TRMA: 2-패스 RFID 상호 인증 프로토콜

안해순*, 남인길**
*대구대학교 컴퓨터정보공학과
**대구대학교 컴퓨터·IT공학부
e-mail: ahs221@hanmail.net, ignam@daegu.ac.kr

TRMA: Two-pass RFID Mutual Authentication Protocol

Hae-Soon Ahn*, In-Gil Nam**
*Dept. of Computer Information Engineering, Daegu University
**School of Computer & Information Technology, Daegu University

요 약

RFID 시스템에서 리더와 태그간의 통신은 안전하지 않은 채널을 통하여 수행된다. 최근 Lee등은 해쉬 함수와 동기화된 비밀 정보를 이용한 RFID 상호 인증 프로토콜인 LAK 프로토콜을 제안하였다. 하지만 Cao-Shen은 LAK 프로토콜이 재전송 공격에 취약하며, 공격자가 합법적인 태그로 위장할 수 있음을 증명하였다. 본 논문에서는 안전한 일방향 해쉬 함수를 기반의 새로운 2-패스 RFID 상호 인증 프로토콜인 TRMA 프로토콜을 제안한다. 제안한 TRMA 프로토콜은 RFID 태그와 리더 간에 2라운드만을 수행하여 상호 인증을 수행할 수 있으며, 여러가지 공격들에 안전하며 통신 효율성을 보장한다.

1. 서론

유비쿼터스 컴퓨팅(Ubiquitous Computing) 네트워크 환경에서 RFID(Radio Frequency IDentification) 기술은 근거리 무선 통신(Near Field Communication) 기술들 중에서 가장 주목받는 기술 중의 하나이다. RFID 시스템은 개체 추적 및 모니터링, 티켓팅, 공급망 관리, 비접촉식 지불 시스템 등과 같은 IT 응용 산업에서 엄청난 생산 이익을 창출하고 있다[1].

일반적으로 RFID 시스템은 태그(Tag), 리더(Reader), 그리고 백-엔드 데이터베이스(Back-end Database) 세 가지 요소로 구성된다. 특히 RFID 시스템에서의 태그와 리더 간의 통신은 안전하지 않은 채널상에서 수행되므로 송수신되는 데이터가 공격자에 의해 쉽게 도청당하고 위조될 수 있다. 따라서 다양한 RFID 응용 환경상에서 보안과 프라이버시 제공을 위해 인증(Authentication) 기능은 필수적으로 제공되어져야 한다[2-5].

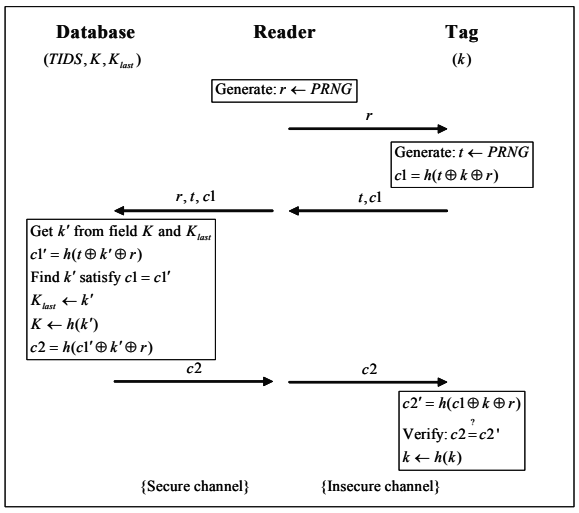
일반적으로 RFID 태그는 제한된 연산과 메모리 자원을 가지고 있는 저비용 태그임으로 대칭키 알고리즘 및 공개키 알고리즘과 같은 비싼 암호화 연산을 수행할 수 없다. 따라서 대부분의 RFID 시스템은 효율성과 안전성을 제공하기 위해서 해쉬 함수와 난수 생성기를 이용한 다양한 경량 RFID 인증 프로토콜들이 구현 및 사용되고 있다. 최근 Lee등은[3] 해쉬 함수와 동기화된 비밀 정보를 이용한 RFID 상호 인증 프로토콜인 LAK 프로토콜을 제안하였다. Chien-Huang[4] 또한 난수 생성기를 기반으로한 Lee 등이 제안한 LAK 프로토콜과 유사한 경량 RFID 인증 프로토콜을 제안하였다. 하지만 Cao-Shen[5]은 LAK 프로토콜이 재전송 공격에 취약하며, 공격자가 임의의 합법적인 태그로 쉽게 위장할 수 있음을 증명하였다. 즉, 공격자는 과거에 수행된 세션에서 리더와 태그 간의 송수신된 정보를 도청하여 임의의 세션에서 도청한 정보를 재전송하는 재전송 공격을 수행할 수 있음을 보였다.

본 논문에서는 위와 같은 보안 취약점들을 해결 할 뿐만아니라 통신 효율성을 고려한 일방향 해쉬 함수 기반의 간단한 2-패스 RFID 상호 인증 프로토콜인 TRMA를 제안한다. 제안한 TRMA 프로토콜은 RFID 태그와 리더간에 2라운드만을 수행하여 상호 인증을 수행할 수 있으며, 알려진 다양한 공격들에도 안전할 뿐만 아니라 통신 효율성면에서도 우수함을 보장한다.

2. LAK RFID 프로토콜

본 논문에서 사용되는 기호의 정의는 다음과 같다.

- Query: 태그의 응답을 요청하는 쿼리, - T: RFID 태그,
- R: RFID 리더,- DB: 백-엔드 데이터베이스
- TID: 태그 T의 ID, - RID: 리더 R의 ID
- k: 태그 T의 현재 비밀값, - k_{last}: 태그 T의 이전 비밀값
- K: DB 내에 태그 T를 위한 현재 비밀값 필드
- K_{last}: DB 내에 태그 T를 위한 이전 비밀값 필드
- TIDS: DB 내에 태그 T를 위한 ID 필드
- Data: DB 내에 태그 T를 위한 제품 정보 필드
- h(): 안전한 해쉬 함수, - PRNG: 의사난수 생성기
- ⊕: 비트 단위 배타적논리합(XOR) 연산, - ||: 연접 연산



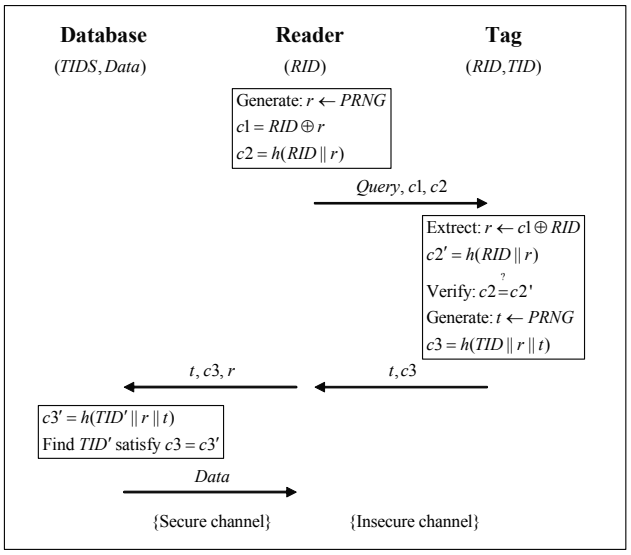
(그림 1) LAK 프로토콜

그림 1은 LAK RFID 상호 인증 프로토콜에서의 인증 수행 과정을 보여준다.

3. 제안한 TRMA 프로토콜

본 장에서는 간단한 2-패스 RFID 상호 인증 프로토콜인 TRMA 프로토콜을 제안한다. 제안한 저비용 RFID 태그 기반의 TRMA 프로토콜은 태그 위조를 방지 및 프라이버시 보호를 위해 간단한 배타적논리합(XOR) 연산과 안전한 일방향 해쉬 함수를 사용한다. 제안한 프로토콜의 가장 중요한 핵심은 셋업(Setup) 단계에서 태그의 메모리 내에 인증된 리더의 ID인 RID 값을 저장한 후, 인증 단계에서 태그와 리더 모두 공유하고 있는 RID 값을 이용하여 안전하게 리더를 먼저 인증하고, 이후 태그를 인증하여 상호인증을 수행하게 된다.

제안한 TRMA 프로토콜에서는 DB, 리더 그리고 태그가 XOR 연산과 안전한 일방향 해쉬 함수인 $h(): \{0, 1\}^* \rightarrow \{0, 1\}^l$을 수행할 수 있다. 또한 리더는 난수 생성기를 가지고 있으며, 태그 또한 리더와 마찬가지로 동일한 난수 생성기를 가지고 있다. 128비트 길이를 가지는 두 비밀값 RID와 TID는 태그 T의 비휘발성 메모리 내에 안전하게 저장되어 있다. RID는 리더의 ID를 식별하기 위해 사용되고, TID는 태그의 ID를 식별하기 위해 사용된다. DB는 RFID 태그 ID들과 각 태그의 제품 정보를 각각 저장하고 있는 TIDS 필드와 데이터 필드를 가지고 있다. 최초에는 TIDS들과 데이터에는 태그 ID값들과 각 태그의 초기 데이터정보로 각각 설정된다. 그림 2는 제안한 TRMA 프로토콜의 인증 수행 과정을 보여준다.



(그림 2) 제안한 TRMA 프로토콜

4. 효율성 분석

<표 1>은 제안한 TRMA 프로토콜과 LAK 프로토콜의 효율성을 비교 및 분석한 결과를 보여준다. LAK 프로토콜은 DB 측에서 n+2번의 해쉬 연산과 2n+2번의 XOR 연산이 요구되지만, 제안한 TRMA 프로토콜은 DB 측에서 n번의 해쉬 연산만 요구된다. 따라서 제안한 TRMA 프로토콜이 LAK 프로토콜보다 훨씬 효율적이라는 것을 알 수 있다. LAK 프로토콜은 리더 측에서 1번의 난수 생성 연산을 하며, 제안한 TRMA 프로토콜은 리더 측에서 1번의 해쉬 연산, 1번의 XOR 연산, 1번의 난수 생성 연산을 한다. 하지만 리더는 태그보다 훨씬 더 강력한 성능을 가짐으로 리더는 1번의 해쉬 연산과 1번의 XOR 연산을 쉽게 수행할 수 있다. LAK 프로토콜은 태그 측에서 3번의 해쉬 연산, 4번의 XOR 연산 그리고 1번의 난수 생성 연산을 수행하지만, 제안한 TRMA 프로토콜은 태그 측에서 2번의 해쉬 연산, 1번의 XOR 연산 그리고 1번의 난수 생성 연산을 한다. 이는 제안한 TRMA 프로토콜이 LAK 프로토콜보다 훨씬 더 효율적이라는 것을 보여준다. 결론적으로 제안한 TRMA 프로토콜이 경량 RFID 시스템에 더 쉽게 채택할 수 있다. 또한, 제안한 TRMA 프로토콜은 LAK 프로토콜과는 달리 더 적은 수의 통신 라운드를 사용한다. 위와 같은 이유로 본 논문에서 제안한 TRMA 프로토콜이 LAK 프로토콜보다 효율성 면에서 훨씬 더 우수함을 명백하게 보여준다.

<표 1> 효율성 비교

프로토콜 / 연산종류	LAK 프로토콜[3]			TRMA 프로토콜		
	DB	리더	태그	DB	리더	태그
해쉬 연산	n+2	0	3	n	1	2
XOR 연산	2n+2	0	4	0	1	1
랜덤 값	0	1	1	0	1	1
통신 라운드수	5			4		

n : 백-엔드 데이터베이스에 저장된 태그수

5. 결론

본 논문에서는 안전한 일방향 해쉬 함수를 기반으로 새로운 간단한 2-패스 RFID 상호 인증 프로토콜인 TRMA 프로토콜을 제안하였다. 결론적으로 제안한 TRMA 프로토콜은 RFID 태그와 RFID 리더 간에 2라운드 수행에 의한 상호 인증을 수행하기 때문에 통신 효율성을 보장할 뿐만 아니라 다양한 공격들에 대해서도 안전하다.

참고문헌

[1] D. Lin, H. G. Elmongui, E. Bertino, and B. C. Ooi, "Data management in RFID applications", International conference on database and expert systems applications, LNCS 4653, pp. 434-444, 2007.

[2] K.Finkenzeller, "RFID handbook: fundamentals and applications in Contactless smart cards and identification", (2nd ed.), Munich, Germany: Wiley, 2003.

[3] S. Lee, T. Asano, and K. Kim, "RFID mutual authentication scheme based on synchronized secret information", In proceedings of the SCIS'06, 2006.

[4] H. Y. Chien and C. W. Huang, "A lightweight RFID protocol using substring", EUC 2007, LNCS 4808, pp. 422-431, 2007.

[5] T. Cao and P. Shen, "Cryptanalysis of two RFID authentication protocols", International journal of network security, In press, 2008.