EPCglobal Class-1 Gen-2 RFID 시스템의 위협과 대안†

김경현*, 최은영*, 이동훈*

*고려대학교, 정보보호대학원

Threats and alternative of EPCglobal Class-1 Gen-2 RFID system

Kyoung-hyun Kim*, Eun Young Choi*, Dong Hoon Lee*

*Graduate School of Information Security, Korea Univ.

요 약

RFID 시스템은 유비쿼터스 컴퓨팅 환경에서 중요한 기술로 주목하고 있다. RFID의 국제 표준으로 자리 잡고 있는 EPCglobal Class-1 Gen-2 RFID 시스템을 통해서 전 세계 어디에서도 문제없이 인식될 것으로 보인다. 그러나 EPCglobal Class-1 Gen-2 RFID 시스템은 위협의 요소들을 가지고 있다. 본 논문에서는 표준에서 승인된 태그의 능력을 사용하여 표준의 수정을 최소화시켜 보안의 문제점을 해결 할 수 있는 방안을 제시한다.

I. 서론

RFID 시스템은 칩을 내장한 태그를 사물에 부착하여 태그에 저장된 데이터를 무선 주파수(RF)를 통해 자동 인식할 수 있도록 하는 시스템이다. *RFID* 시스템은 물류 관리, 유통 관리, 재고 관리 등 여러 분야에서 기존의 바코드 방식보다 많은 장점을 가지고 있다. 바코드 시스템은 데이터를 얻기 위해서는 작업자의 가시권에 라벨이 있어야 하지만, RFID 시스템은 무선이기 때문에 작업 반경에 덜 의존적이다. 또 바코드 시스템은 동시에 여러 개를 읽기가 불가능 하지만, RFID 시스템은 다대다 통신이 가능하다. 이러한 장점들 때문에 RFID 시스템은 바코드 시스템을 대체할 것으로 보이며 가까운 미래에 대량으로 배치될 것으로 기대된다.

RFID 기술이 범용화되기 위해서 RFID 표준화 작업이 필요하게 되었다. EPCglobal과 ISO를 포함한 여러 개의 기관들이 RFID 표준화 작업을 하고 있다. 특히 EPCglobal에서 제안한 중요한 표준 중에 하나는 RFID 태그의 함수와 연산을 정의한 EPCglobal Class-1 Gen-2 RFID이다.

EPCglobal Class-1 Gen-2 RFID는 보안과 프라이버시 문제를 거의 언급하지 않고 있다. 본 논문에서는 EPCglobal Class-1 Gen-2 RFID의 보안의 위협을 제시하고, 표준을 재작업을 하지 않고 표준에서 승인된 태그의 능력을 사용하면서 보안의 문제점을 해결 할 수 있는 방안을 제시한다.

II. RFID 시스템

RFID 시스템은 일반적으로 태그(Tag), 리더(Reader), 백-앤드-서버(Back-End Server)로 구성된다.

2.1 태그(Tag)

태그는 사물에 부착되어지는 작은 칩(chip)을 말한다. 이 태그는 IC 칩(integrated circuit chip)과 안테나(antenna)로 구성된다. IC 칩 속에는 사물에 대한 정보가 저장되어 있고, 연산 동작을 위한 게이트가 구현되었다. 그리고 안테나를 통해서 리더와 통신을 한다.

태그는 전력 공급 방법에 따라서 수동형 태그(Passive Tag)와 능동형 태그(Active Tag)로 나누어진다. 수동형 태그는 리더로부터 받은 신호를 가지고 유도전류를 만들어 태그의 전원으로 사용한다. 능동형 태그는 태그에 배터리를 가지고 있어서 자체 전원을 공급받는다.

2.2 리더(Reader)

리더는 태그로부터 데이터를 요청, 기록, 수신하는 장치이다. 수신된 데이터를 백-앤드-서버에 보내어 사물에 대한 정보를 얻을 수 있다. 리더의 형태는 태그에 쿼리(query)를 줄 수 있는 PDA나 모바일 폰(mobile phone)이 될 수 있다.

2.3 백-앤드-서버(Back-End Server)

백-앤드-서버는 각각의 태그에 대해서 다양한 태그의 정보를 관리, 저장하는 서버 장치이다. 백-앤드-서버에는 태그를 식별할 수 있는 정보를 저장하고 있으며, 리더로부터 전달된 태그의 정보의 진위여부를 판단하는 연산을 수행한다.

III. RFID 시스템의 위협

RFID 시스템은 리더와 태그 간에 RF을 사용하여 태그의 공유 정보를 전송하는 형태로 동작한다. 이것은 RFID 시스템이 여러 위협에 노출되기 쉽다는 것을 의미한다. 이러한 취약점은 공격자가 기존의 시스템과 달리 적은 노력으로 원하는 정보를 얻을 수 있다.

3.1 공격의 종류

3.1.1 도청

공격자는 도청을 통해서 태그에 내장된 상품의 비밀정보를 얻음으로써 사용자의 비밀 정보를 얻을 수 있다. RFID 시스템은 RF를 사용하기 때문에 공격자의 도청을 막는 것은 불가능하다. 그래서 도청을 통해 얻은 정보를 가지고는 사용자의 비밀 정보를 얻을 수 없도록 해야 한다.

3.1.2 위조

공격자가 특정 태그와 리더 사이의 무선 통신을 도청하여 태그의 비밀 정보를 획득한다면 그 공격자는 이전에 통신에서 도청한 정보를 재사용하여 정당한 리더에게 전송함으로서 특정 태그로 위장할 수 있다. 이러한 공격을 재전송 공격(Reply attack)이라고 한다. 이와 같은 위장 공격은 태그가 리더에게 대한 인증 없이 리더에게 정보를 전송하기 때문에 가능하다.

3.2 RFID 시스템의 문제점

3.2.1 프라이버시(Privacy)

RFID 시스템이 범용화 되면, 사용자는 태그가 부착된 다양한 물건을 지니고 다닐 것이다. RFID 시스템의 태그가 인증되지 않은 리더에게 무분별하게 고유 정보를 전송하게 된다면 사용자에 대한 다양한 정보가 사용자의 동의 없이 누출될 수 있다.

3.2.2 추적가능성(Traceability)

사용자가 태그가 부착된 특정한 물건을 가지고 있을 때, 공격자는 사용자와 태그의 정보에 연관성을 가지고 사용자의 이동 경로를 추적할 수 있다.

IV. EPCGlobal Class-1 Gen-2 RFID 시스템[1]

4.1 EPCGlobal Class-1 Gen-2 RFID

EPCGlobal Class-1 Gen-2 RFID는 ISO/IEC 18000-6(860MHz-960MHz의 UHF 대역 RFID 통신) 국제표준으로 편입됐다. 이제 ISO에서 하나의 표준으로 통합함으로써 태그가 전세계 어디에서도 혼선 없이 인식할 수 있게 되었다.

EPCGlobal Class-1 Gen-2 RFID는 다음과 같은 특징을 가지고 있다.

- Gen-2 RFID 태그는 리더로부터 전원 공급을 받는 수동 태그(Passive Tag)이다.
- UHF 밴드(800-960 MHz)에서 통신하며 통신 범위는 2~10m 이다.
- 의사 난수 발생기(Pseudo-Random Number Generator)와 CRC(Cyclic Redundancy Code)가 제공된다.
- 보안을 위해서 두 개의 32비트 PIN이 제공된다.

EPCGlobal Class-1 Gen-2 RFID의 세션 절차는 [그림-1]과 같다.

(1) 리더가 태그에게 필요한 요청을 보낸다.
(2) 요청을 받은 여러 개의 태그 중 각각의 태그는 내장된 의사 난수 발생기로부터 16비트 랜덤값(RN_16)을 만든다. 그리고 각각의 태그는 slot counter에 랜덤한 값

을 입력하여 slot counter를 작동시킨다. slot counter가 0이 되는 순간에 태그는 랜덤값(RN_16)을 리더에게 보내준다.

(3) 리더는 받은 랜덤값(RN_16)를 포함한 ACK를 태그에게 보내준다.

(4) 태그는 리더로부터 받은 ACK에 포함된 랜덤값(RN_16)으로 태그의 RN_16과 비교한다. 서로 같으면 태그는 PC(Protocol-Control), EPC(Electronic Product Code), CRC를 리더에게 보내준다. PC는 물리 계층(Physical-layer)의 정보를 유지하는데 사용된다.

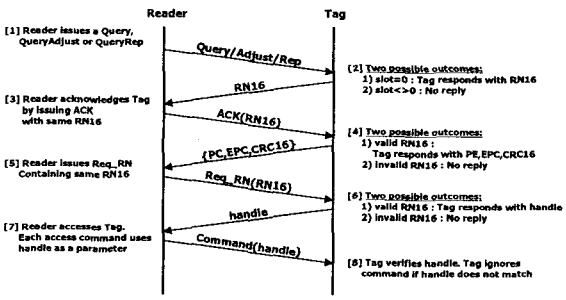
리더가 태그에게 쓰기 명령이나 킬 명령을 하고 싶을 때는 이후에 절차를 추가로 시행한다.

(5) 리더는 RN_16을 포함하고 있는 Req_RN를 태그에게 보낸다.

(6) 태그는 리더로부터 받은 Req_RN에 포함된 랜덤값(RN_16)으로 태그의 RN_16과 비교한다. 서로 같으면 태그는 핸들(Handle)을 리더에게 넘겨준다.

(7) 리더는 명령을 위한 PIN을 보낸다.

(8) 태그는 명령에 따라서 PIN을 비교하고 해당 명령을 수행한다.



[그림 1] EPCGlobal Class-1 Gen-2 RFID의 세션 절차

4.2 의사 난수 발생기(Pseudo-Random Number Generator)[1][2]

정보보호 시스템에서는 인증, 기밀성 등을 보장하기 위해서 알고리즘에 난수를 사용한다. 그래서 난수 발생기는 정보보호 시스템에서 필수적인 항목이며, 그것에 대한 안전성 증명이 가능하도록 설계가 되어야 한다. 그런데 완벽한 난수를 발생하는 것은 현실적으로 불가능하다. 그래서 실제 난수와 구별이 어려운 의사 난수를 사용한다.

의사 난수 발생기는 처음의 입력값를 시드(Seed)로 시작하여 이전의 결과로부터 다음의 결과가 계산되는 결정적인 함수(deterministic function)로 나타낸다. 의사 난수는 순환을 하기 때문에 안전성의 척도는 수열의 길이와 결과들의 확률적인 분포에 의존하게 된다.

EPCGlobal Class-1 Gen-2 RFID에서는 각 세션마다 태그와 리더 사이에 새로운 세션 공유하는데 의사 난수를 사용한다. EPCGlobal Class-1 Gen-2 RFID에서 사용하는 의사 난수는 보안을 위해서 사용하는 것은 아니다. 리더는 여러 개의 태그를 동시에 인식해야 하며. 태그가 동시에 반응할 때는 충돌이 일어날 수 있기 때문에 여러 개의 태그를 구분할 필요가 있다. 그래서 충동을 방지하고 여러 개의 태그 중에서 하나의 태그를 구분하기 위해서 난수가 사용된다.

EPCglobal Class-1 Gen-2 RFID에서는 태그에 다음과 같은 특성을 가지고 있는 16비트 의사 난수 발생기 가지고 있다.

- 하나의 16비트 난수가 뽑힐 확률은 $\frac{0.8}{2^{16}} < P < \frac{1.25}{2^{16}}$ 이다.
- 10000 개의 태그 중에서, 두 태그가 동시에 같은 난수값을 발생할 확률은 0.1% 보다 작다.
- 이전의 결과들이 공격자에게 알려졌다는 가정 하에, 다음 난수값을 알아낼 확률은 0.025%보다 작다.

4.3 CRC(Cyclic Redundancy Code)[1][2]

CRC는 수신, 송신된 데이터의 무결성을 검사하기 위해 사용된다. CRC 알고리즘은 GF(2)의 계수를 가지고 있는 기약 원시 다항식(irreducible and primitive polynomial)을 사용하며 다항식을 계수만을 모아서 표현한다.(예를 들어, x^4+x^2+1은 10101로 표현된다.) CRC 체크섬(check sum)은 CRC 다항식으로 나누어진 나머지로 계산된다.

EPCglobal Class-1 Gen-2 RFID에는 16비트

체크섬(check sum)이 데이터의 에러를 찾기 위해 사용된다. EPCGlobal Class-1 Gen-2 RFID에서 사용되는 다항식은 $x^{16}+x^{12}+x^5+1$ 이다. CRC 체크섬(check sum)을 계산하는 것은 다항식의 나눗셈이지만, 그것은 실제적으로는 하드웨어적으로 쉬프트 연산으로 효율적으로 구현될 수 있고, 또는 테이블로 만들어질 수 있다.

4.4 PIN[1]

EPCGlobal Class-1 Gen-2 RFID는 32비트 킬 패스워드(kill password)와 32비트 접근 패스워드(access password)를 가지고 있다. 킬 패스워드로는 킬 명령어(kill command)를 사용하여서 태그를 일시적으로 사용 못하게 할 때 사용된다. 접근 패스워드를 통해서 안전 모드로 들어갈 수 있으며 안전 모드에서는 메모리에 읽고 쓰기가 가능하다.

V. EPCGlobal Class-1 Gen-2 RFID 시스템의 위협과 대안

5.1 위협

위에서 설명했듯이 표준에 의하면 태그는 리더를 인증하는데 난수를 보내고 ACK를 보내는 정도로 매우 기본적인 방법을 취하고 있다. 그 후에 태그는 리더에게 관련된 EPC를 평문으로 보낸다. 공격자는 단순한 도청만으로도 태그의 EPC를 알아낼 수 있다. EPC 체계는 공개가 되기 때문에 알아낸 EPC만으로도 공격자는 물건에 대한 정보를 어느 정도는 알 수 있다. 따라서 사용자의 프라이버시 문제가 발생한다. 그리고 알아낸 EPC를 가지고, 태그의 복제가 쉽게 발생할 수 있다.

또 태그는 고정된 EPC를 내보내기 때문에 공격자는 공격자가 사용자가 소유한 물건의 정보를 알면 추적이 가능해진다.

EPCGlobal Class-1 Gen-2 RFID의 프라이버시 보호 메커니즘은 킬 명령어를 사용하여서 태그를 일시적으로 사용 못하게 하는 것이다. 그러나 스마트 홈의 경우 RFID 태그는 물건의 구입 이후에도 계속 유용할 것이다. 이런 경우 프라이버시 보호 메커니즘으로 킬 명령이 적합하지 않다.[2]

다른 EPCGlobal Class-1 Gen-2 RFID의 문제점은 PIN를 보낼 때 랜덤값(RN_16)과 XOR되지만 PIN의 비트는 32비트이고 랜덤값은 16비트이기 때문에 랜덥값을 2번 반복하게 된다. 물론 랜덥값을 2번 반복하는 것도 큰 문제가 되지만 랜덤값(RN_16)은 세션 시작때 평문으로 보내지기 때문에 알려진 정보가 된다. 따라서 도청이 가능한 공격자에게는 PIN이 쉽게 노출이 된다. PIN이 노출이 되면 공격자는 태그에 대한 메모리 쓰기, 삭제, 킬이 가능하게 된다.

5.2 대안

킬 명령을 사용하는 보안 메커니즘은 한계가 존재한다. 따라서 새로운 보안 메커니즘이 필요하게 되었다. 그 보안 메커니즘은 EPCglobal Class-1 Gen-2 RFID의 표준의 재작업을 최소화 해야 된다. 표준의 재작업을 최소화 하기 위해서는 승인된 태그의 능력을 사용 보안 메커니즘에 사용하여 해결한다.

표준에 나오는 태그의 요소로는 의사 난수 발생기, CRC, PIN 등이 있다. 의사 난수 발생기를 16비트 의사난수를 발생하기 때문에 보안에 사용하기에는 적합하지 않는다. 32비트 PIN과 함께 사용하기 위해서는 32비트 의사 난수 발생기가 제공되어야 한다. PIN은 태그의 비밀 요소이다. 따라서 PIN과 32비트 여러 개의 의사 난수를 통해서 EPC를 숨길 수 있다면 EPCGlobal Class-1 Gen-2 RFID 시스템 위협에 대안이 될 수 있다.

[참고문헌]

[1] "EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version 1.0.9", EPCglobal Inc, 2004

[2] Dang Nguyen Duc, Jaemin Park ,Hyunrok Lee, Kwangjo Kim, "Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning", Symposium on CIS, 2006