情報保護學會論文誌
第17卷 第5號, 2007. 10

복제 공격 저항성을 갖는 전자봉인 보안 모델*

김 주 해†, 최 은 영, 이 동 훈‡
고려대학교 정보보호대학원

A Security Model for Duplication Resistant eSeal

Joo Hae Kim†, Eun Young Choi, Dong Hoon Lee‡
Graduate School of Information Security, Korea University.

요 약

전자봉인 장치는 능동형 RFID 장치로서, 화물 컨테이너의 문에 설치되어 컨테이너가 허가받지 않은 자에 의해 개봉되지 않았다는 것을 보증해 주는 장치이다. 전자 봉인장치는 RFID를 이용하므로 도청이나 위조를 막아야만 한다. 또한 보안 프로토콜을 사용하는 전자봉인 장치는 복제가 불가능해야 한다. 전자봉인의 복제 방지 기능이 제공되지 않는다면, 공격자는 컨테이너의 내용물을 바꾸어 넣은 다음에 복제된 전자봉인으로 재봉인 함으로서 전자봉인이 개봉 되었었다는 사실을 숨길 수 있을 것이다. 본 논문에서는 도청과 위조를 방지함과 동시에, 봉인의 복제에 대한 저항성을 갖는 프로토콜을 제안하고자 한다.

ABSTRACT

An eSeal(Electrical Seal) is an active RFID device which installed on the door of a container. The main role of the tag is to make sure the seal is not breaking by unauthorized people. Because an eSeal uses RFID system, we need to prevent eavesdrop and impersonate. Moreover, an eSeal which uses a secure protocol must not be able to duplicate. If duplication resistant property is not provide to a eSeal, an attacker may replace a object in the sealed container and reseal the container with duplicated eSeal to hide breaking of the eSeal. In this paper, we provide a protocol which resist duplicate an eSeal during prevent eavesdrop and impersonation.

Keywords : *Low-cost RFID system, Privacy, Authentication protocol*

Ⅰ. 서 론

전자봉인기술(e-Seal)은 화물 컨테이너를 안전하고 효율적으로 관리하기 위한 기술로, 433MHz 주파수 대역을 사용하는 능동형 RFID(Radio Frequency Identification)장치를 이용한다. 전자 봉인은 두 가지 목적을 가지고 사용되는데, 그 첫 번째는 컨테이너의 이동경로와 현재 위치를 추적하는 것이고, 두 번째 목적은 선적이 완료된 컨테이너를 시건 한 후 컨테이너를 비정상적인 방법으로 개봉하려는 시도가 발생하는 경우에 이를 감지하여 주변의 리더에게 알림으로서 목적지에서 개봉 될 때 까지 봉인이 제거되지 않았음을 확신할 수 있도록 해주는 역할을 한다. 2005년 8월

접수일: 2006년 12월 22일; 채택일: 2007년 7월 20일
* 본 연구는 서울시 산학연 협력사업(10665) 지원으로 수행되었습니다.
† 주저자, joshuajh@korea.ac.kr
‡ 교신저자, donghlee@korea.ac.kr

31일에 발표된 ISO18185-4 규격은 전자봉인이 비밀 정보를 가지지 않는다는 전제조건을 제시하면서 어떠한 보호기술도 명시하지 않은 상태이다[1]. 그러나 이러한 전자 봉인은 비밀 정보를 포함하지 않았으므로 도청공격은 무의미 하지만 데이터 위변조에는 취약할 수밖에 없다. 그러므로 컨테이너의 위치를 추적하기 위해 현재 위치를 주위의 리더에게 보고하는 경우에 통신하는 내용을 숨기고 보호함으로써 전자 봉인을 위변조하는 것을 막을 방법이 제시되어야 한다. 또한 전자 봉인을 복제하여 부당하게 컨테이너를 개봉 한 후, 복제된 전자봉인으로 재봉인 하는 것을 막거나 복제되어 다른 봉인으로 대체되었음을 확인할 수 있는 방법이 제시 되어야만 한다. 그렇지 않은 경우, 정상적인 컨테이너의 내용물을 바꿔치기 하여 오랜 시간 도둑맞았다는 사실을 인지하지 못하게 하거나, 테러리스트에 의해 내용물이 공격무기로 대치된 컨테이너를 정상적인 것으로 오인하여 수입이 되는 경우, 수입 컨테이너는 테러 공격의 매개체로서 사용될 가능성도 있다. 그러나 이러한 가능성에 대한 연구는 아직까지 이루어지지 않고 있으며, 하드웨어 적인 연구만 진행되고 있는 상황이다. 하드웨어에 관한 연구와 동시에 안전한 통신 방법과 부차적인 복제 방지 기술이 함께 연구 되어야 실제 사용될 때 안전한 장치로서 의미를 갖게 될 수 있다 하겠다.

본 논문에서는 기존의 알려진 공격 방법에 강하며, 태그 자체를 분석하여 복제하는 공격에 저항성을 갖는 데이터 보호기술에 대해 제안해 보도록 하겠다.

Ⅱ. 안전한 RFID 시스템 설계시 고려사항

이 장에서는 RFID 시스템이 갖는 문제점과 태그와 리더간의 통신에서 비밀정보를 얻어내기 위해 공격자가 행할 수 있는 공격 방법에 대해 알아보겠다.

2.1 RFID 시스템의 문제점

전자봉인기술은 RFID 시스템을 사용하기 때문에, RFID 시스템이 갖고 있는 문제점을 그대로 가지고 있을 수밖에 없다. 그렇기 때문에 RFID가 갖는 보안상의 문제점을 해결하고, 전자봉인 기술이 갖는 요구사항을 충족시킬 필요가 있다. RFID 시스템의 특성상 리더와 태그는 물리적인 접촉 없이 데이터를 주고받으며, 무선으로 통신을 수행하기 때문에 수신 능력이 있으면 누구든지 그 내용을 훔쳐볼 수 있다. 태그 역시 리더의 무선 신호에 반응하여 자신의 고유 정보를 공중으로 방출하기 때문에 전달된 무선 신호가 통신을 해도 되는 정당한 리더가 발생한 신호인지 확인하지 않으면 공격자는 손쉽게 태그에 저장되어 있는 정보를 얻어낼 수 있다.

RFID 시스템이 전자봉인 기술에 사용되는 경우, RFID 태그는 배위에 실린 채로 몇 개월 이상의 시간을 보내야 하고, 자체의 처리장치와 메모리를 갖는 능동형 태그이기 때문에 공격자는 태그 자체의 정보를 물리적으로 추출해내어 복제/대치하는 공격을 수행할 만한 충분한 시간과 가능성을 확보할 수 있다.

2.2 RFID 시스템 공격방법

공격자의 유형은 크게 두 가지가 있는데 첫 번째는 단순히 전달되는 통신 내용을 엿듣기만 하는 형태의 수동적인 공격자이다. 이 유형의 공격자는 사용자가 숨기고자 하는 정보를 훔쳐냄으로서 직접적으로 사용자의 전자봉인을 복제하거나, 유효한 정보를 위조해 낼 수 있으며, 이후에 언급될 능동 공격에 사용될 정보로서 유용할 수 도 있다. 두 번째 공격 방법은 통신 내용을 변조하여 전송하거나, 단순히 재전송 하는 등의 방법을 사용하여 상대방으로 하여금 올바른 통신 상대인 것으로 오인하도록 만드는 등의 공격을 수행하는 능동적인 공격이다. 세 번째 공격의 유형은 태그를 물리적으로 공격하여 태그에 저장되어 있는 비밀 정보를 추출해내는 공격이나, 물리적으로 공격을 수행하는 경우는 정보 전체를 강제적으로 추출해내는 방법으로 만큼 일반적인 공격 방법으로 고려하지는 않도록 하겠다.

2.2.1 도청

리더와 태그 간에 오고가는 통신의 내용을 단순히 도청하여 비밀정보를 얻어낼 수 있다. 앞서 언급한 바와 같이 RFID 시스템은 공간을 통해 데이터가 전송되므로 해당 주파수를 수신할 수 있는 장비를 소유하고 있는 공격자가 도청을 통해 정보를 수집하는 것을 물리적으로 막는 것은 상당히 어려운 문제이다. 그러므로

도청 자체를 막는 것이 아니라, 도청에 성공하여 통신 내용을 얻더라도 그 내용을 확인할 수 없게 하고, 도청을 통해 얻은 정보를 다른 목적으로 사용할 수 없도록 하는 것이 중요하다.

2.2.2 위조

공격자가 가짜 태그나 리더를 정당한 것처럼 동작하게 하여 정보를 빼내거나, 인증과정을 통과하는 공격방법이다. 공격자가 이러한 공격에 성공한다면, 전자봉인을 제거한 다음 위조된 봉인을 설치함으로서 봉인이 열렸었다는 사실 자체를 인지하지 못하도록 할 수 있다. 위조 공격을 하기 위한 정보를 얻어내기 위한 공격 방법으로는 다음과 같은 것들이 있다.

- **재전송 공격(Replay Attack)** : 공격자가 정당한 리더가 태그에게 전송하는 신호를 도청하여 기록해 두었다가 해당 리더의 통신이 완료된 후에 도청된 정보를 해당 리더와 통신했던 태그에게 다시 전송하여 태그가 공격자의 리더를 정당한 리더로 착각하게 만들어 태그의 정보를 얻어내는 공격 방법이다.
  이 공격을 통해 획득된 태그의 정보는 스푸핑 공격 등에 사용되어 특정 태그를 위조하거나 데이터를 전송해준 태그인 척 하는 등의 공격에 사용될 수 있다. 특히 미리 약속된 정보를 요구하는 태그의 정보를 얻어내는데 유용하게 사용되는 공격 방법이다.

- **스푸핑 공격(Spoofing Attack)** : 공격자는 정상적인 리더로 가장하여 위조하고자 하는 태그에게 신호를 보내어 저장되어 있는 정보를 획득한다. 공격자는 리더가 데이터를 요청했을 때 태그로부터 획득한 정보를 전달함으로서 리더를 속여 특정 태그로 인식되도록 할 수 있다.

2.2.3 메시지 차단

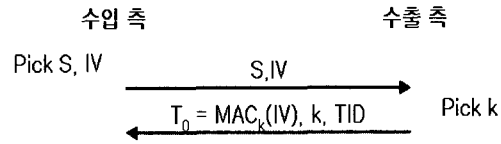
서비스 거부공격(Denial of Service)의 한 유형으로, 데이터베이스에 태그의 현재 상태를 저장하여 태그를 검색하거나 식별하기 위한 정보를 얻어내야 하는 방법을 사용하는 경우 발생할 수 있다. 태그에서 데이터베이스로 전달되는 메시지를 차단하여 태그에서 데이터베이스로 현재 상태에 관한 정보나, 현재 상태가 변경되었다는 사실을 전달하지 못하도록 하여 태그에 저장되어 있는 정보와 데이터베이스에 저장되어 있는 정보를 다르게 만듦으로서 데이터베이스에 태그를 찾아낼 수 있는 정보가 잘못 저장하게 만들어서 태그를 식별하려고 시도 할 때 태그의 정보를 찾아내지 못하도록 함으로서 태그를 더 이상 인식하지 못하게 하여 더 이상 태그를 사용하지 못하도록 하는 형태의 공격이다.

메시지 차단 형태의 공격이 전자봉인에 유효한 이유는, 메시지 차단에 의해 무력화된 전자봉인은 봉인이 깨진 적이 있는 것인지 아닌지 확인할 방법이 없고, 다른 공격을 시도한 후 공격의 유형을 숨기기 위해 무력화 했을 확률이 있기 때문에, 무력화된 전자봉인을 가지고 있는 컨테이너와 함께 선적되었던 다른 컨테이너들의 봉인에 이상이 없어 보일지라도 공격에 성공하여 복제된 것이 있을 확률이 존재하므로, 함께 선적된 모든 컨테이너를 개봉하여 전수조사를 해야만 하는 상황을 만들 수 있다. 이렇듯 모든 컨테이너를 개봉하여 전수조사를 하도록 만드는 것만으로도 막대한 경제적 손실을 입힐 수 있기 때문에 유효한 공격 방법이다.

Ⅲ. 인증 및 봉인 프로토콜

제안된 프로토콜은 전체 프로토콜은 태그와 리더간의 통신 시 안전하게 데이터를 주고받기 위한 인증 부분과 봉인이 복제되지 않았다는 것을 확신하게 해주는 봉인 프로토콜 두 부분으로 구성된다. 여기에서 제안하는 프로토콜은 핸리히 등이 제안한 가변 식별자 태그 기법[2]을 기반으로 하였다.

3.1 초기화 단계



〔그림 1〕 초기화 단계

인증프로토콜을 위하여 초기에 전자 봉인이 사용되는 시점에서 태그와 리더는 태그마다 유일한 비밀 값 S를 공유한다. 이 유일한 비밀 값 S와 초기값(IV:

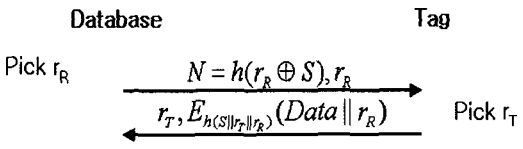
Initial Vector)은 수입 측에서 생성하여 수출 측에게 신용장과 함께 전달하도록 한다. 수출 측에서는 이 값을 가지고 다음과 같이 T_0를 생성하여 전자봉인에 기록한다.

$$T_0 = MAC_k(IV)$$

수출하는 측에서는 해당 값을 전자봉인에 기록하는 시점의 전자봉인 타이머 값과 사용된 키 값, 그리고 해당 태그의 고유 값(TID)을 수입하는 측으로 보낸다.

이때 비밀 값 S와 초기값 IV과 T_0, k, TID 는 기존의 유선 통신망을 통해 데이터를 전송할 때 사용되는 안전한 프로토콜을 사용하여 전달되는 것으로 가정하도록 한다.

3.2 데이터 송수신 프로토콜



〔그림 2〕 데이터 통신 프로토콜

컨테이너의 현재 위치를 확인하는 등의 상황을 위해 태그와 리더 간에 데이터가 오고가야 하는 경우에는 다음과 같은 절차를 수행함으로서 공격자가 전송되는 정보를 도청하여 태그에 저장된 정보를 알아내거나, 비밀 정보를 알아내는데 사용하지 못하도록 한다.

먼저 데이터베이스에서 랜덤 값 r_R을 생성하여 다음과 같은 방법으로 인증 정보를 생성하여 생성된 랜덤 값 r_R과 N을 함께 리더를 통해 태그 측으로 전송한다.

$$N = h(r_R \oplus S)$$

태그는 저장되어 있는 S와 전달된 r_R을 이용하여 N'을 생성하여 전달된 N과 동일한 경우 다음과 같은 방법으로 저장되어 있는 식별 데이터를 전송한다. 이때 전송되는 데이터는 다음과 같다.

$$r_T, E_{h(S\|r_T\|r_R)}(Data \| r_R)$$

이때 r_T는 태그 측에서 생성한 랜덤 값 이다. 데이터베이스는 태그에서 전달된 데이터를 복호화 한 다음에 패딩된 랜덤 값이 자신이 전달한 랜덤 값과 동일한지 여부를 확인하는 것으로 태그에서 전달된 정당한 정보임을 확인할 수 있다.

3.3 복제 방지 프로토콜

배 등을 통해 화물 컨테이너가 이송되는 중에 전자봉인은 $g(T_0)$만큼의 시간이 흐른 후 $T_i = h(T_{i-1})$로 T_i값을 변경한다. T_i값이 변경된 후 다시 태그는 $g(T_i)$ 만큼의 시간이 흐른 후 같은 동작을 반복한다. 이렇게 이전에 대기한 시간의 해시 값을 취하여 대기할 시간의 길이를 결정함 으로서, 공격자는 이전에 어느 정도 시간을 대기 했는지를 확인할 수 없게 되고, 얼마를 더 대기해야 하는지를 예측하기 어렵게 된다.

3.4 전자봉인이 복제 되었는지 여부검증

전자 봉인된 화물 컨테이너가 도착지에 도달한 후 도착지의 검사원은 다음과 같은 방법으로 전자봉인이 복제 되었는지 여부를 확인한다. 먼저, 태그의 봉인이 열리지 않으면 봉인 정보는 확인할 수 없는 것으로 가정 하며, 봉인이 열리는 순간 태그의 타이머는 정지 하도록 한다. 수출 측에게 보낸 IV와 수출 측이 보낸 k를 이용하여 $T_0' = MAC_k(IV)$을 생성 해 낸 후, 태그로부터 현재 시간과 T_n값을 얻어 낸다. $T_i = h(T_{i-1})$를 반복하여 연산을 수행하면 T_n'을 얻을 수 있다. 이때 확인자는 $\sum_{i=0}^{n} g(T_i)$를 계산, 'T_n을 추출한 시점의 시간 - 수출 측에서 보낸 봉인시점의 시간'과 비교하여 허용범위 내인지를 확인하면 되므로 n회만 연산을 수행하면 된다. 이렇게 얻은 값이 오차범위 이내가 아니거나 $T_n \neq T_n'$이라면 태그가 중간에 복제되어 바꿔치기가 되었다는 것을 알 수 있다.

Ⅳ. 프로토콜의 안전성 검증

4.1 데이터 송수신 프로토콜의 안전성

제안된 프로토콜을 공격하기 위해서, 공격자는 전달되는 데이터의 내용을 이해하기 위해서 키로 사용된 $h(S||r_T||r_R)$을 알아내야만 한다. 실제로 r_T와 r_R은 그대로 전달되므로 도청에 의해 확인 될 수 있으나 S값은 노출되지 않았으므로 확인 할 수 없다. 또한 사용된 키는 전달되는 것이 아니라 암호화 하는데 키로서 사용되었으므로 전달되는 정보만으로는 확인 할 수 없다. 그러므로 공격자는 전달되는 데이터를 암호화 하는데 사용된 키를 알아낼 수 있는 방법이 없다. 즉, 전달되는 내용이 도청되더라도 공격자는 그 내용을 확인할 수 없다. 또한 태그는 매번 새로 생성되는 랜덤 값을 키를 생성하는데 사용된 해시 함수의 입력 값으로 사용하였기 때문에 항상 다른 출력이 태그로부터 출력되므로 공격자는 태그로부터 전달된 두 내용이 같은 태그에서 출력된 정보인지 아닌지 식별하는 것이 불가능하다. 그렇기 때문에 아무리 많은 정보를 도청하더라도 도청된 내용을 다른 공격을 수행하는 용도로 사용 할 수 없다. 데이터베이스에서 전달한 값이 데이터에 패딩 되므로 이전의 통신 내용을 재전송하는 것으로 정당한 태그로 가장하는 공격을 수행할 수 없다.

4.2 봉인 프로토콜의 안전성

공격자가 어떤 알려지지 않은 방법을 통해 태그에 저장되어 있는 S값을 알아낸 경우, 공격자는 정상적인 태그인 것처럼 위장할 수 있다. 그러나 공격자는 얻어낸 S값을 이용하여 봉인 검증절차를 통과할 수 는 없는데, 봉인 검증절차에서 사용되는 IV와 T_0는 태그에 저장되어 있지 않기 때문이다. T_n은 T_{n-1}만큼의 대기후에 갱신된 값이므로 공격자가 이 방법을 통해 공격에 성공하기 위해서는 수입 측이 수출 측에게 보낸 IV와 T_0를 알거나, 봉인을 연 시점이 저장된 봉인 정보가 갱신된 후 얼마나 지났는지를 알아야만 한다. 봉인을 연 시점이 저장된 봉인 정보가 갱신된 후 얼마나 지났는지를 알 수 없다면 공격자는 다음 번 갱신 시기를 알 수 없으므로 최종적인 검증을 통과 할 수 없다.

Ⅴ. 결론

본 논문에서는 전자봉인을 복제하는 공격에 대해 저항성을 갖는 방법과 통신되는 정보를 이용하여 태그를 위조하지 못하도록 하기 위한 방법을 제시 하였다. 제시된 방법은 공격자가 통신의 내용을 도청하더라도 그 내용을 이해할 수 없도록 하였으며, 알려지지 않은 어떤 방법으로 공격하여 태그의 내용을 확보하여도 운송되는 도중에만 정당한 태그로 위장할 수 있을 뿐 최종적으로 전자봉인이 개봉된 적이 없다는 것을 확인하는 단계에서는 속일 수 없는 성질을 제공한다.

제안된 프로토콜의 문제점은 오차범위를 크게 잡는 경우에 태그의 내용을 물리적으로 무작정 복제한 경우에 우연히 오차범위 내에 복제된 태그의 타이머가 포함되는 경우 실제 태그가 복제되었음에도 불구하고 복제되지 않은 것으로 착각하는 경우가 있다는 것이다. 그렇기 때문에 전자봉인이 복제되었는지 여부를 검증하는 절차에서 오차범위를 너무 크게 잡는 것은 프로토콜 자체를 무의미 하게 만들 수 도 있다.

앞으로의 연구과제는 운송되는 도중에도 봉인을 분석하여 복제/대체하는 경우에도 그 사실을 확인 할 수 있는 기법을 연구하여 운송 중에라도 문제점을 찾을 수 있는 방법을 제시하는 것이다.

참고문헌

[1] "Freight Container - Identification and Communication, Electronic Seals-Part 4: Data Protection"

[2] D. Henrici and Paul Muller, "Hash-based enhancement of Location Privacy for Radio-Frequecy Identification Devices using Varying Identifiers", PerSec'04 at IEEE PerCom, pp. 149-153, 2004

〈著者紹介〉

김 주 해 (Kim Joo Hae) 학생회원

1996년 2월 : 광운대학교 전산학과 학사
2005년 3월~현재 : 고려대학교 정보보호대학원 석사과정
<관심분야> RFID 정보보호 기술, 유비쿼터스, 암호프로토콜

최 은 영 (Eun Young Choi) 학생회원

2001년 8월 : 고려대학교 수학과 학사
2003년 8월 : 고려대학교 정보보호대학원 공학 석사
2004년 3월~현재 : 고려대학교 정보보호대학원 박사과정
<관심분야> 암호 이론, 정보보호 이론, RFID 정보보호 기술, 유비쿼터스

이 동 훈 (Dong Hoon Lee) 종신회원

1983년 8월 : 고려대학교 경제학사
1987년 12월 : Oklahoma University 전산학 석사
1992년 5월 : Oklahoma University 전산학 박사
1993년 3월 ~ 1997년 2월 : 고려대학교 전산학과 조교수
1997년 3월 ~ 2001년 2월 : 고려대학교 전산학과 부교수
2001년 2월~현재 : 고려대학교 정보보호대학원 교수
<관심분야> 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술