경량화된 RFID 인증 프로토콜

구중두*, 이기성*
*호원대학교 컴퓨터・게임학부
e-mail:jdkooinfo@gmail.com

Lightweight RFID Authentication Protocol

Jung-Doo Koo*, Gi-Sung Lee*
*School of Computer Game, Howon University

요 약

저전력 RFID 시스템은 무선 주파수와 RFID 태그 사용으로 불법적인 위변조, 도청, 추적, 프라이버시 침해 등이 발생할 수 있다. 본 논문에서는 태그와 데이터베이스 간에 해시 체인을 이용하여 키를 생성하는데 이를 통해 공격자는 위의 공격을 수행할 수 없다. 또한 계산량을 줄이기 위해 해시 함수를 이용하여 효율성을 높였다.

1. 서론

RFID/USN(Radio Frequency Identification/Ubiquitous Sensor Network) 기술은 무선 주파수를 이용하여 리더와 태그 간에 데이터 통신을 하는 ADC(Automatic Data Collection) 기술로서, 빠르고 신속성 있고 노출되어 있지 않고 가려져 있거나 이동 중에 있어도 통신이 가능한 시스템이다[1]. RFID 시스템은 3가지로 구성되는데, 리더의 질의에 대하여 사물, 사람 등의 식별 정보를 무선 통신을 사용하여 전송하는 태그(Tag) 또는 트랜스폰더(Transponder)와 태그가 전송하는 데이터를 수신하여 태그를 인식하거나 태그에 새로운 정보를 다시 쓰는 역할을 수행하는 리더(Reader) 또는 트랜시버(Transceiver) 마지막으로 데이터베이스는 태그에 관련된 정보를 저장하고 관리하는 역할을 한다[2].

RFID는 리더와 태그 간에 무선 통신을 사용하기 때문에 사용자의 개인정보 유출 문제 및 군에서 병력의 위치 추적(프라이버시 침해), 재전송 공격과 스푸핑 공격과 같은 위조 공격, 도청과 같은 공격의 위협에 노출될 수 있다. RFID 시스템을 사용하기 전에 위의 공격에 대응해야 한다. 또한 RFID 시스템은 전력과 계산 능력에 제한적이기 때문에 위의 공격을 방지하기 위해 경량화된 암호 알고리즘은 필수적이다.

기존에 제안된 S.Lee가 제안한 동기화된 비밀 정보를 이용하는 상호인증 프로토콜[2]은 공격자가 악의적인 임의의 수(random number)를 전송함으로써 정당한 태그로 위장하여 리더를 속일 수 있는 스푸핑 공격에 취약하다는 것이 Ha 등에 의해 밝혀졌다[3].

Peris-Lopez의 LAMP(Lightweight Mutual Authentication Protocol)[4], M2AP(Minimalist Mutual Authentication Protocol)[5] 및 EMAP(Efficient Mutual Authentication Protocol)[6]은 간단한 논리 연산에 의해 높은 구현 효율성을 제공하도록 설계되었다. 그러나 비동기화공격을 통해 항상 공격자가 비밀 정보를 획득할 수 있는 문제점이 존재한다[7].

제안하는 프로토콜은 RFID 시스템의 제약조건인 계산능력과 제한적인 수명을 고려하여 간단한 논리연산과 해시 체인을 이용하였으며 기존의 여러 공격에 안전하도록 프로토콜을 설계하였다.

본 논문의 구성은 다음과 같다. 2절에서는 제안하는 프로토콜에 대해 설명한다. 3절에서는 프로토콜의 효율성 및 안전성을 검증한다. 마지막으로 결론과 향후 관련연구 방향에 대해 제시한다.

2. 제안하는 프로토콜

2.1 표기법

- T: RFID 태그 또는 transponder.
- R: RFID 리더 또는 transceiver.
- D: 데이터베이스를 가진 Back-end 서버.
- SN: 태그의 serial number.
- $e(k,m)$: 비밀키 k를 이용하여 메시지 m을 암호화하는 대칭키 암호 함수.
- $d(k,m)$: 비밀키 k를 이용하여 메시지 m을 복호화하는 대칭키 암호 함수.
- $h()$: 일방향 해시 함수.
- $h(k,m)$: 비밀키 k를 이용한 해시 함수.
- k_{R-D}^{i}: 리더와 데이터베이스 i번째 비밀키.
- k_{T-D}^{i}: 태그와 데이터베이스 간의 i번째 비밀키.
- r: 랜덤 수.
- $m_1 \| m_2$: 메시지 m_1과 m_2의 비트 결합.

2.2 가정

제안하는 프로토콜에서 태그는 수동적인 태그로서, 해시 함수와 하나의 세션동안 상태를 유지할 수 있는 능력을 가지고 있다. 위에서 소개한 프로토콜과 달리 리더와 태그 및 리더와 데이터베이스 구간은 무선 네트워크로서 안전하지 않은 채널이라고 가정한다. 리더와 데이터베이스 사이에는 비밀 값 k_{R-D}^{0}을 태그와 데이터베이스 사이에는 해시 체인 초기값 k_{T-D}^{0}값을 공유하고 있다고 가정한다. 제안하는 프로토콜에서 RFID 태그에 대한 물리적인 공격은 고려하지 않는다.

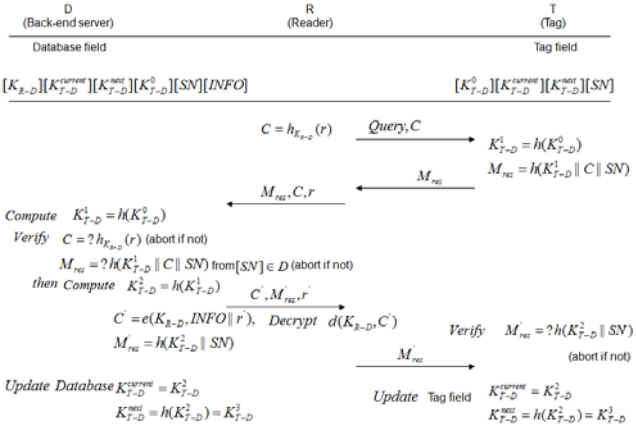
2.3 프로토콜

위에서 분석한 내용을 토대로 저전력 RFID 시스템에 적합한 경량화된 해시 체인 기반의 상호 인증 프로토콜을 그림 1과 같다.

단계 1: 먼저 리더 R은 난스 r를 생성한 후, 데이터베이스 D와 공유하고 있는 비밀키 K_{R-D}를 이용하여 r을 해시한다. 이때, 해시함수는 키를 이용한 일방향 해시 함수이다. R은 $C = h_{K_{R-D}}(r)$을 포함하는 질의 $Query$를 태그 T에게 전송한다. 이때, K_{R-D}는 D에서 R를 인증하기 위해 사용되며 C를 통해 능동 공격자에 대한 중간자 공격(man-in-the middle attack)을 방지할 수 있다.

단계 2: C를 수신한 태그 T는 D와 공유한 해시 체인 초기값 K_{T-D}^{0}을 이용하여 $K_{T-D}^{1} = h(K_{T-D}^{0})$을 계산한다. 그런 후에 $M_{res} = h(K_{T-D}^{1} \| C \| SN)$을 계산하고 R에게 전송한다. M_{res}는 D에게 합법적인 R이라는 것을 확인시키고 능동적 공격인 도청으로부터 M_{res}를 위조 못하게 하기 위함이다.

단계 3: 이 메시지를 수신한 R는 C와 r를 추가하여 전송한다. r은 중간자 공격을 방지하고 C와 함께 D에서 합법적인 R로부터 온 메시지인지를 검증하기 위해 사용된다. 데이터베이스 D에서는 먼저 정당한 R인지 수신한 S와 r을 이용하여 $C = ?h_{K_{R-D}}(r)$을 계산한다. 이때 C값이 올바르지 않을 경우에는 프로토콜을 중지한다. 동시에 D는 K_{T-D}^{0}와 SN을 데이터베이스로부터 추출한다. 그런 후에 $K_{T-D}^{1} = h(K_{T-D}^{0})$를 계산하고 $M_{res} = ?h(K_{T-D}^{1} \| C \| SN)$을 검증한다. D는 R과 T의 정당성을 확인하고 $K_{T-D}^{2} = h(K_{T-D}^{1})$을 계산한다. 합법적인 R이라는 것이 검증되면 K_{R-D}를 이용하여 태그의 정보 $INFO$를 암호화해서 R에게 전송한다. 이는 중간자 공격과 도청을 방지하기 위해 비밀키를 이용하여 암호화한다. 또한 D는 T와 상호인증을 위해 $M_{res}^{'} = h(K_{T-D}^{2} \| SN)$을 전송한다. 마지막으로 D는 현재 업데이트 된 T와의 비밀키 K_{T-D}^{2}를 데이터베이스 $[K_{T-D}^{current}]$필드에 저장하고 다음 세션에 사용할 키를 미리 해시 체인을 통해 계산한 후 $[K_{T-D}^{\neq xt}]$ 필드에 저장해 둔다.



[그림 1] RFID 시스템을 위한 상호 인증 프로토콜

단계 4: R은 수신 메시지 중 C'값을 복호화하고 태그 정보 $INFO$을 획득한다. 이때 복호화가 되지 않을 경우에는 프로토콜을 중지한다. r'는 중간자 공격을 방지하기 위해 포함된 파라미터이다. 그런 후에, R은 T에게 $M_{res}^{'}$ 메시지를 전송한다.

단계 5: T는 $M_{res}^{'}$ 메시지의 정당성을 검증하기 위해 $M_{res}^{'} = ?h(K_{T-D}^{2} \| SN)$을 계산한다. 이를 통해 D를 인증 할 수 있다. 그런 후에 D와의 비밀키를 갱신하기 위해 $K_{T-D}^{current} = h(K_{T-D}^{2}) = K_{T-D}^{3}$을 계산한 후 자신의 메모리 필드 $[K_{T-P}^{current}]$에 저장한다.

3. 성능분석

능동적인 공격자에 의한 도청 가능 메시지는 리더 R이 태그 T에게 전송하는 C값과 T가 R에게 응답하는 M_{res}, R이 D에게 전송하는 r, 기타 $M_{res}^{'}, C', r'$가 있다. 그러나 제안하는 프로토콜에서 리더 R이 발생하는 랜덤수를 제

외한 모든 정보는 일방향 해시함수나 암호화 연산을 거쳐 전송되는 정보이므로 공격자가 전송 메시지를 도청하더라도 비밀키 값이나 태그 정보는 획득할 수 없기 때문에 안전하다.

다음으로 공격자가 합법적인 리더, 태그나 데이터베이스로 위장하여 상대방을 속이거나 유용한 정보를 획득하려는 스푸핑 공격이 있다. 제안하는 프로토콜에서 공격자는 합법적인 리더로 가장하여 태그를 속이기 위해서는 $M_{res}^{'}$ 값을 계산해야 한다. 그러나 공격자는 데이터베이스 D와 T가 공유하고 있는 비밀키 K_{T-D}^{2}를 계산 할 수 없기 때문에 안전하다. 또한, 태그로 위장하고자 할 경우, 공격자는 R이 생성한 C값은 도청할 수 있지만 M_{res}값과 태그의 SN은 계산해야 할 수 없기 때문에 스푸핑 공격에 안전하다.

위치 추적 공격은 공격자가 특정한 태그로부터 동일한 정보나 특정 태그를 구별할 수 있는 정보를 찾아 태그 소유자의 위치를 추적하는 공격이다[3]. 이 공격은 랜덤한 두 개의 태그를 두고 이들을 구별해 낼 수 없으면 비구별성(indistinguishability)를 만족하여 태그의 위치 프라이버시를 보장받을 수 있다. 본 프로토콜에서는 매번 태그가 해시 체인을 이용하여 새로운 비밀키를 생성하기 때문에 공격자는 매 세션마다 나오는 태그의 정보로 위치를 추적할 수 없다. 다시 말해서 M_{res}값이 매 세션마다 동일한 값을 생성하지 않기 때문이다.

마지막으로 비동기화 공격은 공격자가 메시지를 블로킹하여 정상적인 인증 과정을 방해하는 공격으로 태그는 최소한 이전 세션에서 사용된 비밀 정보를 저장하고 있어야 한다. 제안하는 프로토콜에서는 데이터베이스 필드와 태그 필드에 모두 $K_{T-D}^{current}$와 $K_{T-D}^{\neq xt}$를 가지고 있기 때문에 공격자가 메시지를 블로킹하여도 동기를 회복할 수 있다. 마지막으로 기존 프로토콜[2,3]과 달리 모든 구간을 무선 구간으로 간주하고 프로토콜을 설계했기 때문에 더욱 현실적이고 강건할 수 있다.

4. 결론

본 논문에서는 모든 구간의 안전성을 고려한 RFID 상호인증 프로토콜을 제안했다. 무선 통신상에서 쉽게 발생할 수 있는 도청과 스푸핑 공격에 강건함을 보였다. 또한 비동기화공격 역시 태그와 데이터베이스가 동일한 비밀키를 저장하면서 동기화를 맞추기 때문에 공격자가 메시지를 블로킹 하여도 동기를 회복할 수 있었다.

참고문헌

[1] 이병길, 강유성, 박남제, 최두호, 김호원, 정교일, “능동 및 모바일 RFID 서비스 환경에서의 정보보호 기술”, 한국정보보호학회 학회집, 제 15권, 제3호, pp. 40-47, 2005.

[2] 최은영, 이수미, 임종인, 이동훈, “분산시스템 환경에 적합한 효율적인 RFID 인증 시스템”, 한국정보보호학회논문집, 제16권, 제6호, pp.25-35, 2006.

[3] 하재철, 김환구, 하정훈, 박제훈, 문상재, “비밀정보 동기화에 기반한 Strong RFID 인증 프로토콜”, 한국정보보호학회 논문집, 제17권, 제5호, pp.99-109, 2007.

[4] P. peris-Lopez, J. C. Hermandez-Castro, J. M. Estevez-Tapaidor, and Ribagorda, “LAMP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags,” Workshop on RFID Security 2006, pp.137-148, 2006.

[5] P. peris-Lopez, J. C. Hermandez-Castro, J. M. Estevez-Tapaidor, and Ribagorda, “M^{2}AP: A Minimalist Mutua-Authentication Protocol for Low-cost RFID tags,” Proceedings of UIC 2006, pp.912-923, 2006.

[6] P. peris-Lopez, J. C. Hermandez-Castro, J. M. Estevez-Tapaidor, and Ribagorda, “EMAP: An Efficient Mutua-Authentication Protocol for Low-cost RFID tags,” Proceedings of OTM Federated Conferences and Workshop 2006, pp.352-361, 2006.

[7] 권대성, 이주영, 구분욱, “경량 RFID 상호인증 프로토콜 LMAP, M^{2}AP, EMAP 대한 향상된 취약성 분석”, 한국정보보호학회 논문집, 제 17권, 제 4호, pp.104-113, 2007.