난수를 이용한 RFID 태그-리더의 상호 인증 기법

신동훈*, 유수정*, 송주석*
*연세대학교 컴퓨터과학과
neweast@emerald.yonsei.ac.kr

Mutual Authentication Protocol of RFID Tag & Reader Using Random Number

Dong-Hun Shin*, Su-Jung Yu*, Joo-Seok Song*
*Dept of Computer Science, Yonsei University

요 약

RFID(Radio Frequency Identification), 즉, 무선 주파수 인식 기술은 주파수를 이용하여 개별 상품을 식별하는 방식을 일컫는다. 바코드나 스마트카드에 비하여 우수한 특성에 의해 다양한 응용이 가능하여, 향후 유비쿼터스 환경을 구축하는 데 핵심적 역할을 할 것으로 보인다. 그러나 이러한 환경을 제대로 갖추기 위해서는 보안 기술이 필수적이다. 작고 가벼움을 필수조건으로 하는 RFID에서는 기존의 보안 기술을 그대로 적용하기 어렵기 때문에 보다 가볍고 안전한 RFID 보호 프로토콜이 요구된다. 본 논문에서는 태그와 리더가 각각 난수를 생성함으로써 기존의 인증 프로토콜보다 적은 연산만으로도 서로를 안전하게 인증하는 기법을 제시한다.

1. 서론

RFID(Radio Frequency IDentification)는 전자 태그(Tag)를 사물에 부착하여, 사물이 주위 상황을 인지하고 기존 IT 시스템과 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 물류유통, 군사, 식품안전 등 비즈니스 영역에 킬러 애플리케이션으로서 막대한 파급효과를 끼칠 전망이다.

그러나, RFID 시스템은 그 유용성에도 불구하고, 비접촉식 인식 시스템이라는 특징 때문에 안정성과 프라이버시 보호 측면에서 문제점을 지니고 있다. 기본적으로 무선 통신을 이용하기 때문에, 도청과 위치 추적 등의 공격에 노출되기 쉽고, 이에 따라 리더(Reader)와 태그(Tag) 사이의 안전한 상호인증이 매우 중요하다.

또한 RFID 태그에서는 사용할 수 있는 자원의 양이 매우 제한적이다. 그렇기 때문에 기존의 암호학적 기법을 RFID 보안에 사용하는 것은 불가능하고, 자원소모를 최소화시킬 수 있는 인증기법이 필수적이다.

본 논문에서는 기존에 연구되었던 몇 가지 RFID의 인증기법에 대해서 알아보고, 그 기법들의 장,단점에 대해서 설명한다. 그리고 저가형 태그에서 적용될 수 있는 효율적이고 안정성 높은 인증 기법을 제안한다.

2. 관련연구

앞서 말했듯이 RFID는 태그에서 자원양의 한계 때문에 기존의 암호학적 기법을 사용하지 못한다. 그렇기 때문에 많은 자원을 사용하지 않고 기밀성을 유지시키는 방법이 그동안 계속 연구되어왔다.

† 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음.

Weis 등은 해쉬 함수의 단방향성을 이용한 Hash Lock 기술을 제안하였다[4]. Hash Lock 기술에서 리더는 임의로 선택한 키 K를 해쉬한 h(K)를 메타ID로 만들고 이를 데이터베이스에 저장한다. 그리고 리더가 태그에게 메타ID를 보내면 태그는 이를 저장하고 잠김 상태가 된다. 잠김 상태를 풀기 위하여 리더가 태그에게 쿼리를 보내면 태그는 저장되어 있는 메타ID를 리더에게 보내고, 리더는 데이터베이스에서 메타ID에 해당하는 ID와 키값 K를 가져온다. 리더는 태그에게 키를 보내고 태그는 이 키를 해쉬해서 그 결과값이 자신의 메타ID와 동일하다면 태그는 잠김 상태가 풀리고 주위의 리더에게 반응하게 된다.

이 기술은 낮은 비용에 비해 높은 신뢰성을 보인다는 장점이 있다. 그러나 공격자가 메타ID를 통해 태그를 쉽게 추적할 수가 있다. 게다가 키 K가 공기중에 그대로 노출됨으로써 공격자가 이 키를 취득한 후 위장공격을 하는 것이 가능하다.

Weis 등은 같은 논문에서 Hash Lock의 보다 발전된 형태로 Randomized Hash Lock 기술을 제안하였다[4]. 이 기술에서 태그는 랜덤한 숫자 r을 생성하고, 리더로부터 쿼리를 받으면 (r, $h(ID, r)$)을 응답한다. 그 후 리더는 데이터베이스로부터 모든 ID를 받아 이를 검색하여 ID와 r을 해쉬한 것과 동일한 ID를 찾아서 태그에게 보낸다.

이 방법에서는 매번 태그의 응답이 달라지므로 위치추적으로부터 태그를 보호할 수 있다. 그렇지만 공격자가 태그에 쿼리를 보냄으로써 (r, $h(ID, r)$)을 얻을 수가 있고, 이는 태그를 위장하는 데에 이용될 수가 있다.

Ohkubo 등은 해쉬 체인을 이용하여 전방위 안전성(forward security)과 위치트래킹 공격에 안전한 프로토콜을 제안하였다[5]. 이 기법의 기본적 아이디어는 태그가 쿼리를 받을 때마다 아이디를 변경하여 인증된 사용자만 태그를 인증할 수 있도록 하는 것이다. 이 기법은 두 개의 해쉬 함수를 사용하는데, 하나는 태그의 비밀 정보를 새로 고치는데 사용되고, 나머지 하나는 태그의 응답을 도청자로부터 추적불가능하게 만드는 데 사용된다.

이 방법에서 태그는 전방위 안전성이 보장되고, 위치트래킹으로부터 안전하지만, 효율성에서 치명적인 약점을 가지고 있다. 하나의 태그를 판별하기 위해서는 데이터베이스에서 태그의 초기 비밀값을 토대로 각각의 태그마다 n번의 해쉬연산을 계산해야 하기 때문이다. 더구나 해쉬체인 기법은 일방향 인증으로 태그는 리더를 인증하지 못하는 문제점이 있어서 태그가 리더의 명령을 수행하는 데에 있어서 문제가 발생하게 된다[7]. 그리고, 공격자가 태그에 쿼리를 보내어 태그의 응답을 받은 후 그것을 재전송해 자기 자신을 인증하는 데에 사용하는 것이 가능하다는 취약점도 있다.

3. 제안 프로토콜

본 논문에서는 기존 논문들이 갖고 있던 보안상의 취약점을 보완하고, 아울러 태그와 데이터베이스에서의 계산량을 줄인 가볍고 안전한 프로토콜을 제안한다.

제안 프로토콜에서 데이터베이스와 태그는 같은 해쉬함수 $h()$를 갖고 있다. 그리고 리더와 태그는 각각의 난수생성기 RNG(Random Number Generator)를 갖고 있다. 데이터베이스는 태그들의 현재 ID가 기록되어 있는 ID 필드, 그리고 그 태그들의 직전 ID가 기록되어 있는 ID^{-1} 필드로 이루어져 있다. 최초에 ID^{-1} 필드에는 아무것도 기록되지 않는다.

제안하는 프로토콜의 인증 과정은 다음과 같다. (그림1 참조)

(1) 리더는 랜덤 넘버 r_1을 생성한 후 이 r_1과 함께 태그에 질의를 보낸다.

(2) 태그는 또다른 랜덤 넘버 r_2를 생성하고 태그의 주어진 아이디 ID_i에 r_1과 r_2를 XOR 연산하여 그 값을 해쉬한 후 이를 Q에 저장한다. 그리고 r_2와 Q를 함께 리더에 보낸다.

(3) 리더는 태그로부터 받은 Q와 r_2, 그리고 자신이 만든 r_1을 함께 데이터베이스에 보낸다. 데이터베이스에서는 ID필드에 있는 모든 태그의 아이디값에 r_1, r_2를 XOR연산하고 이를 해쉬하여 그 값이 Q와 일치하는지를 검사한다. 일치하는 아이디값을 찾으면 데이터베이스는 태그를 인증하게 되고, 데이터베이스는 해당 아이디에 r_2를 XOR시켜 그 값을 새로운 아이디로 업데이트한다. 이 때 비동기화 문제에 대비하기 위하여 기존의 아이디는 ID^{-1} 필드에 저장한다.

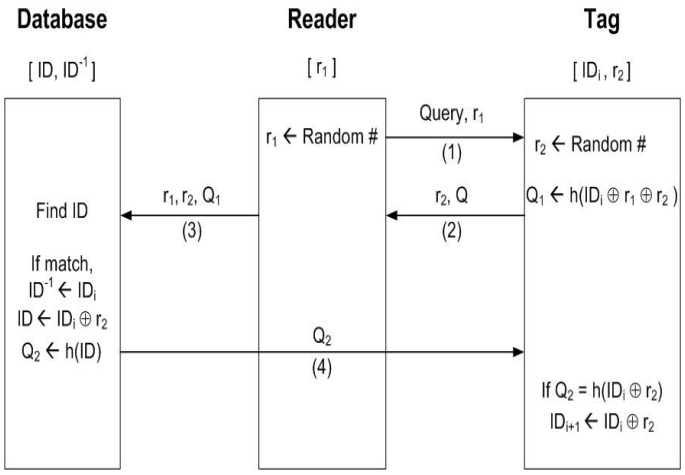

그림 1. 제안 프로토콜

만약, ID 필드에서 해당하는 아이디값을 찾지 못했다면 태그의 직전 아이디들이 저장되어 있는 ID^{-1} 필드에서 해당 아이디를 찾는다. 이 과정에서 검색에 성공한다면 그 값으로 위의 과정을 수행하고, 여기서도 실패한다면 인증이 실패했음을 알린다.

(4) 데이터베이스에서는 업데이트된 아이디를 해쉬하여 그 값을 Q_2에 저장한 후 이를 태그에 보낸다. 태그에서는 기존의 ID_i에 r_2를 XOR시켜서 해쉬한 값이 Q_2와 일치하는지를 검사한다. 일치한다면 태그는 데이터베이스를 인증하게 되고, $h(ID_i \oplus r_2)$를 새로운 아이디로 업데이트한다.

4. 안전성 분석

여기서는 기존에 알려져 있는 RFID에 대한 여러 가지 공격가능성에 대해 제안 기법이 안전함을 보인다.

도청/통신내용분석. 공격자는 태그와 리더, 데이터베이스 사이에서 오가는 메시지들을 엿듣고 그 내용을 취득할 수 있다. 하지만, 오가는 메시지들은 랜덤 넘버인 r_1, r_2 그리고 해쉬의 결과값인 Q_1, Q_2 뿐이다. 해쉬의 일방향성으로 인해 Q값을 통해서 공격자는 아무것도 알아낼 수 없고, 랜덤 넘버들로도 공격자는 태그의 정보를 알아낼 수 없다.

위치트래킹. 제안 프로토콜에서는 태그의 아이디가 매번 지속적으로 업데이트된다. 그렇기 때문에 리더의 질의에 대해 태그의 응답은 매번 바뀌고 아이디가 바뀌는 과정에서 랜덤 넘버를 사용하기 때문에 그 변화를 미리 예측하는 것도 불가능하다. 그렇기 때문에 태그는 위치트래킹 공격에 안전하다.

스푸핑. 공격자가 태그를 위장하려 할 경우 태그의 ID를 모르는 상태에서 (2)를 생성하는 것은 불가능하다. 정당한 태그와 리더 간의 통신 중에 (2)를 가로채더라도, 태그의 아이디가 계속 변화하기 때문에 가로챈 내용을 추후에 사용할 수 없다.

비동기화. 태그와 데이터베이스에서의 아이디 업데이트는 동시에 이뤄지지 않고 데이터베이스에서 먼저, 그리고 태그에서 나중에 이루어진다. 그렇기 때문에 데이터베이스에서 아이디 업데이트가 이루어진 후 (4)를 가로채거나 오염시키는 등의 방법으로 비동기화를 시도하면 데이터베이스와 태그의 아이디가 서로 다른 상태가 되어버린다. 그러나 이러한 상황에도 태그의 아이디는 데이터베이스의 ID^{-1} 필드에 저장이 되어 있다. 태그 인증 과정에서 ID필드에서 아이디를 못 찾는다면 ID^{-1} 필드에서 아이디를 찾게 된다. 이를 통해 태그와 데이터베이스는 비동기화를 비할 수 있다.

5. 결론 및 향후과제

지금까지 기존 RFID 인증 기법과 그 기법의 보안상 취약점에 대해서 알아보았고, 이를 보완하는 우리의 프로토콜을 설명하였다. 안전성 분석을 통해 본 논문에서의 기법이 위치트래킹이나 스푸핑 등 여러 위협으로부터 안전하다는 것을 보였다. 그리고 전체적인 계산량 또한 무리가 없는 수준에서 구현함으로써, 저가형 RFID에도 쉽게 적용이 가능하도록 하였다.

향후에는 리더와 데이터베이스 사이의 통신채널에서의 안전성이 보장되지 않는 경우에도 상호 인증이 가능하도록 프로토콜을 보완하는 연구를 진행할 생각이다.

참고문헌

[1] Gildas Avoine “Cryptography in Radio Frequency Identification and Fair Exchange Protocols” PhD Thesis, 2005

[2] Ari Juels “RFID Security and Privacy: A research Survey” Manuscript, 2005
[3] Tassos Dimitriou “A Lightweight RFID Protocol to protect against Traceability and Cloning attacks” SecureComm, 2005
[4] Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels “Security and privacy aspects of low-cost radio frequency identification systems” International Conference on Security in Pervasive Computing, 2003
[5] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita “Cryptographic Approach to ‘Privacy-Friendly’ Tags” RFID Privacy Workshop, 2003
[6] Ari Juels “Minimalist Cryptography for Low-Cost RFID Tags” International Conference on Security in Communication Networks - SCN, 2004
[7] 이근우, 오동규, 곽진, 김승주, 원동호 “Low-Cost RFID 시스템을 위한 Improved Hash Chain 프로토콜” CISC'S04, 2004