해시 체인 보안 취약성을 개선한 RFID 인증 프로토콜

김승빈, 이택, 이명락, 인호
고려대학교 정보통신대학 컴퓨터전파통신공학부
{consoli, comtaek, lmr2010, hoh_in}@korea.ac.kr

RFID Authentication Protocol of Improved Secure Weakness in Hash-chain Based Scheme

Seungbin Kim, Taek Lee, Myoungrak Lee, Hoh In
College of Information and Communication, Korea University

요 약

RFID 는 자동 객체 식별 기술로써 유비쿼터스 환경과의 연결을 통해서 적용 범위가 더욱 확대되고 있다. 그러나 RFID 시스템은 전파를 이용하는 통신 구조와 낮은 태그 가격 제약으로 인해서 사용자의 프라이버시 문제와 악의적인 공격 노출 등의 위험이 발생하고 있다. 이런 문제점들을 해결하기 위해 물리적인 방법과 암호학적인 접근 방법 등 많은 방법들이 제안되었다. 그 중에서 해시 체인 기법은 다른 방법과 비교하여 강력한 보안 수준을 제공하면서도 간단한 인증 과정이 장점이다. 그러나 재전송 공격과 스푸핑 공격에 취약한 문제점을 가지고 있다. 따라서 본 논문은 기존 해시 체인의 장점을 유지하면서 보안 취약성을 개선한 RFID 인증 프로토콜을 제안한다. 계산 효율성을 고려하여 최소한의 난수와 비트 연산(XOR)을 이용하여 보안 취약성을 개선한다.

1. 서론

RFID 는 IC 칩과 무선 주파수를 이용하여 다양한 개체의 정보를 관리할 수 있는 인식기술이다[1]. RFID 는 비접촉식이며 이동중인식이 가능하고, 장애물 투과가 가능한 특징을 가지기 때문에 유비쿼터스 환경에서 중요한 기술로 주목 받고 있다. RFID 시스템은 전파를 이용하여 통신하며 리더와 태그의 계산 성능 제약을 갖는다. 이러한 특성으로 인해서 과도한 정보 누출, 위치 추적 등과 같은 사용자의 프라이버시 침해가 우려되며 악의적인 사용자에 의한 공격과 같은 보안 문제가 발생할 수 있다. 따라서 상위의 문제점들을 해결하기 위해서 킬 명령, 신호 방해 등과 같은 물리적인 방법과 해시 함수 기반, 재 암호화, 비트 연산(XOR) 기반 등과 같은 암호학적 접근 방법이 제안되었다[2,3,4,5,6,7].

그 중에서 암호학적 접근 방법인 해시 기반 방법은 한 방향 함수(One-way function)를 이용하기 때문에 강력한 보안 수준을 보이면서도 효율적인 계산량과 간단한 인증 구조를 가지는 장점이 있다. 특히 해시 체인 기법은 다른 암호화 방법에 비해서 위치추적이 불가능하고 트래픽 분석 공격에 가장 안전하다[5]. 그러나 인증 값이 보호되지 않으며 상호간의 확인 과정이 없기 때문에 스푸핑 공격, 재전송 공격에 취약한 문제점이 있다.

본 논문은 기존 해시 체인의 장점을 유지하면서 보안 취약성을 개선한 RFID 인증 프로토콜을 제안한다. 계산 효율성을 고려하여 최소한의 난수와 비트 연산을 이용하여 보안 취약성을 개선한다.

논문의 구성은 다음과 같다. 2 장에서는 RFID 시스템의 보안 요구사항에 대해 설명하며, 3 장에서는 기존에 제안된 RFID 프로토콜의 보안 방식에 대해서 알아보고 그의 한계점을 설명한다. 그리고 4 장에서는 해시 체인의 보안 취약성을 개선한 제안 프로토콜에 대해서 설명하며, 5 장에서는 제안 프로토콜의의 안전성을 분석한다. 마지막으로 6 장에서는 결론을 맺는다.

2. RFID 시스템 보안 요구사항

RFID 시스템은 일반적으로 그림 1 과 같이 태그(Transponder)와 리더(Trans-ceiver), 후위 서버(Backend server)로 구성된다. 태그는 부착된 물품의 정보를 가지고 있으며, 리더는 태그와의 무선 통신을 통해 태그의 정보를 수집한다. 태그와 리더의 통신 구간은 안전하지 않은 것으로 간주되며, 통신 보안 방법이 필요하다[1]. 리더는 태그에게 정당한 리더임을 알리고, 태그가 정당한 태그인지 확인하기 위해서는 많은 처리과정이 필요하다. 그래서 리더의 약한 처리 능력을 대신하여 후위 서버가 대신처리하며, 서로의 통신구간은 안전한 구간으로 간주한다.

RFID 시스템은 태그와 리더간의 무선 통신으로 인증이 이루어지기 때문에 여러 위협에 노출되기 쉽다. 따라서 다음과 같은 보안 위협에 대해 안전한 보안 방법이 필요하다[8,9,10].

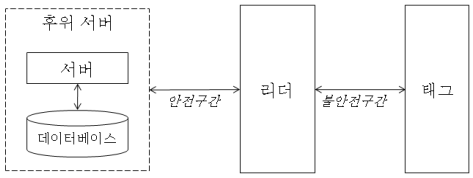

그림 1. RFID 시스템

• **위치 추적 공격 :** 공격자가 태그의 위치 변화를 알아내어 태그의 이동 경로 파악할 수 있다. 태그가 동일한 태그인지 알 수 없도록 통신 값이 매번 달라지는 방법이 필요하다.

• **트래픽 분석 공격 :** 공격자가 리더와 태그간의 정보를 도청하여 비밀 정보와 그렇지 않은 정보를 구분할 수 있다. 태그 정보 전송 시 암호화를 통한 송수신 방법이 필요하다.

• **재전송 공격 :** 공격자가 리더와 태그 사이의 통신을 도청한 후, 이를 재전송하여 정당한 태그나 리더로 인증을 시도한다. 도청된 전송 정보로부터 식별 정보를 얻을 수 없어야 하며, 인증할 때 마다 태그의 전송 정보가 변경되어야 한다.

• **스푸핑 공격 :** 공격자가 정상적인 리더나 태그로 위장하여, 태그 정보를 수집하거나 리더에게 특정 태그인 것처럼 행동한다. 리더와 태그간의 통신과정에서 서로 올바른 개체인지 상호 인증하는 방법이 필요하다.

3. 관련 연구

RFID 시스템에서 2 장과 같은 공격행위로부터 프라이버시를 보호하고 보안 문제들을 해결하기 위해서 많은 암호학적 접근 방법들이 제안되었다[5,6,7,8,9,10]. 그 중에서 해시 기반 기법은 한 방향 특성을 가지는 해시 함수를 이용하기 때문에 강력한 암호화 수준을 제공하면서도 효율적인 계산량과 간단한 인증과정을 보이는 것이 장점이다. 대표적으로 해시 락 프로토콜, 확장된 해시 락 프로토콜, 해시 체인 기법 등이 있다.

• **해시 락 프로토콜 :** 이 방식은 리더의 요청에 대해서 잠김(locked) 상태일 때는 실제 ID 값이 아닌 metaID 값을 전송하고, 풀림(unlocked) 상태일 때 실제 ID 값을 전송하여 사용자의 프라이버시를 보호한다[4]. 리더는 태그의 key 값과 metaID 값을 가지고, 태그로부터 수신된 metaID 값과 key 값을 해시한 결과가 일치할 때만 정당한 것으로 판단한다(metaID = hash(key)). 그러나 공격자가 리더와 태그간의 도청을 수행하여 태그의 ID 값을 얻을 수 있고, 태그는 리더의 요청 시 항상 동일한 metaID 를 사용하기 때문에 위치 추적이 가능한 단점이 있다.

• **확장된 해시 락 프로토콜 :** 이 방식은 랜덤 해시 락 프로토콜로도 불리며, 위치 추적이 가능한 해시 락 프로토콜의 문제점을 개선하였다[4]. 의사난수생성기를 이용하여 생성한 난수와 자신의 ID 를 해시한 결과를 리더에게 전송하기 때문에 난수에 의해서 전송 값이 매번 변경되어 위치 추적이 불가능하다. 그러나 인증 마지막 단계에서 ID 노출 가능성이 있으며, 공격자가 도청을 통해 획득한 값을 재전송하여 사용할 수 있는 문제점이 있다.

• **해시 체인 기법 :** 이 방법은 그림 2 와 같이 태그가 두 개의 해시 함수를 이용하여 하나는 자기의 값을 변경시키고 다른 하나는 인증 값을 변화시켜 리더의 요청에 대해서 매번 다른 응답으로 인증한다[5]. 태그는 리더에게 매번 다른 응답 값을 전송하므로 공격자가 태그의 응답 값을 이용하여 동일한 태그인지 판단할 수 없는 장점이 있다. 서버는 태그로부터 수신한 인증 값을 확인하기 위해서 초기 시드 값을 바탕으로 응답 값을 계산한다. 그래서 공격자가 통신을 도청하여 태그의 i-1 번째 응답을 저장한 후 리더의 i 번째 요청 시 저장된 태그의 이전 응답 i-1 을 사용할 경우 인증이 가능하다. 따라서 스푸핑 공격에 취약한 문제점이 있다.

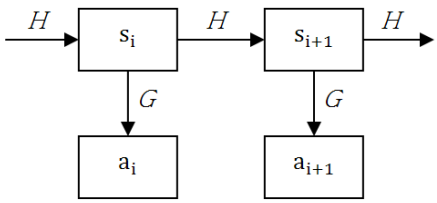

그림 2. 해시 체인 기법

4. 해시 체인 기반 인증 프로토콜

3 장의 관련 연구들은 2 장의 보안 요구 사항들을 일부만 만족한다. 따라서 본 논문은 다음과 같이 해시 체인의 취약성을 개선한 안전한 인증 프로토콜을 제안한다.

4.1. 보안 개선 프로세스

태그와 리더의 메시지는 매번 인증 시마다 새로운 난수를 선택하고, 이 값과 인증 값을 비트 연산(XOR)하여 암호화한다. 또한 동일한 해시 함수를 사용하여 인증 값을 생성하며, 상대방으로부터 수신한 값과 자신의 저장된 값이 서로 일치하였을 때 상대방을 유효한 대상으로 인증한다. 태그와 리더의 인증은 리더가 태그에게 올바른 리더임을 알리는 전송 메시지와 태그가 리더에게 자신의 인증 값을 전송하는 메시지로 구성된다.

리더는 태그에게 올바른 리더임을 알리기 위해서 이전 인증 값 $G(s_{i-1})$를 전송한다. 태그는 이 값과 자신의 저장된 이전 인증 값을 비교하여 같을 경우 유효한 리더로 판단한다. 이를 위해서 리더는 $G(s_{i-1})$를 난수 R 과 비트 연산하여 암호화한 후 전송한다. 이 값은 난수 생성기에 의해서 매 새션마다 새롭게 생성되는 난수 R 에 의해서 값이 달라진다. 그리고 리더

는 R 을 유일한 값 SEED 와 비트 연산한 값을 태그에게 전송하기 때문에, 태그는 리더와 공통적으로 알고 있는 SEED 를 이용하여 R 을 추출한 후 R 로 다시 $G(s_{i-1})$을 구한다. 이 과정은 두 값으로 비트 연산된 결과 값은 어느 한 값으로 다시 비트 연산하면 다른 값을 얻을 수 있는 비트 연산 원리를 이용한다

($A \oplus B = C \rightarrow C \oplus A = B$). 따라서 SEED 를 모르는,

다시 말해서 서로 등록된 정상 태그가 아니면 R 을 얻을 수 없다.

태그가 리더에게 올바른 태그임을 알리는 메시지는 인증 값 $G(s_i)$이다. 리더는 이 값과 자신의 저장된 값을 비교하여 일치할 경우 유효한 태그로 판단한다. 태그가 전송하는 메시지는 리더가 올바른 리더였을 때 진행되는 단계이며, i 번째 통신 시 s_i 값을 해시 함수 H()로 자신의 값을 갱신한 후 리더에게 해시 함수 G()를 사용하여 전송한다. 태그는 전송 메시지 암호화를 위해서 $G(s_i)$와 앞 단계에서 리더로부터 얻은 R 로 비트 연산하여 리더에게 전달한다. 리더는 이 값을 자신이 앞 단계에서 생성했던 R 을 이용하여

$G(s_i)$을 얻는다($R \oplus G(s_i) \oplus R = G(s_i)$). 만약 $G(s_i)$를 추

출할 때 R 을 사용하여 얻은 값과 태그가 계산한 R

이 다를 경우 $R \oplus G(s_i)$에서 얻는 $G(s_i)$가 완전히 달라

진다. 따라서 정상 값을 이용하지 않으면 원래 값을 얻을 수 없다.

4.2. 인증 프로토콜

제안 프로토콜은 등록, 인증, 검증과정으로 이루어지며, 등록과정이 선행된 후 인증과 검증단계를 통해서 서로간의 통신을 수행한다. 등록과정은 리더와 태그 간의 인증을 위한 값들을 미리 저장하는 과정으로 최초 한 번만 수행된다. 공통적으로 태그 식별 번호 PIN, 유일한 값 SEED, 인증 해시 함수 G(), 태그 ID 를 가지고 있다. 리더와 서버는 새로운 난수 R 을 생성하기 위한 난수생성기를 가지며, 태그는 자신의 값 갱신을 위한 해시 함수 H()를 갖는다. 인증과 검증과정은 서로 올바른 리더와 태그인지 확인하고, 데이터를 주고받는 실질적인 인증 프로세스로써 그림 3 과 같이 8 단계로 이루어진다.

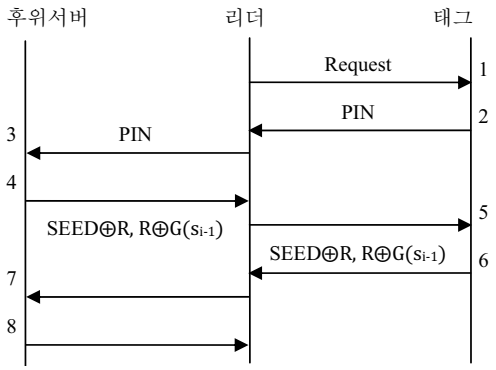

그림 3. 제안 프로토콜 인증 과정

단계 1 : 리더는 태그 정보를 요청한다.

단계 2 : 태그는 자신의 PIN 을 전송한다.

단계 3 : 리더는 등록된 태그인지 확인하기 위해 서버에게 PIN 을 전송한다. 서버는 태그로부터 수신한 PIN 과 저장된 리스트를 비교하여 등록된 태그인지 확인한다. 등록된 태그일 경우 태그의 ID 를 얻기 위해 태그와의 i 번째 인증을 진행한다.

단계 4 : 서버는 태그에게 정당한 리더라는 것을 확인시키기 위해서 i-1 번째 인증 값이었던 $G(s_{i-1})$를 전송한다. 이 값은 비트 연산된 두 개의 값으로 태그에게 전송된다. SEED 를 새롭게 선택된 난수 R 과 비트 연산한 결과 값을 구하고, R 과 $G(s_{i-1})$를 비트 연산한 결과 값을 구해서 리더에게 전송한다.

단계 5 : 리더는 서버로부터 수신한 값을 태그에게 전송한다. 태그는 리더로부터 수신한 값으로부터 $G(s_{i-1})$를 추출하여 정상 리더인지 확인한다. 수신된 첫 번째 값을 SEED 로 비트 연산하여 R 을 구한다

($SEED \oplus R \oplus SEED = R$). 그리고 두 번째 수신 값을 R

로 비트 연산하여 $G(s_{i-1})$를 구한다($R \oplus G(s_{i-1}) \oplus R =$

$G(s_{i-1})$). 태그는 리더로부터 받은 $G(s_{i-1})$과 자신의 $G(s_{i-1})$이 일치하는지 비교하여 유효한 리더인지 확인한다. 올바른 리더일 경우 태그는 해시함수 H()를 이용하여 하여 자신의 비밀 값을 갱신한다 $H(s_i)$. 그리고 리더와의 인증을 위해서 해시함수 G()를 이용하여 인증 값을 구한 후 리더로부터 얻은 R 과 비트 연산

하여 암호화 한다($R \oplus G(s_i)$).

단계 6 : 태그는 리더에게 인증 값을 암호화하여 전송한다.

단계 7 : 리더는 태그로부터 수신 받은 값을 서버에게 전송한다. 서버는 태그로부터 수신한 값에서 인증

$G(s_i)$를 추출하여 유효한 태그인지 확인한다. 단계 4에서 선택한 R 로 비트 연산하여 $G(s_i)$를 추출한다 ($R \oplus G(s_i) \oplus R = G(s_i)$). 그리고 추출한 $G(s_i)$과 저장된 자신의 $G(s_i)$와 일치하는지 확인한다.

단계 8: 일치할 경우, 다시 말해서 유효한 태그일 경우 서버는 리더에게 태그 ID 를 전송하고, 프로세스를 완료한다.

5. 보안 요구사항 검증

제안한 프로토콜은 2 장에서 언급한 RFID 시스템의 보안 위협에 대해서 모두 안전하다.

- **위치 추적 공격 :** 태그와 리더 사이에 주고받는 메시지는 매 세션마다 바뀌는 R 과 인증 시마다 변경되는 $G(s_i)$의 비트 연산 결과이다. 이 값은 매번 다른 값을 가지기 때문에 도청된 정보를 가지고 동일한 태그인지 구분할 수가 없어 위치 추적이 불가능 하다.
- **트래픽 분석 공격 :** 공격자가 정상적인 리더나 태그로 가장하여 도청할 경우 R 또는 $G(s_i)$를 알아야만 인증에 필요한 정보를 얻을 수 있다. 그러나 R 값은 이전 단계 통신에서 $SEED \oplus R$ 로 암호화되며, $G(s_i)$은 $G(s_{i-1})$을 알아내도 해시 함수 G()가 없으면 계산할 수 없다. 따라서 전송 메시지를 이용하여 트래픽 분석 공격을 할 수 없다.
- **재전송 공격 :** 태그와 리더의 인증은 해시 함수로 인증 값이 매번 변경되며 난수 R 에 의해서 $P_i \oplus R$ 값이 항상 바뀐다. 그러므로 이전 인증 과정에서 인위적으로 실패한 후 획득한 정보를 다음 인증 값으로 이용하여 인증할 수 없다. 따라서 인증 과정에서 태그나 리더의 송수신 데이터를 이용한 재전송 공격이 불가능 하다.
- **스푸핑 공격 :** 메시지는 비트 연산으로 암호화하여 전송되며, 인증 단계에서 $G(s_{i-1})$과 $G(s_i)$를 비교하여 서로 올바른 개체인지 확인한다. 따라서 공격자가 정상적인 리더나 태그로 위장하여 데이터를 수신하더라도 그 안의 값을 얻어낼 수 없으며, 인증 결과 값이 일치해야만 다음 단계가 진행되므로 스푸핑 공격을 할 수 없다.

표 1 은 3 장의 해시 기반 프로토콜들과 제안 프로토콜의 안전성을 비교 분석한 결과이다. 제안 프로토콜이 기존 프로토콜보다 안전한 결과를 보인다. 제안 프로토콜은 안전한 통신을 위해서 서버에서 한 번의 난수 생성과 두 번의 비트 연산으로 메시지를 암호화한다. 그리고 태그에서 한 번의 비트 연산으로 메시지를 암호화하여 통신한다.

표 1. 기존 프로토콜들과의 안전성 비교

	해시락	확장된 해시락	해시 체인	제안
위치 추적 공격	X	O	O	O
트래픽 분석 공격	X	X	O	O
재전송 공격	X	X	X	O
스푸핑 공격	X	X	X	O

O : 안전, X : 불안전

6. 결론

본 논문은 난수와 비트 연산을 이용하여 해시 체인의 보안 취약성을 개선한 RFID 인증 프로토콜을 제안하였다. 제안 방법은 프로토콜 통신 시간 복잡도를 고려하여 최소한의 계산량으로 보안 요구사항을 충족한다. 그 결과 기존의 해시 체인 기법의 장점을 모두 만족할 뿐만 아니라 해시 체인 기법의 보안 취약점인 재전송 공격과 스푸핑 공격에 대해 모두 안전한 결과를 보였다.

참고문헌

[1] CM Roberts, “Radio frequency identification”, Computers & Security, 2006

[2] Junko Yoshida, “RFID Backlash Prompts ‘Kill’ Feature”, EETimes, 2003

[3] A. Juels, R. L. Rivest and M. Szydlo, “The Blocker Tag : Selective Blocking of RFID Tags for Consumer Privacy”, CCS 2003, 2003

[4] S. A. Weis, S. Sarma, R. Rivest, and D. Engels, “Security and privacy aspects of low-cost radio frequency identification systems”, LNCS, 2004

[5] M Ohkubo, K Suzuki, S Kinoshita, “Cryptographic approach to “privacy-friendly” tags”, RFID Privacy Workshop, 2003

[6] P Peris-Lopez, JC Hernandez-Castro, JM Estevez, “LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags”, 2nd Workshop on RFID Security, 2006

[7] L Batina, J Guajardo, T Kerins, N Mentens, P Tuyls, “Public-Key Cryptography for RFID-Tags”, PerSec Conference, 2007

[8] 이영진, 문형진, 정윤수, 이상호, “랜덤 부분 ID 를 이용한 저비용 RFID 상호인증 프로토콜”, 한국통신학회, 2006

[9] 박진성, 최명렬, “고기능 RFID 태그를 위한 동적 ID 할당 프로토콜”, 한국정보보호학회, 2005

[10] 김배현, 유인태, “반사공격에 안전한 RFID 인증 프로토콜”, 한국통신학회, 2007