효율적이고 안전한 해쉬함수 기반의 RFID 상호 인증 프로토콜

안해순*, 윤은준**, 남인길***, 부기동****
*대구대학교 컴퓨터정보공학과
**경북대학교 전자전기컴퓨터학부
***대구대학교 컴퓨터IT공학부
****경일대학교 컴퓨터공학부
e-mail:ahs221@hanmail.net

A Efficient and Secure RFID Mutual Authentication Protocol based on Hash Function

Hae-Soon Ahn*, Eun-Jun Yoon**, In-Gil Nam***, Ki-Dong Bu****
*Dept of Computer Information Engineering, Dae-gu University
**School of Electrical Engineering and Computer Science Kyungpook National University
***School of Computer & Information Technology, Dae-gu University
****School of Computer Engineering, Kyung-il University

요 약

본 논문에서는 기존에 제안된 RFID 인증 프로토콜이 임의의 RFID 태그로 위장한 공격자로부터 스푸핑 공격을 당할 수 있음을 증명하고, 이러한 보안 문제점을 해결한 안전하고 효율적인 RFID 상호 인증 프로토콜을 제안한다. 제안한 RFID 상호 인증 프로토콜은 기존의 RFID 인증 메커니즘들이 가지고 있는 보안 문제점들을 해결할 뿐만 아니라, 스푸핑 공격에 대한 취약점을 해결하고, 해쉬함수 연산 오버헤드를 줄여줌으로써 빠른 인증 시간을 보장하여 더욱 강력한 안전성과 효율성을 제공한다.

1. 서론

최근 유비쿼터스 컴퓨팅에 대한 연구와 관심이 증대됨에 따라, RFID(Radio Frequency IDentification) 시스템은 유비쿼터스 기반의 핵심 기술로 주목받고 있다. RFID 시스템은 무선 주파수를 이용하여 움직이는 물체를 인식, 추적, 분류 및 인식기 간의 데이터 통신을 수행하는 자동 데이터 수집 기술이다. 그러나 물리적인 접촉 없이도 인식이 가능한 RFID 시스템의 특징과 객체를 유일하게 식별하기 위해 정보를 가지고 있는 RFID 태그는 시스템의 안전성과 개인의 정보 노출, 위치 추적 등의 프라이버시(Privacy) 침해를 유발할 수 있는 문제점을 가지고 있다[1][2].

2. 관련연구

RFID 시스템에서의 사용자 프라이버시 보호를 위해 제안된 기법들은 크게 물리적 접근기법과 비트연산(XOR) 기반, 해쉬함수 기반, 재 암호화 등 암호학적 접근기법으로 분류된다. 물리적 접근기법의 가장 단순한 방법은 Auto-ID 센터에 의해 제안된 태그 무효화(Kill) 명령어 기법으로서 태그가 자신의 데이터 필드에 저장된 패스워드를 외부에서 받은 경우, 태그를 영구적으로 정지시켜 더 이상 리더의 질의에 응답하지 않게 하는 방법이다. 이 방법은 명령이 수행된 이후, 완료되었는지 확인하기 어렵고, 한번 정지된 태그의 재사용이 불가능하다.

XOR 기반 접근기법으로는 Juels 기법과 Eunyoung 기법 등이 있으며, 읽기와 쓰기가 가능한 저가형 RFID 태그에 적합하지만 읽기전용 RFID 태그에는 적용할 수 없다는 단점이 있다.

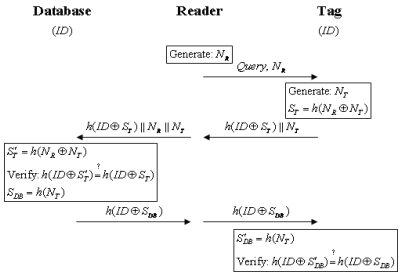
해쉬함수 기반의 대표적 기법인 해쉬락 기법은 해쉬함수를 사용하여 저가의 태그에 적용될 수 있지만, 리더와 태그 간에 동일한 해쉬 값인 metaID=h(key)를 사용하기 때문에 공격자가 태그의 위치를 추적할 수 있고, 재전송 공격, 스푸핑 공격 등이 가능한 단점을 가지고 있다[5]. 해쉬함수 이외의 암호학적 함수를 사용하는 방법으로 재 암호화 접근기법이 있다. 이 방법은 ElGamel 공개키 암호화 알고리즘을 기반으로 하여 유로화 지폐에 RFID 태그를 내장함으로써 사용자 프라이버시를 보호하지만 공개키 암호화 알고리즘을 사용하므로 재 암호화 기법을 사용하기 위해서는 별도의 인프라가 필요하다는 단점을 가진다.

2007년에 Kim-Ryoo는 기존의 RFID 인증 프로토콜 분석을 통하여 해쉬함수를 이용한 새로운 RFID 상호 인증 프로토콜을 제안하였으나[4], 제안한 상호 인증 프로토콜은 RFID 태그로 위장한 공격자로부터 스푸핑 공격에 취약하다는 단점이 있다. 본 연구에서는 이러한 보안 문제점을 개선한 RFID 상호 인증 프로토콜을 제안하고자 한다.

3. Kim-Ryoo의 프로토콜

그림 1은 Kim-Ryoo가 제안한 RFID 상호 인증 프로토콜의 전체적인 구성과 동작 과정을 보여주며, 아래와 같이

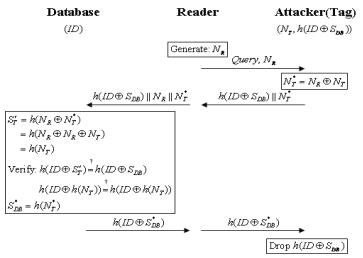
인증 프로토콜이 수행된다.



(그림 1) Kim-Ryoo의 RFID 상호 인증 프로토콜

4. 스푸핑 공격

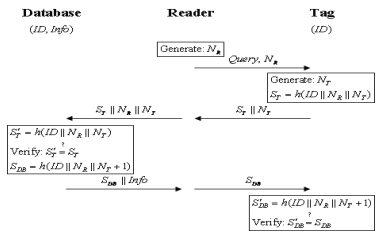
그림 2는 Kim-Ryoo가 제안한 RFID 상호 인증 프로토콜의 인증 단계에서 스푸핑 공격(Spoofing attack)[3] 과정을 보여준다. RFID 상호 인증 프로토콜은 임의의 세션에서 DB가 이전에 재전송된 태그의 인증 메시지를 쉽게 인증하는 스푸핑 공격에 취약하다.



(그림 2) 스푸핑 공격

5. 제안한 RFID 상호 인증 프로토콜

본 장에서는 Kim-Ryoo가 제안한 프로토콜의 보안 취약점을 해결한 안전한 RFID 상호 인증 프로토콜을 제안한다. 그림 3은 제안한 RFID 상호 인증 프로토콜의 전체적인 구성과 동작 과정을 보여주며, 아래와 같이 인증 프로토콜이 수행된다.



(그림 3) 제안한 RFID 상호 인증 프로토콜

<표 1>은 제안한 프로토콜과 해쉬연산 기반의 프로토콜들, Kim-Ryoo의 프로토콜과의 안전성을 비교·분석하였다. 제안한 프로토콜은 기존의 프로토콜과 비교하여 상호 인증을 명시적으로 제공함으로써 도청 공격, 재전송 공격, 스푸핑 공격, 트래픽 분석 공격, 위치 트래킹 공격, 서비스 거부 공격 등에 안전함을 알 수 있다. <표 2>는 제안한 프로토콜과 Kim-Ryoo의 프로토콜과의 효율성을 비교·분석하였다.

<표 1> 관련 프로토콜들과의 안전성 비교·분석

공격	해쉬 락	랜덤해 쉬락	해쉬 체인	재암 호화	Kim-Ryoo 프로토콜	제안 프로토콜
상호인증	○	○	×	○	○	○
도청공격	×	×	×	×	○	○
재전송공격	×	×	○	○	×	○
스푸핑 공격	×	×	×	×	×	○
트래픽 분석 공격	×	○	○	○	○	○
위치 트래킹 공격	×	○	○	○	○	○
서비스 거부 공격	○	○	○	×	○	○

<표 2> 프로토콜의 효율성 비교·분석

	Kim-Ryoo 프로토콜[11]			제안 프로토콜		
	태그	리더	DB	태그	리더	DB
해쉬 연산량	4	0	2n+2	2	0	n+1
XOR 연산량	3	0	2n+1	0	0	0
난수 생성수	1	1	0	1	1	0
태그의 쓰기연산	불필요			불필요		
리더와 정보교환수	3			3		

6. 결론 및 고찰

본 논문은 Kim-Ryoo가 제안한 RFID 상호 인증 프로토콜이 여전히 RFID 태그로 위장하여 공격자가 과거의 세션에서 사용된 인증 메시지들을 이용한 스푸핑 공격을 수행할 수 있음을 증명하였다. 또한 스푸핑 공격에 대한 보안 취약점을 해결할 뿐만 아니라 연산 오버헤드 또한 줄여주는 더욱 안전하고 효율적인 RFID 상호 인증 프로토콜을 제안하였다. 제안한 RFID 상호 인증 프로토콜은 Kim-Ryoo의 프로토콜과 비교하여 더욱더 강한 보안성과 안전성을 제공하며, 불필요한 해쉬함수 연산을 줄여 줌으로써 효율성 측면에서도 우수하다. 따라서 제안하는 상호 인증 프로토콜은 안전성과 효율성을 바탕으로 유비쿼터스 컴퓨팅 환경의 다양한 분야에 활용될 것으로 기대된다.

참고문헌

[1] F. Klaus, “RFID handbook,” Second Edition, Jone Willey & Sons, 2003.
[2] S. A. Weis, “Radio-frequency identification security and privacy,” Master's Thesis, M.I.T. 2003.
[3] 최은영, 최동희, 임종인, 이동훈, “저가형 RFID 시스템을 위한 효율적인 인증 프로토콜,” 정보보호학회논문지 15권 5호, pp.59-71, 2005.
[4] 김배현, 유인태, “반사공격에 안전한 RFID 인증 프로토콜,” 한국통신학회논문지 32권 3호, pp.348-354, 2007.
[5] Weis, S. et al, “Security and Privacy in Radio -Frequency Identification Devices”, Massachusetts Institute of Technology, 2003.