키 교환을 이용한 RFID 상호인증 프로토콜의 설계

임상민*
*(주)리테일테크
e-mail: smrin@naver.com

Design of A RFID Mutual Authentication Protocol using Key Exchange

Sang-Min Lim*
*RetailTech Co.,Ltd

요 약

유비쿼터스 사회를 만들기 위한 핵심 기술인 RFID는 시간과 공간을 초월하여 우리에게 정보를 제공해 줄 것으로 기대되고 있지만, RFID 시스템이 가지고 있는 특성으로 인하여 프라이버시를 침해할 수 있다는 심각한 문제를 안고 있다. 이를 해결하기 위한 방법으로 다양한 연구가 진행되어 왔지만 기존의 연구들은 보안상 문제점과 태그 및 백 엔드 데이터베이스의 과도한 처리능력을 요구하고 있다. 그러나 본 논문에서 제안하는 프로토콜은 해쉬함수와 XOR연산, 키 교환을 이용하여 스푸핑이나, 재전송 공격으로부터 안전 하면서도, 백 엔드 데이터베이스 안에서의 비교연산 횟수를 줄일 수 있는 경량화된 프로토콜을 제안한다.

1. 서론

RFID는 유비쿼터스 컴퓨팅의 가장 근본이 되는 모든 사물을 유일하게 식별할 수 있는 무선 주파수 객체 인식 기술이다. 객체에 RFID 태그가 심어져 있다면 그 객체에 대한 정보를 판독 및 추적 관리가 가능해지기 때문에, 물류 산업 뿐 아니라 의료, 금융, 교통등 다양한 분야에서 높은 활용 가치를 기대하고 있다. 그러나 RFID 태그는 객체를 유일하게 식별한다는 속성을 가지고 있기 때문에, 태그의 소유자가 알지 못하는 사이에 어떤 다른 누군가에 의해 태그 정보가 유출 될 수 있으며, 태그 ID를 추적함으로써 위치정보가 노출될 수 있다는 문제가 발생할 수 있다[1].

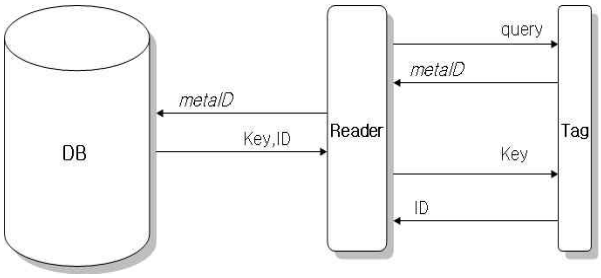
프라이버시 문제를 해결하기 위해 다양한 연구가 진행되어 왔지만, 저가의 RFID 태그가 가지고 있는 제한된 자원과 특성 때문에, 기존의 유·무선망에서 사용한 알고리즘들을 적용할 수 없으며, 간단하면서도 프라이버시 보호가 가능한 프로토콜이 필요하게 되었다. 특히 RFID 태그는 다양한 공격이 가능하지만, 권한이 없는 정당하지 못한 태그나, 리더를 이용하여, 불법적으로 태그 정보를 획득하거나, 태그 정보를 속이는 공격이 가능하므로. 태그와 리더, 리더와 태그사이에는 서로를 인증할 수 있는 매커니즘이 반드시 필요하다[2].

그 중에서도 해쉬함수를 이용하는 기존의 대표적인 인증 매커니즘으로는 해쉬-락기법, 확장된 해쉬-락기법, 해쉬체인 기법, 해쉬 아이디 변형 기법 등이 있다. 그러나 이들 기법은 스푸핑이나 재전송 공격에 취약하다. 본 논문에서 기존의 인증기법의 소개와 문제점을 살펴보고, 태그 안에 구현이 가능한 해쉬함수와 XOR 연산을 이용하여, 태그와 리더사이에 키를 교환하면서 스푸핑이나 재전송 공격에도 강하고, 백 엔드 데이터베이스 많은 연산을 하지 않는 안전성이 높은 프로토콜을 제안한다[2]. 그리고 프로토콜의 안전성을 검증하고, 마지막으로 결론 및 향후 연구 방향을 제시한다.

2. 관련연구

2.1.해쉬-락 기법

그림 1은 해쉬-락의 동작 과정이다. 해쉬-락 기법에서 태그는 랜덤 키를 해쉬한 metaID = H(Key)를 저장한다[1].

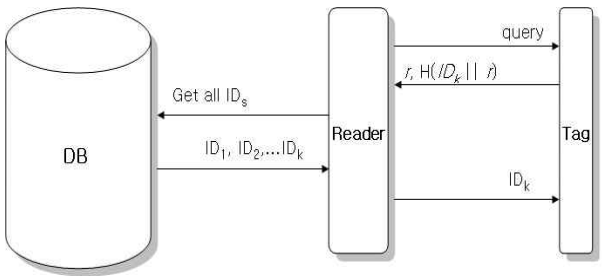


[그림 1] 해쉬-락 기법

리더가 태그에게 접근 요청을 하게 되면, metaID를 리더에게 보낸다. 리더는 metaID를 안전한 채널을 통해 백 엔드 데이터베이스 시스템에 전달하고 태그에 대한 키와 아이디 값을 전달 받는다. 리더는 태그의 키를 다시 태그에게 전달하고 태그는 리더로부터 받은 키에 대한 해쉬값을 계산하여 자신의 metaID와 같은지 비교하여 같을 경우 ID를 리더에게 전달한다. 비록 이 기법은 해쉬를 한번밖에 사용하지 않지만 metaID 값이 항상 일정하기 때문에 태그의 위치를 추적할 수 있다. 또한 정당한 metaID를 수신하였다가, 나중에 metaID를 리더에게 보내는 경우, Key와 ID를 획득할 수 있다는 문제점이 발생할 수 있다.

2.2.확장된 해쉬 - 락 기법

앞의 해쉬-락의 변형 기법으로 난수를 이용하여 태그로부터 리더로 가는 정보는 값이 항상 변하게 한다. 그림 2에서 보는 것과 같이 태그는 난수 r을 발생하여 자신의 ID와 함께 연접한 후 해쉬값을 계산한 뒤 r, H(ID||r)를 리더에게 보낸다[1].

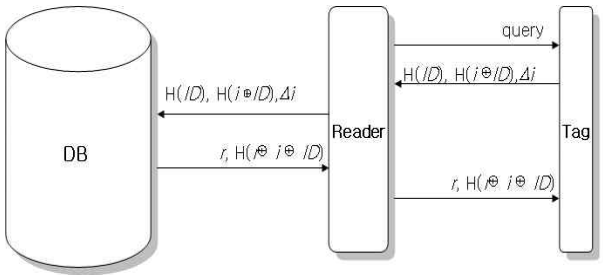


[그림 2] 확장된 해쉬-락 기법

백 엔드 데이터베이스는 이 값을 리더로부터 전달받은 뒤 자신의 DB안에 있는 모든 ID값과 난수 r을 이용하여 태그가 연산한 것과 동일한 값이 있는지 비교하여 같은 것이 있으면 리더에게 ID값을 넘겨준다. 이 기법은 난수를 이용하여 태그에서 리더로 가는 정보가 매번 바뀌므로 스푸핑 공격에는 강하지만 IDk 값이 노출된다는 점과 r, H(IDk || r)을 재전송할 경우 정당한 태그로 가장할 수 있다. 그리고 백 엔드 데이터베이스에서는 태그로부터 온 값과 같은 것이 있는지 모든 식별정보에 대하여 해쉬연산과 비교 연산을 해야 하므로, 서버 측에 부하가 많다. 또한 태그에 난수 발생기를 구현하기에는 게이트 수가 매우 부족하다.

2.3. 해쉬 ID 변형 기법(Protocol of Henrici and Müller)

이 기법은 해쉬 함수를 이용하여 매 세션마다 ID를 계속해서 바꾼다. 태그는 다음의 정보를 포함한다. 현재 ID와, 현재 세션 넘버 i, 그리고 마지막 성공 세션 넘버 i^*를 포함한다. 백 엔드 데이터베이스 시스템은 태그와 같은 정보를 같고 있으며 동시에 H(ID) 값을 가지고 있다. 시스템이 시작 되면 ID와 i 는 랜덤한 값으로 초기화 되고 i^*와 i 는 같은 값을 지닌다. 동작과정은 그림 3과 같다[3][4].



[그림 3] 해쉬 기반 ID 변형 기법

① 리더는 태그에게 요청 메시지를 전달한다.

② 태그는 현재 자신의 세션넘버 i 를 1만큼 증가시키고 그런 다음 H(ID), H(i⊕ID), $\Delta i := i - i^*$ 값을 리더에게 전달한다. H(ID)값은 데이터베이스가 태그를 식별하기 위해 사용되며, H(i⊕ID)는 재생공격을 방지한다. 그리고 Δi 값은 원래 i 값을 복원하기 위해 사용된다. 그러므로 DB는 H(i⊕ID) 값을 계산할 수 있다.

③ DB는 리더로부터 전달받은 데이터에 대해 검증과정을 거친다. 같은 H(i⊕ID) 값이 있다면, 백 엔드 데이터베이스는 랜덤수 r을 발생하여 r, H(r⊕i⊕ID) 값을 리더를 통해 태그에게 보낸다.

④ 태그는 i 와 ID값을 알고 있기 때문에 리더로부터 받은 r을 이용하여 H(r⊕i⊕ID)가 올바른지 리더로부터 전달된 데이터 인지 검사한다, 만약 올바르다면 태그는 새로운 식별자 ID′ := r⊕ID와 i^* := i

을 갱신하고 다음 세션에 식별자로 사용한다. 올바르지 않을 경우는 새로운 ID값으로 갱신하지 않는다.

이 기법은 ID의 무결성을 보장하지 않으며, DB에 ID가 중복될 가능성도 존재한다. 뿐만 아니라, 정당한 리더로 가정하여 H(ID), H(i⊕ID), △i 값을 획득하고 정당한 태그가 다음 세션을 맺어 아이디 값이 변경되기 전에 태그인척 가정하고 리더에게 바로 재전송 공격을 할 경우 정당한 태그로 인증 받을 수 있다. 또한 정당한 세션이 이루어지기 전까지는 H(ID)값은 항상 같으므로 위치 추적이 가능하다는 단점이 있다.

3. 제안하는 프로토콜

3.1. 태그와 리더, DB의 초기정보와 가정

태그는 유일한 식별 번호인 ID와 Key 그리고 H(ID) 값을 가지고 있으며 또한 해쉬함수와 XOR연산을 할 수 있다. 리더는 난수 발생기와 해쉬함수, 그리고 타임어(Timer)를 가지고 있으며, XOR연산을 할 수 있다. DB도 태그와 같은 ID, Key를 공유하고 있으며 H(Key)값을 가지고 있다. 백 엔드 데이터베이스와 리더는 SSL과 같은 안전한 채널로 통신하고 있다고 가정한다[2][5].

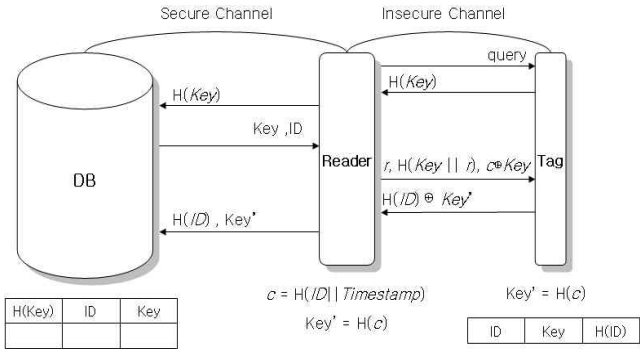
3.2.용어 정리

H() : 단방향 해쉬함수
ID : 객체 정보를 나타내는 고유한 비트
Key : 태그 인증을 위한 비밀 키
⊕ : eXclusive-OR 연산
|| : 연접(concatenation)
c : H(ID||Timestamp)값으로 다음 세션키를 만들때 사용
Key' : H(c)값으로 다음 세션의 새로운 비밀키
r : 리더가 발생하는 난수

3.3 제안한 프로토콜의 동작과정

① 리더는 태그에게 요청 메시지를 보낸다.

② 태그는 H(key)를 해쉬하여 리더에게 보낸다. H(Key)는 DB안에 있는 각각의 식별정보와 Key를 찾기 위한 Primary key로 사용한다. 리더를 통하여 백 엔드 데이터베이스에 전달된 뒤 H(Key)를 이용하여 해당 ID과 Key값을 찾는다. 그리고 백 엔드 데이터베이스는 Key와 ID값을 안전한 채널을 통하여 리더에게 전달한다.



[그림 4] 제안하는 프로토콜

③ 리더는 r, H(Key||r), c⊕Key를 생성하여 태그에게 전송한다. 리더는 랜덤 발생기를 이용하여 랜덤한 숫자 r을 발생시킨 후에 r, H(Key||r)을 만들며. 이것은 태그가 신뢰할 수 있는 리더인지 검증하는데 사용된다. 리더는 키를 갱신하기 위한 c = H(ID||Timestamp)를 만든다. c는 인증을 위한 새로운 Key로 사용되어지며, 유일한 값이어야 하기 때문에 ID와 타임스탬프 값을 해쉬하여 고유한 값을 만든다. 그리고 XOR연산을 이용하여 보내기 때문에, 정당한 Key가 없으면 c 값을 알 수 없다.

④ 태그는 리더로부터 받은 r, H(Key||r) 값을 가지고 자신의 Key와 r를 해쉬한 후 비교하여 리더가 신뢰할 수 있는 리더인지 검증한다. 만일 신뢰할 수 있다면 자신의 Key값을 가지고 c =(c⊕Key)⊕Key를 구한 후에 새로운 키 Key′ = H(c) 값을 계산한다. 리더도 Key′ = H(c)을 계산하여 리더와 태그가 같은 새로운 키 값을 공유한다.

⑤ 태그는 리더에게 H(ID)⊕Key′를 보낸다. 리더는 태그와 같은 키를 공유하고 있기 때문에 자신의 Key′를 이용하여 H(ID)를 얻는다.

⑥ 리더는 백 엔드 데이터베이스에 H(ID), Key′를 전달한다. DB는 현재 ID를 해쉬하여 리더로부터 전달받은 H(ID)값과 비교하여 태그가 신뢰할수 있는지 검증한다. 올바른 태그라면 Key와 H(Key)를 갱신한다.

4. 프로토콜의 안정성 및 효율성

세션이 이루어질 때마다 r와 Key 값은 변하기 때문에, 스푸핑이나, 재전송 공격에 강하다. 정당한 태그를 가정하여 r, H(Key||r), c⊕Key를 가로채더라도 이미 그 다음 세션에는 키 값이 변하기 때문에 태그에서 리더 인증이 이루어지지 않는다.

또한 XOR 연산은 피연산자 어느 한쪽만 알면 나머지 피연산자가 노출되어지는 단점이 있으나, 리더와 태그사이에 전송되어지는 메세지는 키가 갱신되고 피연산자가 각각 다르기 때문에 유추하는 것이 어렵다. 또한 백 엔드 데이터베이스 시스템에서도 H(Key) 값이 해당 ID와 Key값을 찾는 Primary Key로 사용되기 때문에 이전에 설명했던 기법과는 달리 DB안의 모든 식별정보를 해쉬하여 비교할 필요 없이 한번만 검색하면 된다. 해쉬 기반 ID 변형 기법의 경우 ID값을 변환함으로써 ID 값의 무결성을 보장하지 못하였으나, 제안하는 프로토콜의 경우 ID를 변형하기 보다는 meta 정보인 Key값을 변형하였다. 그리고 타임스탬프를 이용하여 해쉬를 하므로 DB에 중복되는 key값은 없다. 뿐만 아니라 키를 이용한 방식은 한번 키가 노출될 경우 피해가 크기 때문에 처음부터 카 교환을 통한 키 갱신 방법을 사용하여 안전성을 높였다.

5. 결론 및 향후 연구 방향

기존의 해쉬를 이용한 인증 프로토콜들은 스푸핑, 재전송, 위치 추적등에 취약했다. 본 논문에서 제안하는 프로토콜은 기존의 방법에 비해 스푸핑, 재전송 공격에 강하며, 백 엔드 데이터베이스 시스템에 무리가 가지 않는다.

해쉬를 이용한 인증 프로토콜은 대칭키나, 공개키 암호화 알고리즘을 사용하지 않고 단순히 해쉬 기술만을 이용하여 보안적 요구사항을 충족시키고 있다. 이러한 인증 기법은 앞으로 RFID 뿐만 아니라, 시스템 리소스가 적은 센서 네트워크에서도 이용될 수 있을 것으로 기대된다. 아직은 RFID 칩 가격이 높고, 기술의 안전성으로 인하여 보편화 되고 있지 않지만, 칩 가격의 하락과, 보안문제의 해결은 RFID의 사용에 더욱더 박차를 가하게 될 것이다.

참고문헌

[1] 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

[2] A. Juels, R. L. Rivest, M Szydlo "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", Proceedings of the 10th ACM conference on Computer and communications security, pp.103-111, 2003

[3] Gildas Avoine and Philippe Oechslin "RFID Traceability : A Mutilayer Problem", Financial Cryptography, March 2005

[4] Dirk Henrici and Paul Müller, "Hash-Based Enhancement of Location Privacy For Radio-Frequency Identification Devices Using Varying Identifiers", Workshop on Pervasive Computing and Communications Security - Persec 2004, pp.149-153, March 2004

[5] István Vajda and Levente Buttyán "Lightweight Authentication Protocols for Low-Cost RFID Tags", Workshop on Security in Ubiquitous Computing, October 2003