익명성을 제공하는 RFID 인증 프로토콜에 관한 연구

박장수*, 이임영
순천향대학교 정보기술공학부
e-mail:pjswise@sch.ac.kr

A Study on RFID Authentication Protocol With Anonymity

Jang-Su Park*, Im-Yeong Lee
Dept of Information Technology Engineering, SoonChunHyang University

요 약

최근 정보통신부의 IT 839정책의 진행으로 RFID에 대한 관심이 국내·외적으로 높아지고 있다. RFID는 바코드를 대체하는 무선 인식 기술로써 물류 유통에 국한하지 않고, 금융, 의료, 교통, 제조, 문화 등 사회 전 반면에 응용할 수 있도록 많은 연구가 진행되고 있다. 하지만 RFID 시스템에서 태그와 리더기 사이의 통신은 Radio Frequency를 이용해서 이루어짐으로 공격자에 의해 도청될 수 있으며, 태그의 정보가 노출되면 사용자의 프라이버시 침해 문제를 가져올 수 있다. 따라서 본 논문에서는 태그의 가상 ID를 사용하여 출력을 매번 다르게 변화시키는 인증 프로토콜을 제안하여 사용자의 프라이버시를 제공하고자 한다.

1. 서론

현재 다가오는 유비쿼터스 환경에서는 자율 컴퓨팅 기능을 갖는 기기 및 사물 등에 의하여 실시간 상황정보의 분석과 이를 통한 서비스가 이루어질 것이다. 이러한 유비쿼터스 환경에서 주목 받고 있는 기술이 RFID(Radio Frequency Identification)기술이다. RFID는 무선 인식 기술로서 저 전력이고, 작은 크기에, 어디서나 통신이 가능하다. 또한 데이터 저장 및 읽고/쓰기가 가능하고, 한 번에 여러 개의 데이터를 식별할 수 있다는 장점을 가지고 있어 물류, 금융, 의료, 교통, 제조 등 다양한 분야에서 사용 되어질 것으로 예측되어진다.[1)]

그러나 RFID시스템이 물리적 접촉 없이도 인식이 가능하다는 특징은 안전성과 프라이버시 측면에서 기존에 발생하지 않았던 여러 문제들을 발생시킨다. 하나의 예로, 식별 가능한 정보를 그대로 전송하는 태그의 경우, 태그와 리더기 사이의 통신내용은 제 3자에 의해 쉽게 도청이 가능하고, 도청된 정보는 사용자의 프라이버시 침해로 직결될 수 있다.

따라서 RFID시스템을 사용한 여러 응용에 대한 연구뿐만 아니라 시스템 이용시 발생 가능한 여러 보안, 프라이버시 침해를 해결하는 데, 많은 연구가 이루어 져야 한다.

본 논문에서는 최소한의 연산 능력 및 저장 공간으로 매번 태그의 출력을 변화시키는 가상 ID를 사용한다. 가상 ID를 사용함으로써 태그의 익명성을 제공하여 사용자의 프라이버시를 침해의 문제점을 해결하고자 한다. 본 논문의 구성으로는 다음과 같다. 2장에서 R○FID 시스템과 위협요소 및 인증 프로토콜 설계시 고려사항에 알아보고, 3장에서는 기존 RFID 인증 프로토콜들을 분석한다. 4장에서는 익명성을 제공하는 RFID 인증 프로토콜을 제안하고 분석하며, 5장에서는 결론을 맺는다.

2. RFID 시스템과 위협요소 및 고려사항

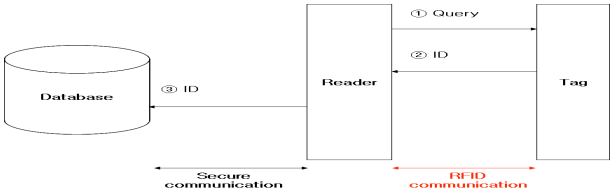
본 장에서는 RFID 시스템의 일반적인 구성과 위

1) 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음

협요소 및 고려사항에 대하여 알아본다.

2.1 RFID 시스템

일반적인 RFID 시스템은 태그의 관련정보를 저장하고 가공하는 데이터베이스(Database), 태그에 정보를 요청하며, 태그에 데이터의 읽기/쓰기를 진행하는 리더기(Reader), 식별정보를 가지고 있고, 리더기의 요청에 응답하여 정보를 주는 태그(Tag)로 구성된다[3,5,6,7].



(그림 1) 일반적인 RFID 시스템

2.2 위협요소 및 고려사항

RFID 시스템은 리더기와 태그간의 통신이 무선으로 이루어졌고, 태그의 연산 능력 및 저장 공간의 제한되어 있어 많은 취약점들을 가지고 있으며 다양한 위협에 노출되기 쉽다. 따라서 인증 프로토콜 설계시 고려사항은 다음과 같다[6,7].

- 도청(Eavesdropping) : 태그와 리더간의 통신방식은 무선으로 이루어져있어 공격자는 쉽게 통신내용을 엿들을 수 있다. 따라서 도청 후 공격자가 공격의 기본 정보로 활용될 수 없도록 해야 한다.
- 통신내용분석(Traffic analysis) : 공격자는 도청을 통해서 얻은 내용을 분석하여 리더의 질의에 대한 태그의 응답을 예측할 수 있다.
- 재전송 공격(Replay attack) : 도청된 내용을 정당한 리더기에게 재전송함으로써 정당한 태그인 것처럼 가장할 수 있다.
- 익명성(Anonymity) : 태그와 리더간의 통신은 도청 될 수 있어, 어떠한 태그로부터 정보가 전송되는지 확인가능하다. 따라서 어떤 태그로부터 데이터가 전송되는지 공격자는 확인할 수가 없어야 한다.
- 효율성(Efficiency) : 저가의 태그는 연산 능력 및 저장 공간의 제한적이다. 따라서 저가의 태그에서도 적용 가능해야한다.
- 물리적 공격(Physical attack) : 사용되는 태그를 훔치거나 파손시키는 등 물리적은 공격이 가능하다.

위에서 설명한 위협요소들 중에서 마지막에 언급한 물리적 공격은 RFID 시스템의 기계적/물리적 특성에 기인한 공격방법이며 인증 프로토콜 설계시 고려할 수 있는 사항이 아니므로 본 논문에서는 언급하지 않는다.

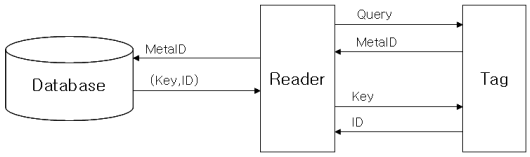
3. 기존 RFID 인증 프로토콜

본 장에서는 기존에 제안된 RFID 인증 프로토콜에 관해 알아보고 각각의 대해 안전성 여부를 설명하도록 한다.

3.1 Hash-Lock 프로토콜

Hash-Lcok 프로토콜은 낮은 태그 가격을 고려하여 MIT에 의해 제시된 방식으로 Key를 태그와 데이터베이스와 사전에 안전하게 공유되어 있다고 가정하며, 인증과정은 다음과 같다[5]. 리더기는 태그에게 Query를 전송하면 태그는 인증시 이용되는 가상 ID인 MetaID=H(Key)를 연산하여 리더기에게 전송하면 리더기는 태그로부터 받은 정보를 데이터베이스에 전송한다. 데이터베이스는 MetaID를 가지고 Key와 ID를 획득하여 리더기에게 전송하고 리더기는 Key를 태그에게 전송한다. 태그는 리더기로부터 전송받은 Key에 해쉬 연산을 통하여 얻은 값과 MetaID가 같은지 비교 후 같다면 ID를 전송함으로써 인증과정이 이루어진다.

이 방법은 일방향 해쉬 함수에 기반하여, 효율적성을 고려하였고, 익명성을 제공하기 위해 MetaID를 사용하였다. 하지만 태그의 식별값인 MetaID가 고정되어 있어, 출력되는 데이터가 같아 해당 태그로부터 데이터가 전송되었는지를 확인할 수가 있다. 또한 리더기와 태그사이의 통신채널은 도청이 가능하기 때문에 악의적인 공격자는 Key를 획득한 후, 해쉬 연산하여 MetaID를 산출하여 인증 받을 수 있다. 마지막으로 악의적인 제 3자는 고정된 MetaID를 재전송함으로써 인증 받을 수 있다.

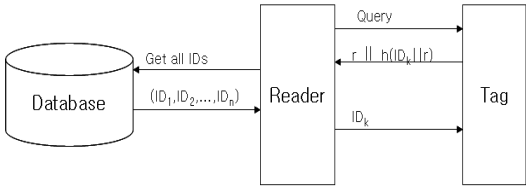


(그림 2) Hash-Lock 프로토콜

3.2 확장된 Hash-Lock 프로토콜

확장된 Hash-Lock 프로토콜은 앞에서 언급한 Hash-Lock 프로토콜의 변형으로 태그는 의사난수 생성기와 해쉬 함수를 포함한다고 가정하며, 인증과정은 다음과 같다[5]. 리더기는 태그에게 Query를 전송하면 태그는 랜덤수 r을 생성하여 $h(ID_k \| r)$과 같이 전송한다. 리더기는 ID_k에 대한 모든 all ID를 $h(IDall \| r)$로 연산한다. 만약 $h(ID_k \| r)$과 같은 값이 나오는 IID_k'를 찾아 태그에게 전송한다. 태그는 ID_k'와 ID_k와 같은지 비교함으로써 모든 세션이 종료된다.

이 방법은 재전송 공격을 막기 위해 의사난수 생성기를 사용하여 생성한 랜덤수를 이용하지만 $r \| h(ID_k \| r)$을 재전송 하는 경우 인증 받을 수 있다. 또한 리더기와 태그사이의 도청공격으로 인해 ID_k를 획득 후 r'를 생성하여 $h(ID_k \| r')$와 함께 전송하면 인증 받을 수 있다. 또한 저가의 태그에서 해쉬 함수와 의사난수 생성기를 동시에 사용하는 것은 제한적인 태그의 연산능력에서 부담이 크다.



(그림 3) 확장된 Hash-Lock 프로토콜

4. 익명성을 제공하는 인증 프로토콜 제안

본 장에서는 기존 인증 기술의 분석을 기반으로 2장에서 언급한 위협요소 및 고려사항을 만족하는 안전한 인증 프로토콜을 제안하고자한다.

4.1 가정사항

익명성을 제공하는 안전한 인증 프로토콜을 제안하기 위해 다음 사항을 가정한다.

- 태그는 수동형 전력공급을 수행하는 스마트태그이다.
- 태그와 데이터베이스는 해쉬 함수와 XOR 연산을 수행한다.
- 태그와 데이터베이스는 태그의 ID를 사전에 공유한다.
- 태그와 데이터베이스는 태그마다 값이 다른 key를 안전하게 공유한다.
- 리더기는 R.N.G(의사난수생성기)를 포함하여 랜덤수를 생성할 수 있다.

4.2 시스템 계수

익명성을 제공하는 인증 프로토콜을 제안하기 위해 다음과 같은 시스템 계수가 필요하다.

- ID_i : 태그의 식별 값으로 현재 세션에 이용되는 ID이다. (i는 세션의 의미로써 (i=1~n까지 순차 카운팅 된다.)
- key : 익명성을 제공하기위해 사용되는 가상 ID 생성에 필요한 값으로 사전에 공유된다.
- MetaID : 인증시 태그의 식별값으로 사용되는 가상 ID이다. MetaID=h(key ‖ R)
- R : 리더기에서 생성되는 랜덤 수
- h() : 해쉬 함수
- ⊕ : XOR 연산

4.3 제안방식 프로토콜

본 제안방식은 XOR 연산과 1번의 해쉬 연산을 통해 이루어지고, 사전에 공유된 key와 랜덤수 R을 이용하여 가상 ID인 MetaID를 생성한다. MetaID를 이용하여 익명성을 제공하며 매 인증시 사용된다. 인증과정은 다음과 같다.

Step 1. 리더기는 랜덤 수 R을 생성 후 query와 연접하여 태그에게 전송한다.

$$query \| R$$

Step 2. 태그는 사전에 공유된 key와 리더기로부터 전송받은 랜덤수 R을 연접하여 해쉬 연산을 통해 MeatID라는 가상 ID를 획득한다. 획득한 MetaID를 리더기에게 전송한다.

$$h(key \| R) = MetaID$$

Step 3. 리더기는 태그로부터 전송받은 MetaID와 자신이 생성한 랜덤수 R을 연접하여 데이터베이스에 전송한다.

$$MetaID \| R$$

Step 4. 데이터베이스는 리더기로부터 전송받은 랜덤수 R과 모든 태그의 key와 연접하여 해쉬 연산을 한다. 해쉬 연산을한 데이터베이스는 태그로부터 전송받은 MetaID와 같은 key′와 ID_i를 획득한다.

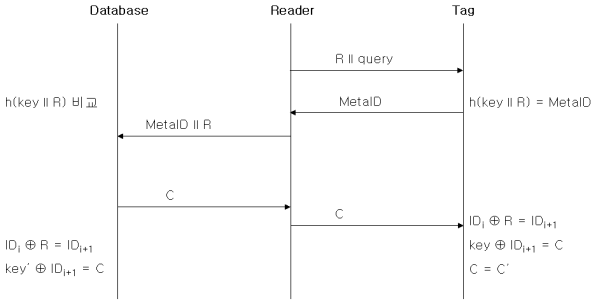
획득한 ID_i와 리더기로부터 전송받은 랜덤수 R과 XOR 연산을 하여 ID_{i+1}을 획득하고, key′와 획득한 ID_{i+1}을 XOR 연산을 통해 C를 획득한다. 획득한 C를 리더기에게 전송하고. C를 전송받은 리더기는 태그에게 전송한다.

$$h(all\_key \| R)$$
$$ID_i \oplus R = ID_{i+1}$$
$$key' \oplus ID_{i+1} = C$$

Step 6. 태그는 리더기로부터 전송받은 C를 확인하기 위해 ID_i와 R을 XOR 연산을 하여 ID_{i+1}을 획득하고, key와 획득한 ID_{i+1}을 XOR 연산을 통해 C′를 획득하여 C와 비교한다.

$$ID_i \oplus R = ID_{i+1}$$
$$key \oplus ID_{i+1} = C'$$
$$C = C'$$

이와 같이 모든 세션이 안전하게 끝났을 경우 태그와 데이터베이스는 ID를 $ID_{i+1} = ID_i \oplus R$로 갱신한다.



(그림 4) 제안 방식 프로토콜

4.4 제안 방식 분석

본 논문의 2장에서 언급한 위협요소 및 고려사항에 대해 제안한 프로토콜의 안전성을 분석한다. 본 제안 방식은 제한적인 연산능력과 저장공간을 고려하여 XOR 연산과 한 번의 해쉬 연산을 이용하여 인증 프로토콜을 제안하였다. 그리고 가상 ID인 MetaID를 이용하여 어떠한 태그로부터 데이터가 출력되는지 알 수 없도록 익명성을 제공하였다. 또한 랜덤수를 이용하여 가상 ID가 매번 변경되어 (MetaID=h(key ‖ R)) 재전송 공격에도 강하다. 그리고 태그의 데이터의 출력을 도청 하더라도 해쉬 연산과 XOR 연산을 통해 공격의 기본 정보로 활용될 수 없도록 설계하였다.

하지만 데이터베이스가 가상 ID를 확인하는 과정에서 key′와 ID_i를 획득하기 위해 모든 key와 R을 연접하여 해쉬 연산을 취하여 검색하는데 있어 ID를 검색하여 응답하는 경우보다 서버의 부하가 많아진다는 단점이 있다.

<표 2> 인증 프로토콜 분석

	해쉬-락	확장된 해쉬-락	제안 방식
도청	취약	취약	안전
통신내용분석	취약	취약	안전
재전송공격	취약	취약	안전
익명성	X	X	○
효율성	○	X	○

5. 결론

RFID 기술은 언제 어디서나 컴퓨팅 능력이 편재되어있는 유비쿼터스 환경에서 곽광을 받고 있는 기술로써 보안에 관한 연구가 반드시 뒤따라야 한다. 따라서 본 논문에서는 비교적 적은 자원으로도 구현 가능한 해쉬 연산을 한 번 이용함으로써 RFID 프라이버시 보호를 위한 익명성을 제공하는 인증 프로토콜을 제안하였다.

참고문헌

[1] A. Juels, R. Pappu, "Squealing euros: Privacy Protection in RFID-enabled banknotes", In Proceedings of Finaancial Cryptography-FC'03, 2003.

[2] A. juels, R. L. Rivest and M. Szydlo, "The Blocker Tag: Selective Bloking of RFID Tags for Consumer Privacy", In Proceedings of 10th ACM Conference on Computer

[3] Ari, Juels, "Privacy and Authentication in Low-Cost RFID Tags", submission., 2003

[4] P. Golle, M, Jakobsson, A Juels and P. Syverson, "Universal re-encryption for mixnets", 2002

[5] S. A. Weis, "Security and Privacy in Radio-Frequency Identification Devices", Mastters Thesis. MIT. May, 2003

[6] 주학수, "RFID 시스테의 보안 및 프라이버시 보호를 위한 기술 분석" , IT리포트, 2004

[7] 한승우, 최재귀, 박지환, "효율적인 식별기능을 갖는 RFID 가변 정보화 방식", 한국멀티미디어학회 춘계학술발표대회, 2004