e-Seal 보안을 위한 효율적인 인증 프로토콜1)

배우식*, 이선영*, 김영주*, 이종연*
*충북대학교 컴퓨터교육과
e-mail : bws@motor.ac.kr, jongyun@chungbuk.ac.kr

An Efficient Authentication Protocol for e-Seal Security

Woo Sik Bae*, Sun Young Lee*, Young Ju kim*, Jong Yun Lee*
*Dept. of Computer Education, Chungbuk National University

요 약

RFID를 이용한 물류 관리 시스템은 컨테이너의 기계적 보안을 대체하고 보다 안전한 물류 환경을 위해 매우 중요한 기술이다. 그러나 RFID시스템에서 태그와 리더 사이의 통신이 무선으로 이루어짐에 따라 보안상 많은 취약점이 존재 한다. 본 논문에서는 여러 보안 문제를 강화 하기위해 데이터베이스에서 시간 난수를 이용하여 매 세션마다 새로운 해쉬 함수를 생성하는 양방향 상호인증 프로토콜을 제안 한다, 본 프로토콜은 무선 인증 시스템에 다양한 유용성을 제공 하며 기존 제안된 프로토콜에 비해 e-seal에 적용할 경우 보안상 강건함을 제공 한다.

1. 서론

최근 들어 RFID(Radio Frequency Identification) 방식의 화물 컨테이너 분야 물류 보안관련 연구가 중요한 이슈로 떠오르고 있다. 그 중에서 e-seal (Electronic Seal)기술은 능동형 RFID[1] 기술의 대표적인 기술로 원격으로 컨테이너 봉인상태를 확인 감시 할 수 있는 컨테이너 봉인 장치이다. 미국을 중심으로 국제 화물 컨테이너의 운송을 보다 안전하고 효율적으로 관리하기 위한 방안으로 e-seal은 수출입 물류에서 컨테이너 문의 비정상적인 개폐나 개폐 시도를 감지하며 그에 대한 정보를 전송함으로 보안 기능을 유지 하게 된다. 그러나 RFID 시스템은 비접촉식 인식 시스템이라는 특징 때문에 안정성과 프라이버시 보호 측면에서 문제점을 지니고 있다.

또한 RFID의 특징인 반도체 칩에 기록된 정보를 제 삼자가 쉽게 판독 및 변조할 수 있다는 취약점을 가지고 있다. 이러한 RFID 취약점을 해결한 e-seal 보안 프로토콜을 적용하기 위해서는 e-seal과 리더 간의 데이터의 보안수준을 높여 암호화함으로서 쉽게 접근할 수 없는 양방향 인증 방식이 필요하다.

따라서 본 논문에서는 RFID의 프라이버시 문제를 해결하기 위해 기존에 제안된 해쉬락(Hash-Lock)기법[2,3,4]에서 해결하지 못한 문제점을 분석하여 보다 안전하고 효율적으로 사용자의 프라이버시를 보호할 수 있는 e-seal 을 위한 강력한 인증 프로토콜을 제안한다. 제안하는 인증프로토콜은 해쉬 함수와 난수를 이용하여 공격자의 공격에 실시간으로 대응함으로써 무선 구간에서의 보안에 강건함을 제공한다.

이 논문은 2008년도 지식경제부 성장동력기술개발 사업의 일환으로 (주)메타비즈의 위탁과제로 수행되었음.

2. 관련 연구

2.1 봉인장치(seal)

컨테이너에 화물을 적재하고 문에 붙이는 봉인장치로서, 화물을 적재한 이후 보호하기 위한 외부 잠금 장치의 하나로 운송과정에서의 컨테이너 무결성을 보장하는 안전장치이다. 통상 금속으로 만들어져 있으며 개별 봉인마다 고유번호를 가지고 있어 봉인의 파손이나 변조 등을 방지 하는데 사용 된다. 최근까지는 기계적 봉인장치가 주로 사용되고 있으며, 그에 관한 국제 표준 규격은 ISO/PAS 17712 이다.

2.2 전자봉인(e-seal)

e-Seal은 RFID 기술을 사용하여 원격에서 자동으로 봉인상태를 확인할 수 있는 컨테이너 봉인장치를 말한다. 아울러 e-seal의 일반적인 요구사항은 다음과 같다.[5,6,7] (1) 유일한 seal ID를 가지며, (2) 최소 물리적 특성에 관한 ISO/PAS 17712 규격을 만족해야한다. (3) 봉인(seal), 개봉(unseal) 등의 동작 event, (4) 위치추적(checkpoint, GPS) 정보, (5) 온도, 진동 등을 감지하는 센서 정보를 날짜/시간과 함께 로그로 저장하고, (6) 위험요소가 감지되면 즉각 경고 메시지를 전송한다. 그 외에, 위성통신을 통한 실시간 위치추적 기능, 컨테이너 내부 화물의 변화 인식, 사용자 정보의 읽기/쓰기, 재사용성 등의 부가적인 요구사항이 있을 수 있다. 이를 위하여, seal, 위치추적, 센서 기능을 통합한 e-seal은 다음과 같은 이점을 제공한다. 경제적인 면에서 (1) 운송 화물의 탈선 및 지연 도착에 대한 신속한 대비책을 마련할 수 있고, (2) 창고 및 항만 터미널의 효율적인 운영과, (3) 도난손실을 줄임으로써 물류비용을 절감할 수 있다. (4) 안전 관리의 자동화를 제공하여 사람들의 부주의와 실수로 인한 안전피해를 줄일 수 있다. 보안적인 면에서 (5) 컨테이너의 운송 경로, 화물 정보 등을 통하여 효율적으로 위험 컨테이너를 선별함으로써 밀매, 테러 등의 방지에 도움을 준다.

2.3 해시락 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 잠겨있게 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.

3. 제안하는 보안 프로토콜

3.1 구조

본 제안 프로토콜은 기존에 제안된 해쉬-락 기법, 확장된 해시락, 해시기반 ID 변형기법 등과 같이 태그가 임의의 난수를 생성하여 상호 인증을 수행하게 하여 재전송 공격을 막도록 하였다. [그림 1]은 제안 프로토굴의 동작과정의 기본 구조를 나타낸 것이다.

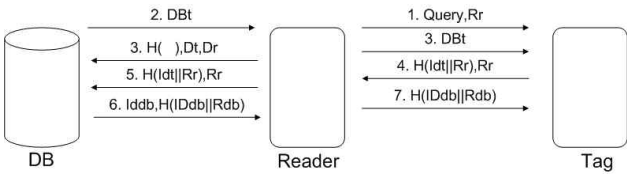
3.1.1 가정 사항

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.

[매개변수]

- Query : 질의, 태그의 응답을 요청
- ID : 태그 고유의 비밀 인증 정보
- H() : 해쉬 함수
- R_r : 리더가 생성하는 난수
- ID_t : 태그가 생성하는 난수
- DB_t : 데이터베이스의 시간
- || : 연접



[그림 1] 제안 프로토콜의 구조

3.2 인증과정

① 리더는 태그에 query와 세션마다 다르게 데이터베이스와 동기화된 R_r 을 전송한다.

Reader → Tag : Query, R_r

Reader → DB : Query

② 태그는 query 와 R_r을 수신후, 임시저장소에 R_r을 저장하고 DB는 Query을 수신후, DB_t를 Reader 응답으로 전송한다.

DB → Reader = DB_t

③ 리더는 데이터베이스로 수신한 DB_t를 Tag에게 전송한다.

리더 → Tag : DB_t

④ Tag 는 DB_t를 수신 후, 임시저장소에 DB_t를 저장하고 자신의 ID_t와 기존에 저장된 R_r을 $H(ID_t||R_r), R_r$ 값을 리더에게 전송한다.

Tag → Reader : $H(ID_t||R_r), R_r$

⑤ Reader는 DB로부터 수신한 $H(ID_t||R_r), R_r$ 과 R_r 를 DB에게 전송한다.

Reader → DB : $H(ID_t||R_r), R_r, R_{id}$

⑥ DB는 저장된 ID_{db} 와 수신한 R_{id} 를 이용하여 $H(ID_t||R_r), R_r$ 를 계산한 후, Tag로부터 수신한 $H(ID_t||R_r), R_r$ 와 일치 여부를 비교 한다. 일치할 경우 DB는 Tag를 인증하게 되고 상호 인증을 하기 위해 ID_{db}와 $H(ID_{db}||R_{db})$를 Reader에 전송한다.

DB → Reader : $ID_{db}, H(ID_{db}||R_{db})$

⑦ Reader는 DB로부터 수신한 $H(ID_{db}||R_{db})$를 Tag에게 전송한다.

Reader → Tag : $H(ID_{db}||R_{db})$

⑧ Tag는 $H(ID_{db}||R_{db})$를 수신하여 자신의 IDt와 기존에 저장된 DB_t을 이용하여 $H(ID_{db}||R_{db})$를 계산후 리더로부터 수신한 $H(ID_{db}||R_{db})$와 데이터의 일치 여부를 비교하여 일치할 경우 Tag는 Reader를 인증하게 된다.

3.3 보안성

제안 하는 프로토콜은 리더가 데이터베이스의 난수와 시간을 이용 하여 리더가 매 세션 마다 전송하는 질의가 변경 된다. 공격자가 정당한 리더로 가장하여 Query, R_r를 전송하면, $H(ID_t||R_r), R_r$ 를 악의적인 태그에 넣어 응답으로 보내지게 되면 이미 시간이 지나간 상태의 정보 $H(ID_t||R_r), R_r$ 로는 인증을 할 수가 없어 스푸핑 공격이 불가능 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 실시간을 이용한 방법이다. 매 세션마다 다른 응답을 전송하므로 계산량 대비 각종 공격에 안전한 방법이며 e-seal에 적용 시 보안상 강건함을 유지할 수 있다.

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] C.Ma and K. Cheng, "Publicly verifiable authenticated encryption," IEEE Electronics Letters, Vol.39, No.3, 2003.

[6] Heiko Knospe and Hartmut Pohl, RFID security, Information Security Technical Report, Volume 9, Issue 4, December 2004, pp39-50

[7] Hung-Yu Chien and Che-Hao Chen, Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards, Computer Standards & Interfaces, 2006.