데이터베이스 난수를 이용한 RFID 보안 인증 프로토콜

배우식*, 신문선**, 연용호***, 이종연*
*충북대학교 컴퓨터교육과
**건국대학교 컴퓨터응용과학부
***목원대학교 공학교육혁신 센터
e-mail:bws@motor.ac.kr*

RFID Security Authentication Protocol Using Database Random Number

Woo Sik Bae*, Moon Sun Shin**, Yong Ho Yon***,
Jong Yun Lee*
*Dept. of Computer Education, Chungbuk National University
**Dept. of Computer Science, Konkuk University
***Engineering Education Innovation Center, Mokwon University

요 약

RFID 시스템은 생활에 바코드를 대체하고 산업 전반에 사용될 중요한 기술이다. 그러나 RFID시스템에서 태그와 리더 사이의 통신이 무선으로 이루어짐에 따라 보안상 많은 취약점이 존재 한다. 본 논문에서는 여러 보안 문제를 강화 하기위해 데이터베이스에서 난수 및 시간정보를 이용하여 매 세션마다 새로운 해쉬함수를 생성하는 인증 프로토콜을 제안 한다, 본 프로토콜은 무선 인증 시스템에 다양한 유용성을 제공 하며 기존 프로토콜에 비해 보안상 강건함을 제공 한다.

1. 서론

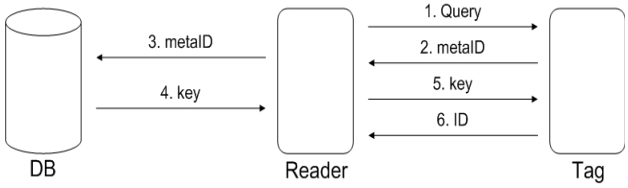
RFID(Radio Frequency Identification)는 전자태그를 사물에 부착하여 사물의 정보나 주위 상황을 인지하고 기존 IT 시스템과 실시간으로 정보를 교환, 처리할 수 있는 기술을 말한다. 그러나, RFID 시스템은 그 유용성에도 불구하고 비접촉식 인식 시스템이라는 특징 때문에 안정성과 프라이버시 보호 측면에서 문제점을 지니고 있다. 이런 RFID 네트워크기술은 EPCIS(Electronic Product Code Information Services)[1]를 사용함으로써 물류 등에 대한 지속적인 정보 서비스를 제공할 수 있게 되며 이로 인해 재고관리, 반품관리, 정품 확인 등 다양한 분야에 걸쳐 사용 가능하다. 세계 어느 곳에서도 표준화된 전자 태그의 코드를 읽음으로써 RFID 코드에 매핑 되는 정보를 찾을 수 있으며 이런 RFID 시스템의 많은 장점을 활용하기 위해 학계와 관련 산업계의 연구 개발이 현재 활발히 진행 중이며 그중에서 EPCglobal에서는 EPC(Electronic Product Code)와 EPCIS에 대한 표준안을 제안하고 있다. 그러나 문제점으로 본 논문에서는 RFID의 프라이버시 문제를 해결하기 위해 기존에 제안된 해쉬락(Hash-Lock)기법[2,3,4]등 에서 해결하지 못한 문제점을 분석하여 보다 안전하고 효율적으로 사용자의 프라이버시를 보호할 수 있는 인증 프로토콜을 제안한다. 제안하는 인증프로토콜은 해쉬 함수와 난수를 이용하여 공격자의 공격에 실시간으로 대응함으로써 무선 구간에서의 보안에 강건함을 제공 한다.

2. 관련 연구

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 데이터

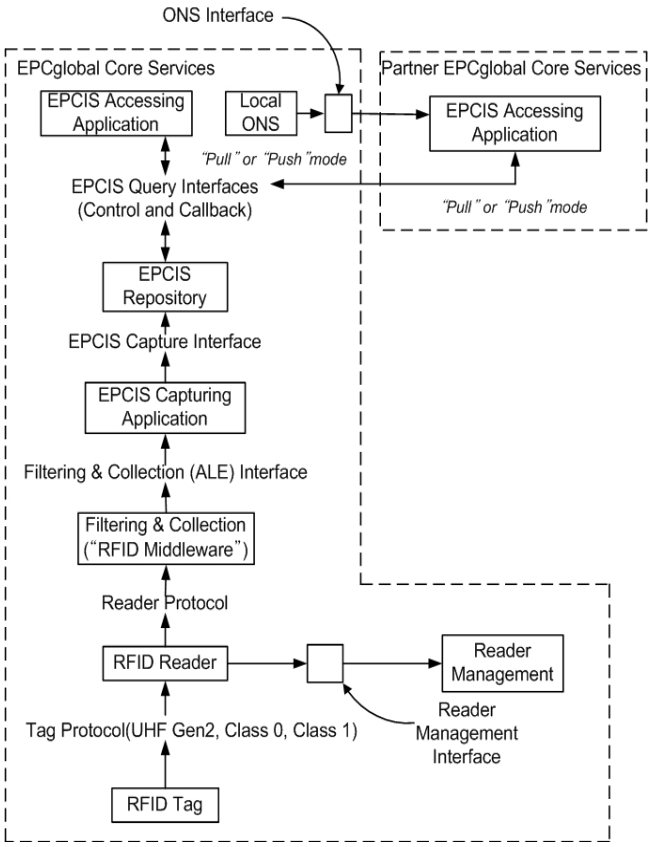
베이스에 전송하고 데이터베이스는 이에 대응하는 키를 리더에게 전송한다. 이어서 태그에게 보내어 태그가 해쉬값을 계산하며 자신의 mataID와 일치하는 경우 풀림상태로 되어 리더에게 자신의 ID를 전송하는 방식이다. 태그의 식별 값인 metaID가 고정되어 있으며 출력되는 데이터가 같아 전송 되었는지 확인할 수 있다. 아래의 [그림 1]은 해-쉬락 기법의 구조도 이다.



[그림 1] 해쉬-락 기법

2.2 EPCIS 네트워크 시스템

EPC 네트워크 시스템은 [그림 2]과 같이 구성되며 Tag, Reader, Middleware, ALE[5], EPCIS, ONS(Object Name Services)[6]로 구성되며 Tag와 Reader 구간은 RF(Radio Frequency)로 통신되며 보안상 불완전한 구간이라 할 수 있다.



[그림 2] EPCIS 구성도

3. 제안 시스템

3.1 구조

본 제안 프로토콜은 리더가 처음 태그에게 질의를 할 때 데이터베이스에서 전송되어진 난수와 실시간 그리고 리더코드를 함께 질의한다. 태그는 리더로부터 수신한 데이터를 자신이 가지고 있는 ID와 해쉬한 값을 이용하여 응답하게 된다. 매 세션마다 다르게 응답함으로써 기존 프로토콜들 에서 문제점으로 지적 되었던 재전송 공격과 스푸핑[7] 공격에 대하여 안전하다. 제안프로토콜에서 데이터베이스는 태그의 ID와 관련 데이터를 저장하고 있으며, 해쉬 함수연산 1회의 연산만을 이용하여 태그를 인증한다. 제안 프로토콜에서 사용되는 파라미터는 다음과 같으며, [그림 3]는 제안하는 프로토콜의 기본 구조를 나타낸 것이다.

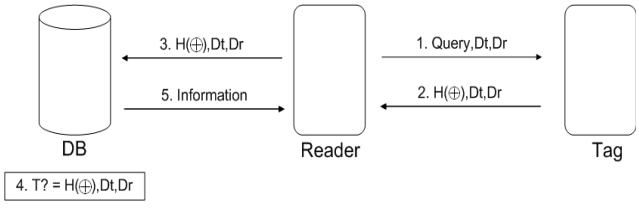
3.1.1 가정 사항

본 제안 프로토콜을 제안하기 위하여 다음 사항을 가정한다.

- 태그와 데이터베이스는 해쉬 함수 연산을 수행한다.
- 데이터베이스는 태그의 ID를 사전에 공유한다.
- 데이터베이스와 리더는 안전한 유선으로 통신을 하고 있다.

[파라미터]

- Query : 질의, 태그의 응답을 요청
- ID : 태그 고유의 비밀 인증 정보
- H( ) : 일 방향 해쉬 함수
- H(⊕) : $H(ID \oplus key)$ 연산
- D_t : DB가 리더에게 전송하는 DB시간(μs)
- D_r : DB가 생성하여 리더에게 전송하는 난수
- D_n : 데이터베이스에서 태그에게 전송되는 명령
- ⊕ : Exclusive OR
- key : DB, 리더, 태그의 공통 비밀키



[그림 3] 제안 프로토콜의 구조

3.2 인증과정

① 리더는 태그에 query와 세션마다 다르게 데이터

베이스와 동기화된 D_t, D_r을 전송한다.

리더 → 태그 : Query, D_t, D_r

② 태그는 ID, D_t, D_r을 해쉬 하여 Query에 대한 응답으로 리더에게 전송한다.

response = $H(\oplus), D_t, D_r$

③ 리더는 $H(\oplus), D_t, D_r$를 데이터베이스로 전송한다.

리더 → 데이터베이스 : $H(\oplus), D_t, D_r$

④ 데이터베이스에 저장된 ID를 $H(\oplus), D_t, D_r$ 값과 리더로부터 수신한 $H(\oplus), D_t, D_r$를 비교하여 만족하는 식별정보가 있는지 확인 한다.

T? = $H(\oplus), D_t, D_r$

확인이 성공하면 관련 정보를 리더에게 전송한다.

3.3 보안성

제안 하는 프로토콜은 리더가 데이터베이스의 난수와 시간을 이용 하여 리더가 매 세션 마다 전송하는 질의가 변경 된다. 공격자가 태그의 응답을 도청하여 재전송 하더라도 세션마다 값이 바뀌게 되어 다음 세션에서는 정당한 태그로 인증 받을 수 없다. 공격자가 정당한 리더로 가장하여 질의를 전송 하여도 태그에서 데이터베이스의 시간과 난수를 요구 하여 해쉬 하기 때문에 태그 데이터를 온전히 습득할 수 없게 되어 스푸핑 공격 및 재전송공격에 안전 하다.

3.4 효율성

기존의 해쉬락 관련 복잡한 프로토콜과 같이 많은 연산량이 필요 하지 않다. 본 제안 프로토콜은 특성상 시간과 난수 값이 일회성을 갖기 때문에 매 인증 시도마다 갱신되어 과거의 정보를 이용 하여 재전송이 불가능 하다. 실제 하드웨어적 제약이 많은 태그에서는 해쉬 함수 구현만을 필요로 하기 때문에 태그 생산 단가를 낮출 수 있다. 또한 리더의 연산이 없기 때문에 타 프로토콜에 비해 효율이 높으며 태그와 리더를 저가형으로 구성이 가능하다. 데이터베이스에서의 연산은 타 프로토콜과 비슷한 연산을 하며 단지 리더에 난수와 시간을 전송하는 동작을 하게 된다.

4. 결론

RFID 기술은 마이크로 칩을 내장한 태그, 카드 등에 저장된 데이터를 무선 주파수를 이용 하여 인증하는 매우 편리한 기술이며 미래의 컴퓨팅 환경을 주도해 나갈 매우 중요한 기술 이다. 그러나 무선구간에서 태그의 사용으로 인해 보안상 문제점이 존재한다. 본 논문에서 제안한 RFID 네트워크 시스템은 기존의 방법에서의 문제점을 해결하고자 개선시킨 RFID 인증 프로토콜을 제안 하였다. 제안한 프로토콜이 데이터베이스서버의 난수 및 시간을 이용한 방법으로 계산량 대비 각종 공격에 안전한 방법이며 향후 데이터베이스의 검색을 효과적으로 할 수 있는 방법으로 연구가 되어야 할 것이다.

참고문헌

[1] EPC Information Services (EPCIS) Version 1.0.1 Specification(2007) EPCglobal, http://www.epcglobalinc.org

[2] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. w. Engels, "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems," Security in Pervasive Computing 2003, LNCS 2802, pp. 201-202, Springer-Verlag Heidelderg, 2004.

[3] S. A. Weis, "Security and Privacy in Radio-Frequency Identification Devices" MS Thesis, MIT.May, 2003.

[4] Burmester, M., van Le, T., and de Medeiros, B. "Provably secure ubiquitous systems: Universally composable RFID authentication protocols" E-print report 2006/131, International Association for Cryptological Research, 2006.

[5] The Application Level Events (ALE) Specification, Version 1.1.1(2009) EPCglobal, http://www.epcglobalinc.org

[6] Object Naming Service(ONS) Version 1.0(2005) EPCglobal, http://www.epcglobalinc.org

[7] Pedro Peris-Lopez, Julio Cesat Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagora, "RFID Systems: A Survey on Security Threats and Proposed Solutions," PWC 2006, LNCS 4217, pp. 159-170, 2006.