RFID/USN 시스템의 암호화 인증알고리즘 연구

최 성, 이현기
남서울대학교 컴퓨터학과
E-mail : sstar@nsu.ac.kr

Study on the Security Algorithm Method of RFID/USN

Sung Choi, Soo Hun Lee
Dept. of Computer Science, Namseoul University

요 약

정보화 사회의 발전에 따라 컴퓨터끼리의 커뮤니케이션을 넘어 물리공간을 융합하는 유비쿼터스 기술이 발전하고 있다. 유비쿼터스를 위한 기술인 RFID는 RFID TAG가 모든 물체에 부착되어 리더와 정보를 주고받을 수 있게 된다. 하지만 RFID의 제한적인 환경으로 인해 현재 보편적으로 쓰이는 보안 기술을 사용하는 것이 어렵게 되어 유비쿼터스 시대에 맞는 새로운 보안 방법의 연구가 필요하다. 본 논문에서는 유비쿼터스 시대에 맞는 암호화 인증 기술에 방법에 대하여 연구하였다.

1. RFID의 제약사항과 취약점

1.1. RFID / USN의 환경적 제약사항

현재 RFID 태그 중 가장 값이 싸며 작은 태그는 Ateml이다. 이 태그는 992비트의 저장 공간을 갖고 있으며 데이터 전송 비율은 약 초당 100Kb이다. 또한 메모리의 내용에 대한 읽기/쓰기를 허용하고 $1.0로 판매가 되고 있다. 그러나 향후 보편적으로 사용될RFID 태그는 US$0.05~US$0.1의 가격 범위에 있기 때문에 강인한 암호프리미티브를 사용하는 것은 현실적으로 가능하지 않다. 이렇듯 RFID를 위한 컴퓨팅 환경은 일반적인 인터넷 환경과는 달리 많은 제약적 사항을 갖는다. 이러한 제약적 사항은 Cellular Phone등을 이용한 무선 인터넷보다 더욱 자원 측면적 한계를 갖는다. 즉 유비쿼터스 등을 위한RFID 환경을 구축하기 위해서는 모든 상품이나 사람 등 객체에 설치되는 가격은 5센트 이하로 구현되어져야하며 대신에 리더나 백 엔드 시스템에서 많은 성능 자원 측면에서 열악한 태그 장비의 자원적 한계를 극복할 수 있도록 설계, 운영되어야 한다. 또한 보안 기술을 적용하여 보안 서비스를 제공하기 위해서는 현재의 일반적인 RFID 환경에 대한 제약사항을 고려해야 한다.

1.2. 발생 가능한 공격 기법 종류

- 도청 공격 : 태그와 리더사이의 통신은 라디오 방식이기 때문에 누구든지 태그에 접근하여 태그의 출력 값을 얻을 수 있어, 인가되지 않은 리더가 적절한 접근 제어기능이 없는 태그에 접근하여 프라이버시를 침해할 수 있다.
- 트래픽 분석(Traffic analysis) : 태그의 내용이 보호되고 있다 하더라도, 예측되는 태그의 응답 값은 태그와 태그 소유자의 신원(Identity)을 연결시킬 수 있는 정보를 제공해 준다. 태그가 유일한 식별정보를 노출하지 않는다 하더라도 태그의 응답 값에 대한 분석을 통해 태그를 소지한 사용자를 추적할 수 있다. 이 공격은 RFID 태그가 의류, 제품 등에 부착하여 사용자를 추적할 수 있는 위치 프라이버시(Location Privacy)에 대한 위협 요인이 될 수 있다.
- 스푸핑(Spoofing) 공격 : 스푸핑 공격이란 외부의 악의적 침입자가 자신이 사전에 지정한 코드가 작동되도록 함으로써 사용자의 권한을 획득하는 해킹 기법으로, 일반 사용자의 태그를 스푸핑한 공격자는 자동화된 체크아웃 혹은 보안 시스템을 속일 수 있으며, 스푸핑된 데이터로 값싼 물품과 비싼 물품을 교체할 수 있다. 예를 들어, 물건에 부착된 태그가 스푸핑되어 비싼 가격의 물건을 싼 가격의 물건으로 바꾸는 일들이 발생하면 기업입장에서는 엄청난 손

해를 입을 수 있으며,신용카드나 현금카드에 사용되는RFID 태그가 스푸핑되어 복제되는 경우 개인이 막대한 피해를 입을 수도 있다.

- 서비스거부 공격 시스템자원에 (Denial of Service) : RFID 대한 정상서비스를 방해하기 위해 공격으로, RF 신호 채널을 방해하거나, 임의의 다른 수단으로 태그를 무력화시키는 등이 해당된다.

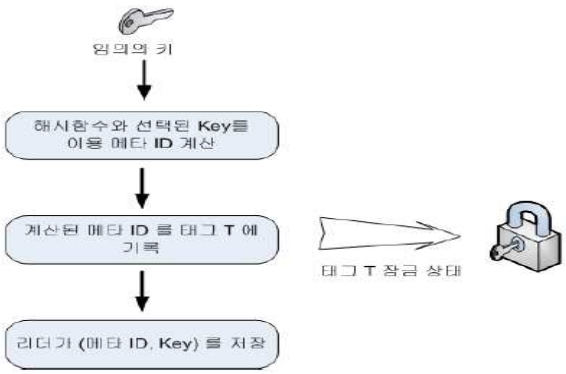
- 세션 가로채기(Hijacking), 재생(Replay) 공격, 중간자 공격(Man In the Middle Attack) : RFID 리더와 태그사이의 상호인증을 위한 인증 프로토콜 수행 시 발생할 수 있는 공격들로, 인증된 세션을 가로채는 세션 가로채기 공격, 공격자가 검증자에게 이전에 수행되었던 프로토콜 부분 중 일부분을 다시 실행시키는 재생 공격, 공격자가 인증 프로토콜 수행 중간에 자신의 정보를 삽입하는 중간자 공격 등이 존재한다.

- 물리적(Physical) 공격 : 태그의 메모리는 물리적 공격에 취약하다. 즉, 스마트카드에 적용될 수 있는 프로브공격, TEMPEST 공격 등의 물리적 공격이 RFID 태그 메모리에도 적용될 수 있다. 그러나 이러한 공격에 강인한 메모리가 RFID 태그에 사용되기에는 비용이 너무 비싸진다는 문제점이 있다. 또한, 향후 스마트카드처럼 암호알고리즘을 지원하는 태그가 설계되는 경우, 스마트카드에 적용될 수 있는 전력해석(Power Analysis), 타이밍 해석(Timing Analysis) 등의 사이드채널공격(혹은 부채널 공격)에 대한 위험요인도 존재할 수 있다.

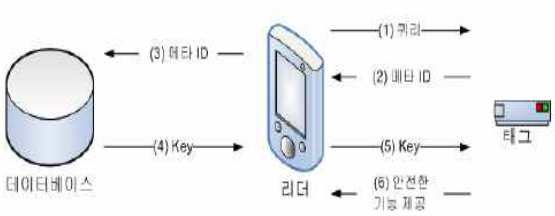
2. 정보 보호 기술

2.1. 인증 및 접근 제어

태그와 리더는 서로를 인증하여 서로를 신뢰하는 경우에만 올바른 동작을 보장해야 한다. 정당한 사용자만이 태그에 접근 할 수 있으며 태그를 잠그거나(Lock) 해제(Unlock) 할 수 있어야 한다. 잠긴 태그는 어떠한 리더의 신호에도 응답하지 않으며 해제된 태그는 정당한 사용자에 한하여 자신의 정보를 전송해야 한다. 인증 및 접근 제어 서비스를 제공하기 위해 해시 기반(Hash- Based) 접근제어'나 '난수(Randomized) 접근 제어'와 같은 방법 등이 제안되고 있다.



(그림 1 : 해시 락의 잠금 과정)



(그림 2 : Hash Lock / Unlock 절차)

- 해시기반 제어 : MIT는 저렴한 비용(50원이하)의 태그에서 자원제한문제를 해결하면서 인가 받은 리더에게만 태그 정보를 전송하기 위해 단방향(One-way) 해시 함수를 기반으로 하는 접근 제어 메커니즘인 Hash Lock 기술이 제안되었다

- 난수 해시 락 : 난수 해시-락은 메타 ID정보에 따른 추적공격이 가능한 해시-락 취약점을 극복하기 위해 제안된 방법이다. 난수 해시-락 방법을 사용하기 위해서, 태그는 단방향(One-way) 해시 함수뿐만 아니라 난수생성기(Random Number Generator)를 가지고 있어야 한다. 그리고 적법한 리더는 태그를 조사하기 이전에 자신이 가지고 있는 태그들을 알고 있다고 가정한다. 또한 태그를 잠그기 위한 다른 절차가 필요 없고, 리더로부터의 간단한 명령을 통해 잠김 상태로 들어갈 수 있다.

2.2 도청 방지 연구방법

정당한 사용자에 의하여 전송된 태그의 정보는 제 3 자가 엿들을 수 없어야 하며 설령 엿듣는다 하더라도 정확히 무슨 정보인지 알 수 없어야 한다. 도청 방지를 위하여 암호화한 방법으로는 바이너리 트리 워킹 충돌방지 기법 상에서 작동하는 고요한 트리워킹(Silent Tree-walking) 이나 랜덤 트리워킹 같은 방법이 있다. 그 외 암호학적인 방법 중에서 비밀키 암호화 방식을 사용하여 암호화된 데이터를 전송하는방법이나 공개키 암호화 방식을 사용하여 암호화 정보를 태그에 기록하는 재암호화(Re-encryption)방

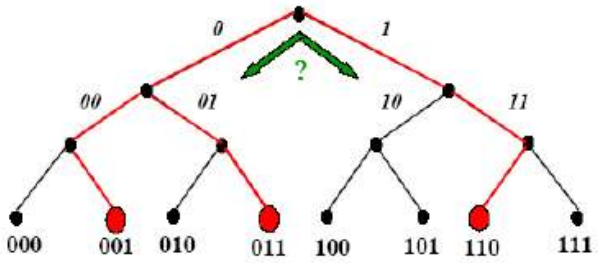
법 등이 있다.

- 트리 워킹 알고리즘 : 정보를 담고 있는 전파를 만들어내는 인코딩의 하나인 맨체스터 인코딩은 0과 1이 동시에 통신매체에 발생하는 것을 검출할 수 있는데, 이를 이용한 방법이 트리 워킹 싱귤레이션 알고리즘이다.

- 고요한 트리 워킹

MIT가 제시한 고요한 트리워킹 알고리즘은 이러한 안전하지 않은 태그의 ID를 리더가 브로드캐스트 하지 않아, 도청공격에 안전하면서 트리워킹 알고리즘과 유사한 수행속도를 갖도록 변형한 변형기법이라 할 수 있다. 고요한 트리워킹 알고리즘은 리더에서 태그로 가는 전 방향(For ward) 채널의 강인한 신호에 대해 도청자로부터 안전하게 하는 방법이다.

- 난수 트리 워킹 : 일반적으로 멀리 존재하는 도청자가 정보를 수집할 수 있는 것은 리더의 정보 전달 거리가 멀고, 리더가 태그로부터 알아 낸 정보를 이용하여 다음 명령을 내리기 때문이다. 그렇기 때문에, 매 회 태그가 자신의 실제ID가 아닌 대리의 값을 이용하여 리더로부터의 질의에 응답을 하고, 리더는 이를 이용하여 태그를 선별해 나간다면 도청자는 실제 ID를 알아낼 수 있는 방법이 없다. 이 아이디어를 이용한 것이 난수 트리 워킹이다



(그림 3 : 난수 트리킹 알고리즘)

2.3 정보 차단

어느 누구도 태그의 정보를 알 수 없도록 태그의 정보를 막는 방법이다. 물리적인 방법으로 킬 태그(Kill tag) 방법이나 패러데이 우리(Fara-day Cage), 방해 전파(Active Jamming)를 사용하는 방법과 차단자 태그(Blocker Tag)를 이용하는 방법이 있다.

- 킬 태그 : 태그 내부에 단락회로를 만들어 놓고 Kill 명령을 받을 시 회로를 끊는 방법이다.

- 패러데이 우리 기술 : 금속성의 그물이나 박막을 입힌 컨테이너를 이용하여 주파수과 투과되지 못하도록 하는 기술이다.

- 방해 전파 : 방해 전파 방법은 근처에 있는 RFID 리더의 기능을 막거나 혹은 방해할 수 있는 라디오 신호를 브로드캐스트 하는 디바이스를 이용하는 것이다.

3. 결론

유비쿼터스 사회에서는 자율 컴퓨팅 기능을 갖는 기술 및 사물 등에 의하여 서비스가 이루어질 것이다. RFID와 USN 기술은 유비쿼터스 사회의 구현을 위한 핵심 기술이다. RFID는 기존 바코드에 비해 저장용량이나 속도 등에서 많은 장점을 갖고 있다. 이런 많은 장점으로 인해 사회 곳곳에서 RFID기술이 쓰이기 시작하였다. 하지만, RFID가 장점만 가진 것은 아니다. 무선이라는 편리함이 있지만, 그로 인한 보안 문제도 심각한 문제이다. RFID 태그 시스템에서 보호되지 않은 태그는 도청, 트래픽 분석, 스푸핑 혹은 서비스거부공격 등에 취약하다. RFID에 저장된 개인정보가 각종 공격에 의해 노출될 경우 개인 프라이버시 침해의 우려가 높다. 따라서 사업자와 개인은 RFID를 이용할 시에 프라이버시의 침해에 대한 우려에서 벗어날 수 있도록 많은 노력이 필요하다.

4. 참조 문헌

[1] ETRI, 전자통신동향분석 제20권 3호, 2007

[2] IITA, 혼합현실기반 u-체험형 콘텐츠 운용플랫폼, 2007

[3] 한국전산원, RFID/USN 확산 저해요인 및 개선대책 연구, 2006