유비쿼터스 환경하에서의 RFID 보안 위협에 대한 분석

김대유, 김정태

목원대학교

Analyses of RFID Security Threat Under Ubiquitious Surroundings

Dae-Yu Kim, Jung-Tae Kim,

Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

요 약

RFID는 전자TAG를 사물에 부착하여, 사물이 주위 상황을 인지하고 기존 IT 시스템과 실시간으로 정보교환과 처리할 수 있는 기술이다. 바코드나 Smart Card에 비하여 우수한 특성에 의해 다양한 응용이 가능하며, 향후 900MHZ 대역 제품이 현재의 13.56MHZ 대역을 대신하여 주력 제품이 될 것이라고 예상 되고 있다. 현재 RFID가 도입되어 사용되는 T-Money(버스카드)와 출입통제 등 여러 가지 분야에서 활용되고 있다. 하지만 RFID는 비접촉식 수신거리에 최대 장점을 가지고 있지만 반대로 수신거리의 문제로 추적이 가능하다는 문제를 가지고 있다. 이것은 사용자의 프라이버시가 될 수 있으며 위조나 변조에 대해서 매우 취약하다는 것에 문제가 있다. 이 논문에서는 보안위협과 제시된 보안기법을 보고 활용성에 대한 고찰을 보겠다.

1. 서 론

RFID는 전자TAG를 사물에 부착하여, 사물이 주위 상황을 인지하고 기존 IT 시스템과 실시간으로 정보교환/처리할 수 있는 기술이다. 바코드나 Smart Card에 비하여 우수한 특성에 의해 다양한 응용이 가능하며, 향후 900MHZ 대역 제품이 현재의 13.56MHZ 대역을 대신하여 주력 제품이 될 것이라고 예상 되고 있다. RFID 시장 초기 단계인 2005년에는 제조·유통·물류기업의 17.6%가 RFID도입(파일럿) 혹은 도입 계획중인 것으로 조사 됐다. 반면, RFID 도입의 장애물로 조사 대상 기업의 1/3이 투자대비효과(ROI)을 꼽아 RFID도입에 작용할 것으로 예상되었다. 시장조사 기관인 IDC는 20일, 최근 내놓은 보고서("'Status of RFID in Western European Verticals'")에서 프랑스, 독일, 이탈리아, 영국, 스페인 등 서유럽 주요 5 개국의 주요 기업들을 대상으로 한 조사결과를 통한 결과 산업별로는 운송 및 물류 업종에서 RFID 도입에 가장 큰 관심을 보였으며 특히 TNT물류, UPS 등과 같은 물류 서비스 업체들이 RFID 기술에 관심을 보였다. 하지만 비용문제 등은 RFID 확산에 장애 요인으로 작용 하고 있다.

보고서는 프로세스 제조업 중에서 제약과 음식, 음료 등 이력추적관리가 필요한 산업에 RFID가 제격이며, 그것은 밸류체인에서 효율성을 증진할 수 있는 방법이지만, 냉동 저장고는 RFID 태그에 위협요소가 될 수도 있다고 분석 했다. 한편, 파일럿 테스트 이후, 도입을 하지 않기로 한 기업은 0.8%에 이르렀다. 또 보고서는 RFID 경우, 태그와 리더기만 있으면 되는게 아니어서 다양한 분야의 IT벤더들에게 새로운 기회를 제공할 것으로 새로운 기회를 제공할 것으로 전망했다. 응답 기업의 50% 이상이 RFID 도입시 IT 서비스, 서버, RFID를 위한 필수 애플리케이션에 투자하게 될 것이라고 응답했다. 이 밖에 RFID 도입시 장애물로 보안, 표준화, 비용 등이 든 응답도 기타에 많이 포함되었다.[1] RFID 보안 위협은 프라이버시 침해와 태그 정보 유출로 인한 복제가 위협 모델링이 될 수 있다. 이와 관련해 RFID 보호 기법에 대한 많은 연구가 있다. 우선 가장 단순하면서도 확실한 방법인 물리적으로 Blocker 태그라는 특정 태그를 사용하여 사용자 프라이버시를 보호하는 방법이 있으며,[2,3] 그 외

에 제안하는 법과 비슷한 개념인 특별한 모바일 기기를 이용한 RFID Guardian 기법이 있다.[4,5] 하지만 각각의 방법들이 완벽하게 프라이버시 보호 문제를 해결하지 못했다.[6]

그 외에 제안 하는 기법은 RFID 애플리케이션에서 태그의 내용을 서버에서 인증을 받아 변경하고 다시 태그에 값을 기록함으로서 태그의 복제 위협에서 보호 할 수 있다. 제안하는 기법은 기존의 태그에서 활용이 가능하며 연산처리를 하는 부분이 없어 도입 현 시점에서 도입이 가능하며 RFID 시스템에 큰 변경 없이 추가적인 구성요소로 적용 가능하다.

2. RFID의 기술 개요

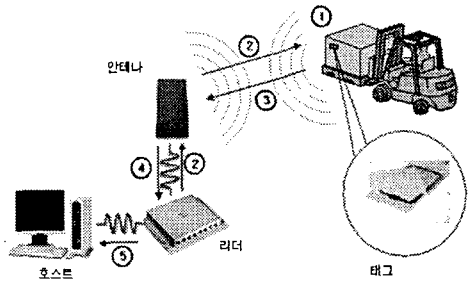
RFID(Radio Frequency Identification)는 IC칩에 내장된 정보를 무선 주파수를 이용하여 비접촉방식으로 읽어내는 기술로서 대상을 자동식별 할 수 있는 기술이다. 일반적으로 안테나와 칩으로 구성된 RFID 태그에 사용 목적에 알맞은 정보를 저장하여 적용 대상에 부착한 후 판독기에 해당하는 RFID 리더를 통하여 정보를 인식하는 방식을 사용한다. RFID 시스템은 바코드 시스템에 비해 보다 다양하고 효율적인 식별 체계 구축을 가능하게 한다. 바코드처럼 사물의 표면에 인쇄될 필요가 없어서 오염에 대해서 걱정할 필요도 없으며, 인식작업도 편리하다. 단순히 식별 코드만을 인쇄하는 바코드와는 달리 제품 하나하나 마다 고유한 ID를 가지는 태그를 부착하는 것이 일반적이다. 그리고 무선 전파를 이용한 장치의 특성상 수 미터 또는 수십 미터의 거리에 있는 사물에 대해 빠르고 다중적인 자동 인식을 제공하기 때문에 수년 내로 RFID 시스템이 바코드 시스템을 대신하여 유통, 물류 산업 등의 다양한 분야에 큰 변화를 줄 것이라고 전망 하고 있다.[7,8,9] 그러나 물리적 접촉 없이 무선으로 인식 가능하다는 RFID시스템의 특징은 프라이버시 측면에서 새로운 문제점을 발생시킨다. 현재의 RFID 태그는 인증 프로토콜을 거치지 않고 어떤 리더에게나 태그 내부의 고유한 값을 응답 해준다. 따라서 RFID리더를 가진 사람이라면 누구나 태그의 정보를 읽어 낼 수 있기 때문에, 태그가 삽입된 물품을 소유한 사람의 프라이버시가 쉽게 침해당할 수 있다.[10] 이러한 문제로 물류 관련업에서는 RFID 도입이 어려운 실정이며 현재 사용되고 있는 RFID 분야 중 출입통제는 태그를 복제 당했을 경우 심각한 피해를 예상 할 수도 있다. 이러한 복제 문제는 RFID 뿐만 아니라 바코드와 스마트 카드에서도 있을 수 있는 문제이다.

2.1 RFID의 구성

2.1.1 RFID 시스템의 구성

RFID 시스템은 일반적으로 태그, 리더, 그리고 백 앤드 데이터베이스로 구성되며, 각각의 구성과 기능은 다음과 같다 (그림)은 RFID 시스템의 구성에 대하여 나타낸 것이다.

[그림 3-1 RFID 시스템의 구성]



2.2 RFID 태그

태그는 RFID 시스템에서 리더의 요청에 대하여 사물, 동물, 사람 등의 식별 정보를 송신하는 것으로서 트랜스 폰더(Transponder)라고도 한다. 태그의 구성은 무선 통신을 위한 결합장치(Coupling element)와 연산을 수행하고 정보를 저장하는 마이크로 칩으로 이루어져 있으며, 전력을 공급받는 방법에 따라 능동형(Active Tag), 수동형(Passive Tag) 태그로 분류 된다.

· 능동형 태그(Active Tag) : 태그에 자체 내장된 배터리로부터 전력을 공급 받으며, 원거리 정보 전송이 가능하다. 그러나 배터리가 내장되어 있으므로 태그의 가격이 높으며, 태그의 수명이 배터리의 수명에 종속적이라는 단점이 있다. 능동형 태그는 주로 차량 타이어 압력감지 시스템 환자 관리 시스템 등에서 사용 된다

· 수동형 태그(Passive Tag) : 리더로부터 수신한 전자기파에 의한 윤 전류를 전원으로 사용하며, 태그의 전송 전력이 리더의 전송 전력에 비해 상대적(1/10 정도)으로 낮기 때문에 근거리 정보

전송에 주로 이용된다. 수동형 태그는 배터리를 내장하고 있지 않으므로 태그의 가격이 낮으며, 태그의 수명이 반영구적이라는 장점을 갖고 있기 때문에 물류 관리 분야에 주로 사용된다.

[표 1-1 태그의 구분]

RFID 방식별 구분		원 리
읽기쓰기 가능여부	읽기전용	제조 시 정보 입력, 정보내용은 변경 불가 가격이 저렴하여 바코드와 같이 단순인식 분야 사용
	한번 사용 기능	사용자가 데이터를 1회 입력할 수 있으며 입력 후에는 변경 불가
	읽기 쓰기 가능	여러 번 데이터 입력과 변경이 가능 가격은 높지만 고가 상품 등에 활용 가능
태그전원 유무	능동형 (Active)	태그에 배터리가 부착, 수십m 원거리 통신용 가격 고가, 수명 제한, UHF대역이상에서 사용
	수동형 (Passive)	태그에 배터리가 없으며, 10m 이내 근거리 통신용 가격 저렴, 수명 반영구적(약 10년 이상)

2.3 RFID 리더

리더는 태그가 송신한 식별 정보를 수신하여 태그를 인식하는 역할을 하는 장치로서 트랜시버(Tranceiver)라고도 한다. 리더는 태그에게 RF 신호(RF Signal : Radio Frequency Signal)를 전송하여 전력을 공급하고, 태그로부터 수신한 정보를 백-엔드 데이터베이스로 전송한다. 그리고 리더는 태그의 정보를 읽거나 기록 할 수 있다.

2.4. RFID 시스템의 요구 조건

2.4.1 시스템 측면

■ 저비용 (Low cost)

시장의 활성화를 위해서는 낮은 비용으로 RFID태그를 제조 할 수 있어야 한다.

■ 효율적인 인식(Efficient Identification)

인식 속도가 빨라야 하며, 이동중에도 인식이 가능해야 한다.

■ 다중 태그 인식(Multiple Tag Identification)

다른 물체에 부착된 각기 다른 태그에 대해서도 동시에 인식 할 수 있어야 한다.

2.4.2 안전성 측면

■ **위조불가(Unforgeability)**

태그에 부여된 유일한 ID에 대해서는 위조가 불가능해야 한다. 예를 들어 출입통제 시스템에 이용될 RFID시스템에서 인증된 태그와 동일한 정보를 전송하는 또 다른 태그(인증되지 않은)가 위조 가능하다면, 위조된 태그를 지닌 자동차도 출입이 허락되어 시스템 자체의 안전성을 위협할 것이다.

■ 추적불가(Non Tracking)

리더가 읽어 들이는 태그 정보, 즉 태그로부터 나오는 정보로 소비자의 정보 즉, 소비 경향 또는 위치추적이 불가능 해야 한다. 예를 들어 제품관리를 위해 타이어에 RFID태그를 내장시킨다고 생각했을 경우, 제품관리라는 원래의 의도와는 달리 RFID태그 내장 타이어가 부착된 자동차의 위치 추적에 악용될 가능성이 있다.

3. 관련연구

3.1.1 KILL 명령어

유일한 8비트 패스워드를 가지는 각 태그는 패스워드를 전송하자마자, 태그 스스로 자신의 정보를 삭제 시키는 방식이다. 즉 어떤 물건에 부착된 태그는 고객이 물건을 구입한 이후에는 RFID칩이 더 이상 작동되지 않도록 하는 방식이다. 이 방법은 완벽하게 프라이버시를 보호할 수는 있으나, 이 속성으로 인해 사실상 태그를 이용한 정보 관리나 태그의 재사용 등의 RFID 시스템을 장점을 제거해 버린다. 게다가 패스워드 길이가 8비트 이므로, 공격자로 하여금 쉽게 패스워드 추측을 가능하게 만드는 문제가 있다.

3.1.2 hash lock 방식

각 태그는 다음과 같이 리더를 확인한다. 리더는 각 태그마다 유일한 (k)를 가지고 있으며, 이에 해당하는 태그는 meta ID = H(k)를 가지고 있다. 이 때 H( )는 해쉬함수를 의미한다. 태그가 ID접근 신호를 받으면,

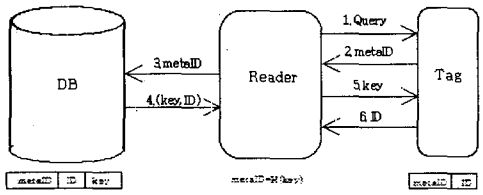
■ 태그는 자신의 meta ID를 리더에 보낸다.

■ 리더는 이에 해당하는 키 (K)를 태그에 보낸다.

■ 태그는 리더로부터 받은 키(k)를 해쉬한 값과

자신의 meta ID를 비교하여, 그 값이 동일하면 자신의 ID를 전송한다.

이 방식은 해쉬함수만을 요구하므로 저비용으로 구현될 수 있는 장점을 지니나, meta ID가 고정되어 있으므로, 공격자는 meta ID를 이용하여 해당 태그의 위치를 추적할 수 있는 문제가 있다.



3.1.3 Randomized hash lock 방식

이 방식은 hash lock 방식을 개선한 것으로, 태그는 해쉬 함수와 난수 생성기를 가져야 한다. 방식은 다음과 같다.

■ 각 태그는 난수 생성기로부터 생성된 난수값(r)과 자신의 ID를 연접하여 해쉬값, c = H(ID || r)을 계산후, c,r 을 리더에 전송한다.
■ 리더는 이 값 (c, r)을 데이터베이스 서버에 전송한다.
■ 데이터베이스에는 각 태그의 ID가 저장되어 있고 서버는 전송받은 c와 같은 값이 나올 때 까지 모든 태그의 ID와 전송받은 r을 해쉬하여 c와 관련된 ID를 검색하고, 이것을 리더에 보낸다.

이 방식은 접근 때마다 태그에서 다른 출력값이 나오므로, 태그에 대한 추적은 불가능하다. 그러나 서버에서 태그의 ID를 식별할 경우, 만족하는 ID가 나올때까지 해쉬함수를 반복 수행해야 하므로, 평균 N/2번의 해쉬 수행이 요구되는 단점이 있다. 이 때 N은 서버에 저장된 모든 태그의 수이다. 게다가 이 방식은 태그 안에서 해쉬 함수와 함께 난수 생성이 이루어져야 하므로 저비용으로 구현하기도 어렵다.

3.1.4 Anonymous ID 방식

이 방식은 익명의 ID를 출력함으로 태그의 실제 ID를 공격자가 알 수 없도록 하는 방법이다. 그러나 이 방식 역시 동일한 익명 ID가 출력되므로, 추적 가능이라는 문제를 해결할 수 없다.

3.1.4 Universal re-encryption 기반의 ID가변 정보화 방식

이 방식은 universal re-encryption 방식과 one-time pad에 기반함으로 태그의 출력 값이 매회 다르게 출력되도록 만들고, 기존의 방식과는 달리 읽기 전용 리더와 one-time pad 갱신용 리더를 따로 두어 태그 안의 계산량을 줄임으로 프라이버시 보호와 저비용 태그 구현을 동시에 이루었다.

6. RFID 도입에 대한 고찰

RFID의 최고 장점은 이동시에도 인증이 이루어진다는 것이다. 하지만 스마트 카드에 비해서 보안수준과 데이터 저장용량이 적다는 문제를 가지고 있다. 스마트 카드는 이동시에는 인증이 불가능하지만 RFID에 비해서 인증이 매우 우수하며, 데이터 공간을 많이 확보 할 수 있다는 장점을 두고 있다. RFID의 최대 장점인 이동시에도 인증이 가능 하다는 것이 가장 큰 문제가 되고 있다.

[표 1-2 RFID, 스마트 카드, 바코드의 장단점]

Technology	RFID	Smart Card	바코드
Distance	3-10M	Present	Present
Authentication	Lite	Encryption	Lite
Data	Lite	Rich	Lite

바코드와 RFID를 놓고 보았을 경우, 바코드는 RFID보다 수신거리의 제약이 있었다. 하지만 RFID는 프라이버쉬의 문제로 도입이 어렵다는 문제를 가지고 있다. 이 문제는 사용자가 RFID가 장착된 물건을 샀을 경우 일어난다. RFID 카드가 부착된 상품을 들고 다닐 경우 제 3자가 사용자를 추적 할 수 있기 때문이다. 하지만 일회성 태그를 사용하게 된다면 바코드보다 활용도가 높아질 것이다. 예를 들면 사용자가 상품을 사게 될 경우 부착된 태그로 계산대 위에 올려놓기만 하면 계산이 되기 때문이다. 그리고 팔려나간 물건에 부착된 RFID 태그는 일회성으로 더 이상 추적이 불가능 해진다. 이처럼 태그의 성능과 활용에

따라 RFID 보안에 문제없이 도입이 가능하다는 것이다. 아래의 표는 보안기법과 활용도에 따른 위협요소를 나타낸 표이다. 보안기법에 따른 활용도는 달라질 것이다.

[표 1-3 보안기법에 따른 위협요소]

RF 시스템		위협 요소		
보안기법	사용태그	익명성	위조	변조
일반 해쉬 기법	무관	×	×	×
Kill Command	Block	×	△	×
확장된 해쉬	Active(읽기/쓰기)	△	○	×
가변 인증	Passive(읽기/쓰기)	△	○	×
모바일 인증	무관	○	○	○

○ : 안전, △ : 보통, × : 취약

[표 1-3 RFID 보안기법에 따른 활용도]

보안기법	사용태그	활용도
일반해쉬 기법	무관	- 교육용 - 잃어버리기 쉬운 공동 물건 및 가축
Kill Command	Block	- 바코드 대용
해쉬기반 가변 인증	Passive(읽기/쓰기)	- 출입통제 및 인증 시스템
모바일 인증	무관	- 금융 결제

7. 결론

RFID 시스템은 유비쿼터스 컴퓨팅 환경을 실현시킬수 있는 기술로 많은 연구가 진행되고 있다. 그러나 RFID 시스템의 자동 인식 특징은 생활의 편리함 뿐만 아니라 다양한 프라이버시 침해 문제도 발생시킬 수 있다. 이러한 문제를 해결하기 위해 지금까지 사용자의 프라이버시를 보호할 수 있는 방법에 대한 연구가 진행되어 왔으니 기존에 제안된 여러 보안 기법들은 여전히 안전성 문제를 가지고 있으며 실제 유비쿼터스 환경에 적용하기에는 많은 문제점을 가지고 있다. 본 논문에서는 현재까지 제시된 RFID 보안기법을 사용해서 얼마나 많은 분야에 적용 될 수 있는지 살펴 보았다. 하지만 센서 네트워크와 같은 저 전력으 무선 네트워크가 실제 산업과 생활에 적용되고 상용화 되기 위해서는 보다 안정되고 상호 운영이 가능한 네트워크 프로토콜의 실제 구현이 요구되는데, 이런 요구사항을 해결 할 수 있는데 까지는 더욱 많은 연구가 요구 될 것이라 생각된다.

참고 문헌

[1] 분산 데이터베이스 환경에 적합한 안전한 RFID인증 프로토콜

[2] 효율적인 식별 기능을 가진 위조 불가 RFID Tag 가변 ID방식

[3] 센서네트워크 애플리 케이션 동향