# Tag ID가 없는 안전한 RFID 인증프로토콜

이승민°,조창현,김태은,주소진,전문석
숭실대학교 컴퓨터학과 대학원
cowaboonga@ssu.ac.kr°, hist0001@hotmail.com, eunii31@ssu.ac.kr,
yetiblow@ssu.ac.kr, mjun@compuintg.ssu.ac.kr

# Excepted ID of Tag Method based Secure RFID Authentication Protocol

Seungmin Lee° Jaesik Lee. Taeeun Kim. Sojin Ju. Moonseog Jun
Department Computing, Soongsil University

요 약

RFID/USN이 큰 이슈가 되면서 RFID 에 대한 각종 연구와 응용이 현재 활발히 진행 중이다. 유선 네트워크상에서의 보안은 지금까지의 연구와 개발로 신뢰적인 통신이 가능하다. 그러나 RFID는 Air Interface를 전송매체로 사용하기 때문에 유선의 상황보다 외부의 노출정도가 훨씬 크다. 따라서 외부의 공격에 쉽게 노출 될 수 있으며 이를 보완하기위해 Tag안에 ID를 직접 넣지 않고 DataBase에서만 ID를 관리하는 방식의 RFID 인증 프로토콜을 제안했다. 기존의 RFID 인증 프로토콜보다 Reader의 작업량을 줄였고, 태그로부터 정보를 탈취하여 복호화 한다 하더라도 ID가 없기 때문에 쓸모없는 정보가 된다.

## 1. 서 론

RFID(Radio Frequency Identification) 시스템은 air interface를 매체로 한다. 주파수를 이용하여 리더기(Reader)와의 접촉 없이 태그(Tag)의 정보를 읽거나 쓰기가 가능한 시스템이다. RFID는 비접촉식(Contact-less)이고 비가시선(non-line-of-sight)의 데이터 수취 기술로써 초소형 IC 칩에 식별정보를 입력하고 무선주파수를 이용하여 이 칩을 지닌 물체, 동물, 사람 등을 판독, 추적, 관리할 수 있기 때문에 M2M(machine to machine)에서의 위치추적 및 상황인식을 가능케 하는 역할을 하게 되어 새로운 개념의 비즈니스를 실현시켜줄 핵심이 된다.

RFID 기술은 자동인식 기술이기 때문에 사용자의 정보 즉, 태그의 정보가 노출, 추적이 될 수 있다. 이러한 정보 노출의 문제를 해결하기 위해 많은 연구와 기술개발이 진행 중에 있다. 본고에서는 리더와 태그사이의 물리적 자원의 한계를 고려해서 상호 인증(Mutual Authentication)이 가능한 프로토콜을 제안하였다. 2장에서는 RFID 시스템의 구성, RFID 설계시 제약조건, 관련 공격기법 및 위험요소, 연구된 여러 프로토콜을 살펴보겠고, 3장에서는 제안한 프로토콜에 대하여 설명한다. 4장에서는 제안한 프로토콜의 보안성을 살펴보고, 5장에서 결론을 맺도록 하겠다.

## 2. RFID 관련 연구

RFID 시스템은 스마트카드와 매우 밀접한 관련이 있다. 스마트카드 시스템과 같이 데이터는 데이터 운반 장치인 트랜스 폰더(Transponder)에 저장이 된다. 그러나 데이터 운반 장치에 전원 공급 및 데이터 운반 장치와 리더 사이의 데이터 교환이 전기적 접촉 없이 자계 또는 전자계 영역을 이용하여 이루어진다는 점이 스마트카드와 다르다. RFID 시스템은 다른 인식 시스템과 다르게 오접촉(훼손, 오염, 단방향 삽입, 삽입시간 지체 등)에 대한 단점을 보완한 방법이다.

### 2.1 RFID의 제약조건

현재 RFID 태그는 값이 싸고 작아야한다. 현재 상용화되어있는 제품 중에는 메모리의 내용에 대한 읽기/쓰기를 허용하고 $1.0로 판매되는 제품이 있다. 그러나 향후 보편적으로 사용될 RFID 태그는 US$0.05~US$0.1의 가격대에 있기 때문에 강인한 암호프리미티브를 사용하는 것은 어렵다. 낮은 가격의 범위를 벗어나지 않으면서 보안 및 프라이버시 위험을 고려한 태그 및 리더의 설계가 주요한 문제가 되고 있다.

CRYPREC 보고서에 따르면 대칭키 암호알고리즘의 구현이 6~13K 게이트로 알려져 있으며 대칭키를 기반으로 설계할 수 있는 해쉬함수도 유한한 수의 게이트가 요구될 것으로 기대된다[1].

### 2.2 관련 공격기법 및 위험 요소

① 도청공격(Evesdropping) : 태그와 리더사이의 통신은 라디오 주파수 방식이기 때문에 누구든지 태그에 접근하여 태그의 출력 값을 얻을 수 있어, 허가 되지 않은 리더가 정당한 리더로 가장하여 태그의 정보를 얻을 수 있음.

② 트래픽 분석(Traffic analysis) : 태그의 내용이 보호되고 있다 하더라도, 예측되는 태그의 응답 값은 태그와 태그 소유자의 신원을 연결시킬 수 있는 정보를 제공해 주게 된다. 그러므로 태그를 소지한 사용자를 추적할 수 있음.

③ 스푸핑(Spoofing) 공격 : 외부의 공격자가 정당한 리더로 가장하여 태그로부터 정보를 수집하고 이 정보를 이용하여 정당한 태그인 것처럼 가장한다.

④ 서비스거부(Denial of Service) 공격 : RF 신호 채널

을 방해하거나, 임의의 다른 수단으로 태그를 무력화 하는 방법

⑤ 세션 가로채기(Hijacking), 재전송공격 : RFID 리더와 태그사이의 상호인증을 위한 인증 프로토콜 수행 시 발생할 수 있는 공격들로, 인증된 세션을 가로채는 가로채기 공격, 공격자가 검증자에게 이전에 수행되었던 프로토콜 부분 중 일부분을 다시 실행시키는 재전송 공격을 한다.

2.3 RFID 정보 보호를 위한 프로토콜

다음에 나올 여러 프로토콜 기법들은 다음을 가정한다.

-Database와 Reader사이는 보안 채널이다.

-Reader와 Tag사이에서는 비보안 채널이다.

2.3.1 해쉬-락 기법

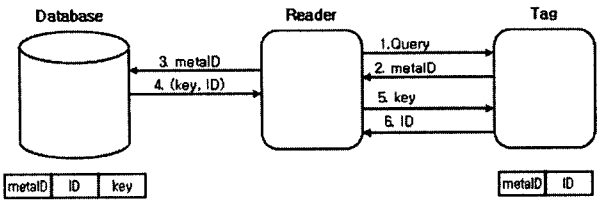


그림1 해쉬-락 기법

해쉬-락 기법은 태그가 ID를 리더에게 직접 전달해 주는 것이 아니고 먼저 metaID를 건내주게 되고 리더는 그 metaID를 가지고 Back-end-Database에게 넘겨주게 된다[2]. 그림1에서 Database는 해당 metaID에 맞는 key값과 ID를 리더에게 넘겨주게 된다. 리더는 key값을 다시 태그에게 넘겨주게 되고 태그는 key값이 정확한지 확인을 하고 ID를 넘겨주게 된다. 여기서는 metaID가 악의적인 리더에게 바로 노출되기 때문에 meatID의 탈취가 가능하고 악의적인 태그가 이 metaID 값을 이용하여 정당한 Tag로 위장할 수 있다. metaID 값을 그대로 받아서 전송이 가능하므로 재전송공격에 약하다. 그리고 해당 metaID를 넘겨준 태그가 어느 태그인지 추적이 가능하다. 단계의 마지막에서는 key와 ID를 알기 때문에 거의 모든 단계의 정보를 알 수 있으므로 스푸핑 공격에 약하다. RFID 초창기에 고안된 프로토콜이므로 여러 가지 취약점이 많다.

2.3.2 확장된 해쉬-락 기법

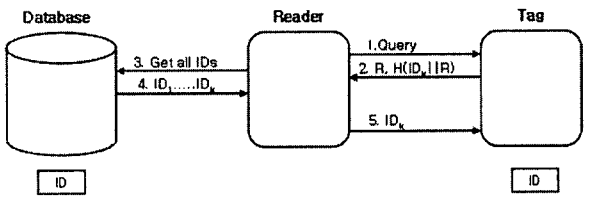


그림2 확장된 해쉬-락 기법

확장된 해쉬-락 기법은 위의 해쉬-락 기법에서 태그가 metaID를 사용하는 것이 아니라 난수 값과 ID값과 난수값을 해쉬한 값을 전송하는 것이 주요 특징이다[3]. 리더가 Query를 태그로 전송하게 되면 태그는 반응하여 자신이 생성한 난수 값 R과 ID와 R 값을 해쉬한 $H(ID_k||R)$를 다시 리더로 전송하게 된다. 리더는 Database에 모든 ID를 요청하게 되고 ID는 $ID_1$~$ID_k$값을 전송해준다. 리더는 자신이 받은 $H(ID_k||R)$ 과 비교하여 알맞은 $ID_K$을 골라 다시 태그에게 넘겨주게 된다. 여기서는 $ID_K$가 외부에 노출된 상태 그대로 태그에게 전송되기 때문에 공격의 대상이 될 수 있다. 정당한 리더로 가장하여 R, $H(ID_k||R)$을 얻어 낼 수 있고 이 정보를 악의적인 태그에 넣어 리더에 대한 응답으로 대신 보낼 수 있다. 따라서 재전송 공격에 대해 약하고, 스푸핑 공격에 무방비 상태가 된다.

2.3.3 개선된 해쉬 기반 ID 변형 기법

그림3의 개선한 ID 변형 기법은 기존의 해쉬 기반 ID 변형 기법보다 스푸핑 공격에 강하게 만들었고 태그의 연산도 줄였다[4]. 하지만 역시 위치추적 공격에는 안전하지 못하다. 또, 정당한 리더로 가장하여 태그 내의 데이터를 얻을 수 있어 스푸핑 공격의 우려가 있다. 마지막 단계인 half_R(H)의 전송을 방해한다면 ID가 갱신되지 않아 문제가 발생할 것이다.

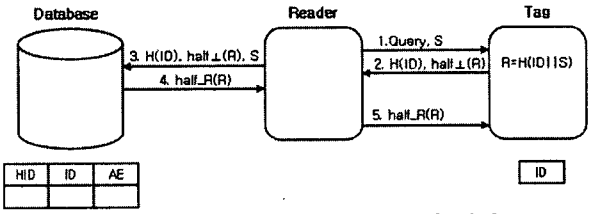


그림3 개선된 해쉬 기반 ID 변형 기법

3. 제안 프로토콜

본고에서 제안한 Tag ID가 없는 안전한 RFID 인증프로토콜 은 그동안의 연구된 해쉬-락 기법, 확장된 해쉬-락기법, 해쉬 기반 ID 변형 기법, 개선된 해쉬 기반 ID 변형 기법 등의 단점을 보완하였고, 분산된 Back-end-Database를 이용하기 때문에 Reader가 갖고 있던 작업의 부담을 줄였다. 또한 태그가 ID를 직접 보유하지 않기 때문에 중간에서 데이터의 내용을 가로채 복호화 한다 하더라도 ID가 공개되지 않는다.

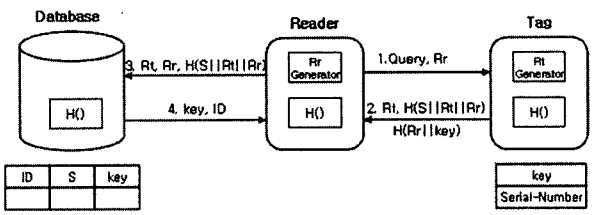


그림4 제안한 프로토콜

ID : 태그의 Identification Number

Rr : 리더가 생성한 난수

Rt : 태그가 생성한 난수

H(): One-way 해쉬 함수

S : 태그의 고유 Serial number

key:태그마다 보유하고 있는 고유의 키값

||:문자열 연접 연산

그림4에서 태그는 난수를 발생하는 난수발생기, 고유의 key값, S인 Serial number값, 해쉬함수(H())를 갖는다.
리더는 난수 발생기, 해쉬함수(H())와 연산에 필요한 저장공간을 갖는다.
데이터베이스는 ID, S(Serial Number), key 필드를 갖고 있고 해쉬함수(H())도 갖는다.

단계 1 : 리더는 태그에게로 Query와 자신이 생성한 난수를 전달한다.
단계 2 : 태그는 태그 자신의 난수발생기로부터 난수 Rt를 생성한다. 해쉬 함수를 이용하여 H(S||Rt||Rr)을 계산한다. 또한 태그 고유의 키 값인 key를 이용하여 H(Rr||key)을 계산한다. Rt, H(S||Rt||Rr), H(Rr||key)를 리더에게 전송한다.
단계 3 : 리더로부터 받은 Rt, Rr, H(S||Rt||Rr)을 데이터베이스에 전송한다.
단계 4 : 데이터베이스는 리더에게 key과 ID를 전송한다.

리더는 데이터베이스로부터 받은 key를 이용하여 H(Rr||key')를 계산하여 또한 단계 2에서 받은 H(Rr||key)과 비교한다. 값이 같다면 리더는 ID를 이용할 것이고 값이 같지 않다면 ID를 폐기한다.

## 4. 프로토콜의 보안성

### 4.1 스푸핑에 대한 보안성

악의적인 공격자가 리더로 가장하여 태그가 전송하는 Rt, H(S||Rt||Rr), H(Rr||key)를 탈취하였다 가정하더라도 리더는 계속 난수를 생성하기 때문에 단계 3의 과정에서 데이터베이스에 보내는 Rr이 탈취한 Rr과는 다르기 때문에 마지막 리더의 H(Rr||key) 비교 단계에서 걸러지게 된다. 리더의 난수의 생성과 해쉬함수를 이용하am로 스푸핑 공격을 막을 수 있다.

### 4.2 재전송 공격에 대한 보안성

태그가 전송하는 정보를 탈취하여 재전송 한다 하더라도 리더가 난수를 사용하기 때문에 데이터의 내용이 바뀌므로 마직막 단계 4에서 태그로부터 온 정보와 데이터베이스로부터 온 정보과 다르기 때문에 재전송 공격이 불가능하다.

### 4.3 위치추적에 대한 보안성

리더만 난수를 발생하는 것이 아니고, 동시에 태그도 난수발생기로부터 난수를 생성하기 때문에 같은 태그가 같은 값을 두 번 전송하지 않는다. 따라서 탈취 한 값에 대한 추적은 불가능하다.

### 4.4 ID의 보안성

본고에서 제안하는 프로토콜에서는 태그는 ID를 직접 가지고 있지 않기 때문에 중간의 정보를 탈취해서 그것을 복호화 한다 하더라도 ID가 없기 때문에 쓸모없는 정보가 된다. 태그가 공장 출하 시 생성되는 Serial-Number 값과 비밀키를 이용하여 데이터베이스에서 ID를 찾기 때문에 Back-end-Database와 리더사이에 secure channel이 보장된다면 안전하다.

### 4.5 정당한 리더로 가장하는 리더

제안한 프로토콜에서는 태그가 리더를 인증하는 단계가 생략되었는데, 정당한 리더로 가장하여 태그가 전송하는 정보를 탈취한다 하더라도 그 해쉬 된 정보 속에는 ID 값이 존재 하지 않는다. 또 그 정보를 이용하려면 정당한 태그로 가장하여야 하기 때문에 막히게 된다. 위에서 설명한 스푸핑 공격이나 재전송 공격에 안전하다는 것이 위장한 태그를 분별한다는 말과 일맥상통하기 때문이다. 위장한 리더가 데이터베이스와 리더사이의 secure channel에 직접 개입하지 않는 이상 리더 인증은 생략될 수 있다.

## 5. 결론

현대는 유비쿼터스 환경의 도입에 따른 언제 어디서든 정보를 획득할 수 있게 된다. 정보의 공유 등으로 인해 보안의 위협 및 개인의 프라이버시가 침해 등 역 기능에 대한 문제가 심각해지고 있다. 실례를 들면 유명 브랜드의 상품도용에 대한 문제가 커지고 있는데 RFID를 이용하여 이 문제를 해결 할 수 있다고 매스컴을 통해서 크게 보도 된 바 있지만 RFID를 이용한다 하더라도 앞에서 설명한 보안상의 취약점을 해결하지 못한다면 RFID는 애물단지로 전락할 수도 있다. 인증 프로토콜의 수많은 연구들이 진행되고 결과가 나왔지만 역시 보안상의 취약점이 존재하여 그 취약점들을 보완하고 ID를 최대한 노출 시키지 않는 범위 내에서 본고에 설명한 프로토콜을 제안하였다.

## 참고문헌

[1] CRYPTOREC reports. published 2002 (in Japanese)
[2] S. E. Sarma, S. A. Weis, D. W. Engels, "RFID systems, Security & Privacy Implications", White Paper MIT-AUTOID-WH-014, MIT AUTO ID CENTER, 200
[3] S. A. Weis, "Security an Privacy in Radio-Frequency Identification Devices" MS Thesis. MIT, May, 2003.
[4] 황영주, 이수미, 이동훈, 임종인, "유비쿼더스 환경의 Low Cost RFID 인증 프로토콜", 한국정보보호학회 하계정보보호학술대회 논문집 Vol.14, No.1, pp.109-114
[5] Electronic Privacy Information Center, Radio Frequency Identification(RFID) System, Washington D.C., August 11, 2003, p. 2. www.epic.org/privacy/rfid/
[6] 유성호, 김기현, 황용호, 이필중, "상태기반 RFID 인증 프로토콜", 한국정보보호학회 논문집 제 14권, 6호 2004. 12
[7] Sandra Dominikus, Elisabeth Oswald, Martin Feldhofer, "Symmetric Authentication for RFID Systems in Practice"