강한 프라이버시를 제공하는 YA-RFID 인증 프로토콜

윤은준*, 부기동**, 유기영***
*경북대학교 전자전기컴퓨터학부
**경일대학교 컴퓨터공학부
***경북대학교 컴퓨터공학과
e-mail:ejyoon@knu.ac.kr, kdbu@kiu.ac.kr, yook@knu.ac.kr

YA-RFID Authentication Protocol providing Strong Privacy

Eun-Jun Yoon*, Gi-Dong Bu**, Kee-Young Yoo*
*School of Elec. Eng. and Comp. Sci., Kyungpook National University
**School of Computer Engineering, Kyungil University
***Dept of Computer Engineering, Kyungpook National University

요 약

최근 Yang과 An은 기존의 RFID 인증 메커니즘들이 가지고 있는 프라이버시 침해 문제를 분석하고 보다 안전하고 효율적인 사용자의 프라이버시를 보호할 수 있는 RFID(YA-RFID) 인증 프로토콜을 제안하였다. 그들은 제안한 YA-RFID 인증 프로토콜이 공격자의 재전송 공격, 스푸핑 공격, 그리고 위치 트래킹 공격에 대해 안전하다고 주장하였다. 하지만 본 논문에서는 그들의 주장과는 달리 YA-RFID 프로토콜이 여전히 위치 트래킹 공격에 취약함을 증명하며, 더 나아가 동일한 연산 효율성을 보장하며 위치 트래킹 공격을 막을 수 있는 간단히 개선된 일회성 난수와 안전한 일방향 해쉬 함수 기반의 RFID 인증 프로토콜을 제안한다.

1. 서론

일반적으로 RFID(Radio Frequency Identification) 시스템은 태그(tag), 리더(reader), 그리고 백-엔드 데이터베이스(back-end Database)의 3가지 구성요소로 구성된다[1]. 현재 RFID 시스템은 바코드 인식 시스템이나 자기 인식 장치들이 근본적으로 내재하고 있는 실용성 및 보안성 문제점들을 보완할 수 있는 대체 시스템으로 각광받고 있으며 다양한 산업 응용 분야에서 사용되어 지고 있다. 특히 교통카드, 출입구 보안 및 출결 카드 분야를 포함한 상거래와 직접적인 관련이 있는 물류관리, 재고관리, 항만관리, 동물관리 등 물류 및 유통 분야에서도 빠르게 응용 및 확산되어 사용되어 지고 있다[2,3].

RFID 시스템이 가져다주는 위와 같은 실용성과 편리함 이면에는 개인 정보 노출 및 개인의 위치 정보 누출 등으로 인한 개인의 프라이버시(privacy) 침해 문제가 상당히 발생할 수 있다[4,5]. 이러한 프라이버시 침해 문제를 해결하기 위해 지금까지 많은 연구자들에 의해 해쉬-락 기법, 확장된 해쉬-락 기법, 해쉬-기반 ID 변형 기법, 개선된 해쉬-기반 ID 변형 기법, 블로커 태그를 이용한 기법, 해쉬-체인 기법 등 다양한 RFID 인증 프로토콜(authentication protocol)들이 최근까지 개발되어져 오고 있다[4-16]. 하지만 현재까지 제안되어져 오고 있는 대부분의 RFID 인증 프로토콜들은 태그의 재사용이 불가능하거나, 태그의 위치추적으로 위치 트래킹 공격(location tracking attack)이 쉬우며, 재전송 공격(replay attack)이나 스푸핑 공격(spoofing attack)에 취약하는 등 다양한 보안 취약점과 프라이버시 침해 문제들을 가짐을 많은 연구자들에 의해 발견되어 지고 있다[7-16].

최근 Yang과 An은 위와 같은 기존의 RFID 인증 메커니즘들이 가지고 있는 보안 취약점과 프라이버시 침해 문제를 분석하고 보다 안전하고 효율적인 사용자의 프라이버시를 보호할 수 있는 일방향 해쉬 함수와 난수를 이용한 RFID(YA-RFID) 인증 프로토콜을 제안하였다[11]. 그들은 제안한 YA-RFID 인증 프로토콜이 공격자의 재전송 공격, 스푸핑 공격, 그리고 위치 트래킹 공격에 대해 안전하다고 주장하였다. 하지만 본 논문에서는 그들의 주장과는 달리 YA-RFID 인증 프로토콜이 여전히 위치 트래킹 공격에 취약함을 증명한다. 위치 트래킹 공격(location tracking attack)은 공격자가 태그의 위치변화를 감지함으로 인해 태그 소유자의 이동 경로를 파악하여 사용자의 프라이버시를 침해하는 공격이다. YA-RFID 인증 프로토콜에서 공격자는 합법적인 리더로 위장하여 과거에 임의의 세션에서 도청한 송수신 정보를 이용하여 간단하게 위치 트래킹 공격을 성공할 수 있다. 이로 인해, 사용자의 프라이버시 침해 문제를 야기 시킬 수 있다. 이러한 보안 취약점을 해결하기 위해 본 논문에서는 동일한 연산 효율성을 보장하며 위치 트래킹 공격을 막을 수 있는 간단히 개선된 일회성 난수와 안전한 일방향 해쉬 함수 기반의 RFID 인증 프로토콜을 제안한다. 한 결론으로 제안한 RFID 인증 프로토콜은 YA-RFID 인증 프로토콜과 비

교하여 더욱더 강한 보안성을 제공하며 효율성 측면에서도 동등하다.

2. 관련 연구

본 장에서는 관련 연구로써 용어 정의와 Yang과 An이 제안한 YA-RFID 인증 프로토콜[11]을 소개한다.

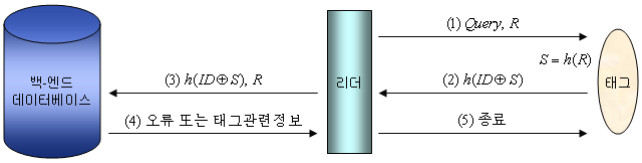
2.1 용어 정의

본 논문에서 사용되는 파라미터들에 대한 용어 정의는 다음과 같다.

- *Query*: 태그의 응답을 요청하는 리더의 요청
- *ID*: 태그에게 할당된 고유 정보
- $h()$: 일방향 해쉬 함수
- R: 리더가 매 세션마다 생성하여 태그에게 전송하는 난수
- N: 태그가 매 세션마다 생성하여 리더에게 전송하는 난수
- $\oplus$: 배타적 논리합 연산
- $\|$: 연접(concatenate function) 연산

2.2 YA-RFID 인증 프로토콜

[그림 1]은 Yang과 An이 제안한 YA-RFID 인증 프로토콜의 구성과 동작 과정을 보여주며, 다음의 5단계를 거쳐 인증 과정이 이루어진다.



(그림 1) YA-RFID 인증 프로토콜

(1) 리더 → 태그: $Query$, R
리더는 태그에게 $Query$와 난수 R을 전송한다.

(2) 태그 → 리더: $h(ID \oplus S)$
리더로부터 수신한 R을 이용하여 태그는 랜덤 해쉬 값 $S=h(R)$을 계산하고, 이를 이용하여 응답(response) 메시지 $h(ID \oplus S)$를 생성하여 리더에게 전송한다.

(3) 리더 → 백-엔드 데이터베이스: $h(ID \oplus S)$, R
리더는 수신한 응답 메시지 $h(ID \oplus S)$와 R을 데이터베이스에게 전송한다.

(4) 백-엔드 데이터베이스: → 리더: 오류 또는 태그정보
백-엔드 데이터베이스는 리더로부터 전송받은 R을 이용하여 랜덤 해쉬 값 $S=h(R)$을 계산한다. 백-엔드 데이터베이스는 저장하고 있는 모든 ID와 S값을 이용하여 리더로부터 수신한 값과 아래와 같은 검증 연산으로 비교하여 일치하는 값을 검색한다.

계산된 $h(ID \oplus S)$?= 수신한 $h(ID \oplus S)$ (1)

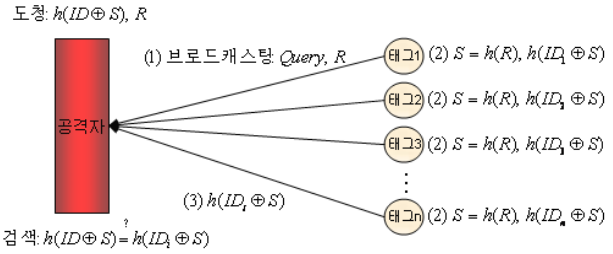
만약 일치하는 값이 검색되지 않으면, 오류(error) 메시지를 리더에게 전송하고, 일치하는 값이 검색되면 태그를 인증하고 태그에 대한 관련정보(related information)를 리더에게 전송한다.

(5) 리더 → 태그: 종료
리더는 백-엔드 데이터베이스로부터 수신한 값이 오류일 경우, 태그와의 통신을 중단하고, 정상적인 인증이 되었을 경우에서는 백-엔드 데이터베이스로부터 전송받은 태그에 대한 관련정보를 이용하여 상품에 대한 요금부과와 같은 과정을 수행하며, 태그에게 인증 과정의 종료를 알리는 종료 메시지를 전송한다.

3. YA-RFID 프로토콜에 대한 위치 트래킹 공격

본 장에서는 Yang과 An이 제안한 YA-RFID 인증 프로토콜이 위치 트래킹(location tracking) 공격에 취약함을 증명한다. 위치 트래킹 공격은 공격자가 태그의 위치변화를 감지함으로 인해 태그 소유자의 이동 경로를 파악하여 사용자의 프라이버시(privacy)를 침해하는 공격이다. 일반적으로 RFID 시스템에서의 위치 트래킹 공격은 동일한 태그로부터 나오는 응답들을 모두 수집하여, 그 응답이 가지고 있는 연관성을 파악하여 응답들에 대한 링크를 통해 공격이 이루어진다.

YA-RFID 프로토콜에서 임의의 공격자가 이전 세션에서 도청한 리더가 생성한 난수 R과 태그가 전송한 응답(response) 메시지 $h(ID \oplus S)$을 소유하고 있다고 가정하자. 공격자는 임의의 세션에서 리더로 위장하여 다음과 같은 과정을 수행하여 위치 트래킹 공격을 성공할 수 있다. [그림 2]는 YR-RFID 인증 프로토콜에 대한 위치 트래킹 공격에 대한 예를 보여주고 있다.



(그림 2) YA-RFID 인증 프로토콜에 대한 위치 트래킹 공격

(1) 공격자 → 임의의 태그들: $Query$, R
공격자는 임의의 태그들에게 이전 세션에서 도청한 $Query$와 난수 R을 브로드캐스팅(broadcasting)한다.

(2) 임의의 태그들 → 공격자: $h(ID \oplus S)$
공격자로부터 수신한 R을 이용하여 임의의 태그들은 랜덤 해쉬 값 $S=h(R)$을 각각 계산하고, 이를 이용하여 응답 메시지 $h(ID \oplus S)$를 생성하여 공격자에게 전송하게 될 것이다.

(3) 공격자는 임의의 태그들로부터 전송받은 $h(ID \oplus S)$을 이용하여 이전 세션에서 도청한 응답(response) 메시지 $h(ID \oplus S)$와 아래와 같은 검증 연산으로 비교하여 일치하는 값을 검색한다.

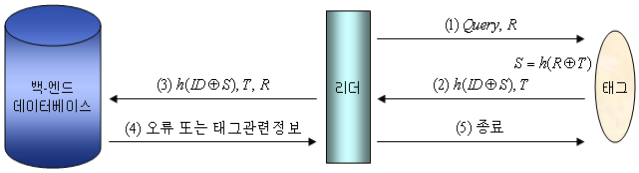
이전에 도청한 $h(ID \oplus S)$?= 수신한 $h(ID \oplus S)$ (2)

만약 일치하는 값이 검색되면 공격자는 그 일치하는 $h(ID \oplus S)$를 전송한 태그가 이전 세션에서 도청한 $h(ID \oplus S)$를 전송한 태그와 동일한 태그임을 알게 되어 태그의 위치변화를 쉽게 감지할 수 있다. 이로 인

해 태그 소유자의 이동 경로를 쉽게 파악하여 사용자의 프라이버시(privacy)를 침해할 수 있음으로 YA-RFID 인증 프로토콜은 위치 트래킹 공격에 취약함을 알 수 있다.

4. 제안한 RFID 인증 프로토콜

본 장에서는 YA-RFID 인증 프로토콜의 위치 트래킹 공격에 대한 취약점을 제거한 개선된 RFID 인증 프로토콜을 제안한다. 제안한 프로토콜에서는 위치 트래킹 공격에 안전하기 위해 태그 측에서도 리더와 마찬가지로 임의의 난수를 생성하도록 설계하였다. 그림 3]은 제안한 RFID 인증 프로토콜의 구성과 동작 과정을 보여주며, 다음의 5단계를 거쳐 인증 과정이 이루어진다.



(그림 3) 제안한 RFID 인증 프로토콜

(1) 리더 → 태그: $Query$, R
리더는 난수 R을 생성한 후, 태그에게 $Query$와 함께 R을 전송한다.

(2) 태그 → 리더: $h(ID\oplus S)$, T
태그는 난수 T를 생성한 후, 리더로부터 수신한 R을 이용하여 랜덤 해쉬 값 $S=h(R\oplus T)$을 계산하고, 이를 이용하여 응답(response) 메시지 $h(ID\oplus S)$를 생성하여 리더에게 전송한다.

(3) 리더 → 백-엔드 데이터베이스: $h(ID\oplus S)$, T, R
리더는 수신한 응답 메시지 $h(ID\oplus S)$ 및 T와 자신이 생성한 R을 데이터베이스에게 전송한다.

(4) 백-엔드 데이터베이스: → 리더: 오류 또는 태그정보
백-엔드 데이터베이스는 태그와 리더로부터 전송받은 T와 R을 이용하여 랜덤 해쉬 값 $S=h(R\oplus T)$을 계산한다. 백-엔드 데이터베이스는 저장하고 있는 모든 ID와 S값을 이용하여 리더로부터 수신한 값과 다음의 검증 연산으로 비교하여 일치하는 값을 검색한다.

계산된 $h(ID\oplus S)$?= 수신한 $h(ID\oplus S)$ (3)

만약 일치하는 값이 검색되지 않으면, 오류(error) 메시지를 리더에게 전송하고, 일치하는 값이 검색되면 태그를 인증하고 태그에 대한 관련정보(related information)를 리더에게 전송한다.

(5) 리더 → 태그: 종료
리더는 백-엔드 데이터베이스로부터 수신한 값이 오류일 경우, 태그와의 통신을 중단하고, 정상적인 인증이 되었을 경우에서는 백-엔드 데이터베이스로부터 전송받은 태그에 대한 관련정보를 이용하여 상품에 대한 요금부과와 같은 과정을 수행하며, 태그에게 인증 과정의 종료를 알리는 종료 메시지를 전송한다.

5. 보안성 분석

본 장에서는 제안한 RFID 인증 프로토콜에 대한 보안성 분석을 한다. 먼저, 제안한 인증 프로토콜의 안전성 분석을 위해 필요한 중요한 보안 항목을 다음과 같이 정의한다[17][18].

[정의 1]. 강력한 비밀 키(ID)는 높은 엔트로피(entropy)를 가지는 값으로써 다항식 시간(polynomial time) 내에 추측되어 질 수 없다.

[정의 2]. 안전한 일방향 해쉬 함수(secure one-way hash function) $y=h(x)$에서, 주어진 x를 이용하여 y를 계산하는 것은 쉽지만, 주어진 y를 이용하여 x를 계산하는 것은 어렵다.

위의 [정의 1]과 [정의 2]를 기반으로 제안한 프로토콜은 다음과 같이 재전송 공격, 스푸핑 공격, 위치 트래킹 공격에 안전하다.

(1) 재전송 공격(replay attack): 재전송 공격은 수동적 공격자가 과거에 리더와 태그 사이에 통신한 내용들을 도청한 후 이를 재전송하여 합법적인 태그 또는 리더로 인증 받으려는 공격이다. 제안한 프로토콜의 임의의 세션에서 공격자가 리더와 태그 사이에서 전송되는 정보를 모두 도청한 후, 다음 세션에서 정당한 리더나 태그로 위장을 시도하는 재전송 공격을 수행한다고 가정하자. 제안한 프로토콜에서는 매 세션마다 리더가 생성하는 새로운 난수 R 과 태그가 생성하는 새로운 난수 T를 이용하여 백-엔드 데이터베이스에 의해 인증을 수행하기 때문에, 과거에 공격자에 의해 재전송된 난수 값들은 백-엔드 데이터베이스의 인증 과정 중에 쉽게 검출된다. 즉, 이전 세션의 난수를 알고 있는 공격자라 하더라고 새로운 세션에서의 난수를 알지 못하면 리더에게 정당한 태그인 것처럼 위장하여 속이는 것은 불가능하다. 따라서 제안한 프로토콜은 재전송 공격에 안전하다.

(2) 스푸핑 공격(spoofing attack): 스푸핑 공격은 공격자가 정당한 태그로 위장하여 리더로부터 인증에 필요한 정보를 획득하거나, 정당한 리더로 위장하여 태그로부터 인증에 필요한 정보를 획득하여 이를 이용하여 정당한 태그 또는 리더로 인증 받는 공격이다. 제안한 프로토콜에서 공격자가 백-엔드 데이터베이스와 태그 간에 공유된 비밀키 값인 ID를 얻을 수 있으면, 리더 또는 태그로의 스푸핑 공격을 성공할 수 있다. 하지만 제안한 프로토콜에서 공개 통신 채널 상으로 전송되는 정보들인 {$h(ID\oplus S)$, T, R}을 이용하여, 공격자는 백-엔드 데이터베이스와 태그 내에 각각 안전하게 저장하고 있는 비밀키 값인 ID를 직접적으로 얻을 수 있는 방법이 없다. 또한 송수신되는 통신 메시지 $h(ID\oplus S)$내의 비밀키 값인 ID는 난수 T와 R 그리고 안전한 일방향 해쉬 함수에 의해 보호되어져 있다. 따라서 제안한 프로토콜은 스푸핑 공격에 대해 안전하다.

(3) 위치 트래킹 공격(Location Tracking Attack): 위치 트래킹 공격은 공격자가 태그의 위치변화를 감지함으로 인해 태그 소유자의 이동 경로를 파악하여 사용자의 프라이버시를 침해하는 공격이다. 제안한 프로토콜에서는 YA-RFID 인증 프로토콜과 달리 태그 측에서도 난수를 생성하여 인증에 이용한다. 즉, 난수 T와 R에 의해 계산

된 $S=h(R\oplus T)$와 $h(ID\oplus S)$는 매 세션마다 변경되기에 공격자는 현재 세션에서 태그의 응답이 과거 세션에 도청한 응답과 동일한지를 비교할 수 없다. 즉, 매 세션마다 서로 다른 난수 T와 R에 생성함으로, 매 세션마다 서로 다른 두 개의 응답이 동일한 태그로부터 송신된 것인지 여부를 쉽게 구별할 수 없음으로, 태그의 이동경로를 쉽게 추적을 할 수 없을 뿐만 아니라, 특정한 태그를 식별할 수 없기에 위치 트래킹 공격을 수행 할 수 없다. 이로 인해 사용자의 프라이버시 보호할 수 있다. 따라서 제안한 프로토콜은 위치 트래킹 공격에 안전하다.

<표 1>은 제안한 프로토콜과 YA-RFID 인증 프로토콜과의 안전성을 비교한 표이다. <표 1>과 같이 제안한 프로토콜은 YA-RFID 인증 프로토콜과 비교하여 재전송 공격, 스푸핑 공격, 그리고 위치 트래킹 공격 등에 안전하여 보다 강한 보안성을 제공함을 알 수 있다.

<표 1> 보안성 비교

프로토콜 / 공격유형	YA-RFID 인증 프로토콜	제안한 RFID 인증 프로토콜
재전송 공격	안전함	안전함
스푸핑 공격	안전함	안전함
위치 트래킹 공격	안전하지 않음	안전함

6. 결론

본 논문에서는 최근에 Yang과 An이 제안한 YA-RFID 인증 프로토콜이 여전히 위치 트래킹 공격에 취약함을 증명하였으며, 더 나아가 동일한 연산 효율성을 보장하며 위치 트래킹 공격을 막을 수 있는 간단히 개선된 일회성 난수와 안전한 일방향 해쉬 함수 기반의 RFID 인증 프로토콜을 제안하였다. YA-RFID 인증 프로토콜과 비교하여 제안한 RFID 인증 프로토콜은 동일한 연산 효율성을 보장하며 보다 높은 안전성을 제공한다. 향후 연구로는 전방향 보안성을 고려한 RFID 상호 인증 프로토콜 개발을 통한 실용적인 RFID 시스템 개발에 목표를 둔다.

7. 감사의 글

본 연구는 2단계 두뇌한국 21 프로젝트(2009)의 연구결과로 수행되었습니다.

참고문헌

[1] F. Klaus, “RFID Handbook”, Second Edition, Jone Willey & Sons, 2003.

[2] S.A. Weis, "Security an Privacy in Radio-Frequency Identification Devices”, MS Thesis. MIT. May, 2003.

[3] 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. 201-212, Springer-Verlag Heidelberg, 2004.

[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] A. Juels and R. Pappu, “Squealing Euros: Privacy Protection in RFID-enabled Banknotes”, In proceedings of Financial Cryptography-FC'03, Vol. 2742 LNCS, pp. 103-121, Springer-Verlag, 2003.

[6] A. Juels, R. L. Rivest, M Szydlo “The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy”, In Proceedings of 10th ACM Conference on Computer and Communications Security, CCS 2003, pp. 103-111, 2003.

[7] S. Junichiro, H. Jae-Cheol and S. Kouichi, “Enhancing Privacy of Universal Re-encryption Scheme for RFID Tags”, EUC 2004, Vol. 3207 LNCS, pp. 879-890, Springer-Verlag, 2004.

[8] S.A. Weis, S. Sarma, R. Rivest, D. Engels, “Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems”, Security in Pervasive Computing 2003, LNCS 2802, pp. 201-212, Springer-Verlag, 2004.

[9] 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.

[10] 이근우, 오동규, 곽진, 오수현, 김승주, 원동호, “분산 데이타베이스 환경에 적합한 Challenge-Response 기반의 안전한 RFID 인증 프로토콜”, 한국정보처리학회 논문지C, 제12-C권, 제03호, pp. 309-316, 2005.

[11] 양형규, 안영화, “유비쿼터스 컴퓨팅 환경에 적합한 RFID 인증 프로토콜에 관한 연구”, 전자공학회논문지, 제42권, 제CI-1호, pp. 45-50, 2005.

[12] 최은영, 최동희, 임종인, 이동훈, “저가형 RFID 시스템을 위한 효율적인 인증 프로토콜”, 정보보호학회논문지, 제15권, 제05호, pp. 59-71, 2005.

[13] 이영진, 정윤수, 서동일, 이상호, “부분ID를 이용한 읽기전용 RFID태그 인증프로토콜”, 한국정보처리학회 논문지 C, 제13-C권, 제05호, pp. 595-600, 2006.10.

[14] 김대중, 전문석, “일회성 난수를 이용한 안전한 RFID 상호인증 프로토콜 설계”, 정보과학회논문지, 정보통신, 제35권, 제03호, pp. 243-250, 2008.

[15] 강수영, 박종혁, 이덕규, “유비쿼터스 환경에서의 RFID 보안 기술 및 산업 동향에 관한 고찰”, 보안공학연구논문지, Vol. 5, No. 2, pp. 53-68, May 2008.

[16] 강부중, 임을규, “RFID 시스템을 위한 상호 인증 프로토콜”, 보안공학연구논문지, Vol. 5, No. 4, pp. 13-22, November 2008.

[17] A.J. Menezes, P C. Oorschot, and S.A. Vanstone, “Handbook of Applied Cryptography", CRC Press, New York, 1997.

[18] B. Schneier, “Applied Cryptography Protocols", Algorithms and Source Code in C, 2nd edn. John Wiley, Chichester, 1995.