RFID 시스템을 위한 난수 기반의 보안 인증 프로토콜

배우식*, 이종연*
*충북대학교 컴퓨터교육과
e-mail : bws@motor.ac.kr

Random Number-based Security Authentication Protocol for RFID System

Woo Sik Bae*, Jong Yun Lee*
**Dept. of Computer Education, Chungbuk National University

요 약

RFID 시스템에서 태그와 리더사이의 통신이 무선통신을 통해 이루어짐에 따라 보안상 많은 취약점이 존재한다. 본 논문에서는 여러 보안 문제 중 프라이버시 보호를 위한 기존 기법의 취약점을 보완하여 태그가 리더로부터 수신한 해쉬값과 난수 값을 기반으로 한 인증 프로토콜을 제안한다. 제안한 프로토콜은 단순한 EPCIS를 위한 RFID 간소화 및 프로토콜의 성능 향상을 제안 한다. 제안을 바탕으로 구현 할 때 리더의 해쉬된 값과 난수 값으로 인하여 보안성은 향상되며 태그의 연산 사용을 줄이고 EPCIS를 구현할 수 있는 시스템 이다.

1. 서론

RFID(Radio Frequency Identification)는 전자태그를 물품에 부착하여 기존 IT시스템과 실시간으로 정보를 교환, 처리할 수 있는 기술을 말한다. RFID는 높은 인식률, 비 접촉형 인식매체, 도달거리, 다른 통신망과의 연계 및 통신 가능성 등의 확장성으로 인해 특히 물류, 유통, 군사, 식품안전 등 비즈니스 영역에 막대한 파급효과를 끼칠 전망이다. 그러나, RFID 시스템은 그 편리성에도 불구하고 무선구간의 비접촉식 인식 시스템이라는 특징 때문에 안정성과 프라이버시 보호 측면에서 문제점을 지니고 있다. 보안상 안전하지 않는 태그를 사용하는 경우 물리적 공격, 위조, 스푸핑, 도청, 트래픽 분석, DOS 공격 등에 의한 보안적 취약점에 노출되어 진다. 이러한 취약점을 방지하기 위해 태그에 저장 관리되는 식별 정보를 보호하기 위한 다양한 분야의 방법이 제안되고 있다[1].

본 논문에서는 RFID의 프라이버시 문제를 해결하기 위해 기존에 제안된 해쉬락(Hash-Lock)기법[2,3,4]등 에서 해결하지 못한 문제점을 보완하여 보다 안전하고 효율적으로 사용자의 프라이버시를 보호할 수 있는 인증 프로토콜을 제안한다. 제안하는 인증프로토콜은 리더의 해쉬 함수와 난수를 이용하여 공격자의 공격에 대응함으로써 추후 예상되는 각종 공격에 보안성을 제공하는 프로토콜이다.

2. 관련연구

2.1 해-쉬락 기법

해쉬-락 프로토콜은 MIT에 의해 제시된 방식으로 태그의 식별 값인 MetaID가 고정되어 있어 악의적인 공격자는 Key를 획득한 후, 해쉬 연산 하여 MetaID를 산출하여 인증을 받을 수 있다. 이러한 단점으로 스푸핑 공격 및 사용자 추적이 가능한 문제점이 있다..

2.2 해쉬 기반 ID변형기법

해쉬 기반 ID 변형기법[5]은 ID가 인증세션마다 바뀌므로 변형되는 ID를 저장하고 있는 데이터베이스가 존재해야만 하는 문제점이 있다. 본 프로토콜은 매 세션마다 태그의 ID가 난수 R에 의해 갱신되므로 재전송 공격으로부터 안전하다. 그러나 공격자가 태그로부터 H(ID), H(i⊕ID), Δi를 획득하고, 정당한 태그가 다음 인증세션을 수행하기 전에 정보들을 리더의 질의에 대한 응답으로 전송하면 프라이버시를 침해받을 수 있는 문제가 있다.

2.3 Won 외 4명의 인증 프로토콜

Won 외 4명의 인증 프로토콜은[6] 리더와 태그간의 인증 방법으로 태그에서 난수생성, $h(h(s,id_R)\|r_1r_2$ 등 복잡한 해쉬 함수 계산 $f_3 = h(h(s,id_R)\|f_1)\oplus h(id_T)$의 비교, XOR 연산 및 고용량 전송등 태그와 리더에 복잡한 계산이 집중되어 있다. 본 장식은 데이터베이스가 없는 시스템에서 사용 가능하겠지만 연산 성능이 우수한 태그를 이용해야 하므로 상당한 비용 지출이 예상되어 현실성이 부족한 문제가 있다.

3. 제안 프로토콜

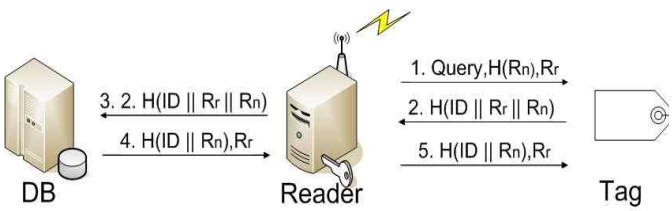
3.1 구조

본 제안 프로토콜의 리더는 난수 생성기를 갖고 있으며, 리더가 처음 태그에게 질의를 할 때 난수와 해쉬된 값을 함께 전송하고, 태그는 리더로부터 수신한 난수와 해쉬값을 자신이 가지고 있는 ID와 해쉬한 값을 이용하여 매 세션마다 다르게 응답함으로써 재전송 공격과 스푸핑 공격에 대하여 안전하다. 제안프로토콜에서 데이터베이스는 태그의 ID와 관련 데이터를 저장하고 있으며, 해쉬 함수 1회의 연산만을 이용하여 태그를 인증한다.

제안 프로토콜에서 사용되는 파라미터는 다음과 같으며, [그림 1]은 제안하는 프로토콜의 기본 구조를 나타낸 것이다.

[파라미터]

- Query : 질의, 태그의 응답을 요청
- ID : 태그 고유의 정보
- H( ) : 해쉬 함수 연산
- $H(R_n)$: 리더가 태그에게 전송하는 해쉬된 리더 코드
- R_r : 리더가 생성하여 태그에게 전송하는 난수
- || : 연접(Concatenate function)



[그림 1] 제안 프로토콜의 구조

3.2 인증과정

[Step 1] 리더는 태그들에게 Query와 $H(R_n)R_r$를 함께 브로드캐스팅 한다.

리더 → 태그 : Query, $H(R_n)R_r$

[Step 2] 태그는 ID와 자신이 가지고 있던 ID를 연접한 후 해쉬 하여 Query에 대한 응답으로 리더에게 전송한다.

태그 → 리더 : $H(ID\|R_r\|R_n)$

[Step 3] 리더는 $H(ID\|R_r\|R_n)$를 백-엔드 데이터베이스로 전송한다.

리더 → 백-엔드 데이터베이스 : $H(ID\|R_r\|R_n)$

[Step 4] 백-엔드 데이터베이스에 저장된 ID를 해쉬한 값과 리더로부터 수신한 $H(ID\|R_r\|R_n)$를 비교하여 태그를 인증한다.

백-엔드 데이터베이스 → 리더 :

계산된 $H(ID\|R_r\|R_n)$ =

수신한 $H(ID\|R_r\|R_n)$

인증이 성공하면 $H(ID\|R_n),R_r$를 리더에게 전송한다.

[Step 5] 리더는 백-엔드 데이터베이스로부터 수신한 $H(ID\|R_n),R_r$를 태그에게 전송한다.

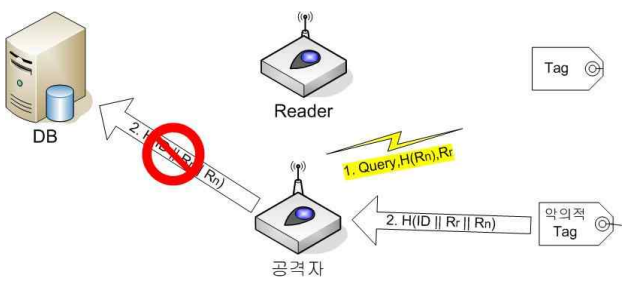
리더 → 태그 : $H(ID\|R_n),R_r$

태그는 자신의 ID와 인증 세션에서 생성된 $H(ID\|R_r\|R_n)$ 리더로 부터 수신된 $H(ID\|R_n),R_r$를 확인하여 인증 성공적으로 종료 한다.

3.3 제안프로토콜의 안전성

3.3.1 스푸핑 공격에 대한 안전성

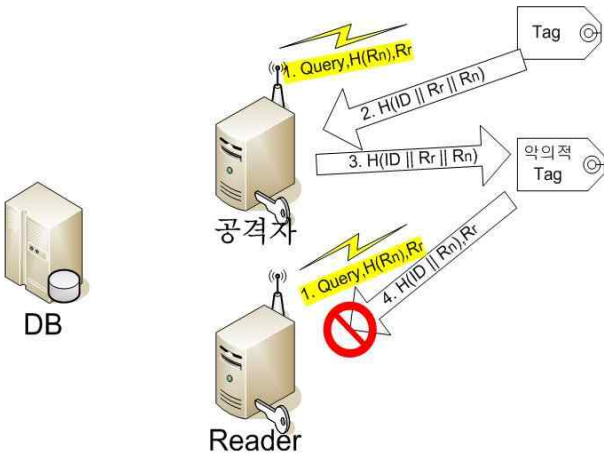
공격자가 정당한 리더로 가장하여 Query와 $H(R_n)R_r$를 전송하면, Query와 $H(R_n)R_r$를 획득할 수 있으나 악의적인 태그에 넣어 응답으로 보내지게 되면 세션이 바뀐 후의 정보 Query와 $H(R_n)R_r$ 로는 인증을 할 수가 없어 [그림 2]와 같이 스푸핑 공격이 DB의 거부로 불가능 하게 된다.



[그림 2] 스푸핑 공격 거부

3.3.2 재전송 공격에 대한 안전성

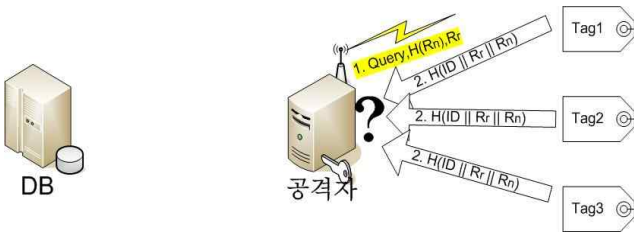
정당한 리더의 Query와 $H(R_n)R_r$는 매 세션마다 변하기 때문에 $H(ID \| R_r \| R_n)$도 매 세션마다 바뀌게 된다. 그러므로 공격자는 도청으로 획득한 $H(R_n)R_r$를 [그림 3]처럼 다음 세션에서는 응답으로 사용할 수 없으므로 재전송 공격에 안전하다.



[그림 3] 재전송 공격 거부

3.3.3 트래픽 분석과 위치 추적에 대한 안전성

공격자가 Query와 $H(R_n)R_r$를 태그에게 전송하여도 이후 세션에서는 DB에서 의 인증이 필요하여 매 세션마다 변하는 응답을 전송하므로 [그림 4]와 같이 공격자는 트래픽 분석이 불가능 하고 태그의 위치도 추적할 방법이 없게 된다.



[그림 4] 위치추적 공격 안전성

3.3.4 정보전송 방해에 대한 안전성

제안 프로토콜은 상호 인증을 제공하므로 정보전송 방해 공격을 탐지할 수 있으며 [표 1]은 기존 프로토콜과의 안전성 비교표 이다.

[표 1] 제안프로토콜의 안전성

	해쉬-락 기법	해쉬기반 ID변형기법	Won등의 프로토콜	제안프로토콜
스푸핑 공격	취약	취약	안전	안전
재전송 공격	취약	안전	안전	안전
트래픽 분석 공격	취약	안전	안전	안전
위치정보 노출	취약	취약	안전	안전
전송방해 공격	안전	안전	안전	안전

3.4 제안 프로토콜의 효율성

태그는 [표 2]와 같이 인증세션동안 해쉬 함수 2회, 난수 1회의 연산만을 수행 하므로 연산 부담도 크지 않으며 저가의 태그에 적용이 가능하다.

[표 2] 제안프로토콜의 효율성

	해쉬-락 기법	해쉬기반 ID변형기법	Won 등의 프로토콜	제안프로토콜
태그 연산량	해쉬1회	해쉬3회	난수 1회 해쉬 5 회 비교 1회 XOR 1회	해쉬1회
리더 연산량	-	-	난수 1회 비교 1회 XOR 1회	난수1회
DB연산량	-	해쉬3회 난수1회	-	해쉬1회

4. 결론

최근 들어 바코드를 대신하여 각 산업 분야에서 RFID 시스템이 본격적으로 사용되기 시작하였다, 그러나 보안적인 측면의 인식과 고려가 부족하여 프라이버시 문제에 노출되어 있다. 본 논문에서 제안한 인증 프로토콜은 태그가 리더로부터 수신한 난수 및 해쉬된 리더코드로 부터 새로운 해쉬 함수를 생성하여 매 세션마다 응답을 전송할 수 있도록 했다. 공격자의 재전송 공격, 스푸핑 공격, 위치추적 등에 안전한 인증 프로토콜로써 안전성과 효율성을 충족

할 수 있다. 특히 태그의 연산이 적으며 데이터베이스의 부담을 줄여주는 구조로 되어 있어 구축 비용 면에서도 효과적 이라고 할 수 있다.

참고문헌

[1] 주학수, “RFID 시스템의 보안 및 프라이버시 보호를 위한 기술 분석”, 전자정보센터, 2004.

[2] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. w. Engels, "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems," Security in Pervasive Computing 2003, LNCS 2802, pp. 201-202, Springer-Verlag Heidelderg, 2004.

[3] S. A. Weis, “Security and Privacy in Radio-Frequency Identification Devices” MS Thesis, MIT.May, 2003.

[4] S. E. Sarma, S. A. Weis, D. W. Engels. “RFID systems, Security & Privacy Implications”, White Paper MIT-AUTOID-WH-014, MIT AUTO-ID CENTER, 2002.

[5] Gildas Avoine and Philippe Oechslin "RFID Traceability : A Multilayer Problem", Financial Cryptography, March 2005.

[6] 원태현, 유영준, 천지영, 변진욱, 이동훈,“온라인 백-엔드 데이터베이스가 없는 안전한 RFID 상호 인증 프로토콜”, 정보보호학회논문지, 제20권, 제1호, pp. 63-72, 2010.