가 활발히 진행되고 있지만 수동형 태그의 제한된 연산 능력 및 저장 능력을 고려해야 되기 때문에 경량화를 고려하지 않을 수 없다. 따라서 본 방식은 한번 사용하고 폐기하는 일회용 패스워드 OTP를 이용하여 모바일 환경의 RFID 보안을 제공하는 방식이다. OTP 방식이 향후 인증 수단으로 발전했을 경우 태그를 제외한 리더의 역할을 대체할 수 있을 것이며, S/Key 방식에 타임스탬프로 재전송공격을 막고 더 안전한 방식을 제안함으로써 모바일 환경에서 사용할 수 있다.

1. 서론

RFID는 u-Healthcare나, 금융 분야와 같이 사용자의 정보가 반드시 보호 되어야 하는 분야에서 사용되고 있기 때문에 보안의 필요성이 대두되고 있다. 하지만 일반적으로 사용되고 있는 수동형 태그에 보안을 적용해야 하기 때문에 제한된 연산 능력 및 저장 공간을 고려해야만 한다. 따라서 본 논문은 2장에서 RFID 시스템에서의 보안 요구 사항에 대해서 언급하고 3장에서는 관련 연구에 대하여 기술한다. 또한 4장에서는 보안 요구 사항을 제공하는 제안 방식을 제안하고 5장에서는 제안 방식을 분석한 뒤 6장에서 결론을 맺도록 한다.

2. 보안 요구 사항

RFID 시스템에서 태그와 리더 간의 통신 채널은 무선 기술을 사용하기 때문에 불안전한 통신을 하고 있다. 따라서 다음과 같이 RFID 시스템에서 제공되어야 할 요구 사항을 도출한다.

◈ Man-in-the-middle Attack : 통신 객체가 통신할 경우 악의적인 제 3자가 통신 내용을 획득하여 위조 및 변조하는 공격 유형이다.
◈ 재전송공격과 전방위 보안 : 도청으로 획득한 데이터를 재전송하여 중요 값을 획득할 수 있으므로 값을 갱신하거나 가변적이게 생성해야 한다..
◈ 데이터 기밀성과 익명성 : 태그의 중요 값은 정당한 객체만이 공유해야 하며 노출되더라도 어떤 태그의 값인지 알 수 없어야 한다.
◈ 데이터 무결성과 상호 인증 : 전송되는 데이터는 통신 중 위조 및 변조되지 않아야 하며, 통신하는 객체들 간의 정당성을 검증해야 한다.

3. 관련 연구

본 장에서는 관련된 연구에 대하여 기술하고 분석한다.

3.1 OTP(One Time Password)

OTP란 한번 사용하고 폐기하는 일회용 패스워드를 의미하며 다음 세션에 사용할 경우 사용된 패스워드를 해쉬하고 이전 패스워드는 폐기한다. OTP 방식은 입력 값에 따라 S/Key 방식, Challenge-Response 방식, 시간 동기화 방식으로 분류할 수 있다.

3.2 RFID 보안 기술

RFID는 연산량이 많지 않아 해쉬 연산 및 XOR 연산을 사용하여 보안을 제공하는 것이 일반적이다. 기존 기술로 Radomized Hash-Lock 방식은 난수를 사용하여 보안을 제공하지만 효율성 측면이 취약하며 Low-Cost 방식은 해쉬 연산 2회로 보안을 제공하지만 비동기화 발생 시 위치 추적이 가능한 문제점이 발생하였다.

4. 제안 방식

본 장에서는 제안 방식을 제안하는데 정해진 가정 사항과 제안 방식에서 사용되는 시스템 계수에 대하여 기술하고 제안 프로토콜의 과정을 자세히 기술한다.

◈ 등록 과정

데이터베이스는 PIN과 초기 값 $seed$를 해쉬하여 OTP를 n개 생성하고 역순으로 리더에게 전송한다. 또한 정당한 객체들 간에 PIN을 공유하기 위해 데이터베이스에서 리더를 통해 태그로 전송한다. 태그는 리더의 신호에 ID를 리더에게 전송하고 리더는 ID를 해쉬하여 $metaID$를 생성한다. 리더는 $metaID$를 태그에게 입력하고 데이터베이스에 $metaID$와 ID를 전송하여 정당한 태그를 등록한다.

◈ 인증 과정

단계 1. 리더는 재전송공격을 막기 위하여 타임스탬프를 생성하고 PIN과의 연산 및 해쉬 값을 태그에게 전송한다.

$$V_1 = PIN \oplus TS_R$$
$$H_1 = H(PIN \| TS_R)$$

단계 2. 태그는 V_1으로 $TS_R{}'$를 획득하고 해쉬 값을 검증하여 무결성을 확인한 후 TS_T를 갱신한다.

$$V_1 \oplus PIN' = TS_R{}'$$
$$H_1 = ?H(PIN' \| TS_R)$$
$$TS_T = TS_R + LT$$

단계 3. 태그는 $metaID$와 TS_T의 연산 값 및 해쉬 값을 생성하여 리더에게 전송한다.

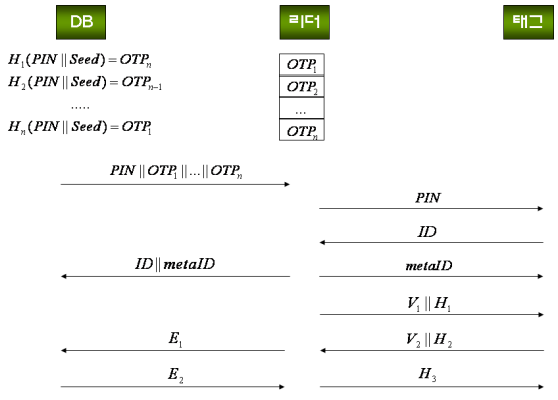
$$V_2 = metaID \oplus TS_T$$
$$H_1 = H(metaID \| TS_T)$$

단계 4. 리더는 저장하고 있는 OTP 중 $n-1$번째 패스워드인 OTP_{n-1}과 V_2, H_2, TS_T를 PIN으로 암호화하여 E_1을 생성여 데이터베이스로 전송한다.

$$E_1 = E_{PIN}[OTP_{n-1}, V_2, H_2, TS_T]$$

단계 5, 데이터베이스는 E_1을 복호화하여 OTP_{n-1}과 V_2, H_2, TS_T를 획득하고 $metaID$와 OTP_n을 검증하여 인증하고 OTP_n과 TS_{DB}를 생성한다.

$$D_{PIN}[E_1] = OTP_{n-1} \| V_2 \| H_2 \| TS_T$$
$$V_2 \oplus TS_T = metaID'$$
$$metaID = ?metaID'$$
$$OTP_n = ?H(OTP_{n-1})$$
$$OTP_n \leftarrow OTP_{n-1}$$
$$TS_{DB} = TS_T + LT$$



(그림 1) 등록 과정 및 인증 과정

<표 1> 제안 방식 분석

	Man-in-the-middle Attack		재전송 공격	데이터 기밀성
RHLP	가능		부분가능	제공못함
LCAP	불가능		부분가능	제공
제안방식	불가능		불가능	제공
	데이터 무결성	태그 익명성	상호 인증	전방위 보안
RHLP	제공 못함	제공못함	제공못함	제공
LCAP	제공	제공	제공	제공
제안방식	제공	제공	제공	제공

단계 6. 데이터베이스는 ID와 TS_{DB}를 PIN으로 암호화하여 E_2를 생성하여 리더로 전송한다.

$$E_2 = E_{PIN}[ID \| TS_{DB}]$$

단계 7. 리더는 E_2를 복호화하고 TS_{DB}를 검증하고 ID와 TS_T를 해쉬하여 태그에게 전송한다.

$$D_{PIN}[E_2] = ID \| TS_{DB}$$
$$TS_{DB} = ?TS_T + LT$$
$$H_3 = H(ID \| TS_T)$$

단계 8. 태그는 H_3을 검증하여 인증한다.

$$H_3 = ?H(ID \| TS_T)$$

5. 제안 방식 분석

제안 방식은 타임스탬프를 이용하여 값을 가변적이게 하고 갱신함으로써 재전송공격을 막고 전방위 보안을 제공함으로써 태그의 익명성을 제공할 수 있다. 또한 해쉬 함수를 사용하여 전송되는 값이 위조 및 변조되지 않았음을 검증할 수 있기 때문에 데이터의 무결성을 제공하므로 상호 인증이 제공된다.

6. 결론

유비쿼터스 환경이 조성됨에 따라 RFID의 사용량이 증가하고 있다. 하지만 보안 취약점으로 인해 보안 기술에 대한 연구가 증가하고 있다. 본 방식은 모바일 환경에서 각 객체들 간의 상호 인증을 제공하는 방식이며 RFID 시스템뿐만 아니라 향후 OTP가 인증 수단으로 발전할 경우 태그를 사용하지 않고 OTP 기기와 데이터베이스 간의 인증 절차를 포함하여 제안 방식을 응용하고 있다. 또한 리더와 데이터베이스 간의 인증 방식은 S/Key 방식에서 타임스탬프를 포함시킴으로써 더욱 향상된 기법이다. 하지만 태그에서 3회의 해쉬 연산을 수행해야하기 때문에 현재 태그의 연산 능력으로는 구현이 불가능하며 경량화에 대한 연구가 진행되어야 할 것이다.

참고문헌

[1] Haller, N.M. “The S/KEY One-time Password System” RFC 1760. Feb. 1995

[2] Mitchell, C.J., Chen, L. “Comments on the S/KEY User Authentication Scheme” ACM Opera-ting Systems Review. Vol. 30. No. 4. 12-16 1996

[3] Stephen Weis, "Security and Privacy in Radio Frequency Identification Devices", Master Thesis, May 2003

[4] 황영주, 이수미, 이동훈, 임종인, “유비쿼터스 환경의 Low-Cost RFID 인증 프로토콜”, 2005년 정보보호학회 하계정보보호학술대회 논문집, pp109~114