비밀키를 이용한 RFID보안 인증 프로토콜

배우식*, 이종연*, 한군희**
*충북대학교 컴퓨터교육과
**백석대학교 정보통신학부
e-mail : bws@motor.ac.kr*

RFID Security Authentication Protocol Using Secret Key

Woo-Sik Bae*, Jong-Yun Lee*, Kun-Hee Han**
*Dept. of Computer Education, Chungbuk National University
**Division of Information & Communication Baekseok University

요 약

RFID 시스템은 향후 바코드를 대체하고 우리 생활 전반에 걸쳐 사용될 획기적인 시스템 이지만 태그의 정보가 외부에 노출될 경우 심각한 문제가 발생 할 수 있다. RFID는 태그와 리더사이의 통신은 무선을 통해 이루어짐에 따라 보안상 많은 취약점이 존재한다. 본 논문에서는 여러 보안 문제중 프라이버시 보호를 위해 태그가 리더로부터 수신한 난수로부터 매 세션마다 비밀키 및 실시간으로 새로운 해쉬 함수를 생성하는 인증 프로토콜을 제안한다. 제안된 해쉬 기반 인증 프로토콜은 각종공격에 대해 안전하며 연산을 최소화하여 다양한 적용성을 제공한다.

1. 서론

RFID(Radio Frequency Identification)는 현재 바코드를 대체하기 위한 기술로서 바코드의 저장 정보는 매우 적고 다시 프로그래밍을 할 수 없는 단점이 있으며 이를 극복하기 위해서 현재 기술로는 반도체에 데이터를 저장하는 방법이 있다. 일상생활에서 많이 사용되는 형태는 신용카드, 교통카드, 전화카드, 보안카드등 스마트카드 종류가 있다. 이 스마트카드방식에는 두 가지 인터페이스가 있는데 접촉식과 비접촉식으로 구분되며 이중 비접촉식 스마트카드 시스템은 RFID 시스템의 한 범주라 할 수 있다. 이 분야는 앞으로 사용의 편리성 향상으로 개인 및 산업 전반에 활용이 예상 되며 국내·외적으로 많은 연구가 진행 되고 있다. 그러나 반도체 칩에 내장된 정보를 무선주파수를 이용하여 읽어내기 때문에 RFID기술은 도청, 트래픽 분석, 서비스거부 공격, 메시지유실, 트래킹 공격, 스푸핑 공격등 많은 취약점 들을 지니고 있어서 보안이나 프라이버시 보호에 심각한 문제를 야기할 수 있다[1][2]. 따라서 RFID시스템이 활성화되기 위한 한 가지가 바로 보안 문제이며 반드시 해결 되어야 하는 분야이다.

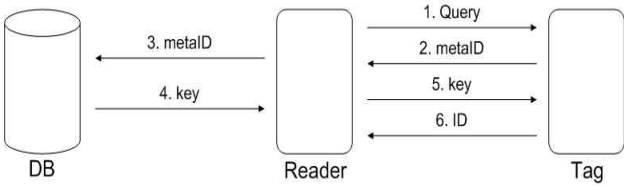
본 논문에서는 RFID의 프라이버시 문제를 해결하기 위한 기존 제안된 해쉬락(Hash-Lock)기법[3], 해쉬 체인(Hash Chain)기법[4][5], 해쉬기반 ID변형 기법[6] 등이 해결하지 못한 문제점 분석을 통해 보다 안전하고 효율적으로 사용자의 프라이버시를 보호할 수 있는 인증 프로토콜을 제안 한다.

2. 관련연구

2.1 해-쉬락 기법

태그와 데이터베이스는 태그의 ID, 키 값을 공유하여 저장하게 되며 데이터베이스와 연결된 모든 리더는 태그에 대한 키를 알 수 있으며 태그는 mataID를 저장하고 있는 상태로 기본적으로 잠겨 있게 된다. 태그가 리더의 범위에 들어오면 mataID를 전송하며 이때 리더는 태그의 mataID를 데이터베이스에 전송하고 데이터베이스는 이에 대응하는 키를 리더에게 전송한다. 이어서 태그에게 보내어

태그가 해쉬값을 계산하며 자신의 mataID와 일치하는 경우 풀림상태로 되어 리더에게 자신의 ID를 전송하는 방식이다. 태그의 식별 값인 metaID가 고정되어 있으며 출력되는 데이터가 같아 전송 되었는지 확인할 수 있다. 아래의 [그림 1]은 해-쉬락 기법의 구조도 이다.

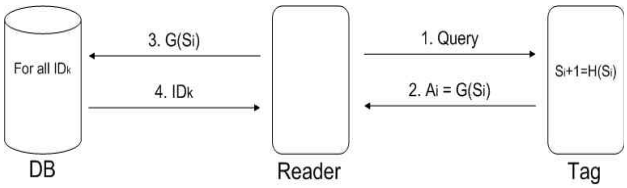


[그림 1] 해쉬-락 기법

2.2 해쉬 체인 기법

서로 다른 두개의 해쉬 함수 H와 G를 사용하는 해쉬 체인 기법은 태그가 정보 Si를 가지고 있으면, 리더와의 통신에서 Ai=G(si)를 보내고 태그의 정보는 si+1=H(si)로 갱신하여 보안을 유지하는 방식이다. 리더에게는 H함수를 사용하고 태그의 비밀 값을 갱신할 때는 G 함수를 사용하기 때문에 경로 파악을 방지할 수 있다. 그리고 잘못된 응답이 수신 되었을 경우 데이터베이스는 고유한 모든 ID에 대해 ∞번의 해쉬를 수행할 가능성이 있으며 두 개의 해쉬 함수를 사용하기 때문에 해쉬락 방식에 비해 계산 량이 많은 단점이 있다.

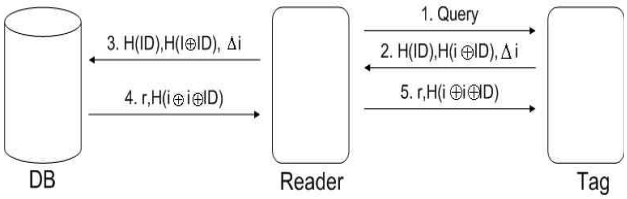
[그림 2]는 해쉬 체인 기법의 동작 과정 이다.



[그림 2] 해쉬 체인 기법

2.3 해쉬 기반 ID변형 기법

[그림 3] 는 공격자가 정당한 리더로 가장해 태그로부터 H(ID), H(i⊕ID),Δi를 획득하고, 정당한 태그가 다음 인증세션을 수행하기 전에 이 정보들을 리더의 질의에 대한 응답으로 이용하면 공격자는 정당한 태그로 인정받을 수 있는 단점이 있다.

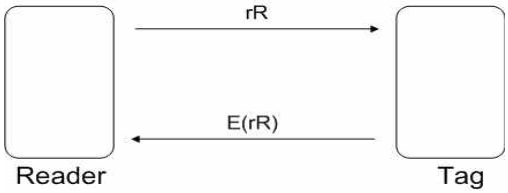


[그림 3] 해쉬 기반 ID 변형 기법

2.4 대칭형 암호화 인증 기법

[그림 4] 는 대칭형 암호화 알고리즘인 AES를 RFID에 내장하여 리더가 보낸 난수 rR를 태그가 암호화 하여 인증하는 방식이다. 수동형 태그에 13.56MHz 대역의 비접촉식 스마트카드와 유사한 통신환경이다[7][8].

대칭형 암호화 방식은 다양한 암호화 기법이 개발되었으며 암호화와 복호화 속도가 빠르다는 장점이 있지만 단점으로 키의 교환 상에 어려움이 있다. 그래서 데이터 암호화에는 대칭형 암호 방식을 많이 쓰며 데이터 교환 시에 필요한 키를 교환할 때에는 비대칭형 암호 방식을 많이 쓴다.



[그림 4] 대칭형 암호화 인증기법

3. 제안 프로토콜

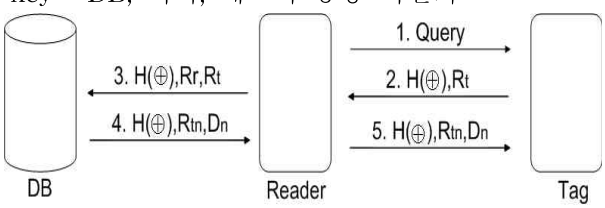
3.1 구조

리더가 처음 태그에게 질의를 할 때 난수와 실시간을 함께 전송하고, 태그는 리더로부터 수신한 난수와 실시간을 자신이 가지고 있는 ID, 비밀키 및 실시간으로 해쉬한 값을 이용하여 응답하게 된다.

제안 프로토콜에서 사용되는 파라미터는 다음과 같으며, [그림 5]는 제안하는 프로토콜의 기본 구조를 나타낸 것이다.

[파라미터]

- Query : 질의, 태그의 응답을 요청
- ID : 태그 고유의 비밀 인증 정보
- H( ) : 일 방향 해쉬 함수
- H(⊕) : $H(ID \oplus R_r \oplus T_t \oplus key)$ 연산
- R_t : 리더가 태그에게 전송하는 DB시간(μs)
- R_r : 리더가 생성하여 태그에게 전송하는 난수
- T_t : 태그에 저장되어 있는 시간(μs)
- R_{tn} : 태그에 기록될 시간(μs)
- D_n : 데이터베이스에서 태그에게 전송되는 명령
- ⊕ : Exclusive OR
- key : DB, 리더, 태그의 공통 비밀키



[그림 5] 제안 프로토콜의 구조

3.2 인증과정

① 리더는 태그들에게 Query를 브로드캐스팅 한다.

리더 → 태그 : Query,

② 태그는 ID와 자신이 가지고 있던 T_t를 R_r와 XOR연산 후 해쉬 하여, R_t와 함께 Query에 대한 응답으로 리더에게 전송한다.

태그 → 리더 : $H(\oplus), R_t$

③ 리더는 R_r와 $H(\oplus), R_t$를 백-엔드 데이터베이스로 전송한다.

리더 → 백-엔드 데이터베이스 : $H(\oplus), R_r, R_t$

④ 백-엔드 데이터베이스에 저장된 ID를 R_t, R_r,key와 해쉬한 값과 리더로부터 수신한 $H(\oplus), R_r, R_t$를 비교하여 태그를 인증한다.

백-엔드 데이터베이스 → 리더 :

계산된 $H(\oplus), R_r, R_t$ =

수신한 $H(\oplus), R_r, R_t$

인증이 성공하면 $H(\oplus), R_{tn}, D_n$를 리더에게 전송한다.

⑤ 리더는 백-엔드 데이터베이스로부터 수신한 $H(\oplus), R_{tn}, D_n$를 태그에게 전송한다.

리더 → 태그 : $H(\oplus), R_{tn}, D_n$

태그는 자신의 ID와 인증 세션에서 생성한 R_t, T_t를 XOR하여 해쉬한 값과 리더로부터 수신된 $H(\oplus), R_{tn}$를 확인하여 인증하고 R_{tn}을 기록하며 필요에 따라 D_n명령을 수행하고 인증세션을 성공적으로 종료 한다.

3.3 제안프로토콜의 안전성

3.3.1 스푸핑 공격에 대한 안전성

악의의 공격자가 정당한 리더로 가장하여 Query를 전송하면, $H(\oplus), R_t$를 획득할 수 있다. 그러나 정당한 리더의 암호화 비밀 KEY 값을 알 수가 없으며 알아낸다 할지라도 이후 데이터베이스에 응답으로 보내지게 되면 이미 시간이 지나간 상태의 정보 $H(\oplus), R_t$로는 데이터베이스에서의 인증을 할 수가 없어 결국은 스푸핑 공격이 불가능 하게 된다.

3.3.2 재전송 공격에 대한 안전성

정당한 리더의 Query에 대한 응답은 매 세션마다 변하기 때문에 $H(\oplus), R_t$도 매 세션마다 바뀌게 된다. 공격자는 매번 바뀌는 시간과 난수 및 비밀 key 값을 알아야만 공격에 필요한 자료를 얻을 수 있다. 그러므로 도청으로 획득한 $H(\oplus), R_t$를 다음 세션에서는 응답으로 사용할 수 없으므로 재전송 공격에 안전하다.

3.3.3 위치 추적에 대한 안전성

제안 프로토콜에서는 태그의 값이 매 세션 때마다 지속적으로 업데이트 되며 새로운 값으로 생성 된다. 때문에 세션이 바뀔 때는 물론 리더의 질의에 대한 태그의 응답이 바뀌므로 예측 하거나, 공격자가 Query를 태그에게 전송하여도 다음 세션에서 태그는 매 세션마다 변하는 응답 $H(\oplus), R_t$를 전송하게 된다. 그러므로 공격자는 인증이 안 되어 트래픽 분석이 불가능 하고 태그의 위치도 추적할 방법이 없게 된다.

3.4 제안 프로토콜의 효율성

태그는 해쉬 함수 연산, XOR 연산 및 실시간 데이터 저장만 하므로 저가 태그 및 모든 태그에서 구현 가능할 것이다. 또한 [표 1]과 같이 인증세션동안 해쉬함수 2회, XOR 연산2회, 난수 1회의 연산만을 수행 하므로 연산 부담도 크지 않으며 보안상 기존 프로토콜과 비교해 매우 안정적 이므로 모든 태그에 적용이 가능하다.

[표 1] 제안프로토콜의 효율성

	해쉬-락 기법	해쉬-체인 기법	해쉬기반 ID변형기법	제안프로토콜
인증	양방향	단방향	양방향	양방향
태그 연산량	해쉬1회	해쉬2회	해쉬3회	해쉬2회
리더 연산량	-	-	-	난수1회
XOR 연산량	-	-	XOR 4회	XOR 2회
DB연산량	-	n(1+i)회	해쉬3회 난수1회	해쉬1회

4. 결론

본 논문에서 제안한 프로토콜은 태그에서의 연산을 최소화 하며 비밀 키를 이용하여 기존의 연구와는 달리 공격자의 도청, 재전송 공격, 스푸핑 공격 등에 효율적으로 대처하여 보안 효과는 최대한의 효과를 낼 수 있도록 하였다. 또한 안전성 면에서도 현재까지 여러 공격 가능한 상황에 대해 안전함을 보였고 추후에는 안정성을 해치지 않은 범위 내에서

태그의 연산 량을 줄일 수 있는 방안에 대해 연구가 지속 되어야 하겠다. 비밀 키와 실시간을 이용하여 앞으로 신기술이 적용된 태그에도 실시간 데이터를 지속적으로 입력 하게 된다. 그리하여 미래에 도처에 산재되어 있는 수많은 태그 중 필요한 태그만 사용하고 오래되고 불필요한 태그들은 데이터베이스에서 보내지는 KIll 신호로 동작을 종료해 줌으로써 불필요 태그에 의한 서버부담을 줄이고 효과적으로 불필요 태그를 처리할 수 있는 방법이 될 것으로 기대된다.

참고문헌

[1] 한국정보보호진흥원 “개인정보보호 백서”, 2003.

[2] 임영덕, “유비쿼터스 컴퓨팅에서의 개인정보보호”, 성균관대학교, 석사학위논문, 2005.

[3] S. Weis et al., "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems," Security and Pervasive Computing 2003, LNCS2802, pp. 201-202.

[4] Miyako Ohkubo. Koutarou Suzuki and Shingo Kinoshita, Cryptographic Approach to "Privacy-Friendly" Tag RFID Privacy Workshop@MIT, Nov, 2003.

[5] M. Ohkubo, K. Suzuki and S. Kinoshita, "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID," Proceedings of the SCIS 2004, pp. 719-724, 2004.

[6] Gildas Avoine and Philippe Oechslin "RFID Traceability : A Multilayer Problem", Financial Cryptography, March 2005.

[7] M. Feldhofer, "A Proposal for an Authentication Protocol in a Security Layer for RFID Smart Tags," MELECON 2004 IEEE Proceedings, pp. 759-762, 2004

[8] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, " Strong Authentication for RFID Systems Using the AES Algorithm." Springer, In Conference of Cryptographic Hardware and Embeded Systrms 2004 Proceedings, pp. 357-370, 2004.