제한적 위임을 지원하는 RFID 인증 프로토콜†

함형민, 오희국
한양대학교 컴퓨터공학과
e-mail:hmham@infosec.hanyang.ac.kr, hkoh@hanyang.ac.kr

A RFID Authentication Protocol Providing Limited Delegation

Hyoungmin Ham, Heekuck Oh
Department of Computer Science Engineering, Hanyang University

요 약

태그의 식별을 DB에 의뢰하는 것에 의존적인 RFID기반 시스템은 리더와 DB가 서로의 통신반경 밖에 있거나 기반 통신망이 없어 DB와 연결이 어려운 환경에서는 응용이 제한적이며, 정상적인 경우에도 병목현상의 가능성을 갖고 있다. 본 논문은 DB가 태그의 인증기능을 리더에게 대리 위임하여 자체적으로 인증을 수행할 수 있는 RFID인증프로토콜을 제안한다. 제안하는 기법은 DB와의 통신범위 제한에 비교적 자유롭고, 리더 자체적으로 태그인증이 가능하며, 부가적으로 DB의 연산부하를 경감시킬 수 있다.

1. 서론

RFID는 USN환경에 핵심적인 기술이다. 특히 수동형 RFID 태그는 바코드를 대체할 수단으로 주목받고 있으며, 이미 각종 RFID 태그가 공정라인이나 유통단계, 결제수단 등 다양한 응용분야에 적용되고 있다. RFID 태그는 비교적 소형에 생산단가 또한 낮은 편으로 USN에서 필요한 기본 요건을 충족하지만, 보안을 적용하지 않은 태그가 개인에게 확산될 경우 프라이버시문제가 발생하게 되며, 이에 여러 가지 프라이버시 연구가 이루어졌다[3][4][5][6][7]. 상당수의 보안 기법들은 태그의 식별을 DB에 의뢰하는 것에 의존하고 있으나, 이러한 형태의 시스템은 리더가 DB와 연결할 수 없는 환경에서는 응용이 어렵고, DB에 병목현상이 일어날 수 있다. 본 논문은 DB와 리더간에 역할의 분산이 가능한 위임인증기법을 제안한다. 2장에서 위임기법의 개념을 소개하고, 기존에 제안된 RFID 위임기법을 분석한 뒤, 3장에서 새로운 위임인증기법을 제안하고 이를 분석한 후 결론을 맺는다. 위임기법은 DB에의 병목현상을 완화시켜주고, DB와 리더의 통신이 어려운 특수한 환경에서도 응용 가능하므로 앞서 제시한 문제의 적절한 해결책이 될 수 있다.

2. 관련연구

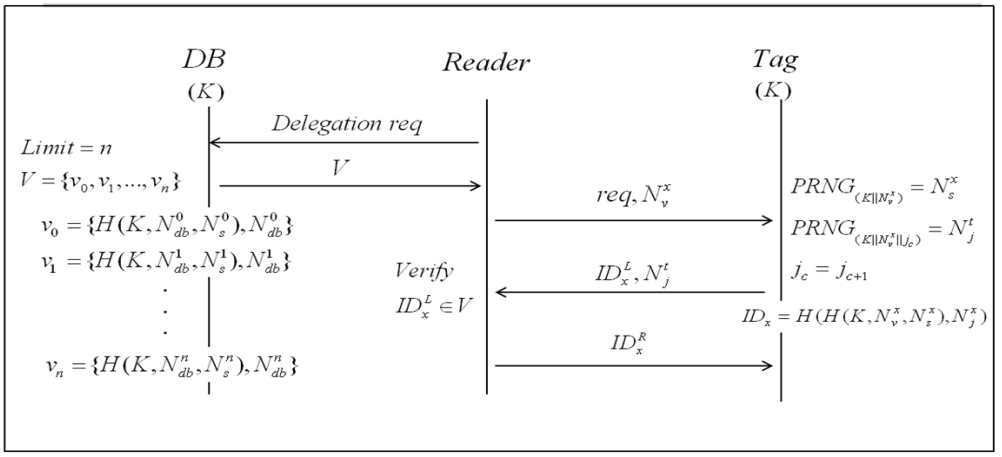
2.1. 위임(Delegation)[1][2]

위임이란 특정권한을 갖는 소유자가 다른 위임자에게 자신이 가진 권한의 일부 혹은 전부를 부여하여 대리수행을 가능하게 하며, 권한을 다시 회수할 수 있는 제한적인 권한 이동 행위를 말한다. RFID 위임은 다음과 같은 특징을 갖는다. 첫째, 리더를 위임 대상으로 한다. 이는 DB를 증설하는 것보다 효율은 떨어지지만 일정수준 집중현상을 완화시켜주고, 추가비용 없이 비교적 간단히 적용할 수 있는 이점이 있다. 둘째, DB와 연결 없이도 제한적으로 식별이 가능하다. 위임이 가능한 RFID 프로토콜은 DB와 연결이 어려운 환경에서 활용할 수 있으므로 응용측면에서 장점을 갖는다.

2.2. 기존에 제안된 위임 기법

D. Molnar등은 Pseudonym을 이용한 위임기법을 제안하였다[1]. 태그와 DB간에 트리형태의 Pseudonym set을 공유하고 매 세션마다 1회성 Pseudonym을 이용하여 비구별성을 만족한다. 공유한 Pseudonym을 다 소비했다면 응답이 불가능하므로 DB와 공유된 Pseudonym 트리를 새로 저장해야 한다. 태그를 폐기한다고 해도 태그의 수명이 길어질수록 이에 비례하여 메모리 용적량이 증가하므로 일부 저가형 태그에는 적절하지 않을 수 있다. 위임된 리더는 DB로부터 Pseudonym 트리의 서브트리를 위임받고, 서브트리의 Pseudonym만큼 태그를 식별할 수 있다. S. Fouladgar등은 태그의 저연산 능력을 고려한 위임 프로토콜을 제안하였다. 태그를 인증할 수 있는 정보 K_S를 리더에게 위임하고 원하는 때에 K_U를 태그에게 전달해 K_S를 갱신하여 권한을 회수하는 방식이다. 그러나 리더를 무조건 신뢰하기 어려운 환경일 경우[8], 리더는 무제한으로 태그의 식별이 가능하므로 응용분야가 한정될 수 있다.

† 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터(홈네트워크연구센터) 육성·지원사업의 연구결과로 수행되었음.



(그림 1) 위임 인증 프로토콜

3. 제안하는 프로토콜

제안하는 프로토콜의 보안요구사항은 다음과 같다.

첫째, 인증프로토콜은 일반적인 RFID 보안요구사항을 만족해야 한다. 이는 기본적으로 RFID 보안프로토콜에서 보장되어야 할 사항으로, 태그의 응답은 비구별성을 만족해야하고, 도청에 강건하도록 기밀성을 유지해야하며, 재전송공격이 불가능해야 한다. 추가적으로 제조단가 문제로 태그에 물리적저항성 구현이 어려우므로 태그의 현재 상태가 노출되었을 때, 전방향 안전성을 보장할 수 있어야 한다.

둘째, 리더가 위임받은 정보는 외부에 노출되어도 DB의 정보 노출과 관련이 없어야 한다. 모바일리더는 휴대되고, 이동되므로 분실되거나 정보가 노출될 가능성이 상대적으로 높다. 리더가 유지하는 위임 정보로부터 DB의 고유정보와의 연관성을 찾는 것이 불가능해야 한다.

제안하는 프로토콜에서 가정하는 리더는 기존연구에서 제안된 것처럼 DB와 무선통신이 가능하며, 일반적인 RFID 리더보다 향상된 메모리 및 연산능력을 갖춘 모바일 디바이스를 의미한다[8][9][10][11].

3.1. 표기법

DB : 데이터베이스

$Reader$: 리더

Tag : 태그

K : DB와 Tag간 공유 비밀정보

N : nonce

$PRNG_{(.)}$: nonce생성

$H(.)$: 일방향해시함수

ID : 태그의 응답. $ID_i = ID_i^L \| ID_i^R$

V : 자체 식별을 위한 위임 정보.

$V = \{v_0, v_1, ..., v_n\}$

v_x : $v_x = \{H(K, N_v^x, N_s^x), N_v^x\}$

3.2. 프로토콜 진행

프로토콜은 다음과 같은 순서로 진행된다.

(1) 초기화

- DB와 리더간에 안전한 채널로 V를 받는다.

(2) 대리인증

- 리더는 임의의 v_x를 선택한다.
- v_x의 N_{db}^x을 요청과 함께 태그에 전달한다.
- 태그는 N_s^x, N_j^t를 계산하고 임의의 상수j_c를 증가시킨다.
- 태그는 ID_x를 계산하고 질반을 전송한다.
- 리더는 $ID_x^L \in v_x$인지 검증한다.
- 리더는 검증이 성공하면 ID_x^R을 전송한다.

프로토콜 진행을 수식으로 표현하면 다음과 같다.

$$R \rightarrow T : req, N_v^x$$
$$T : PRNG_{(K\|N_v^x)} = N_s^x$$
$$PRNG_{(K\|N_v^x\|j_c)} = N_j^t$$
$$ID_x = H(H(K, N_{db}, N_s^t), N_j^t)$$
$$T \rightarrow R : ID_x^L, N_j^t$$
$$R : Verify\ ID_x^L \in V$$
$$Verify$$
$$if\ (ID_x^L \in v_x)$$
$$R \rightarrow T : ID_x^R$$
$$else$$
$$fail$$
$$discard\ v_x$$

4. 프로토콜 분석

안전성 분석은 다음과 같다.

4.1. 기밀성

제안하는 기법은 통신 메시지에 K를 포함하여 K의 비밀성에 의존해 안전한 통신을 지원한다. 공격자는 도청으로 통신에 필요한 정보를 얻을 수 없으며, 메시지의 변조 공격이 어렵다.

4.2. 비구별성

태그는 세션마다 자체적으로 생성하는 난수 N_j^t를 응답에 포함한다. 공격자는 K, N_s^{cr}를 알지 못하면 난수 N_j^t에 의해 매번 달라지는 태그의 응답을 구별할 수 없다. 제안하는 프로토콜은 기밀성을 만족하므로 공격자는 응답을 구별하기 위한 정보를 얻을 수 없으며, 태그의 응답은 비구별성을 만족한다.

4.3. 전방향 안전성

공격자가 일정기간 동안 태그의 이동범위 안에서 이전 세션의 모든 메시지를 수집해두었고, 그 이후에 물리적인 공격으로 태그의 K가 노출되었다고 가정하였을 때, 태그의 과거 행적이 추적 가능하므로 완전한 전방향 안전성을 보장하지 못한다.

5. 결론

태그의 식별을 DB에 의뢰하는 것에 의존하는 시스템은 리더가 DB와 연결할 수 없는 환경에서의 응용이 제한되고, 요청의 집중으로 DB에 병목현상이 일어날 수 있다. 본 논문에서는 이러한 문제를 해결하기 위한 방안으로 DB에서 리더로 역할의 분산이 가능한 RFID 위임기법을 제안하였다. 제안된 RFID 위임기법은 기존에 제안된 기법에 비해 태그가 반영구적으로 사용될 수 있으며 리더는 권한 만료까지 자체적으로 태그의 인증이 가능하므로 응용의 폭이 넓고, 부가적으로 태그 인증에 필요한 DB와 리더의 통신 빈도 및 DB의 연산량을 감소시킬 수 있어 병목현상을 완화할 수 있는 장점이 있다. 안전성 측면에서는 수동적, 능동적 공격으로부터 안전하지만 키의 노출을 가정할 경우 전방향 안전성을 만족하지 못한다.

참고문헌

[1] D. Molnar, A. Soppera, and D. Wagner, “A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags,” Selected Areas in Cryptography-SAC 2005, Lecture Notes in Computer Science, Volume 3897/2006, 2005.

[2] S. Fouladgar and H. Afifi, “A Simple Delegation Scheme for RFID Systems (SiDeS),“2007 IEEE International Conference on RFID Gaylord Texan Resort, Grapevine, TX, USA, March 26-28, 2007.

[3] Chiu C. Tan, Bo Sheng, and Qun Li, ”Serverless Search and Authentication Protocols for RFID,” Proc. 5th IEEE Conf. on Pervasive Computing and Communications Workshop, Newyork, USA, pp. 3-12, 2007.

[4] T. Dimitriou, “A lightweight RFID protocol to protect against traceability and cloning attack,”In Proc. of the SecureComm 2005, pages 59 - 66, 2005.

[5] M. Ohkubo, K. Suzuki, S. Kinoshita, “A cryptographic approach to a ′privacy-friendly′ tags,” RFID Privacy Workshop, MIT, 2003.

[6] D. Molnar, D. Wagner, “Privacy and security in library RFID: issues,” practices and architectures, Proceedings of the 11th ACM conference on Computer and communications security, ACM Press, pp. 210 - 219, 2004.

[7] A. Juels, “RFID Security and Privacy: A Research Survey,” Selected Areas in Communications, IEEE Journal on, Vol. 24, pp. 381- 394, 2006.

[8] KONIDALA Divyan M, KIM Kwangjo, ”Mobile RFID applications and security challenges”, Information security and cryptology:(ICISC 2006), 9th International conference, Busan, Korea, 2006.

[9] A. Juels, P. Syverson, and D. Bailey, “High-Power Proxies for Enhancing RFID Privacy and Utility”, CHACS2005, LNCS 3856, pp.210-226, 2005.

[10] Soo-Cheol Kim, Sang-Soo Yeo, Sung Kwon Kim, “MARP: Mobile Agent for RFID Privacy Protection.” 7th Smart Card Research and Advanced Application IFIP Conference(CARDIS′06), Lecture Notes in Computer Science, vol. 3928, pp. 300-312, 2006.

[11] M. Rieback, B. Crispo, and A. Tanenbaum, “RFID Guardian: A Battery-powered Mobile Device for RFID Privacy Management,” ACISP 2005, LNCS 3574, pp. 184-194, 2005