RFID 인증을 위한 해쉬함수 기반의 네트워크 보안 프로토콜

박종대° 김현석 최진영

고려대학교 컴퓨터정보통신대학원 컴퓨터공학과

pjd2000@korea.ac.kr hskim@formal.korea.ac.kr choi@formal.korea.ac.kr

Hash-based Network Security Protocol For RFID Authentication

Jongdae Park°, Hyunseok Kim, Jinyoung Choi

Department of Computer Engineering, Korea University

요 약

RFID는 무선주파수를 이용하여 부착된 태그의 정보를 얻어올 수 있는 시스템이다. 향후에 바코드를 대체할 RFID는 식품,가전, 출판,물류,재고관리,교통 등 우리생활의 전반에 걸쳐 사용될 획기적인 시스템이지만, 개인,상품 등의 프라이버시의 노출로 인한 심각한 문제가 발생될 소지가 있다. 이를 해결하기 위하여 암호화 기법, 해쉬 락 기법, 해쉬 체인 기법 등이 제안되었다.

본 논문에서는 기존에 제시되었던 인증기법들에 대해서 알아보고, 해쉬함수와 공통키를 이용하여 좀더 안전한 방법으로 리더와 태그간의 통신을 인증할 수 있는 프로토콜을 제안한다.

1. 서 론

RFID는 무선주파수인식으로 태그가 부착된 물체의 정보를 비접촉방식으로 데이터를 읽어낼 수 있는 시스템이다. 바코드를 대체할 획기적인 시스템으로 그 사용범위는 상상을 초월한 정도로 다양하다. 출입통제장치, 교통티켓발매, 개인신분확인, 차량확인 및 관리, 생산라인 감시,수화물 취급, 도서관 도서관리, 컨테이너 선적관리 등 여러 산업분야에 이용될 수 있다.[1,2] RFID 시스템의 관련기술이 발달하고, 태그의 가격이 하락하고, 법적으로 각종 제도가 마련된다면 RFID 시스템은 우리생활 도처에 존재할게 될 것이다. 또한 다양한 방법을 동원한 공격자들로 인해 개인정보나 태그정보의 유출이 발생한다면 이는 상상을 초월하는 막대한 피해를 가져올 수 있다. RFID 시스템에 있어서 보안이 중요시되는 이유가 여기에 있다. 보안문제로 생각할 볼 수 있는 것은 태그에 있는 자료의 위조, 태그와 리더사이에서의 도청, 리더와 태그가 정상적으로 통신을 하지 못하도록 하는 DOS(Denial of Service)공격, 재생공격(replay attack), 공격자 중간공격(man-in-the-middle attack) 등이 있다.[3] 이러한 보안문제를 해결하기 위해서는 좀더 안전한 방법으로 리더와 태그간에 통신이 이루어져야 한다.

본 논문에서는 RFID 시스템의 리더와 태그에 대한 안전한 인증을 위한 매커니즘에 대해서 설명하고자 한다. 2장에서는 RFID시스템의 구성과 보안요구사항 및 관련연구에 대해서 알아보고, 3장에서는 기존의 시스템을 보완한 새로운 통신 프로토콜을 제안한다. 4장에서는 프로토콜의 안전성에 대해 분석하며, 마지막으로 5장에서는 결론 및 향후 연구방향에 대해서 설명한다.

2. 관련연구

2.1 RFID 시스템의 구성

RFID 시스템은 세가지 주요 요소로 구성된다. 추적이 필요하거나 식별이 필요한 물품에 부착되는 태그, 태그에 전원을 공급 및 식별, 데이터 읽기 및 쓰기, 데이터 수집 응용 서비스를 관리하는 리더와 리더로부터 데이터 수집, 데이터베이스로의 정보입력, 수혜기관에 유용한 형태의 데이터 접근 기능을 제공하는 Back-end 서버이다.[2]

2.2 RFID 보안 요구사항

RFID 인증 시스템에서 요구되어지는 보안 사항은 다음의 사항을 만족해야 한다.[3,4,5]

A. 상호인증: 태그와 리더 사이에 상호인증이 제공되어야 한다.

B. 불추적성: 태그와 소유자 사이에 긴 시간동안의 추적이 불가능해야 한다.

C. 전방향 안전성: 공격자가 메모리의 내용을 읽더라도 이전에 수집한 다양한 태그로부터의 응답 중에서 메모리를

읽은 태그의 응답을 찾아낼 수 없어야 한다.

D. 재생공격 방지: 공격자가 태그와 리더간의 통신 중에 수집한 내용을 가지고 리더로부터 인증을 받아서는 안된다.

2.3 Hash Lock 방식

리더의 질의에 대해 태그는 ID를 해쉬한 metaID를 리더에 넘겨준다. Back-end DB에서는 metaID에 의한 ID를 찾아서 key값과 함께 리더를 통해 태그에 전달한다. 태그는 이를 확인하고 자신의 ID를 리더에게 전송한다. 하지만, ID와 key값의 도청이 가능하고, 스푸핑, 재전송 공격 등이 가능한 단점이 있다.[7] 즉 위의 보안 속성 중 A,B,C,D를 만족하지 못한다.

2.4 Hash Chain 방식

M. Ohkubo가 제안한 방식으로 서로 다른 두개의 해쉬함수를 사용해서 매번 리더의 요청에 대한 태그의 응답하는 값이 다르기 때문에 i번째 전송되는 값이 노출되었을지라도 공격에 대해서 안전하다. 하지만, Back-end DB에서의 계산이 늘어나는 단점이 있다.[8] 따라서 대량의 태그를 위한 환경에는 부적합한 방식이다.

3. 제안 프로토콜

3.1 용어 설명

- Query : 리더가 태그에 질의
- R.N.G : 난수 생성기
- R : 리더의 난수 생성기에 의해서 만들어진 난수
- h(ID) : ID를 해쉬한 값
- Data : ID에 따른 태그의 정보
- h() : 단방향 해쉬함수
- □ : Exclusive OR
- ID : 태그마다 가지는 고유한 값
- key : Back-end DB,리더,태그가 공통으로 가지는 비밀키
- AE : 메모리 연결을 위한 연결된 DB엔트리
- ID′= R□key□ID

3.2 전제조건

Back-end DB와 리더 사이는 안전한 구간이고, 리더와 태그는 무선통신으로 불안전구간으로 생각한다. 공통키 역할을 하는 key는 Back-end DB, 리더, 태그에 초기에 동일한 값을 셋팅한다. 사용되어지는 태그는 수동형(Passive)이다.

3.3 제안 프로토콜의 인증과정

6단계의 과정을 통해서 인증이 이루어진다.

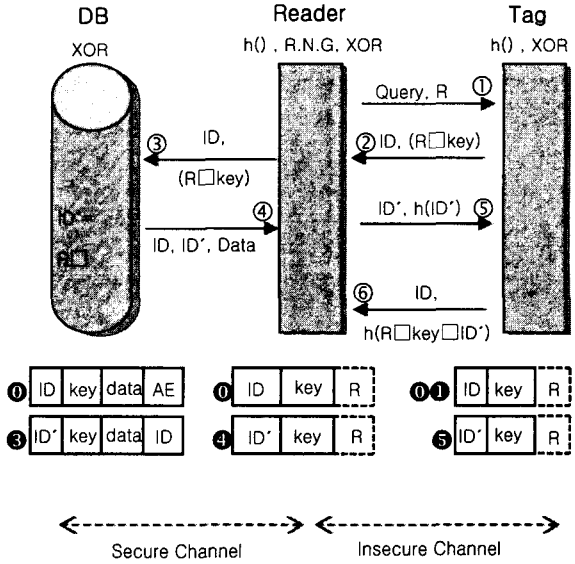

그림 1. 제안 프로토콜의 인증과정

[1 단계] 리더에서 태그로 질의 (번호①)

리더는 R.N.G를 통해 난수 R을 생성하고 질의와 함께 R을 태그에 전송한다. 리더는 메모리 영역에 R을 저장한다.

[2단계] 태그에서 리더로 응답 (번호②)

태그는 리더로부터 받은 R을 메모리 영역에 저장하고, 자신이 가지고 있던 ID를 해쉬한 값과 R과 공통키 역할을 하는 key를 XOR 연산한 후 해쉬한 값을 리더에게 전송한다.

● 정당한 태그인지 인증

태그로부터 받은 (R□key)와 리더가 가지고 있는 R과 key를 XOR연산한 값을 비교하여 일치하면 리더가 생성한 난수를 가지고 있던 정당한 태그로 인식해서 인증을 한다. 또한 비밀키인 key를 가지고 있지 않은 태그라면 리더로부터 인증을 받을 수 없다.

[3단계] 리더에서 Back-end DB로 전송 (번호③)

리더는 태그로부터 전송받은 ID, (R□key)를 Back-end DB로 전송한다. 전송받은 ID와 Back-end DB의 ID를 비교하여 ID에 따른 태그의 상세정보를 가지는 Data를 찾는다.

Back-end DB에는 복사본 역할을 하는 새로운 record를 생성한다. 새로운 record의 ID(ID′로 부름)는 R□key□ID 값으로 된다. AE는 자료 유실을 방지하기 위해 만들어졌고, 메모리연

결을 위한 DB엔트리며, 새로운 record의 AE에는 이전 record의 ID값을 저장한다.

[4단계] Back-end DB에서 리더로 DATA전송 (번호④)

태그 정보인 Data, ID와 새로이 갱신된 ID(ID')를 리더에게 전송한다. 리더는 ID를 이용하여 ID'값을 가지는 새로운 자료를 생성한다. 여기서 ID'는 6단계의 통신에서 리더가 통신을 하고 있는 태그의 정당성을 판단하는데 사용된다.

[5단계] 리더에서 태그로 ID'를 전송 (번호⑤)

리더는 h(ID')와 변경할 ID인 ID'를 태그에 전송한다. 태그는 자신이 가지고 있던 ID, key와 R을 이용하여 계산된 값과 리더로부터 받은 h(ID')를 비교하여 동일하다면 정당한 리더로 인증을 하고, 전송된 ID'값을 태그의 ID로 갱신한다. 태그는 Back-end DB와 동일한 값을 가지는 새로운 ID(ID')를 가지게 된다. ID'는 공격자에 의해 도청된 ID에 의한 스푸핑 공격, 재생공격과 ID위조 방지에 사용될 수 있다.

[6단계] 태그에서 리더로의 확인 (번호⑥)

마지막으로 리더는 Back-end DB에서 변경된 ID가 태그에도 정확히 반영이 되었는지를 확인하기 위하여 태그가 가지고 있는 ID와 h(R□key□ID')를 전송 받는다. 리더는 자신이 가지고 있는 ID의 (R□key□ID')를 해쉬한 값과 태그로부터 전송받은 값을 비교하여 동일한지를 비교한다. 동일하다고 판단되면 태그에도 Back-end DB와 동일한 ID'로 갱신이 되었음을 의미한다. 리더는 메모리에서 해당 ID, ID', R을 삭제하고 프로세스를 완료한다.

4. 프로토콜의 안전성 분석

A. 상호인증- 리더와 태그는 공통적으로 key를 가지고 있고, 이것을 비교 판단하여 서로를 인증한다. Key는 리더와 태그의 통신 중에 노출이 되지 않으며, 공격자가 key를 유추하기란 쉽지 않다.

B. 불추적성- 태그의 ID가 공격자 공격에 의해 노출이 되었다 할지라도 Back-end DB에서는 ID가 ID'로 바로 갱신이 되기 때문에 다음번 세션에서는 ID추적이 어렵다.

C. 전방향 안전성- 공격자가 어떤 경로를 통해 key를 획득했다고 해도 세션키에 해당하는 (R□key)에서 R은 매번 변하기 때문에 공격자가 key를 가진다고 해도 과거 세션에 사용된 (R□key)를 계산할 수 없다.

D. 재생공격- 태그가 리더로부터 인증을 받기 위해서는 key를 알아야 하지만 유추하기 힘들며, 리더에서 난수 생성기에 의한 R이 매번 변하기 때문에 ID를 알고 있어도 (R□key)값을 가지고 인증을 받지 못한다.

또한, 제안하는 프로토콜에서는 메시지 유실방지기능을 가진다. Back-end DB에 메모리 연결을 위한 연결된 DB엔트리(AE)를 가지고 있어서 메시지 유실에 대비할 수 있다. AE에는 바로 이전의 ID값을 저장하므로 비정상적인 세션의 종료로 인한 메시지를 복구할 수 있다.

5. 결론 및 향후 연구방향

해쉬함수 기반의 공통키를 이용하여 제안한 프로토콜은 기존연구들과는 달리 공격자의 위조, 재생공격에 효율적으로 대처하도록 설계되었으며, 불추적성, 전방향 안전성을 만족한다.

리더와 태그뿐만 아니라, Back-end DB와 리더간에도 무선으로 통신을 할 경우에 대비한 안전하고 정당한 인증절차에 의한 보안 프로토콜이 계획되어야 한다. 향후 연구 방향으로서 RFID시스템의 활용성에 문제가 되고있는 비용문제를 해결하기 위해서는 저전력, 저비용의 태그를 만들기 위한 연구를 병행하고자 한다.

6. 참고문헌

[1] 닛케이BP북 RFID 테크놀러지 편집부,"IC태그 활용 가이드 RFID", 복두출판사, pp.190~200, 2005.

[2] Steven Shepard,"알기 쉬운 전파식별",홍릉과학, pp.141~161, 2005.

[3] 김현석,김일곤,오정현,최진영,"RFID 네트워크 보안분석을 위한 정형적 방법론",정보과학회논문지 제32권 2호, pp91~93, 2005.

[4] 황영주,"Low-Cost RFID를 위한 인증 프로토콜", 고려대학교 대학원:정보보호학과, pp.6~7, 2004.

[5] 김호원,김주원,"FRID보안기술 및 프라이버시 보호기술", RFID-TECH, pp.38~46, 2006.

[6] 장재득,장문수,최송인,"무선 주파수 인식[RFID] 시스템 기술 분석", 전자통신동향분석 제19권 제2호, 2004년 4월.

[7] Weis, S. et al. "Security and Privacy in Radio-Frequency Identification Devices", Massachusetts Institute of Technology, 2003.

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