RFID 시스템에서 개선된 Challenge-Response 인증프로토콜 설계

양성훈*, 이경효*, 김민수*, 정석원*, 오병균*

목포대학교 정보보호전공*

Design of Improvement Challenge-Response Authentication Protocol for RFID System

SungHoon Yang*, KyungHyo Lee*, MinSu Kim*, Seokwon Jung*, ByeongKyun Oh*

Information Security, Mokpo University*

요 약

RFID(Radio Frequency Identification) 시스템이란 무선 라디오 주파수를 이용하여 사물을 식별 및 추적할 수 있는 기술로서 산업 전반에 걸쳐 그 적용성이 확대되고 있으나 불안전한 통신상에서 데이터 송·수신 및 태그의 제한적인 계산능력과 한정된 저장 공간의 자원으로 인한 위치 추적, 스푸핑 공격, 재전송공격, 사용자 프라이버시 침해 등의 취약점이 존재한다.

본 논문에서는 기존의 RFID 시스템에 대한 인증 프로토콜들을 분석하고, Challenge Response(C-R) 인증 프로토콜에서 연산량을 줄임으로서 위치 추적과 스푸핑 공격, 재전송 공격에 효율적으로 개선된 C-R 인증 프로토콜을 제안한다.

1. 서론

RFID(Radio Frequency Identification) 시스템은 무선 주파수를 이용하여 물리적 접촉 없이 개체에 대한 정보를 읽거나 기록하는 무선 인식 시스템으로, 최근 전자문서 관리, 화물 및 컨테이너 추적, 동물의 이동경로 추적, 차량 접근 및 제어, 신원 확인 등 여러 분야에서 활용되고 있다.

그러나 RFID의 무선 인식 기술을 역이용하여 태그가 부착된 사물 및 사람에 대해 언제든 그 위치를 파악할 수 있으며, 태그와 리더간의 통신내용을 불법으로 취득, 분석하여 태그의 위조나 변조를 행함으로써 개인 프라이버시의 침해하거나 태그가 부착된 상품의 가격 등을 바꿀 수 있다. 따라서 RFID가 발전될수록 무선 인식 기술이 불법적으로 악용될 가능성이 있으므로 리더와 태그의 정당성에 대한 인증과 태그와 리더사이의 통신내용에 대한 보안 기능이 마련되어야 한다.[1]

이처럼 RFID의 기술을 역이용하거나 공격하는 유형으로는 태그의 정보를 얻고자 시도하는 공격, 정상적인 리더와 태그 사이의 데이터를 공격자가 엿듣는 경우, 공격자가 정상적인 데이터를 위조하여 리더 또는 태그를 혼란시키는 공격, 태그와 관련된 데이터를 입수하기 위하여 정보 서버에 불법적으로 접근해 해킹하는 경우, 인증되지 않는 DoS 트래픽으로 공격하는 경우가 있으며 이러한 공격 등을 막기 위한 기술로 인증, 암호 알고리즘, 보안 프로토콜, 네트워크 인프라 공격대응이 있다.[1]

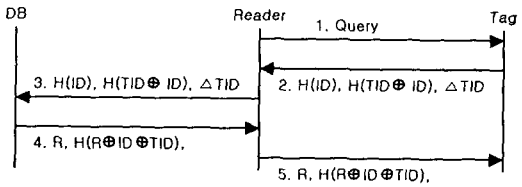
본 논문에서는 위에서 나열한 4가지 보안 기술 중 인증기술에 해당하는 인증 프로토콜을 설계한 것이며, 논문의 구성은 2장에서 인증에 대한 관련연구로 기존의 인증 프로토콜들을 분석하고, 3장에서 난수를 이용한 RFID 인증프로토콜을 제시하였으며, 4장에서 결론을 기술하였다.

2. 관련 연구

RFID에서 리더와 태그 사이의 RF 신호를 이용한 정보전달은 악의적인 행위가 가능한 공격자들에게 노출되어 있어 위치추적, 스푸핑 공격, 메시지 유실, 도청, 통신내용 분석 등의 공격이 가능하다. 또한, 저가의 RFID의 경우 태그의 가격 제한으로 인해 안전한 통신을 위한 암호화 기법을 적용하기가 어렵다는 문제가 있다. 이러한 문제를 해결하기 위해 다양한 인증기법들이 연구되었다. 본 장에서는 기존 인증 프로토콜들의 기능과 특성을 분석한다.

2.1 해쉬기반 ID 변형 프로토콜

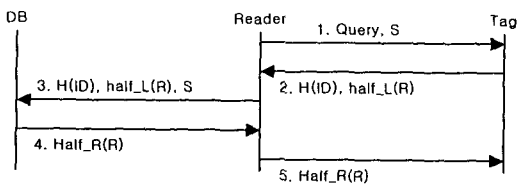
[그림 1]의 해쉬기반 ID 변형 기법[3]은 매 세션마다 태그의 ID를 변형시켜 인증하는 기법으로 태그의 인증 정보 ID가 난수 R에 의해 갱신되고 Transaction ID인 TID와 Last Sucess Transaction ID의 LST가 갱신되므로 공격자의 재전송 공격으로부터 안전하다.[7] 그러나 매 세션마다 전송되는 H(ID)가 같으므로 위치 추적이 가능하고, 공격자가 Step 2의 값을 획득한 후 다음 인증 세션을 수행하기 전에 리더의 질의에 대한 응답으로 이용할 경우 공격자는 정당한 태그로 인증이 가능하게 된다.



[그림 1] 해쉬기반 ID 변형 프로토콜

2.2 향상된 해쉬기반 ID 변형 프로토콜

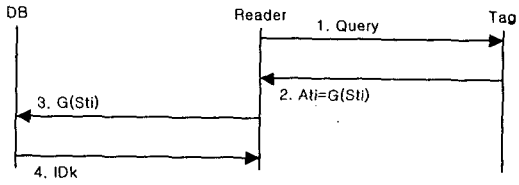
[그림 2]는 해쉬기반 ID 변형 프로토콜의 문제점을 보안하고 태그의 해쉬 횟수를 1회 줄인 개선된 해쉬기반 프로토콜로[2] 리더에서 생성된 랜덤난수 S를 이용하여 태그를 인증하고 ID를 갱신하는 프로토콜이다. 공격자는 S에 해당하는 R(R=ID||S)을 만들어 낼 수 없으므로 스푸핑 공격에 안전하며, 인증에 사용되는 값이 해쉬한 결과의 반이어서 해쉬를 두 번만 수행하므로 효율적이다. 그러나 이 프로토콜 또한 세션마다 H(ID)가 같으므로 위치 추적에 안전하지 못하며, 공격자가 도청 등을 통해 Step 1, 2, 5값을 얻고 Step 5를 태그에게 주지 않는다면 태그의 ID가 변경되지 않은 채 Step 1과 동일한 S를 태그에게 질의하고 Step 2의 응답에 도청한 Step 5의 값을 태그에게 주면 태그는 리더를 인증하고 데이터를 주게 된다.



[그림 2] 향상된 해쉬기반 ID 변형 프로토콜

2.3 해쉬 체인 프로토콜

[그림 3]은 두 개의 서로 다른 해쉬 함수를 이용하는 해쉬 체인 프로토콜[3]로 리더의 질의에 대하여 항상 다른 응답을 하므로 공격자가 태그의 응답 Ati를 알더라도 어떤 태그가 응답하였는지 알 수 없으며, 서로 다른 응답에 대해서 동일한 태그의 응답이라는 것도 알 수 없다.

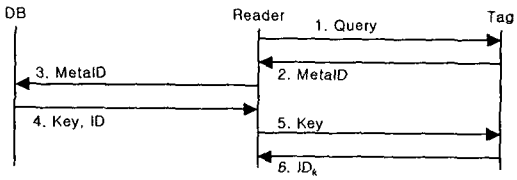


[그림 3] 해쉬 체인 프로토콜

그러나, 태그의 ID와 S1만 가지고 있으므로 태그로부터 수신된 ai = G(Si)값에 해당하는 ID를 검색하기 위해서는 최악의 경우 데이터베이스가 보유한 모든 s1에 대해서 H와 G를 I번 수행해야 하며 태그로부터 잘못된 응답을 수신 받을 경우 무한번의 해쉬를 수행할 가능성도 배제할 수 없다. 또한, 해쉬 체인 기반기법은 일 방향 인증으로 태그가 리더를 인증하지 못하므로 태그의 동작을 제어하는 리더의 명령을 수행함에 있어 문제가 발생하게 된다.

2.4 해쉬 락 프로토콜

태그의 ID 노출을 방지하기 위한 [그림 4]의 해쉬 락 프로토콜[4]은 metaID를 사용하는 프로토콜로 태그 ID에 대한 metaID 또한 고정되어 있기 때문에 위치 추적이 가능하며, 공격자가 Step 2의 값을 획득하여 다음 세션에서 이용하였을 경우 태그의 key와 ID를 얻을 수 있으므로 스푸핑 공격에도 취약하다.

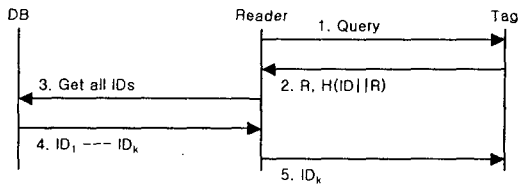


[그림 4] 해쉬 락 프로토콜

2.5 확장된 해쉬 락 프로토콜

[그림 5]의 확장된 해쉬 락 기법[5]는 태그가 난수를 생성하여 매 세션마다 다른 응답을 리더에게 전송하는 방법이다. 이 프로토콜은 공격자

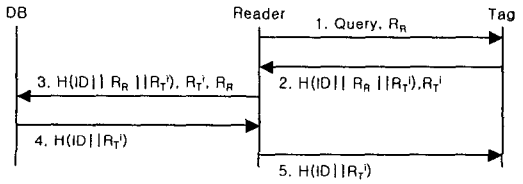
가 Step 2의 값을 획득 하여 재전송 하였을 경우 정당한 태그로의 위장이 가능하다.



[그림 5] 확장된 해쉬 락 프로토콜

2.6 Challenge-Response(C-R) 프로토콜

[그림 6]의 C-R 인증 프로토콜[6]은 리더가 처음 태그에게 질의할 때 난수를 함께 전송하고, 태그는 리더로부터 수신한 난수와 자신이 생성한 난수 R_T^i를 이용하여 응답함으로써 재전송 공격과, 스푸핑 공격, 위치 추적에 안전하다.



[그림 6] C-R 프로토콜

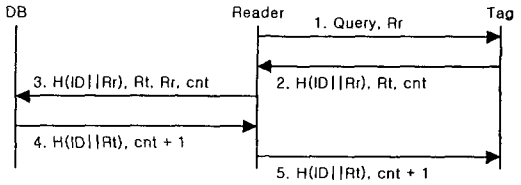
그러나 태그의 난수 R_T^i 를 생성하기 위해 1회 해쉬 연산을 수행하고 리더의 질의응답으로 Step 2의 값을 생성하기위한 1회의 해쉬 연산을 수행하게 되므로 태그는 총 3회의 해쉬 연산을 하게 된다. 또한, 태그가 처음 생산될 때 H(key)값이 아닌 단순 key값만 저장된 채로 생산이 된다면 첫 번째 인증 세션에서 R_T^0값을 위해 key를 해쉬해야 하는 1회의 해쉬 연산이 추가되어 전체 4회의 해쉬 연산을 필요로 하게 된다. 이러한 C-R 프로토콜은 기존 인증 프로토콜들에 비해 태그의 해쉬 연산이 많기 때문에 연산의 효율성 측면에서 좋지 않다.

3. 제안하는 개선된 C-R 프로토콜

본 논문에서 제안한 프로토콜은 기존의 C-R 프로토콜[7]에서 연산의 효율성을 개선한 기법으로서 제안하는 프로토콜에서 태그가 처음 생산될 때 DB에 태그의 ID와 COUNT NUMBER를 저장하며 태그에는 ID와 cnt=0의 값을 저장 후 한 세션이 성공적으로 종료되면 cnt 값은 1 증가되어 태그의 다음 cnt 값으로 갱신된다. DB에서 태그의 ID를 찾기 위한 해쉬 연산은 태그의 수 /cnt_i 회만을 필요로 한다.

[파라미터]

- Query : 질의, 태그의 응답을 요청.
- ID : 태그 고유의 비밀 인증 정보.
- H( ) : 일 방향 해쉬 함수.
- Rr : 리더의 랜덤 난수.
- Rt : 태그의 랜덤 난수.
- || : 연접(Concatenate function)
- cnt : count number, COUNT$\in Z_4$ {0, 1, 2, 3}



[그림 7] 개선된 C-R 프로토콜

- DB

ID	ID1	ID2	ID3	… …	IDn-2	IDn-1	ID
cnt	0	1	2	… …	1	2	3

3.1 인증과정

- Step 1 : 리더

태그에게 Query와 리더의 난수 Rr을 브로드 캐스팅 한다.

- Step 2 : 태그

리더로부터 수신한 Rr과 태그 자신의 ID를 연접 해쉬한 값과 태그의 난수 Rt, cnt 값을 리더에게 전송한다.

- Step 3 : 리더

태그로부터 수신한 값 H(ID||Rr), Rt, cnt와 리더의 난수 Rr을 백 엔드 데이터베이스로 전송한다.

- Step 4 : DB

수신한 값 H(ID||Rr), Rt, Rr, cnt를 이용하여 리더를 인증하고, 해당 ID를 찾아 태그를 인증한다. 태그 ID를 찾기 위한 해쉬 연산횟수는 태그의 수/cnt_i로 DB에 저장된 모든 ID를 검색할 필요가 없으며, DB는 cnt = 3 이면 COUNT 을 1 증가시켜 H(ID||Rt),cnt+1 을 리더에게 전송한다.

- Step 5 : 태그

DB에서 전송된 값 H(ID||Rt), cnt+1은 리더를 통해 태그에게 전달되고 태그는 자신의 ID와 난수 Rt를 이용하여 백 엔드 데이터베이스를 인증하고 cnt를 갱신 시킨 후 세션은 종료된다.

3.2 제안하는 프로토콜의 안정성 분석

기존의 인증 프로토콜들은 재전송 공격, 스푸핑 공격에 취약하였으며, 태그의 추적 또한 가능하였다. 그러나 제안하는 프로토콜은 세션마다 리더, 태그가 난수를 생성하여 세션을 진행하게 되므로 재전송 공격과 스푸핑 공격에 안전하며, 공격자에 의한 추적도 방지할 수 있다.

· 도청/통신내용분석 : 공격자가 태그에게 질의를 하여 얻은 응답을 분석하는 방법으로 공격자는 분석한 결과를 이용하여 위치트래킹 공격이나 스푸핑 공격에 활용할 수 있다[2]. 그러나 제안하는 프로토콜에서는 매 세션마다 달라지는 랜덤 난수와 해쉬의 일방향성으로 인해 공격자는 태그의 응답을 분석할 수가 없다.

· 위치 추적 : 제안하는 프로토콜은 매 세션마다 달라지는 리더와 태그의 난수로 인해 태그의 ID 해쉬한 결과 값도 세션마다 달라지므로 공격자에 의한 위치 추적의 취약점도 보안이 가능하다.

· 스푸핑 : 공격자가 정당한 태그로 인증을 받기 위해서는 Step 2, 5를 획득한 후, 내용을 수정하여 정당한 리더에게 전송해야 하는데 정당한 리더는 세션마다 랜덤 난수 Rr를 질의 하므로 태그의 ID를 모르는 공격자는 H(ID||Rr)을 만들 수 없다. 또한 이전 세션에서 획득한 H(ID||Rr), Rt를 리더 질의응답으로 사용하더라도 다음세션에서 생성된 Rr', Rt' 값이 같지 않는 이상 H(ID||Rr'), Rt' 값이 달라 인증에 실패하게 된다. 그리고 리더로 가장하여 이전 세션의 Step 1, 2, 5의 값을 이용하더라도 매번 달라지는 Rr, Rt에 의해 DB에서의 인증은 실패하게 되며 Step 5의 값을 정당한 태그에게 전송하여도 태그는 이전 세션의 H(ID||Rr||Rt)과 계산된 H(ID||Rr||Rt)이 다르기 때문에 인증은 실패하게 된다.

5. 결론

[표1]과 [표2]는 RFID의 취약성과 기존 RFID 인증 프로토콜들에 대한 효율성과 안전성을 분석하여 C-R 프로토콜의 연산량을 줄이기 위한 새로운 인증 프로토콜을 제시하였다.

본 논문에서 제안한 프로토콜은 기존에 제안된 프로토콜들이 가지는 도청/통신내용분석, 위치추적, 스푸핑 공격이 가능한 취약점을 보완하고 연 산의 효율성을 높이므로 안전하고 효율적인 RFID 인증 프로토콜이 요구되는 시스템에 쉽게 적용이 가능하다.

[표 1] 인증 프로토콜들의 효율성

기법	연산량(회수)		
	태그	리더	DB
해쉬 기반 ID 변형	해쉬 함수 : 3	-	난수 생성 : 1 해쉬 함수 : 3
향상된 해쉬 기반 ID 변형	해쉬 함수 : 2	난수 생성 : 1	해쉬 함수 : 2
해쉬 체인	해쉬 함수 : 2	-	해쉬 함수 : (태그의 수/2)*i
해쉬 락	해쉬 함수 : 1	-	-
확장된 해쉬 락	난수 생성 : 1 해쉬 함수 : 1	해쉬 함수 : 태그의 수/2	-
Challenge -Response	해쉬 함수 :3(4)	난수 생성 : 1	해쉬 함수 : (태그의수/2)+1
제안 프로토콜	난수 생성 : 1 해쉬 함수 : 2	난수 생성 1:	해쉬 함수 : (태그수/cnt_i)

[표 2] 인증 프로토콜들의 안전성

기법 / 종류	해쉬 락	확장 해쉬 락	해쉬 체인	해쉬 기반 ID변형	개선된 해쉬기반 ID 변형	C-R	제안 프로토콜
스푸핑	×	×	×	×	O	O	O
재전송	×	×	×	O	O	O	O
내용분석	×	×	O	O	O	O	O
위치추적	×	×	O	△	△	O	O
전송방해	O	O	O	O	O	O	O

O : 안전, × : 취약, △ : 중

[참고문헌]

[1] 유승화, 유비쿼터스 사회의 RFID, 전자신문사

[2] 황영주, 이수미, 이동훈, 임종민, "유비쿼터스 환경의 Low Cost RFID 인증 프로토콜", 한국정보보호학회 하계정보보호학술대회 논문집 Vol.14, No.1, pp.109-114, 2004.

[3] 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.

[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] S. A. Weis, "Security an privacy in Radio frequency Identification Devices" MS Thesis, MIT. May, 2003.

[6] 이근우, 오동규, 곽진, 오수현, 김승주, 원동호, 분산 데이터베이스 환경에 적합한 Challenge response 기반의 안전한 RFID 인증 프로토콜, 이근우 외, KRF, 2004.