일회성 난수를 사용하는 RFID 상호인증 프로토콜

오세진*, 정경호*, 안광선*
*경북대학교 전자전기컴퓨터학부
e-mail:170m3@knu.ac.kr

An RFID mutual authentication protocol using one-time random number

Sejin Oh*, Kyungho Chung*, Kwangseon Ahn*
*School of Electrical Engineering and Computer Science, Kyungpook National University

요 약

무선을 이용한 RFID 시스템의 메시지 전송은 보안에 취약하다. 그 중 서비스 거부 공격은 백-앤드 서버, 리더 또는 태그에게 많은 연산량으로 비동기화를 일으키는 것을 말한다. 특히, 서버에서 ID를 검색하는데 많은 시간 및 연산량으로 인한 문제점들이 있다. 이를 해결하고자 인증된 개체와의 메시지를 서버에 전달한 후 ID를 검색하도록 하여 서버에 대한 부하를 최소화 한다. 또한 인증에 사용되는 값은 일회용 난수를 키와 메시지로 활용하여 보안에 안전한 프로토콜을 제안한다.

1. 서론

RFID(Radio Frequency Identification)는 무선 주파수를 이용한 비 접촉식 자동인식 기술이다. 무선 상의 노출된 메시지 전송은 도청, 서비스 거부 공격, 트래픽분석 등과 같은 다양한 문제점이 있다. 그 중, 서비스 거부 공격은 많은 소요 시간과 연산량으로 인하여 해당 시스템의 의도된 용도로 사용하지 못하게 하는 공격이다. 연산량이 많은 서버의 부하를 줄이기 위하여 인증과정을 거친 메시지에 대해서만 ID를 검색하게 하여야 한다. 여러 문제점을 해결하기 위해 해쉬 함수를 이용하거나 재 암호화 XOR 연산 등을 이용한 방법들이 있다. 이 중에서 해쉬 함수에 기반한 방법들이 많이 제안 되었으나 많은 연산량을 요구하므로 RFID 시스템에는 적합하지 않다[1,4].

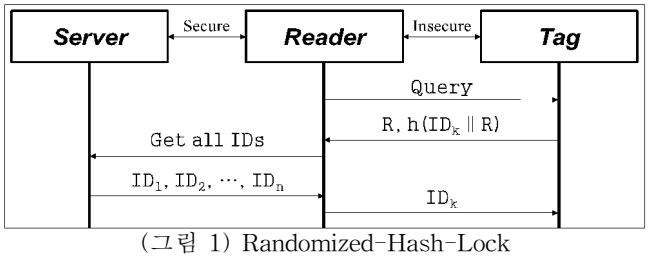
M. Feldhofer는 저전력 AES를 통해 난수를 이용한 단방향 인증 프로토콜을 제안하였다[2,3]. 그러나 같은 키로 암호화함으로써 위치 추적과 같은 여러 문제점이 있었다. 이를 해결하기위해 임의의 키로 암호화 하고 전달되는 난수는 암호화함으로써 인증 과정을 안전하게 한다.

2. 관련연구

2.1 서비스 거부 공격

RFID 시스템의 태그가 소유한 ID를 백-앤드 서버에 전달하여 DB에서 검색하는데 많은 시간이 소요되는 단점이 있다. Randomized-Hash-Lock의 경우 DB에서 정당한 태그를 찾기 위해 m개의 태그가 있을 경우 평균 ⌈m/2⌉번의 해쉬 연산이 필요하며 다수의 태그를 인식해야하는 시스템일 경우는 서버에 많은 부하를 가지게 된다. 이런 취약점을 바탕으로 서비스 거부 공격을 할 수 있다[4].

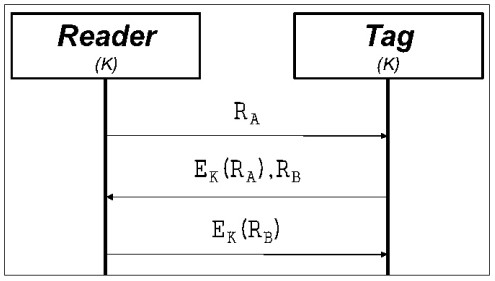
(그림 1)은 Randomized-Hash-Lock 기법이며 Hash-Lock 프로토콜에서 발생했던 문제점을 해결하고자 제안된 방식이다. 하지만 공격자에 의해서 $R, h(ID_k \| R)$를 획득 할 경우 인증을 할 수 없다. 그리고 Serverless환경에서 리더의 계산량이 많아지기 때문에 부적절하다[5].



(그림 1) Randomized-Hash-Lock

2.2 상호인증

RFID 시스템의 전송되는 메시지를 정당한 개체와 통신을 하기 위해 인증 단계를 거쳐야한다. (그림 2)의 M. Feldhofer의 Challenge-Response의 노출된 난수 값과 고정된 키를 사용하여 암호화하기 때문에 정보노출 등의 문제점이 있다[6].



(그림 2) M. Feldhofer의 Challenge-Response

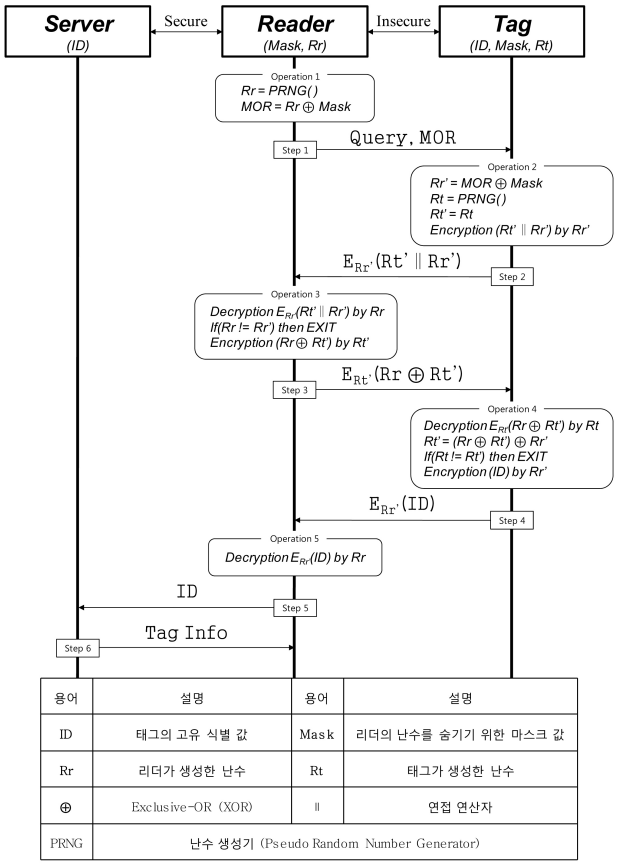
3. 제안 프로토콜

3.1 가정 사항 및 용어 정의

본 논문에서 RFID 시스템은 다음과 같은 가정 하에서 동작한다. 첫째, 서버와 리더 간 안전한 채널, 리더와 태그 간 통신 채널은 공격자의 공격에 취약하다. 둘째, 리더와 태그는 대칭키 기반의 암·복호화 연산이 가능하며, 리더와 태그 모두 난수를 생성할 수 있다. 셋째, 리더와 태그는 사전에 동일한 마스크 값(Mask)를 가지고 있다. 넷째, 태그는 리더로부터 전원을 공급받는 수동형태그로 가정한다.

3.2 상세 프로토콜

(그림 3)은 본 논문에서 제안한 RFID 시스템의 인증 프로토콜의 암·복호화 및 인증과정이다.



용어	설명	용어	설명
ID	태그의 고유 식별 값	Mask	리더의 난수를 숨기기 위한 마스크 값
Rr	리더가 생성한 난수	Rt	태그가 생성한 난수
⊕	Exclusive-OR (XOR)	‖	연접 연산자
PRNG	난수 생성기 (Pseudo Random Number Generator)		

(그림 3) 제안 프로토콜

Operation 1에서는 리더의 난수 Rr과 MOR을 생성하여 Step 1과 같이 태그에게 전송한다. 이를 받은 태그는 Operation 2와 같이 Rr′을 얻고 태그 난수 Rt′을 생성한다. 그리고 Rt′과 Rr′을 연접하여 Rr′을 키로 암호화 하여 Step 2와 같이 전송한다. Operation 3에서는 리더가 생성한 난수 Rr로 복호화 하여 얻은 Rr′과 Rr를 비교하여 인증 과정을 수행한다. 인증을 통과하였을 때 Rr과 Rt′을 XOR연산하여 Rt′을 키로 사용하여 암호화 한다. 암호화된 메시지를 Step 3와 같이 태그에게 전송한다. Operation 4에서는 암호화된 메시지를 복호화 하여 Rt와 Rt′ 값을 비교하여 인증 과정을 수행한다. 그 후 태그의 ID값을 Rr′을 키로 암호화 하여 Step 4와 같이 리더에게 전달한다. Operation 5에서는 Rr을 사용하여 복호화 하여 ID값을 서버에 전달한다. ID값을 전달 받은 서버는 DB를 검색하여 리턴 값, 태그의 정보를 리더에 전송하여 통신을 완료한다. Step 6에서 백-앤드 서버가 인증된 ID에 대한 DB 검색으로 인하여 매우 큰 기대치를 올릴 수 있다. 가령 다수의 리더가 존재하는 대형 마트에서 리더와 태그의 인증과정에 서버가 포함된다면 작은 연산이라도 다수의 리더에서 오는 메시지를 매번 수행한다면 상당한 부하를 일으키는 점을 이용하여 공격자가 서비스 공격을 할 수 있다.

4. 결론

최근 서비스 거부 공격으로 인한 피해로 그 심각성은 매우 크게 인식되고, 그에 많은 보안이 요구되는 가운데, RFID 시스템의 많은 연산량이 요구되는 ID검색은 백-앤드 서버에 부하로 인하여 시스템 전체에 많은 영향을 끼친다. 본 논문은 리더와 태그의 인증 단계를 거쳐야 리더가 백-앤드 서버에 ID를 검색을 요청하기 때문에 백-앤드 서버에 대한 서비스 거부 공격은 강한 안전성을 보장한다.

본 논문에서는 자원이 제한된 RFID 태그에 적합한 AES 알고리즘을 적용했다. M. Feldhofer가 제안한 단방향 인증 프로토콜은 난수 값이 그대로 노출되며, 고정된 키로 암호화하기 때문에 정보가 노출되는 문제점이 있다. 그러나 리더가 생성한 난수는 Mask값을 이용하여 숨기게 하여 노출을 막고, 암·복호화 시 사용되는 키는 리더와 태그가 매 세션마다 생성한 난수를 사용하기 때문에 키 값과 메시지의 노출 문제점을 해결하였다.

참고문헌

[1] 유성호, 김기현, 황용호, 이필중, “상태기반 RFID 인증 프로토콜”, 정보보호학회논문지, 제14권, 제6호, pp. 57-68, 2004. 12.

[2] M. Feldhofer, S. Dominikus, Rijmen, J. Wolkerstorfer, “Strong Authentication for RFID Systems Using The AES Algorithm,” ICCHES, pp. 357-370, 2004.

[3] 구본석, 유권호, 양상운, 장태주, 이상진, “RFID 태그를 위한 초소형 AES 연산기의 구현”, 정보보호학회논문지, 제16권, 제5호, pp. 67-77, 2006. 10.

[4] 하재철, 박제훈, 하정훈, 김환구, 문상재, “검색 정보 사전 동기화를 이용한 저비용 RFID 인증 방식”, 정보보호학회논문지, 제18권, 제1호, pp. 77-87, 2008. 02.

[5] 정장영, 홍영식, “Serverless 환경에서 RFID 인증프로토콜 검증”, 2008 한국컴퓨터종합학술대회 논문집 Vol. 35, No. 1(A), pp. 77-87, 2008. 06.

[6] 조정환, 여상수, 김성권, “AES를 기반으로 하는 개선된 RFID 프라이버시 보호 프로토콜”, 한국컴퓨터종합학술대회 2005 논문집 Vol. 32, No. 1(A), pp. 100-102, 2005. 07.