EPC Gen2 플랫폼 상에 구현 가능한 경량의 상호 인증 프로토콜

이홍진 ○ 김성호 맹범기 정한울 박용수

한양대학교 전자컴퓨터통신공학과

maddrum@hanyang.ac.kr, mptstory@hanyang.ac.kr maengbk@hanyang.ac.kr wooli44@hanyang.ac.kr

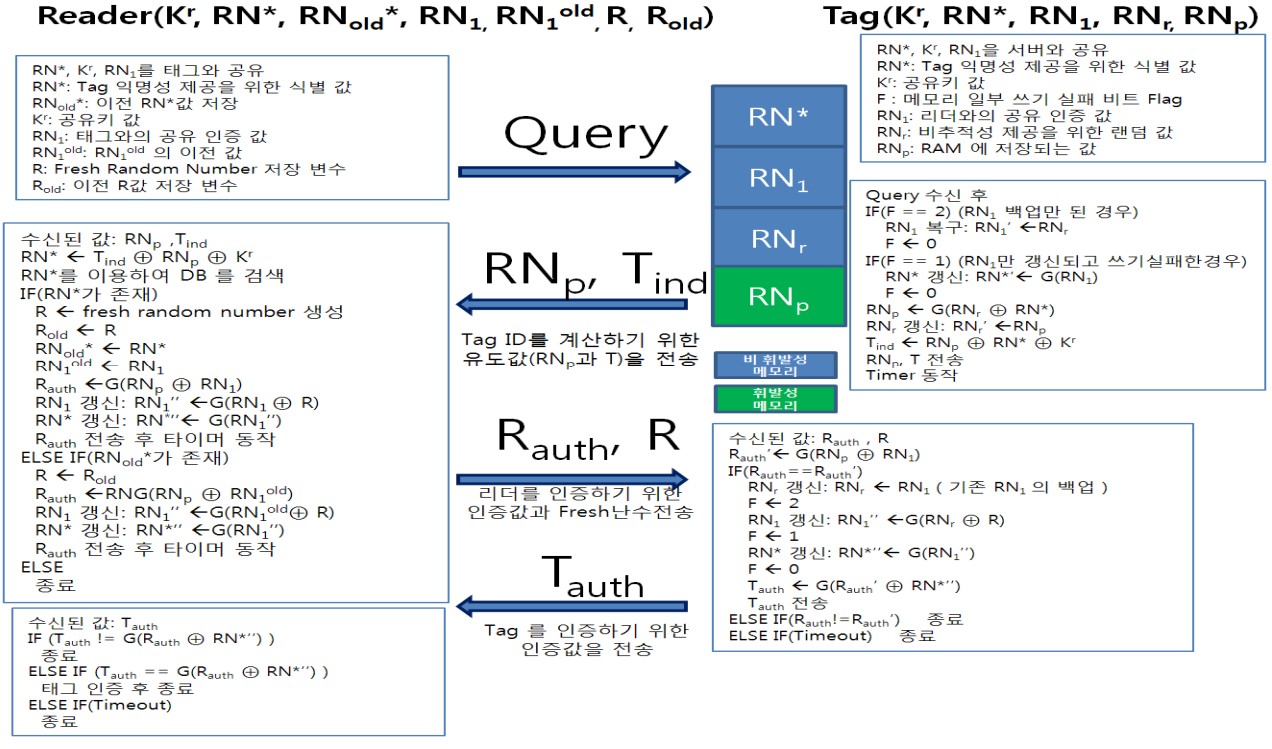
yongsu@hanyang.ac.kr

A Lightweight Mutual Authentication Security Protocol tailored for EPC Gen2 Platforms

Hongjin Lee○ Sungho Kim Beomki Maeng, Hanwool Jeong, Yongsu Park

Department of Electronics Computer Engineering, Hanyang University

RFID 태그의 통신을 위하여, EPCglobal 사에서 제정한 Class1 Gen2 Revision[1] 표준 프로토콜이 통상 널리 사용되고 있다. 그러나 EPC Gen2 표준 프로토콜은 효율성에만 중점을 둔 나머지 통신 도청을 통한 재생공격, 스푸핑공격, 트래킹 공격 등을 통한 프라이버시 문제 등 보안문제에 매우 취약하다. 따라서 본 논문에서는 EPC Gen2 플랫폼상에서 사용하는 안전하지 못한 PRNG(Pseudo Random Number Generator) 와 XOR(Exclusive OR)만을 사용하면서도 위의 보안 위협 사항 및 요구사항을 해결한 안전하면서도 효율적인 프로토콜 설계방식을 제안한다. [2]에 발표된 [3] 프로토콜을 개선하여 설계하였으며, [3]에서 실제 태그의 물리적 ID 및 공유키를 저장하는 공간을 제외한 프로토콜 메시지 교환 및 내부 값 갱신을 위해 사용되는 메모리 공간의 사용량을 줄였다. 제안 프로토콜은 16 비트를 저장하기 위한 4개의 공간만이 사용되며 이 중 3개의 공간은 비휘발성 메모리로 나머지 1개의 공간은 휘발성 메모리로 사용되지만 [3]에서 사용되는 메모리 공간은 비휘발성 메모리에 16비트 2공간, 휘발성 메모리에 3공간이 사용된다. 이외에도 본 논문에서는 다양한 프로토콜 위협 사항 및 보안 위협사항에 대한 적용 및 분석을 하였으며, 구현 효율성 및 보안 기능을 제공함에 있어 기존에 발표된 타 프로토콜과의 보안 기능성을 비교해 봄으로써 이를 입증하였다.



* 본 연구는 2010 년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2009-0069740, 2009-0090108)

RFID 리더는 서버와 서로 연결되어 있으며 안전하다고 가정하며 태그 식별을 위해 사용되는 값과 인증을 위해 사용되는 값이 각각 존재하고 이 두 값은 랜덤화되어 태그 인증이 수행될 때마다 계속하여 변경되는 동시에 동기화가 수행된다. 또한 EPC Gen2 태그 플랫폼에서 사용하는 약한 안전성을 제공하는 PRNG를 사용하게 되므로 리더측에서 매번 신선한(Fresh) 난수(Random Number)를 태그에게 전송하여 안전성을 보강하는 방식을 사용한다.

위의 그림은 제안 프로토콜의 통신과정을 도시한 그림이다. 프로토콜 작동 방식을 간단하게 설명하면 다음과 같다. (1) 리더가 태그에게 Query 메시지 전송한다. (2) Query를 수신한 태그는 재생 공격 및 트래킹 공격을 막기 위하여 통신 수행마다 계속하여 변경되는 태그 식별 값 계산 유도 및 정당한 리더를 확인하기 위한 목적의 챌린지 메시지를 생성하여 리더에게 응답한다. 이 때 통신을 수행할 때마다 태그응답메시지를 계속하여 변경하기 위하여 비추적성 제공 목적으로 저장된 랜덤값(RN_r)을 사용하며 이 값은 PRNG를 통해 계속하여 변경된다. 또한 태그 리더간 공유키(K^r)값은 태그 식별값(RN*)을 값을 감추는데 사용한다. PRNG($RN_r \oplus RN*$)를 RN_p라 하면 결국 태그의 응답 메시지는 RN_P, $RN_P \oplus RN* \oplus K^r$ 를 함께 보내는 것으로서 구성된다. (3) 리더는 태그로부터 태그 식별 유도 챌린지(RN_P, $RN_P \oplus RN* \oplus K^r$) 메시지를 수신하고 수신된 RN_P 와 리더에 저장된 공유키(K^r)를 이용하여 태그 식별값(RN*)을 계산해 낸다. 또한 태그에게 리더를 인증시키기 위한 값(R_{auth})을 PRNG($RN_P \oplus RN_1$)을 계산하여 만들어 낸다. 계산된 태그 식별값(RN*)은 리더와 연결된 데이터베이스를 통해 검색되고 해당 태그가 검색되면 태그 식별을 위한 값(RN*)과 인증을 위해 사용되는 값(RN_1)을 신선한 랜덤넘버(R)를 생성해 RN_1' ←PRNG($RN_1 \oplus R$), RN*' ← PRNG(RN_1')의 방법으로 변경한다. 각 값들은 비동기화를 막기 위해 각각의 이전 값들(RN_{old}*, RN_1^{old}, R_{old})을 함께 저장한다. 이후 R_{auth}, R을 함께 태그에게 전송한다. (4) 태그는 PRNG($RN_P \oplus RN_1$)를 계산하여 수신된 R_{auth} 값과 비교해 보고 같을 경우 기존의 RN_1을 RN_r에 백업하고($RN_r \leftarrow RN_1$) 수신된 R을 이용하여 RN_1과 RN*를 RN_1' ← G($RN_r \oplus R$), RN*' ← G(RN_1')의 방법으로 갱신한다. 이후 G($R_{auth} \oplus RN*$')를 T_{auth}라 하면 리더에게 태그를 인증시키기 위하여 T_{auth}값을 리더에게 전송한다. (5) T_{auth} 값을 수신한 리더는 G($R_{auth} \oplus RN*$')를 계산하여 T_{auth} 와 서로 같으면 성공적인 태그 인증을 수행한다..

제안 프로토콜을 사용하면 통신 재생 공격, 트래픽 분석 공격, 스푸핑 공격, 트래킹 문제, 태그 및 리더로의 위장 공격, 오프라인 중간자 공격, 태그 및 리더의 비동기화로 인한 태그 서비스 거부 공격 문제 등을 해결하기 위하여, 태그 리더간 상호 인증 기능, 태그의 기밀성 보호 및 익명성 제공을 위한 불추적성 기능, 태그 가용성 제공을 위한 비동기화 공격 저항 기능 및 그외 다양한 공격(스푸핑, 재생공격, 오프라인 중간자 공격 등)에의 저항 기능, 트래픽 분석을 통해 이전 및 미래의 통신 내용을 추측할 수 없게 하기 위한 전•후방향 안전성 기능 등을 수행 할 수 있으며, 이외에도 통신 과정 중 태그 내 메모리 쓰기실패가 발생할 경우 이를 복구할 수 있도록 태그의 인증값을 백업하는 기능이 제공된다.

또한 EPC Gen2 표준에 적합한 의사난수생성기(PRNG)를 구현하는 비용은 [4]에서 제시한 방법으로 구현할 경우 1435 게이트(gate)이가 필요하며 [5]에서 제시한 방법으로 구현할 경우 1566 게이트가 필요하게 되는데, 일반적으로 안전성을 위하여 해시 함수를 사용하여 태그를 구현할 경우 필요한 게이트 수는 최소 3000 게이트 이상으로 알려져 있으므로[6] 본 프로토콜은 하드웨어 구현 비용의 측면에서 비교적 저렴함을 알 수 있다.

참고 문헌

[1] EPCGlobal Gen2 Class1 Revison, http://www.epcglobalinc.org/standards/uhfc1g2

[2] RFIDsec' 09, The 5th Workshop on RFID Security, June 30 - July 2, Leuven, 2009.

[3] Burmester, M., and Munilla, J." A Flyweight RFID Authentication Protocol", In RFIDSec09 The 5th Workshop on RFID Security, June 30 - July 2, Leuven, Belgium, 2009.

[4] Coppersmith, D., Krawczyk, H., and Mansour, Y., The shrinking generator. In Proc. Advances in Cryptology (CRYPTO 1993). LNCS. Springer, 22- 39. 1994.

[5] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., and Ribagorda, A. , LAMED - A PRNG for EPC Class-1 Generation-2 RFID specification., Comput. Stand. Interfaces 31, 1, 88- 97, 2009.

[6] M. O' Neill (McLoone)," Low-cost SHA-1 Hash Function Architecture for RFID Tags", in workshop on RFID Security(RFIDSec' 08), 2008.