논문 2010-47TC-2-16

상호인증을 제공하는 개선된 RFID 인증 프로토콜

(Improved RFID Authentication Protocol Providing Mutual Authentication)

전 서 관*, 은 선 기*, 오 수 현**

(Seo-Kwan Jeon, Sun-Ki Eun, and Soo-Hyun Oh)

요 약

RFID 시스템은 비접촉식 무선 인식 기술로 유통 및 물류, 환경, 교통, 보안 분야 등 산업 전반에 걸쳐 다양하게 활용되고 있다. 그러나 RFID 통신 환경의 제약적인 특징에 의하여 프라이버시 문제를 비롯한 여러 가지 보안 문제가 제기되면서 이를 해결하기 위한 많은 기술들이 연구되고 있다. 최근 들어 Shin과 Park은 프라이버시를 보호하고 해쉬 함수와 배타적논리합(XOR) 연산을 이용하는 효율적인 RFID 인증 프로토콜을 제안하였다. 그러나 Ahn과 Bu 등은 Shin과 Park이 제안한 인증 프로토콜의 문제점이 있음을 지적하고 이를 개선하여 좀 더 안전하고 효율적인 인증 프로토콜을 제안하였다. 그러나 Ahn과 Bu 등이 제안한 인증 프로토콜들은 리더와 태그 사이의 상호인증이 완벽하게 이루어지지 않아 악의적인 리더로의 위장이 가능하다는 문제점이 있다. 본 논문에서는 이러한 문제점을 해결하기 위해 상호인증을 제공하는 개선된 RFID 인증 프로토콜을 제안한다. 제안하는 RFID 인증 프로토콜은 리더와 태그 간 상호인증을 제공하며 재전송 공격과 스푸핑 공격에 대해 안전하고, 태그의 익명성 보장 및 악의적인 리더들의 공모에 의한 위치 트래킹에 대해 안전하다는 장점이 있다.

Abstract

RFID system is the contact-less recognition technology and used for distribution system, environment, transport, security and so on. However, it may create many security relevant problems such as privacy because constraints of RFID communication environment. So several methods of resolving these problems have been proposed. Recently, Shin and Park proposed an efficient RFID authentication protocol with protecting user's privacy using hash function and exclusive-OR.. But Ahn and Bu et al. poia problem that a attacker can to masquerade as malicious reader because their protocol can't providing mutual authentication.nted out weakness of Shin and Park's protocol and proposed more secure and efficient protocol. Unfortunately, Ahn and But's protocol has In this paper, We propose an improved RFID authentication protocol providing mutual authentication. The proposed protocol has advantages that providing mutual authentication between a tag and a reader, secure against replay attack and spoofing attack. Also, it guarantees anonymity of RFID tag and secure against location tracking attack by collusion of malicious readers.

Keywords: 인증 프로토콜, 상호인증, 프라이버시, 해쉬 함수, RFID 시스템

I. 서 론

네트워크 및 무선통신의 발달로 새로운 컴퓨팅 환경이 조성되면서 현재 유비쿼터스 시대를 맞이하고 있다. 유비쿼터스 환경에서는 장소에 제약이 없는 네트워크 환경을 위해서 각 도처에 널리 퍼져있는 디바이스들을 이용하여 통신이 가능하다. 이러한 유비쿼터스 환경을 실현하기 위하여 핵심 기술 중 하나로써 RFID(Radio Frequency IDentification) 기술이 주목받고 있다.

RFID 시스템은 소형 저자 칩과 안테나로 구성된 전자 태그를 사물에 부착하여 전자 태그 고유의 주파수를 통해 사물을 자동으로 인식/처리(Automatic Identification Data Collection: AIDC)하는 시스템이다. RFID 시스템의 장점은 기존의 바코드 시스템과는 달리 여러 개의 정보를 동시에 판독하거나 수정이 가능하기 때문에 바코드 대체 기술로써 현재 유통분야 뿐

* 학생회원, ** 정회원, 호서대학교 정보보호학과
(Department of Information Security, Hoseo University)
접수일자: 2009년8월24일, 수정완료일: 2010년2월17일

만 아니라 물류, 교통, 보안 분야까지 다양한 분야에 활용되고 있다.[1]

RFID 시스템은 기본적으로 리더, 태그, 백-엔드 데이터베이스로 구성된다. RFID 태그는 리더나 백-엔드 데이터베이스에 비해 연산 능력이 제한되고 태그를 식별하기 위한 정보만을 가지기 때문에 정보의 노출, 위치 추적 등으로 인하여 태그 소유자의 프라이버시 침해가 발생할 수 있다.[2]

따라서 프라이버시 침해 문제를 해결하기 위하여 많은 연구들이 진행되고 있다. 대표적으로 해쉬-락 기법, 확장된 해쉬-락 기법, 해쉬-체인 기법, 블로커 태그를 이용한 기법 등 다양한 RFID 인증 프로토콜들이 개발되었다.[4~7]

그러나 위와 같은 RFID 인증 기법들은 재전송 공격이나 스푸핑 공격 등에 취약하며, 트래픽 분석을 통한 태그의 위치추적이 가능함이 발견되었다. 이에 대해서 Shin과 Park은 해쉬 함수와 배타적 논리합(XOR)을 이용한 SPRFID 인증 프로토콜을 제안하고 패스워드 추측공격, 메시지 재전송 공격, 위장 공격에 대하여 안전하다고 주장하였다. 이에 대해 Ahn과 Bu 등은 위와 같은 문제가 여전히 존재하며, 태그의 익명성 또한 제공하지 않음을 증명하면서 개선된 인증 프로토콜을 제안하였다. 그러나 Ahn과 Bu 등이 증명한 보안 문제점에 모순이 있고 리더와 태그간 상호인증이 이루어지지 않아 악의적인 리더로의 위장이 가능하다는 문제점이 있다.

본 논문에서는 Ahn과 Bu가 증명한 보안 문제점의 모순을 수정하고 리더와 태그간의 상호인증을 제공하는 개선된 RFID 인증 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. II장에서는 관련연구로써 RFID 시스템의 일반적인 구성과 RFID 시스템의 보안 요구사항에 대해서 설명하고, III장에서는 Shin과 Park이 제안한 인증 기법과 Ahn과 Bu 등이 제안한 인증 기법을 분석한다. IV장에서는 상호인증을 제공하는 개선된 인증 프로토콜을 제안하고, V장에서는 제안하는 인증 프로토콜의 안전성을 분석하고 마지막으로 V장에서 결론을 맺는다.

II. 관련 연구

1. RFID 시스템 구성

RFID 시스템 구성은 일반적으로 다음과 같다.

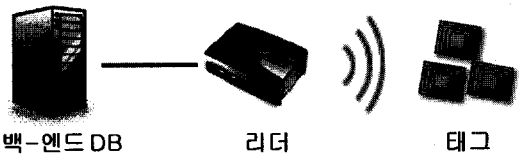


그림 1. RFID 시스템
Fig. 1. RFID System.

가. RFID 태그

RFID 태그는 통합된 안테나를 갖춘 IC칩을 말하며 장비나 사물 등에 삽입되어 무선 주파수를 사용한 리더기를 통해 인식되는 과정을 거친다. 태그는 전원의 유무에 따라 전원을 가지고 있는 능동형 태그(Active tag)와 리더에 의해 전원을 공급받는 수동형 태그(Passive tag)로 나눌 수 있으며, 제한적인 연산 능력을 가지고 있다.

나. RFID 리더

RFID 태그에게 응답을 요청하고 식별정보를 수신하거나 RF 신호를 이용해 정보를 전송하는 역할을 수행한다. 또한 수동형 태그의 경우 RF 신호를 통해 전력을 공급하여 RFID 태그를 활성화시키고 수신한 정보를 자신과 연결된 백-에드 데이터베이스에 전송하며, RFID 태그 내의 식별정보에 대한 읽기/쓰기를 수행할 수 있다.

다. 백-엔드 데이터베이스

RFID 태그에 관련된 식별정보를 및 제품 정보를 저장하고 처리하며 RFID 태그나 RFID 리더에 비해 연산 능력이 상대적으로 뛰어나므로 연산을 대신 수행하는 역할을 한다. 또한 인증 프로토콜에서는 RFID 태그에 대한 인증 정보를 가지고 인식하는 역할도 한다.

2. RFID 보안 요구사항[3]

RFID 시스템은 무선통신의 특성과 제한적인 RFID 태그의 연산능력으로 인해 리더와 태그간의 통신 과정 중에 정보가 노출 등 다양한 보안 취약점이 존재한다. 본 절에서는 RFID 인증 프로토콜을 설계할 때 고려해야 할 보안 요구사항에 대하여 알아본다.

가. 재전송 공격

RFID 시스템 환경에서 리더와 태그간의 통신은 불안전한 통신 구간으로써 전송되는 메시지들을 도청할

수 있다. 공격자는 이러한 도청을 통해 RFID 리더와 태그 사이에 전송되는 메시지들을 획득하여 재전송 공격을 통해 RFID 리더나 태그로 위장할 수 있다. 이를 방지하기 위해서는 매 세션마다 다른 인증정보를 이용해야 한다.

나. 스푸핑 공격

스푸핑 공격은 공격자가 정당한 RFID 리더로 가장하여 RFID 태그로부터 인증 프로토콜에 필요한 정보를 획득하고 이 정보를 이용하여 정당한 RFID 태그로 가장하는 공격방법을 말한다. 이러한 공격으로 인하여 공격자는 태그의 중요한 정보를 얻거나 위치를 추적하여 태그 소유자의 프라이버시를 침해할 수 있다. 이를 해결하기 위해서는 리더와 태그간의 상호 인증을 제공해야 한다.

다. 트래픽 분석 공격

트래픽 분석 공격은 리더와 RFID 태그간의 정보를 도청할 수 있는 공격자가 도청된 정보를 이용하여 인증 프로토콜에 필요한 비밀정보를 분석하는 공격방법을 의미한다. 트래픽 분석을 통해 공격자는 태그의 비밀정보 등을 유추할 수 있기 때문에 인증 프로토콜을 설계할 때는 이를 고려해야 한다.

마. 위치 프라이버시

불법적인 리더의 응답 요청에 의해 의도하지 않게 태그 소유자의 프라이버시 침해가 일어날 수 있다. 이를 방지하기 위해서는 매 세션마다 갱신되는 RFID 태그의 ID를 사용함으로써 공격자로부터 프라이버시를 보호해야 한다. 또한 두 개의 서로 다른 응답 메시지에 대해서 공격자는 동일한 RFID 태그로부터의 응답인지 구분할 수 없어야 한다.

바. 서비스 거부 공격

서비스 거부 공격(Denial of Service Attack)은 RFID 리더나 태그 사이에 올바른 통신을 방해하여 정당한 서비스를 받지 못하게 하는 공격이다. 이러한 공격은 현실적으로 방어가 불가능하기 때문에 통신을 방해하는 요소를 사전에 제거해야 한다.

사. 물리적 공격

물리적 공격은 RFID 태그를 의도적으로 도난이나 훼손하는 공격방법을 의미한다. 이를 예방하기 위해서는 물리적 공격으로부터 별도의 안전한 장치를 구축하여야 한다.

III. 기존에 제안된 인증 프로토콜의 문제점

본 장에서는 Shin과 Park이 제안한 SPRFID 인증 프로토콜과 최근 Ahn과 Bu등이 제안한 개선된 SPRFID 인증 프로토콜의 인증 과정을 분석하고, 각 프로토콜이 가지고 있는 보안상의 문제점에 대해 기술한다. 앞으로 사용될 프로토콜의 표기법은 다음 표 1과 같다.

표 1. 표기법
Table 1. Notation.

기호	의미
Tag	RFID 태그
Reader	RFID 리더
DB	백-엔드 데이터베이스
query	태그의 응답을 요구하는 리더의 요청
ID	태그의 고유 식별자
k	Tag와 DB간에 공유된 비밀 키
sk	Reader와 DB간에 공유된 비밀 세션키
info	Tag와 관련된 정보
Res	태그의 인증 성공 응답 메시지
E()	대칭키 암호 시스템
h()	안전한 일방향 해쉬 함수
prng()	의사난수생성기
r	리더가 생성한 난수
t	태그가 생성한 난수
$\oplus$	배타적 논리합(XOR)
$\|\|$	연접 연산

1. SPRFID 인증 프로토콜[8]

본 절에서는 Shin과 Park이 제안한 인증 기법에 대해서 분석한다. RFID 시스템에서 백-엔드 데이터베이스와 리더간의 통신은 사전에 세션 키를 공유한 후에 이루어지는 안전한 통신이고, 리더와 태그간의 통신은 무선통신 구간으로 도청이나 트래픽 분석이 가능한 불안전한 채널이라고 가정한다. 또한 각 태그의 비밀 키 k는 백-엔드 데이터베이스 등록되어 있다고 가정한다.

가. SPRFID 인증 프로토콜

Shin과 Park이 제안한 RFID 인증 프로토콜은 그림 2와 같다.

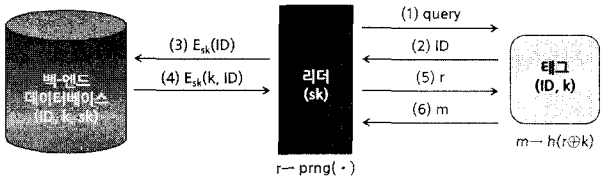


그림 2. SPRFID 인증 프로토콜
Fig. 2. SPRFID authentication protocol.

① 리더는 태그에게 query를 전송한다.
② 태그는 리더에 대한 query의 응답으로 자신의 ID를 전송한다.
③ 리더는 세션 키 sk를 사용하여 태그의 ID를 암호화하여 데이터베이스에게 전송한다.
④ 데이터베이스는 리더로부터 수신한 메시지를 리더와 공유한 세션 키 sk로 복호화 한 후, 태그의 ID를 확인하여 ID와 매치되는 태그의 비밀 키 k를 찾아 ID와 k를 sk로 암호화하여 리더에게 전송한다.
⑤ 리더는 데이터베이스로부터 수신한 메시지를 복호화하여 태그의 비밀 키 k를 저장한 후 난수 r을 생성하여 태그에게 전송한다.
⑥ 태그는 수신한 r값과 자신의 비밀 키 k를 이용하여 메시지 m=h(r⊕k)를 계산하여 리더에게 전송한다.
⑦ 리더는 m′=h(r⊕k)를 계산하여 태그로부터 수신한 m과 비교하여 태그를 인증한다.

나. SPRFID 인증 프로토콜 분석

(1) 태그의 익명성

본 인증 기법에서는 태그의 ID가 리더에게 그대로 전달되기 때문에 태그의 익명성을 보장할 수 없다.

(2) 스푸핑 공격

태그는 리더를 인증하기 않기 때문에 본 프로토콜에서는 악의적인 리더로 위장이 가능하다.

(3) 악의적인 리더 공모에 의한 위치 트래킹 공격

정당한 리더들이 악의적으로 공모하여 본 프로토콜 과정의 ④번 메시지를 분석하여 태그의 이동 경로를 파악할 수 있다.

(4) 리더의 세션 키 노출에 의한 피해

SPRFID 인증 프로토콜에서는 리더가 태그의 인증과정 중에 태그의 비밀 키를 저장하기 때문에 만일 악의적인 공격자가 리더의 세션 키를 획득했을 경우, 태그의 비밀 키가 노출될 수 있다.

2. 개선된 SPRFID 인증 프로토콜[9]

Ahn과 Bu 등은 Shin과 Park이 제안한 인증 기법이 태그 키 유출 공격과 스푸핑 공격, 위치 트래킹 공격에 취약하다는 사실을 증명하고 개선된 인증 프로토콜을 제안하였다. 그러나 취약점 증명과정에서 태그 키 유출 공격에 대해 모순점이 발견되었고, 개선된 프로토콜도 여전히 스푸핑 공격에 취약하다는 문제점이 있다.

가. 개선된 SPRFID 인증 프로토콜

Ahn과 Bu등이 제안한 인증 프로토콜은 그림 3과 같다.

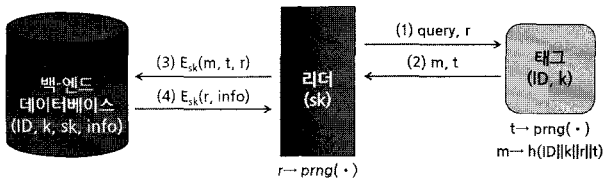


그림 3. Ahn과 Bu 등의 RFID 인증 프로토콜
Fig. 3. RFID authentication protocol proposed by Ahn and Bu.

① 리더는 난수 r을 생성하여 query와 함께 태그에게 전송한다.
② 태그는 난수 t를 생성한 후, 리더로부터 수신한 r과 자신의 ID 및 비밀 키 k를 이용하여 메시지 m=h(ID||k||r||t)를 계산하여 t와 함께 리더에게 전송한다.
③ 리더는 세션 키 sk를 이용하여 태그로부터 수신한 메시지 m, t와 리더가 생성한 난수 r을 암호화하여 E_{sk}(m, t, r)를 데이터베이스에게 전송한다.
④ 데이터베이스는 리더로부터 수신한 메시지를 복호화 한 후, 난수 r, t와 자신의 데이터베이스 내에 저장하고 있는 ID와 k쌍을 이용하여 m′=h(ID||k||r||t)를 계산하여 수신한 m과 비교하여 일치되는 값이 없을 경우 오류(error) 메시지를 리더에게 전송하고, 일치하는 값이 존재할 경우 태그를 인증하고 이에 관련된 상품정보인 info와 리더가 생성했던 난수 r값을 세션 키 sk로 암호화하여 E_{sk}(r, info)를 리더에게 전송한다.
⑤ 리더는 백-엔드 데이터베이스로부터 수신한 값이

오류일 경우, 태그와의 통신을 중단하고, 정상적인 인증이 되었을 경우에는 백-엔드 데이터베이스로부터 수신한 $E_{sk}(r, info)$를 복호하여 자신이 생성한 r값과 동일한지 검증한다. 만약 r값이 일치하면, 리더는 태그에 관련된 정보인 info를 이용하여 상품에 대한 요금부담 같은 작업을 수행한다.

나. 개선된 SPRFID 인증 프로토콜 분석

본 절에서는 개선된 SPRFID 인증 프로토콜의 취약점 증명과정에서 발견한 모순점과 추가적인 보안 문제점에 대해서 기술한다.

(1) SPRFID 인증 프로토콜의 태그 키 유출

Ahn과 Bu 등은 SPRFID 인증 프로토콜에서 악의적인 리더를 통해 태그의 비밀 키 k를 유출할 수 있다고 주장하였다. 그러나 일반적으로 RFID 시스템에서 백-엔드 데이터베이스와 리더 사이의 통신은 사전에 공유한 비밀 키를 이용한 안전한 채널로 가정한다. RFID 시스템에서 악의적인 리더라는 것은 백-엔드 데이터베이스와 공유 비밀 키를 자지지 않은 불법적인 리더를 의미하며, 이러한 리더는 태그로부터 정보를 수신하더라도 백-엔드 데이터베이스에게 정상적인 정보를 전송할 수 없고 수신한 정보를 복호할 수 없기 때문에 아무런 정보를 얻을 수 없게 된다.

그러나 Ahn 과 Bu 등이 제기한 태그 키 유출 공격은 악의적인 리더임에도 불구하고 백-엔드 데이터베이스와 정상적인 통신을 할 수 있는 상황을 가정하였으므로, 공격 환경 자체에 모순이 발견된다.

(2) 스푸핑 공격

개선된 SPRFID 인증프로토콜 역시 태그는 리더에 대한 인증을 하지 않기 때문에 악의적인 리더로의 위장이 가능하다. 만약 읽고 쓰기가 가능한 태그의 경우, 공격자는 악의적인 리더를 이용하여 인증과정을 무시하고 태그에게 직접적으로 요금을 부과하거나 부당한 명령을 전달할 수 있다.

Ⅳ. 상호인증을 제공하는 개선된 인증 프로토콜 제안

본 장에서는 기존에 제안된 인증 프로토콜의 문제점을 해결하면서 RFID 리더와 태그사이에 상호인증을 제공하는 개선된 인증 프로토콜을 제안한다. 제안하는 프로토콜은 상호인증(mutual authentication)의 접두사를 사용하여 MA-RFID 인증 프로토콜로 표기한다.

1. MA-RFID 인증 프로토콜

본 프로토콜을 수행하기 전에 태그의 ID와 비밀 키 k는 안전하게 백-엔드 데이터베이스에 등록되어 있으며, 오직 태그와 데이터베이스만이 알고 있다고 가정한다. 또한 리더와 데이터베이스는 사전에 세션 키 sk를 공유하고 있으며 안전한 통신채널을 이용한다고 가정한다. 제안하는 MA-RFID 인증 프로토콜의 동작과정은 다음과 같다.

① 리더는 태그에게 query와 리더가 생성한 난수 r을 전송한다.

② 태그는 난수 t를 생성하여 리더로부터 수신한 난수 r을 사용하여 인증메시지 $m_1=h(ID||t||r)$을 계산하여 m_1과 t를 리더에게 전송한다.

③ 리더는 태그로부터 수신한 m_1과 t, 그리고 자신이 생성한 난수 r을 세션 키 sk를 사용하여 암호화하여 백-엔드 데이터베이스에게 전송한다.

④ 데이터베이스는 $E_{sk}(m_1, t, r)$를 복호하여 저장된 태그들의 ID_i들을 이용하여 다음을 만족하는 ID를 검색한다.

$$m_1 \doteq h(t \,||\, r \,||\, ID_i)$$

만일 일치되는 값이 없으면 리더에게 인증 실패 메시지를 전송하고, 일치되는 값이 있으면 태그를 인증하고 $m_2 = E_{sk}(h(ID||k||t), info)$를 생성하여 리더에게 전송한다. 여기서 info는 과금 등에 사용하는 태그와 관련된 정보를 의미한다.

⑤ 리더는 데이터베이스로부터 수신한 m_2를 복호하고 태그가 정당함을 인증한 후, $m_3 = h(h(ID||k||t), r)$를 계산하여 태그에게 전송한다.

⑥ 태그는 자신의 비밀 키 k를 이용하여 $h(h(ID||k||t), r)$을 계산하여 m_3와 일치하는지 확인한다. 일치하는 경우 정당한 리더로 인증하고 이에 대한 응답 메시지로써 Res를 전송하고, 일치하지 않을 경우 통신을 중단한다.

⑦ 리더는 태그의 응답을 확인하고 태그에 관련된 정보 info를 이용하여 원하는 작업을 수행한다.

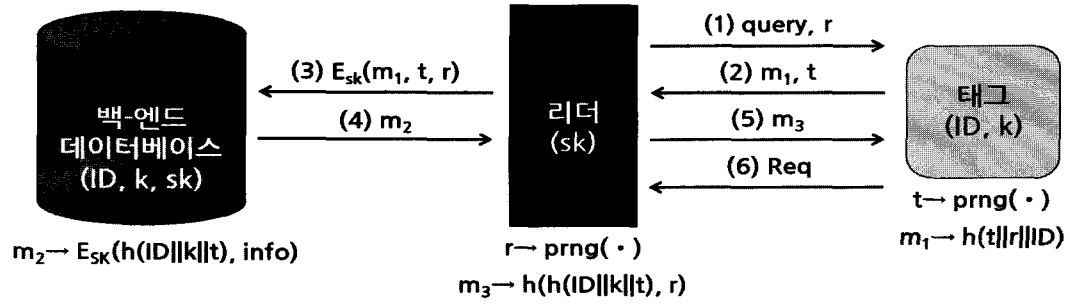


그림 4. 제안하는 MA-RFID 인증 프로토콜
Fig. 4. Proposed MA-RFID authentication protocol.

V. 안전성 분석

본 장에서는 제안한 MA-RFID 인증 프로토콜의 안전성에 대하여 분석한다. 안전성 분석 과정에서 물리적 공격에 대해서는 고려하지 않는다.

1. 제안하는 RFID 인증 프로토콜의 안전성 분석

(1) 재전송 공격

제안하는 프로토콜에서 사용하는 인증 메시지에는 매 세션마다 리더와 태그가 생성하는 난수를 포함한다. 따라서 공격자가 이러한 인증 메시지를 도청하여 재전송 하는 경우에 백-엔드 데이터베이스에 의해 검출될 수 있다. 따라서 제안한 프로토콜은 재전송 공격에 대해 안전하다.

(2) 스푸핑 공격

스푸핑 공격은 태그의 비밀 키를 얻어 태그로 위장하거나 리더와 태그간의 상호인증이 이루어지지 않을 경우 악의적인 리더로 위장하는 것이다. 제안하는 프로토콜에서 전자의 경우, 태그의 비밀 키 k는 안전한 해쉬 함수에 의해 변형된 값으로 전송되므로 태그의 비밀 키는 보호된다. 후자의 경우, m_1,과 m_3의 검증을 통해 리더와 태그간 상호인증을 제공하기 때문에 악의적인 리더로의 위장은 불가능하다. 따라서 제안하는 프로토콜은 스푸핑 공격에 대해 안전하다.

(3) 태그의 익명성

제안하는 프로토콜에서 태그의 ID는 백-엔드 데이터베이스와 태그만이 알고 있으며, 태그의 ID가 전송될 때에도 리더와 태그가 각각 생성한 난수 t, r과 함께 태그의 ID를 해쉬한 결과 값을 전송함으로써 태그의 익명성을 보장할 수 있다.

(4) 위치 프라이버시

제안하는 프로토콜에서 사용하는 모든 메시지는 리더와 태그가 생성한 난수를 포함하기 때문에 공격자는 두 개의 서로 다른 응답 메시지에 대해서 동일한 RFID 태그로부터의 응답인지 구분할 수 없다. 따라서 제안하는 인증 프로토콜을 사용하는 경우, RFID 태그의 위치 프라이버시를 보호할 수 있다.

(5) 악의적인 리더 공모에 의한 위치 트래킹 공격

악의적인 리더들의 공모에 의해 태그에 대한 인증 메시지 m_2를 획득하더라도 인증 메시지 m_2는 태그가 생성한 난수 t로 인해 매 세션마다 변하는 정보이므로, 악의적인 리더들은 두 개의 다른 인증 메시가 동일한 태그에 대한 인증 메시지인지 확인할 수 없다. 따라서 제안하는 인증 프로토콜은 악의적인 리더들의 공모에 의한 위치 트래킹 공격에 대해 안전하다.

(6) 리더의 세션 키 유출에 의한 피해

만일 악의적인 공격자가 임의의 리더와 벡-엔드 데이터베이스 사이의 세션 키를 획득하더라도, 리더가 태그를 인증하는 과정에서 태그의 비밀 키를 알지 못하므로 SPRFID 프로토콜과 달리 태그의 비밀 키를 유출하지 않는다.

2. 기존 연구들과의 비교 분석

본 절에서는 재전송 공격, 스푸핑 공격, 상호인증, 태그의 익명성, 악의적인 리더 공모에 의한 위치 트래킹, 태그 키 노출에 대해 기존 연구들과의 안전성을 비교한다.

SPRFID 인증 프로토콜에서는 인증 메시지를 생성할

표 2. 안전성 비교
Table 2. Comparison of security.

	SPRFID 인증 프로토콜	개선된 SPRFID 인증 프로토콜	MA-RFID 인증 프로토콜
MA	X	X	O
RA	O	O	O
SA	X	X	O
TA	X	O	O
LP	X	O	O
LT	X	O	O
TKE	O	O	O

O : 안전함, X : 안전하지 않음
- MA(Mutual Authentication): 상호인증
- RA(Replay Attack): 재전송 공격
- SA(Spoofing Attack): 스푸핑 공격
- TA(Tag Anonymity): 태그의 익명성
- LT(Location Tracking by collusion malicious reader): 악의적인 리더 공모에 의한 위치 트래킹
- TKE(Tag Key Exposure): 태그 키 노출

때 리더가 생성한 난수와 태그의 비밀 키 이용하여 매번 다른 인증 메시지를 생성하기 때문에 재전송 공격 및 태그 키 노출에 대해서는 안전하지만, 태그는 리더를 인증하지 않기 때문에 공격자는 악의적인 리더로 위장이 가능하고 태그의 익명성 보장과 리더들의 공모에 의한 위치 트래킹 공격에 대해서는 취약하다.

이에 대해 개선된 SPRFID 인증 프로토콜에서는 태그의 익명성이나 위치 트래킹 공격에 대해 안전하도록 개선하였지만, 여전히 리더와 태그 사이에 상호인증이 이루어지지 않아 공격자는 악의적인 리더로의 위장이 가능하기 때문에 스푸핑 공격에 취약하다. 본 논문에서 제안한 상호인증을 제공하는 RFID 인증 프로토콜은 이 같은 문제점을 모두 해결하였다. 기존 연구들과 제안하는 프로토콜의 안전성을 비교하면 표 2와 같다.

VI. 결 론

RFID 기술은 유비쿼터스 컴퓨팅 환경을 조성하기 위한 핵심 기술로써 산업에 전반적으로 활용되어 많은 이익을 남기고 있다. 그러나 이에 대한 역기능으로 RFID 시스템의 보안 위협으로 인해 더 큰 손해가 발생할 수 있다. 본 논문에서는 보다 안전한 RFID 시스템을 위하여 최근에 연구되었던 RFID 인증 기술을 분석하여 보다 안전한 통신을 위해 상호인증을 제공하는 RFID 인증 프로토콜을 제안하였다. 제안한 인증 프로토콜은 리더와 태그간 상호인증을 제공함으로써 악의적인 리더나 불법적인 태그로의 위장을 방지할 수 있으며, 손상된 리더에 대하여 태그의 비밀 키를 보호할 수 있다.

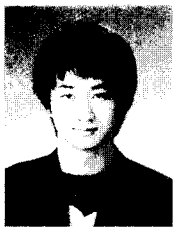
참 고 문 헌

[1] 한국 RFID/USN 협회, http://www.karus.or.kr
[2] A. Juels, "RFID Security and Privacy: AResearch Survey," IEEE Journal on Selected Areas in Communications, 24(2): 381-394, Feb. 2006.
[3] 이근우, 곽진, 오수현, 김승주, 원동호, "RFID 표준화 및 프로토콜에 관한 연구,"
[4] S. A. Weis, "Security and privacy in radio-frequency identification device," MS Thesis. M.I.T. May, 2003.
[5] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "gSecurity and privacy aspects of low-cost radio frequency identification systems," Security in Pervasive Computing 2003, LNCS 2820, pp. 201-212, Springer-Verlag Heidelberg, 2004.
[6] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash-chain based forward-secure privacy protection scheme for low-cost RFID," Proceedings of the SCIS 2004, pp. 719-724, 2004.
[7] 김진목, 유황빈, "유비쿼터스 환경에서 Pre-Distribution을 기반으로 한 안전한 RFID 시스템," 전자공학회논문지, 제42권, 제 CI-6호, pp.29-36, 2005.11.
[8] 신진섭, 박영호, "RFID/USN에서의 EXOR과 해쉬함수를 이용한 인증 프로토콜," 한국산업정보학회 논문지, 제12권, 제02호, pp.24-29, 2007.6.
[9] 안해순, 부기동, 윤은준, 남인길, "RFID/USN 환경을 위한 개선된 인증 프로토콜," 전자공학회 논문지, 제 46권 CI-1호, 2009.1.
[10] 김경신, 김세일, 천지영, 이동훈, "경량 RFID 시스템에서의 안전한 상호 인증 기법," 한국정보과학회 학술발표논문집, 제35권 2호, 2008.10.
[11] 박한나, 김세일, 천지영, 이동훈, "RFID를 위한 이차잉여 기반의 개선된 상호인증 기법," 정보과학회 논문지, 제15권 6호, 2009.6.

저 자 소 개

전 서 관(학생회원)
2008년 호서대학교 정보보호학과 학사 졸업
2008년~현재 호서대학교 정보보호학과 석사과정
<주관심분야 : 암호학, 네트워크 보안, 보안 프로토콜>

오 수 현(정회원)
1998년 성균관대학교 정보공학과 석사 졸업
2000년 성균관대학교 전기전자 및 컴퓨터공학과 석사 졸업
2003년 성균관대학교 전기전자 및 컴퓨터공학과 박사 졸업
2004년~현재 호서대학교 정보보호학과 교수
<주관심분야 : 암호학, 네트워크 보안 프로토콜>



은 선 기(학생회원)
2008년 호서대학교 정보보호학과 학사 졸업
2009년~현재 호서대학교 정보보호학과 석사과정
<주관심분야 : 네트워크 보안 프로토콜, 시스템 평가 및 인증>