복제 공격 저항성을 갖는 전자봉인 보안 모델[1)]

김주해, 최은영, 이동훈
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 정당한 사용자가 아닌 다른 사용자가 개봉하였다는 사실을 인지하도록 하는 역할을 하는 장치이다. 전자 봉인장치는 RFID를 이용하므로 허용된 사용자 외에는 그 정보를 식별 할 수 없도록 할 필요가 있으며, 오랜 시간 고정된 장소에 존재하기 때문에 물리적으로 공격당하여 컨테이너의 내용물을 훔치거나 다른 물건으로 바꾸어 넣은 후 기존의 봉인의 내용을 복사한 새로운 봉인을 설치함으로서 봉인이 깨졌었다는 사실을 인지하지 못하도록 만드는 일을 막을 수 있어야만 한다. 본 논문에서는 리더와 태그가 통신하는 그 내용을 제 삼자가 인식하지 못하도록 함과 동시에, 봉인의 내용을 복사하더라도 원래 봉인을 대체할 수 없도록 하는 방법에 대해 제안 하고자 한다.

I. 서론

전자봉인기술(e-Seal)은 433MHz 주파수 대역을 사용하는 능동형 RFID(Radio Frequency Identification)장치를 이용하여 화물 컨테이너를 안전하고 효율적으로 관리하기 위한 기술이다. 전자봉인은 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 31일에 발표된 ISO18185-4 규격은 전자봉인이 비밀 정보를 가지지 않는다는 전제조건을 제시하면서 어떠한 보호기술도 명시하지 않은 상태이다. 그러나 이러한 전자 봉인은 비밀 정보를 포함하지 않았으므로 도청공격은 무의미 하지만 데이터 위변조에는 취약할 수밖에 없다.

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

1.1 RFID 시스템의 문제점

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 eSeal에 사용되는 경우, RFID 태그는 배위에 실린 채로 몇 개월 이상의

1) 본 연구는 서울시 산학연 협력사업(10665)지원으로 수행되었음

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.

공격자가 전자봉인을 위조하기 위해서는 봉인이 제거 되었을 때 태그로부터 리더에게 전송되는 전자봉인 제거 신호를 차단해야 할 필요가 있는데, 이 경우에는 태그의 전파신호를 차단하는 패러데이 케이지(Faraday Cage)나 액티브 재밍(Active Jamming)등을 사용함으로서 태그로부터 리더로 전송되는 전자봉인 제거 신호를 차단할 수 있다.

II. 안전한 RFID 시스템 설계시 고려사항

이 장에서는 태그와 리더간의 통신에서 비밀정보를 얻는등의 자신의 목적을 달성하기 위해 공격자가 행할 수 있는 공격 방법에 대해 알아보고, 기존에 많이 사용되는 정보보호 기법들의 안전성에 대해 분석해 보겠다.

2.1 RFID 시스템 공격방법

공격자의 유형은 크게 두가지가 있는데 첫번째는 단순히 전달되는 통신 내용을 엿듣기만 하는 형태의 수동적인 공격자이다. 다른 하나는 통신 내용을 변조하여 전송하는 등의 방법을 사용하여 올바른 통신 상대인 것으로 오인하도록 만드는 등의 공격을 수행하는 능동적인 공격자이다. 추가적으로 태그를 물리적으로 공격하여 태그에 저장되어 있는 비밀 정보를 추출해내는 공격자 역시 고려되어야 할 사항이다. 그러나 물리적으로 공격을 수행하는 경우는 정보 전체를 강제적으로 추출해내는 방법이니 만큼 일반적인 공격 방법으로 고려하지는 않도록 하겠다.

2.1.1 도청

리더와 태그간에 오고가는 통신의 내용을 도청하여 비밀정보를 얻어낼 수 있다. 실제로 앞서 언급한 바와 같이 RFID 시스템은 공간을 통해 데이터가 전송되므로 공격자가 도청을 통해 정보를 수집하는 것을 물리적으로 막는것은 상당히 어려운 문제이다. 그러므로 도청 자체를 막는 것이 아니라, 도청에 성공하여 통신 내용을 얻더라도 그 내용을 확인할 수 없게하고, 도청을 통해 얻은 정보를 공격등의 목적으로 사용할 수 없도록 하는 것이 중요하다.

2.1.2 위조

공격자가 가짜 태그나 리더를 정당한 것 처럼 동작하여 정보를 빼내거나, 인증과정을 통과하는 공격방법이다.

공격자가 이러한 공격에 성공한다면, 전자봉인을 제거한 다음 위조된 봉인을 설치함으로서 봉인이 열렸었다는 사실 자체를 인지하지 못하도록 할 수 있다.

2.1.2.1 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.

2.1.2.2 스푸핑 공격(Spoofing Attack)

공격자는 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.

2.1.2.3 메시지 차단

서비스 거부공격(Denial of Service)의 한 유형으로, 데이터베이스에 태그의 현재 상태를 저장하는 보안모델에서 발생할 수 있다. 메시지

차단을 통해 태그에 저장되어 있는 정보와 데이터베이스에 저장되어 있는 정보를 다르게 만듦으로서 데이터베이스가 태그를 더 이상 인식하지 못하게 하여 리더가 더 이상 태그를 사용하지 못하도록 하는 형태의 공격이다.

III. 인증 및 봉인 프로토콜

전체 프로토콜은 태그와 리더간의 통신 시 안전하게 데이터를 주고받기 위한 인증 부분과 봉인이 복제되지 않았다는 것을 확신하게 해주는 봉인 프로토콜 두 부분으로 구성된다.

3.1 초기화 단계

인증프로토콜을 위하여 초기에 전자 봉인이 사용되는 시점에서 태그와 리더는 태그마다 유일한 비밀 값 S를 공유한다.

두 번째로 전자 봉인을 위한 프로토콜을 위해 컨테이너를 이용하여 수출입을 수행하는 것으로 결정 되는 시점에서 수입하는 측에서 수출하는 측으로 초기값(IV: Initial Vector)을 전달하고, 수출하는 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 고유값(TID)을 수출하는 측으로 보낸다.

3.2 데이터 송수신

태그와 리더간에 데이터가 오고가야 하는 경우에는 다음과 같은 절차를 거친다.

먼저 리더 측에서 랜덤 값 r_R을 생성하여 다음과 같은 방법으로 인증 정보를 생성하여 생성된 랜덤 값 r_R과 N을 함께 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.

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

이때 r_T는 태그 측에서 생성한 랜덤 값 이다. 이렇게 전달된 데이터는 비밀 값 S를 알고 있는 정당한 리더만이 분석하여 그 의미를 알 수 있다.

3.3 복제 방지를 위한 태그의 동작

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. Ti값이 변경된 후 다시 태그는 g(Ti) 만큼의 시간이 흐른 후 같은 동작을 반복한다.

3.4 전자봉인이 복사 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 하며, 봉인이 열리는 순간 태그의 타이머는 정지 하도록 한다.

수출 자에게 보낸 IV와 수출 자가 보낸 k를 이용하여 $T_0' = MAC_k(IV)$을 생성 해 낸 후, 태그로부터 현재 시간과 T_n값을 얻어 낸다.

$T_0 = h(T_{i-1})$를 반복하여 연산을 수행하면 T_n'을 얻을수 있다.

이때 확인자는 $\sum_{i=0}^{n} g(T_i)$를 계산, 'T_n을 추출한 시점의 시간 - 수출자 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

5.1 봉인 프로토콜의 안전성

공격자가 봉인 프로토콜을 깨고 태그에 저장되어 있는 정보를 그대로 복사하는 경우는 두 가지 상황이 있다. 첫 번째는 검사원으로 가장하여 무선 통신을 통해 봉인정보를 얻어내고 이를 바탕으로 태그의 봉인 시기를 추측하고, 비밀 정보를 얻어내어 새로운 태그를 만들어 내는 방법이다. 그러나 이 방법은 봉인이 열리기 전에는 봉인 정보를 내보내지 않는다는 전제가 있으므로 봉인을 열기 전에는 정보를 얻

어 낼 수 없고, 인증 프로토콜을 깨야만 수행할 수 있는 공격방법 이다.

두 번째 방법은 봉인을 열고 물리적인 방법을 동원하여 태그에 저장되어 있는 정보를 추출해내어 새로운 봉인에 써 넣는 방법이 있다. 이 방법을 통해 공격에 성공하기 위해서는 수입자가 수출자에게 보낸 IV를 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 통과할 수 없다.

5.2 인증 프로토콜의 안전성

인증 프로토콜의 안전성은 해쉬함수 h()에 의존되며, 해쉬함수 h()가 해쉬 함수의 출력값을 가지고 입력값을 알 수 없는 한 인증 프로토콜은 안전하다.

공격자가 전달되는 값에서 해쉬 함수의 입력값을 알아낼 수 없는 한 사용되는 비밀 값 S를 알아낼 수 없으며, 매 라운드마다 태그와 리더는 각각 랜덤 값을 생성하여 전송하기 때문에 어느 한쪽의 값을 이용하여 재전송 공격을 할 수 없고, 해쉬 함수의 입력으로 랜덤 값이 사용되므로 같은 입력에 대해서도 매번 다른 값을 출력하게 되어 공격자는 리더나 태그에서 방출되는 정보와 랜덤 값을 구별 할 수 없다.

V. 결론

본 논문에서는 전자봉인을 복사하는 공격에 대해 저항성을 갖는 방법과 통신되는 정보를 이용하여 태그를 위조하지 못하도록 하기 위한 방법을 제시 하였다. 제시된 방법은 불구분성과 전방향 안전정을 제공하여, 공격자가 통신의 내용을 도청하더라도 그 내용을 이해할 수 없도록 하였으며, 물리적으로 공격하여 태그의 내용을 확보하여도 운송되는 도중에만 리더를 속일 수 있을 뿐 최종적으로 전자봉인이 개봉된 적이 없다는 것을 확인하는 단계에서는 리더를 속일 수 없는 성질을 제공한다.

앞으로의 연구과제는 운송되는 도중에도 봉인을 분석하여 복사/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] A. Juels, R.L Rivest and M. Szudlo, ''The Blocker Tag: Seelective Blocking of RFID tags or Consumer Privacy'', In the 8th ACM Conference on Computer and Communications Security, pp.103-111, ACM Preass. 2003.

[3] M. Ohkubo, K. Suzuki, S. Kinoshita, ''Cryptographic Approach to Privacy-Friendly Tags'', RFiD Privacy workshop, November, 2003

[4] 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