RFID 태그 보안과 프로토콜의 취약점 분석 및 보안성 향상을 위한 기법

김정태*

Technique for Enhancing Security and Analyses of Vulnerability of RFID Tag security and Protocol

Jung Tae Kim*

이 논문은 2010년도 교육과학기술부의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2010-0024133)

요 약

RFID 는 유비쿼터스 환경하에서 필수불가결한 기술이 되도 있다. 그러나 RFID 의 본질적인 단점으로 인하여 프라이버시와 같은 보안적인 취약점을 기자고 있다. 따라서 본 논문에서는 이러한 태그에서의 취약점과 프로토콜의 위협 요소를 살펴보고, 이를 위한 실제적인 기술적인 요소에 대해서 상세히 분석하였다. 특히 현재 표준안으로 사용되고 있는 EPCglobal RFID Gen2에 적용하기 위한 보안성 향상을 위한 기술적인 방법에 대해서 분석하였다.

ABSTRACT

Radio Frequency Identification(RFID) has been considered as an key infrastructure for the ubiquitous society. However, due to the inherent drawbacks, RFID causes var- ious security threats like privacy problems, tag cloning, etc. This paper proposes a novel practical approach, which are fully conformed to EPCglobal RFID Gen2 standard, for enhancing security of currently used RFID Gen2 tags against the various security threats.

키워드

RFID 프로토콜, 인증 알고리즘, 보안성, 취약점 분석

Key word

RFID Protocol, Authentication Algorithm, Security, Vulnerability Analyses

* 종신회원 : 목원대학교(교신저자, jtkim3050@mokwon.ac.kr)

접수일자 : 2011. 05. 27
심사완료일자 : 2011. 05. 27

Ⅰ. 서 론

RFID 기술은 유비쿼터스 환경하에서 활용성이 아주 많은 기술 중의 하나이다. RFID 시스템은 기본적으로 태그와 리더기 그리고 서버로 구성된다. 태그는 물체의 식별을 위하여 고유한 정보를 칩에 내장하고 있다. 리더기는 라디오 주파수를 이용하여 태그로 부터 식별 정보를 수신하여, 수신한 식별 정보를 서버로 전송하는 역할을 하고 있다. RFID는 기존의 바코드에 비하여 물체를 개별적으로 일일이 식별할 필요 없이 라디오 주파수를 이용하여 모든 물체를 한꺼번에 인식할 수 있는 장점을 가지기 때문에 물리적인 접촉이 필요 없다.

따라서 이러한 장점 때문에 센서 기술과 융합하여 차세대의 무선 센서네트워크 같은 유비쿼터스의 핵심 기술로 발전될 것으로 기대된다. 서버와 리더기는 안전한 채널로 형성이 되지만, 리더기와 태그 사이의 통신 채널은 무선 환경으로 인하여 안전하지 못하다고 가정한다. 서버와 리더기간의 통신은 무선 통신 혹은 유선 통신으로 연결할 수 있지만 둘 다 강력한 암호화 기법을 통해 안전한 채널을 형성할 수 있다. 반면에 태그와 리더기간의 통신은 태그의 자원 제약성으로 인하여 안전하지 않다고 가정된다. 그리므로 프로토콜을 설계할 때 태그와 리더기 사이의 통신에 대한 안전성 문제가 아주 중요한 이슈로 되고 있다. (그림 1)은 RFID의 시스템 구성을 나타내며 3가지의 주요 요소로 이루어지며, 태그, 리더기, 미들웨어 응용 소프트웨어 등으로 구성된다. RFID 태그는 안테나와 간단한 구조의 칩으로 구성된다.

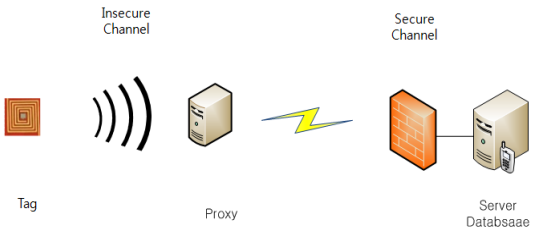

그림 1. 기본적인 RFID 시스템 구성도
Fig. 1 Configuration of basic RFID System

안테나는 리더기로 부터 수신된 무선 신호를 내장된 칩이 신호를 수신하여 정보를 저장한다. 현재 사용되고 있는 태그들은 물체를 인식하고 위치 추척을 위한 물리적인 요소를 내장하기에 충분하지 않을 정도로 작다. 이러한 태그들은 단지 읽기 혹은 저장을 한번만 가능한 구조로 되어 있다[1].

따라서 저가의 RFID 시스템을 구성하기 위한 필수적인 요구조건이 필요하다. 이러한 저가의 시스템에서 발생하는 기본적인 위협 요소와 보안성에 대한 취약점은 다음과 같은 보안성을 만족하여야 한다. 외부의 공격자는 다양한 공격을 시도하여 RFID 시스템에 대한 보안 및 프라이버시에 대한 문제를 야기 시킬 수 있다. 태그와 리더기 사이의 무선통신을 도청할 수도 있고, 정당하지 않은 리더기를 이용하여 태그로 부터 얻은 정당한 정보를 리더기의 요청에 의해 스푸핑 공격(Spoofing Attack) 을 할 수 도 있다. 공격자는 도청한 데이터를 재전송하는 재생 공격(Reply Attack)과 메모리에 저장된 정보를 알아내기 위해 별도의 암호학적인 보안성을 가지지 않는 저가의 태그에 대한 물리적인 공격(Tampering Attack)을 시도할 수 도 있다. 또한 보안 요구사항 이외에도 개인정보 노출이나 위치 정보 추적 등의 프라이버시 위협에 대한 요소도 존재한다. <표 1>은 RFID 시스템의 대표적인 기능을 나타낸다.

표 1. RFID 시스템의 대표적인 기능
Table. 1 Representative Function of RFID

기능	예제
리더기의 동작	- 태그를 인식, 태그를 읽기, 쓰기 접속 동작 - 시스템의 성능을 최적화하고 간섭을 최소화하기 위하여 리더기를 제어
태그의 데이터 처리	- 미들웨어 혹은 다른 응용 시스템에 태그의 응답 및 수집 - 읽혀지지 않는 태그를 인식함으로써 원하지 않는 태그의 인식을 제거
디바이스 관리	- 설비의 구성, 관리 매체를 모니터하여 성능을 원격적으로 관리 - 리더기와 디바이스를 자동적으로 인식 - 오류를 관리하고, 안전한 RFID 구조를 제공

Ⅱ. 관련 연구

RFID 시스템에서 보안성을 위협할 수 있는 공격으로 도청, 트래픽 분석 등의 수동적 공격과 위조, 서비스 거부 공격 등의 능동적 공격들이 있으며, 이런 공격들로부터 안전한 RFID 시스템 설계를 위해서는 전달되는 인증 정보의 기밀성 및 무결성, 태그 식별 정보의 익명성 등의 기본적인 보안 요구사항이 만족되어야 한다. 하지만 RFID 시스템의 경우, 연산 능력과 저장 능력에 제한이 있으므로 기존의 공개키 방식이나 대칭키 방식의 암호화 알고리즘을 적용하기는 적절하지 않다. 초기 RFID 보안 대책으로 kill tag, faraday case, active jamming, blocker tag를 이용한 방식들이 알려졌으며 이후 해쉬 연산을 이용한 해쉬락, 재암호화, 해쉬체인 방식 등이 소개되었다[2].

최근에는 경량화된 대칭키 및 공개키 암호에 대한 연구가 활발히 연구되고 있다 [18]. 이러한 보안 문제점을 해결하기 위한 많은 연구결과들이 발표되었다. Air Juels 가 발표한 논문에 따르면 저가 소형의 RFID 태그 사용에 있어 프라이버시와 인증 문제를 주요 보안 주제로 언급했으며, 이를 극복하기 위한 방법으로 태그 Killing, 태그 Sleeping 과 같은 물리적인 기법, 암호학적인 재암호화 방법과 같은 정보 변경 방법, RFID Enhancer Proxy 방법들이 발표되었다[3]. 그러나 지금까지 발표된 연구결과의 대부분은 태그 내부에서의 실질적인 대칭키 암호 연산을 통한 보안 문제 해결로 접근하는 연구결과를 찾아보기 힘들다. 특히 수동형 RFID 태그가 가지는 자원 제약적인 환경 때문에 실제적인 표준 알고리즘인 AES 알고리즘을 사용하는 프로토콜의 사용이 현재 개발 진행 중에 있다. 일반적으로 저가형 태그는 배터리가 없어 제한적인 연산 능력과 메모리 공간을 가진 것으로 간주되고 있다. 하지만 기술적인 발전으로 인하여 최근에는 저가형 태그에 적합한 암호 알고리즘에 대한 연구가 활발히 진행 중에 있으며 A.Bogdanov 등은 저가형 태그 보안을 위한 보안 프리미티브의 요구사항인 2000 게이트 이하, 10uW 이하의 소비 전력, 10,000 클럭 사이클을 만족하는 암호학적 해쉬 함수의 구현이 가능하다는 연구 결과를 발표하였다[4]. 또한 M Feldhofer 등은 AES(Advanced Encryption Standard) 역시 저가형 태그에 구현이 가능하다는 연구결과를 발표하였다[5].

Ⅲ. 보안 및 프라이버시 요구사항

일반적으로 위에서 언급한 위협 요소를 해결하기 위해서는 RFID 프로토콜은 다음과 같은 요구사항을 충족하여야 한다[6].

1) 기밀성(Confidentiality)
   태그와 리더기 사이의 모든 통신이 공격자에게 도청되더라도 어떠한 의미 있는 정보도 노출되지 않아야 한다. 즉 공격자는 도청을 하더라도 어떠한 정보를 얻을 수 없어야 한다. 일반적으로 이러한 기밀성을 위하여 기존의 암호학적인 방법이 요구되고 있으나 태그에서의 메모리, 연산 능력, 면적 등의 문제로 인하여 기존의 방법으로는 해결되지 않고 있다.
2) 태그에 대한 익명성(Anonymity)
   공격자가 태그와 리더 간의 통신을 통해서 태그의 위치를 추적 혹은 감시할 수 없어야 하는 성질을 말한다. 이러한 익명성을 보장하기 위하여 구별 불가능성(Indistinguishability) 과 전방향 안전성(Forward Secrecy)을 만족해야 한다. 구별 불가능성은 태그에서 전송되는 정보를 통해서는 어떠한 태그로 부터의 정보인지를 구별할 수 없어야 한다. 또한 전방향 안전성은 태그의 현 데이터가 노출되더라도 이전의 데이터가 추적되지 않아야한다.
3) 상호 인증(Mutual Authentication)
   상호 인증은 태그와 리더가 서로 정당한 객체임을 확인하는 절차이다. 어느 한 방향이라도 인증과정을 통과하지 못하면 공격자는 재상 공격 등을 통하여 태그나 리더에 대한 위조가 가능하다.
4) 가용성(Availability)
   리더와 서버는 항상 합법적인 태그임을 인식하기 위하여 항상 정당한 과정을 거쳐 신원을 인증해야 한다.

또한 RFID 시스템에서 고려되어야 하는 주요 보안 위협은 다음과 같다.

1) 태그 Clonig
RFID 리더기에 의해 쿼리 신호를 보내면 RFID 태그는 EPC(Electronic Product Code)라고 명명되는 고유의 숫자를 방사한다. 공격자는 다수의 태그를 스캐닝하고 수집하고자 하는 동일의 EPC를 발산하는 cloned 태그를 발생한다.

2) Privacy Invasion
EPC 숫자는 고유값을 가지므로 공격자는 다른 사용자에 의해 운반된 태그를 인식 혹은 추적할 수 있다.

3) 서비스 거부 공격
대량의 거짓된 태그 혹은 악의적인 리더기에 의해 연산량의 자원을 남용하면 서비스에 대한 자원을 고갈시킬 때 발생한다.

4) 태그 위치 추적
비록 태그의 자세한 정보는 알 수 없을 지라도 태그로부터 일정한 응답을 얻게 된다면, 그 리더기는 이 정보를 이용해서 태그를 가지고 있는 사람의 움직임 정보를 알 수 있다. 이것이 바로 위치 사생활 침해라고 알려진 것이다. 이러한 추적은 각각의 태그가 동일상황에서 매번 다른 응답을 함으로써 혹은 이전의 태그 응답과 연관성이 없는 응답을 함으로써 해결 될 수 있다.

5) 메시지 도청 및 가로채기
좀 더 악의적인 공격자는 리더와 태그의 메시지를 도청함으로써, 사용자의 비밀스런 정보를 얻을 수 있다. 이는 리더와 태그간의 전송에 암호화된 메시지를 송・수신함으로써 방지 할 수 있다. 또한 공격자는 리더와 태그 사이에 전송되는 데이터를 가로채거나, 전송 자체를 막아 버리는 공격을 할 수 도 있는데 이러한 공격은 태그와 서버간의 동일성을 잃게 하는 문제를 야기 시킨다.

6) 응답공격
태그 및 리더 흉내 내기가 있다. 비교적 비활동적인 공격자는 RFID시스템에서 태그와 리더 사이에 자신이 직접 쿼리를 보내거나 응답하는 방법을 사용하기도 한다. 즉, 자신이 태그 혹은 리더 인양 행동하는 것이다.

Ⅳ. 보안성 향상을 위한 기법

현재까지 제안된 RFID 인증기법을 태그에서의 연산능력과 저장능력에 따라 크게 네 가지 형태로 분류하면 첫째, 중량 인증방식은 해시함수, 암호화, 공개키 알고리즘 등 전통적 암호기법을 사용하는 프로토콜이다. 둘째, 단순인증 방식은 난수생성기와 일방향 해쉬함수를 사용하는 프로토콜이다. 셋째, 경량인증방식은 EPC class-1 Gen-2 가 PRNG와 CRC만 지원하기 때문에 해쉬함수를 사용하지 않고 난수 생성과 CRC만 사용하는 프로토콜이다. 넷째, 초경량 인증방식은 xor, and, or 같은 간단한 비트연산만을 사용하는 프로토콜이다. 저가의 태그는 제한적인 연산능력과 저장 공간의 한계로 인해 대칭키, 공개키, 해쉬 같은 전통적인 암호기법의 사용이 힘들다[7]. 이러한 저가형 태그를 위한 저비용의 안전한 인증기법과 암호기법의 연구를 필요로 하고 있다. 다음은 안전한 RFID 시스템을 위한 현재까지 연구 중인 대표적인 프로토콜이다[8].

1) 해쉬기반 프로토콜(Hash-based Protocols)
2) LPN 기반 프로토콜(LPN based Protocols)
3) 초경량 프로토콜(Ultra-light Protocols)
4) Universial Composability Protocols
5) 다중 태그 스캐닝 프로토콜(Multi Tag Scanning Protocols)
6) 거리 반송 프로토콜(Distance bounding Protocols)
7) RFID에 대한 부채널 분석 및 방지(Side channel analysis and protection)

다음은 태그의 보안 위협과 그 대응책을 나타내면 다음과 같다.

1) 태그의 보안성 강화를 위한 방법
- 패스워드, 키 해쉬 기반의 인증 및 디지털 서명을 이용한 강력한 인증 기법을 태그에 구현
- 리더기와 태그의 적당한 위치에 배치, 제한된 전송 전력, 태그 메모리 접근 제어, 물리적인 제어, 태그의 전자기파 차폐 기술
- 태그와 리더기 간의 안전한 프락시 기능을 사용
- 태그가 더 이상 사용되지 않을 경우 태그를 파괴

- 외부로 유출되지 않는 태그의 인식 형식을 사용

2) 태그들은 훼손, 탈취 혹은 대체
- 물리적인 보안(접근 제어, 감시 시스템)
- Fall-back 인식 시스템을 구현
- Temper resistant에 강한 태그를 구현

3) 40비트의 암호화키는 브루터스 공격에 의해 예측 가능
- 128 비트의 비밀키로 암호학적 구현

4) 전력 분석 기법에 의해 사이드 채널 공격 가능
- 주문형반도체로 암호화 기능을 내장함

5) 태그들은 RFID 시스템에서 저장 혹은 바이러스를 확산 가능
- 모든 서버에 안티바이러스 소프트웨어를 갱신

6) 태그들은 외부의 공격에 의해 리더기에 가용성을 지원하지 않을 수 있음
- Tag Kill 키 기능은 오직 인가된 사용자에 의해 가능함
- 리더기와 태그 간의 통신은 안전한 통신으로 이루어짐

표 2. 리더기의 보안 위협과 대응방법
Table. 2 Reader Security Threats and Countermeasures

리더기의 보안 위협	해결책
네트워크 기반의 공격	- 안전한 망 구축 및 접근 제어 (방화벽, 침입탑지시스템) - Fall-back 인식 시스템을 구현
도청	- 데이터 암호화 기법 - RF 장치의 정확한 지점에 배치 - RF 전송 전력을 제한 - 리더기 접속을 위한 인증 메카니즘 - 물리적 접근 제어
태그 스푸핑	- 상호 인증 및 데이터 암호화, 디지털 서명 기법 - 태그와 리더기의 적당한 위치 배치
Man-in-the-middle 공격	- 리더기에 대한 태그의 반응 시간의 엄격한 요구조건
재생 공격	- 산호인증을 위한 해시기반의 기법

V. 결 론

RFID는 유비쿼터스 환경에서 센서네트워크과 물체의 인식 기술에서 반드시 해결해야 될 부분이 보안성 문제이다. 따라서 본 논문에서는 이러한 RFID 시스템에서 요구되는 보안성 문제와 보안성을 향상시키기 위한 기법에 대해 분석하였다. 일반적으로 RFID 그 자체는 소규모의 자원적인 제약으로 인하여 현재의 표준안에서는 16비트 랜덤 수 발생기, 16비트 CRC, XOR연산자 그리고 모든 수동형 GEN2 태그를 지원하는 A/Killpwd에 기초를 둔 새로운 프로토콜이 주로 제안되어 지고 있다. 이러한 프로토콜은 완벽하게 사생활과 보안문제를 해결할 수 있진 않지만, 이전에 제안되었던 프로토콜에서 해결하지 못했던 여러 문제점을 해결 하였다. 따라서 향후에 사용될 프로토콜은 좀 더 저렴하며 경량의 안전한 인증 프로토콜이 될 것이다. 추후의 연구과제로는 경박단소한 인증 프로토콜로 구성될 것이며 XOR 연산 및 CRC 계산 그리고 간단한 해쉬 함수 계산이 가능할 것이며, 향후 이러한 부분에 대한 연구가 좀 더 깊이 진행될 필요가 있겠다.

감사의 글

이 논문은 2010년도 교육과학기술부의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2010-0024133)

참고문헌

[1] George Poulopoulos, Konstantinos Markantonakis, Keith Mayes, "A Secure and Efficient Mutual Authentication Protocol for Low-Cost RFID Systems", pp.706-p.711, 2009 International Conference on Availability, Reliability and Security

[2] A. Juels, "RFID Security and Privacy : A research survey", selected Areas in Communications, IEEE Journal, 2006

[3] S.A.Weis, S.E. Sarma, R.L. Rivest, and D.W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In Security in Pervasive Comp., volume 2802 of LNCS, pages 201-212, 2004.

[4] A. Bongdanov, etal, " Hash Functions and RFID Tags: Mind the Gap," Proc. of the CHES08, V. 5154 of LNCS, p.283-299, 2008

[5] M. Feldhofer, etal, "Strong Authentication for RFID Systems Using the AES Algorithm," Proc. of the CHES04, V.3156, p.85-140, 2004

[6] Faouzi Kamoun, "RFID System Management: State-of-the Art and Open Research Issues", IEEE Transaction on Network and Service Management, v.6, n.3, Sep, p.190-1205, 2009

[7] H.-Y. Chien, "SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity", IEEE Transactions on Dependable and Secure Computing, Vol. 4, No. 4, 2007, pp.337-340.

[8] Faouzi Kamoun. "RFID System Management: State-of-the Art and Open Research Issues" IEEE Transactions on Network and Service Management, V.6, N. 3, pp.190-205, Sep. 2009

저자소개

김정태(Jung Tae Kim)

2001년 8월 : 연세대학교 대학원 전자공학과 박사
1991년 8월～1996년 2월 : 한국전자통신연구원(ETRI) 선임연구원
2002년 10월～현재 : 목원대학교 전자공학과 교수
※관심분야: Network Security, 보안 컨설팅, RFID&USN Security, ASIC Design.