주 제

RFID 시스템에서의 보안 동향

한국항공대학교 신택현, 김동성, 박종서

차례

I. 서 론

가. RFID 시스템의 개요

RFID(Radio Frequency IDentification)는 무선 주파수를 이용해 상품과 사물에 내장된 정보를 먼 거리에서도 읽어내는 기술이다. 물류 · 유통 · 조달 · 군사 · 식품 · 안전 등 다양한 산업 영역에서 막대한 경제적 파급효과를 창출할 수 있는 핵심 기술로 각광 받고 있을 뿐만 아니라, 미래 컴퓨팅 기술인 USN (Ubiquitous Sensor Network)의 기초 기술로 활용되어 향후 인간의 생활 방식과 기존 산업구조를 혁신적으로 변화시키는 분야로 인식되고 있다.[6]

1) RFID 시스템 구성요소 및 동작흐름

RFID는 (그림 1)처럼 태그, 리더, 서버 및 네트워크로 구성되어지고 각 구성 요소별 기능은 다음과 같다.

1. 태그 : 태그는 자신만의 고유한 ID를 갖고, 태그가 부착된 사물의 정보의 요청이 있을 시, 자신의 ID 정보를 알려주는 기능을 한다.
2. 리더 : 리더는 태그들로부터 ID를 수집하는 역할을 한다.
3. 미들웨어 : RFID 네트워크에서 Application과 리더 사이에 위치하고, 내장된 기능들에 대하여 표준화된 인터페이스를 제공하여 Application의 개발 생산성 · 신뢰성 · 상호 연동성 등을 향상시킨다. 그리고 하드웨어 계층의 인터페이스와 객체정보 관리 및 검색서비스에 대한 표준화 인터페이스를 제공하는 역할을 한다.

(그림 1) RFID 시스템 구성 요소 및 동작 흐름

4. ONS 서버 : ONS 서버는 객체검색시스템으로서 네트워크를 이용하여 RFID 태그가 부착된 객체에 대한 정보를 제공하는 정보서버내의 컨텐츠를 찾아주는 역할을 한다.
5. 정보 서버 : 정보서버는 외부에서 정보를 받아들여 자체 데이터베이스에 저장하거나, 외부에서 질의를 받아 자체 정보를 PML 형식으로 제공하는 역할을 한다.[15] [18] [22]

2) RFID의 장점 : RFID는 바코드에 비해 다음과 같은 장점들을 가지고 있다.

· 여러 각도에서 비접촉 방식으로 데이터 인식
· 한번에 여러 태그 인식 가능
· 태그의 재사용 가능
· 온도, 습도, 진동에 강한 내구성과 긴 수명
· 충분한 데이터 저장 공간

3) RFID의 분류 : RFID는 다음과 같이 분류되어 진다.

· 송신 여부에 따른 분류
  – 수동형 : 내장 전지가 없어서 스스로 전파를 송신할 수 없다.
  – 능동형 : 내장 전지 또는 외부 전원을 공급받아 스스로 전파를 송신한다.
· 데이터의 판독에 따른 분류
  – 읽기 전용 : ID기능만 보유
  – 기록 가능 : 읽기와 쓰기 모두 가능
· 주파수에 따른 분류 : 저주파, 고주파, 극초단파, 마이크로파

나. RFID의 적용사례 : RFID는 다양한 분야에서 널리 사용될 수 있다.

1) 도서 대출/반납 시스템

한국에서 RFID 시스템을 적용한 첫 도서관으로 기록될 은평구립도서관은 6만여 권에 달하는 도서에 RFID 태그를 부착하고 태그를 읽는 리더를 통해 전체 도서를 관리한다. 은평구의 RFID 전자도서관 시스템은 자가 반납기 · 대출기 도난방지기 · 사서용 데스크톱 리더 · 장서 점검기 · RFID 관리서버 등으로 구성된다. 사용된 RFID의 주파수 대역은 13.55MHz로서 10cm에서 최대 120cm 정도로 떨어져 있는 RFID 태그의 정보를 리더를 통해 읽을 수 있다.

은평구립도서관의 경우 2003년 5월 RFID 시스템 환경을 구축해 서비스에 들어간 이후, 이용자가 스스로 책을 대출하는 자가 대출기 사용실적이 80%~90% 정도이다. 또 자가 반납기 사용실적은 25%~45% 정도이다. 따라서, 이용자는 대출 · 반납 전 과정에서 도서관 직원의 얼굴을 마주할 필요가 없다. 또한, 장서 점검기로 서가를 지나가기만 하면 책이 올바른 위치에 꽂혀 있는지 파악할 수 있어 재고관리에 드는 시간도 기존의 10% 정도이다. (주)이씨오는 은평구립도서관 · 의정부 정보도서관 · 청주시립도서관 · 김천시립도서관 등에 RFID 도서시스템을 보급함으로써 국내 최대의 RFID 도서시스템을 공급하였다.

2) 개인신분카드

1995년 내무부는 주민등록증 · 운전면허증 · 국민연금증 · 의료보험증 · 인감증명서 등에 필요한 7가지 개인 신원정보를 내장한 전자주민카드 사업을 추진하였으나 프라이버시 침해 우려로 사업이 백지화되었다. 2001년 전 국민을 대상으로 하는 '전자건강보험증' 발급 사업도 시민단체의 반대로 역시 사업이 중단되었다.

2003년 7월 세 번째로, 민간 주도의 '스마트카드 컨소시엄'은 민 · 관 · 산 · 학이 공동으로 참여한 컨소시엄 및 포럼 형태를 표방하였고 KAIST 지식기반전자정부연구센터를 중심으로 삼성SDS · LG

CNS · 서오텔레콤 등의 시스템통합(SI)업체와 은행 및 카드사 등 주요 금융기관들도 준비하고 있다. 이 컨소시엄은 스마트카드가 활성화될 수 있도록 3차 진료기관인 대형병원의 스마트카드 활용사업을 시범적으로 추진하고, 향후 이를 원카드시스템에 대한 기반으로 하여 전자주민카드사업으로 확대할 방침이다.

'국방전자카드(군인공제회원전자카드)'는 전군의 장교 · 부사관 · 군무원 등 15만 명을 대상으로 스마트카드 기반의 신분증을 보급하는 사업이다. 국방전자카드는 신용카드 · 교통카드 · 전자화폐기능과 공인인증서를 탑재하여 골프장 · 체력단련장 · 군내 식당 등 복지시설 이용과 가정에서 금융거래용으로도 사용할 수 있다.

3) 전자지갑

충전식 선불카드인 '해운대 서머비치' 카드는 손목밴드형과 목걸이형의 2가지 형태가 있다. 최저 5천원에서 50만원까지 충전할 수 있으며, 다 쓴 경우에는 재충전해 사용할 수 있다. 전자화폐 회사인 (주)마이비가 2004년 7월, 8월 두 달간 부산 해운대와 송정 해수욕장 일대에 총 600대의 '해운대 서머비치' 카드리더를 설치하여, 피서객들은 수영복 차림으로 해수욕장내 탈의장 · 샤워장 · 스낵코너 그리고 각 종 식당과 편의시설 등을 이용할 수 있게 하였다

4) 기타

이밖에 RFID는 금융, 회계정산, 택배관리, 항공수하물관리, 도난방지, 출입관리 등 여러 다양한 분야에서 서비스를 제공할 수 있다.[1]

다. RFID 시스템의 제약 조건 및 보안 취약점

1) 제약조건

현재 RFID 태그 중 가장 값이 싸며 작은 태그는 Atmel TK5552이다. 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 사용될 RFID 태그는 US$0.05 ~ US$0.1의 가격범위에 있기 때문에 강인한 암호프리미티브를 사용하는 것은 현실적으로 가능하지 않다. 낮은 가격의 범위를 벗어나지 않으면서 보안 및 프라이버시 위험을 고려한 태그 및 리더의 설계가 중요한 문제가 되고 있다. 저렴한 RFID 태그는(5센트 이하) 기본적으로 패시브 형태의 사용을 요구하고 있으며, 저렴한 태그의 비용 요구사항(5센트 이하)은 태그가 사용할 수 있는 전력, 처리시간, 저장 공간, 게이트 수 등의 자원을 제한한다. 5센트의 태그를 만들기 위한 IC 칩 비용은 2센트를 넘으면 안되며 이는 게이트 수를 7.5K~15K 게이트로 제한한다. 현재 100비트의 EPC 칩은 약 5~10K 게이트를 요구함에 따라, 안전성 측면에서 요구되는 게이트의 수는 2.5K~5K를 넘어서면 안 되는 제약조건을 갖고 있다[11]. CRYPREC[16] 보고서에 따르면 대칭키 암호알고리즘의 구현이 6~13K게이트로 알려져 있으며 대칭키를 기반으로 설계할 수 있는 해쉬 함수도 유사한 수의 게이트가 요구될 것으로 기대된다. 더 적은 게이트 수가 요구되는 Tiny Encryption Algorithm[13]이 저렴한 RFID 태그에 앞으로는 사용될 수 있는 가능성이 있으나 현재 사용하기에는 비싸다. 또한, 대칭키 암호에 비해 더 많은 게이트 수가 요구되는 공개키 암호를 RFID에 사용하기 위해서는 더 비싼 비용이 소요될 것으로 기대할 수 있다. 현재 NTRU社는 NTRU 공개키 암호기법을 RFID와 비접촉형 스마트카드에 적용한 솔루션 GenuID를 개발하였으며, 비접촉형 스마트 카드에 NTRU 암호기법을 구현 할 경

우 약 $2의 비용이 소요될 것으로 예측하고 있다[17]. 그러나, NTRU 공개키 암호도 저렴한 RFID 태그에서 이용할 수 있는 리소스 이상을 사용하기 때문에 현재 5센트 이하의 저렴한 RFID태그에 적용할 수는 없고 더 비싼 스마트 태그에서 사용하여야 한다.[5]

1) 프라이버시 침해

RFID 시스템에서 태그와 리더 사이는 무선 환경에서 서로 정보를 전달한다. 그래서 공격자는 쉽게 도청을 할 수 있다. 만약 태그와 리더사이에 어떠한 정보보호기술이 적용되지 않는다면 태그 정보가 고스란히 공격자에게 넘어가게 된다. 이러한 정보들을 통해서 공격자는 사용자의 옷 입는 취향, 현재 소유 현금, 여권 같은 신분증이 있다면 주소 · 연락처, 또한 약을 갖고 있다면 몸 상태 등 여러 가지 개인정보를 습득할 수가 있다. 그래서 태그와 리더사이에서는 태그의 정보를 숨길 수 있는 암호화 기술이나 그런 보안 기술 적용이 필요하다. 그런데 태그의 정보를 암호화 한다고 해도 또다른 문제점이 존재하게 된다. 태그는 리더의 쿼리에 대해 반드시 어떠한 형태로든 응답을 해야된다. 그런데 이러한 응답이 유일하고, 일정하게 되면 공격자는 리더를 갖고 사용자가 현재 존재여부를 알 수 있게 된다. 그래서 공격자가 다수의 리더를 이용하게 되면 사용자의 위치추적이 가능하게 된다. 이러한 위치추적을 방지하기 위해서 태그는 리더의 쿼리에 대해 매번 응답을 달리하는 정보보호기술이 적용되어야 한다.

2) 위변조 문제

RFID의 사용이 확대되어 대부분의 물건에 부착이 된다면, RFID 위변조 문제가 심각하게 대두될 것으로 예상된다. 태그 위변조에 대한 대응 방안이 미미하다면, 판매자나 소비자 모두 큰 피해를 입을 수 있다. 예를 들면, 고가 물품의 태그를 변조해서 가격을 낮춘다면 판매자는 엄청난 손해를 입을 수 있고, 가짜 명품에 진짜 명품 태그를 위조해서 부착한다면 소비자 또한 피해를 입을 수 있다. 그리고 신용카드 등에 사용되는 RFID가 복제된다면 개인이 막대한 피해를 입을 수 있다.

II. 본 론

RFID 정보보호기술은 통신 구간에 따라 크게 포핸드보안, 백엔드 보안, 멀티도메인 보안으로 나눌 수 있다.

가. RFID 포핸드 시스템 보안

RFID 포핸드 보안 기술은 다음과 같이 크게 세 가지로 분류할 수 있다.

1) 도청방지 기술

· Silent Tree-Walking[12]

RFID 시스템에서 효율적인 다중인식 기술을 위해서는 리더가 태그를 충돌 없이 인식해야하므로 태그 충돌방지 알고리즘이 요구된다. 현재 RFID 시스템에서는 Binary Search방식과 Frame Aloha방식이 태그 충돌방지 알고리즘으로 널리 쓰이고 있다. 그 중 Binary Tree Walking Anti-collision 알고리즘은 리더가 태그에게 ID의 각 비트를 브로드캐스트하기 때문에 전방향 채널(리더→태그)에 존재하는 도청공격에 취약하다. MIT가 제안한 Silent Tree-Walking 알고리즘은 태그가 리더에게 보내는 데이터는 도청할 수 없다는 점에서 착안하여 리더가 태그에게 보내는 데이터를 XOR연산을 통해 공격자로부

터의 도청공격에 안전하면서도 Binary Tree Walking Anti-collision 알고리즘과 유사한 수행속도를 갖을 수 있도록 변형한 알고리즘이다.

· Re-Encryption[8]

Re-Encryption은 RSA 연구소에서 Euro에 내장하기 위하여 개발한 보안기술로, 노출되는 태그의 정보를 보호하면서 권한이 있는 정부기관이 지폐를 추적할 수 있는 기술이다. 하지만 공개키 방식의 암호화 알고리즘이 태그에 삽입되어야 한다는 점 때문에 태그의 가격이 상승되어야 한다는 단점이 있다.

· Blocker Tag[9]

Blocker Tag는 RFID 태그위에 붙이는 것으로, 태그 탐색을 위한 리더의 모든 질문에 대해서 'Yes'로 응답하는 태그를 말한다. 그래서 이 방식은 Binary Tree Walking이나 ALOHA Anti-collision 알고리즘을 사용하는 태그에서 사용할 수 있다.이런 Blocker Tag는 Privacy Zone을 만들어서 Blocker Tag와 동일한 시작비트를 갖는 태그들을 보호할 수 있다. 하지만 악의적인 목적을 가진 사용자에게 리더로의 DoS 공격을 가능하게 하는 툴로써 이용될 수 있는 단점이 있다.

2) 정보차단 기술

· Active Jamming[9]

Active Jamming 기술은 RFID 리더의 기능을 막거나 방해하는 신호를 브로드캐스트 하는 장치를 이용하는 방법이다. 그래서 태그의 정보를 악의적인 목적을 가진 리더로부터 차단해 보호할 수 있다. 하지만 이 방법을 사용하면 주변의 다른 정당한 리더에게도 영향을 미칠 수 있고, 이 방법 자체가 공격방법으로 사용될 수 있으므로 특별한 경우가 아니면 사용할 수 없는 매우 강력한 해결책이다.

· Kill Tag[9]

AutoID센터의 Kill Tag 기술은 사용자의 프라이버시를 보호하는 기술 중 가장 일반적인 기술이다. 이 방법은 8비트의 패스워드를 포함한 Kill command를 전송해 태그의 기능을 정지시키는 방법이다. 하지만 이렇게 기능이 정지된 태그는 재사용이 불가능하기 때문에 재사용이 요구되는 응용분야에는 적용할 수 없다. 예를 들면 물건을 구입을 하고, 반품이 가능한 경우에는 태그의 기능이 살아 있어야 반품이 가능하기 때문에 이 방법을 사용할 수 없다. 그리고 패스워드가 8비트밖에 안되므로 악의적인 사용자에 의해서 공격으로 이용될 소지가 있기 때문에 EPCglobal에서는 패스워드를 32비트로 규정하고 있다.

· Faraday Cage[9]

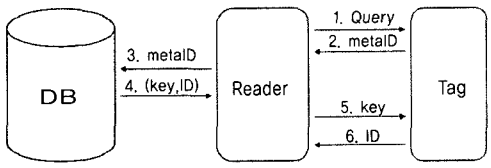
Faraday Cage는 "전파는 금속을 투과할 수 없다"라는 성질을 이용한 방법이다. 실제로 2005년 유로화의 RFID 시스템의 도입에 대비하여 돈 봉투에 금속성 그물을 입힌 상품이 나오기도 하였다. 그러나 이 경우 사용범위가 극히 제한적이고, 침묵하지 말아야 할 태그를 침묵시키는 역효과가 나타날 수 있다. 또한 상품에 삽입된 태그의 위치를 알게 되면 태그 크기의 박막을 붙이는 것만으로도 이 상품은 도난을 방지할 수 없게 된다.

3) 인증 및 접근제어 기술

· 해쉬-락[12]

해쉬 기반 접근제어 기술은 RFID 태그의 리소스 문제를 해결하면서 정당한 리더에게만 태그의 정보를 전송하기 위한 방법으로, 일 방향 해쉬 함수의 역원을 구하기가 매우 어렵다는 것에 기반하여 개발되

었다. 인증과정은 다음과 같다. 먼저 태그는 랜덤 키의 해쉬값 metaID=hash(key)를 저장하고 잠김 상태로 된다. 그리고 (key, metaID)를 백엔드 DB 서버에 저장하는 초기화 단계를 거친다. 그리고 리더와 백엔드 DB 서버 사이의 통신채널은 안전하다고 가정하고 다음과 같은 인증과정을 거친다.

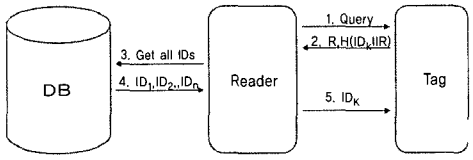


(그림 2) Hash-Lock Access Control

1. 리더는 태그에게 쿼리를 보낸다.
2. 쿼리를 받은 태그는 자신의 metaID로 응답한다
3. 리더는 metaID를 백엔드 DB 서버로 보낸다.
4. 백엔드 DB 서버는 metaID를 이용해서 저장되었던 key값을 찾아 ID와 함께 리더로 보낸다.
5. 리더가 찾은 key를 태그에게 보내면 태그는 hash값을 계산하여 자신의 metaID와 일치하는지 검증한다.
6. metaID 값이 일치하면 태그는 잠김 상태를 해제하고 자신의 정보를 제공한다.

· 랜덤화된 해쉬-락[12]

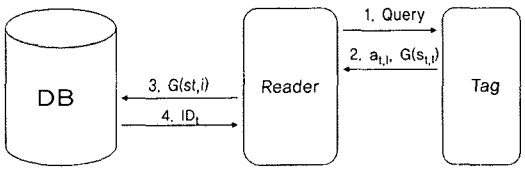
랜덤화된 해쉬-락 기법은 러더의 쿼리에 대해 태그가 매번 일정한 값의 metaID를 응답해서 위치추적이 가능한 해쉬-락 기법의 단점을 보안하기 위해서 나온 기법이다. 태그는 리더의 쿼리를 받으면 의사난수생성기를 이용해서 랜덤 넘버 R을 생성해서 IDk 값을 연접해서 해쉬 값을 생성해 매번 다른 값으로 응답한다. 하지만 IDk가 노출되므로 여전히 위치추적의 가능성이 존재한다. 또한 의사난수생성기가 태그에 들어가야 하므로 태그의 가격이 상승하고, 태그의 양이 증가 할수록 백엔드 DB 서버의 부하가 증가해서 많은 수의 태그에는 부적합하다. 그리고 재전송공격과 스푸핑 공격에는 안전하지가 않다.



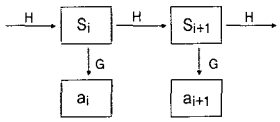
(그림 3) Randomized Hash-Lock Access Control

· 해쉬-체인[10]

이 방법은 두 개의 서로 다른 해쉬 함수를 이용해서 리더의 질의에 대하여 항상 다른 응답을 하는 구조로 위치추적에 강한 기법이다. 하지만 공격자가 태그의 응답을 재전송하는 경우 정당한 태그로 가장할 수 있으므로 재전송공격과 스푸핑 공격에는 취약하다. 그리고 두 개의 해쉬 함수로 인해 태그의 가격이 상승하고, 백엔드 DB 서버에서의 연산량이 커서 많은 수의 태그에는 부적합하다.



(그림 4) Hash-Chain Based Protocol



(그림 5) Hash-Chain

이러한 기술들 외에도 상태기반 인증 프로토콜, 시도-응답 인증 프로토콜 등 포핸드 보안에서의 인증 및 접근제어 기술들에서 나타나는 여러 단점들을 보

완하는 여러 알고리즘들이 개발되고 있다.

나. RFID 백엔드 시스템 보안

RFID 백엔드 시스템 보안은 구성요소별 보안과 구성요소간의 안전한 통신채널 확보 및 서비스 거부 공격에 대한 방어대책이 필요하다.

1) 미들웨어 보안

미들웨어는 태그의 정보를 받은 리더의 질의를 ONS 서버에 전달하고 ONS 서버는 태그에 정보를 가지고 있는 정보 서버의 위치를 전달한다. 미들웨어는 리더로부터 받은 정보에 대한 기밀성, 무결성을 제공해야 하며, 백엔드 응용 서버들과 상호 신뢰 관계를 맺어야 한다. 또한 태그나 리더에서 발생한 서비스 거부 공격 혹은 유해 트래픽을 적절하게 탐지하고 대응할 수 있어야 한다. 초기에 미들웨어는 EPC global에서 MIT Auto-ID연구를 확장한 EPC Network 표준을 개발 중에서 Savant[19] 미들웨어를 개발 하였으나, 현재는 ALE specification[21]에 따라서 미들웨어가 개발되고 있다. 한편, 일본은 앞서 소개하였던, u-ID센터 중심으로 u-Code 및 TRON 엔진, e-Tron 보안 기술 기반의 미들웨어를 개발 중이다. 이외 솔루션 업체인 Savi, Sun, MS, IBM에서도 미들웨어를 개발 중이다. 이 중 EPC global에서 제시하였던 대표적인 미들웨어인 Savant 미들웨어의 경우, 대표적인 미들웨어인 CORBA, .NET, J2EE 등에서 적용되는 접근 제어 기술이 사용되고 있지 않은 실정이다. 향후 RFID 백엔드 시스템의 가용성 보장을 위해 RBAC(Role Based Access Control)과 같은 접근 제어 기능이 포함되어야 한다.

2) ONS 보안

ODS(Object Directory Service, EPCglobal에서는 ONS라고도 함)는 질의된 RFID 코드에 해당되는 정보 서버의 IP 주소를 저장하고 있는 NAPTR (Naming Authority Pointer) 레코드를 얻어오도록 하는 디렉터리 시스템이다. ODS는 기존의 DNS보다 중요한 정보와 역할을 가지고 있기 때문에 공격자는 서비스거부 공격, ONS 질의 도청, ONS 응답 메시지 기밀 및 권한 침해 같은 공격을 해 올 수 있다. 이에 대해 ONS의 데이터 무결성 및 인증을 보장하는 보안 방안을 고려해 볼 수 있다.

· Transaction Signature[14]

TSIG는 ONS 보안을 위해 트랜잭션 서명을 이용하여 ONS간 트랜잭션의 보안을 보장하는 기술이다. TSIG는 설정이 단순하며, ONS가 이용하기에 충분할 만큼 가벼우며, ONS 메시지를 안전하게 만들기 쉬운 특징을 지니고 있다. 서명자는 ONS 메시지에 TSIG 레코드를 붙여 보내고, 수신자는 TSIG 레코드를 제거하고 메시지 변조 여부를 확인한 후 후속작업을 진행한다. TSIG 레코드는 ONS 메시지 전체에 대해 계산한 해쉬 값을 포함하고 있다. 현재 사용되고 있는 TSIG 레코드는 ONS 메시지 전체나 기타 필드를 단방향 해시 함수에 입력해 해쉬 값을 계산해 낸다. TSIG 레코드의 기타 필드에는 그 ONS 메시지가 서명된 시간에 대한 정보가 포함되어 있어 재전송 공격을 방어할 수 있다. 서명된 ONS 메시지의 수신자는 시간정보를 검사해 그 값이 허용할 수 있는 어떤 범위 안에 포함되는지 여부를 검사한다. 이 TSIG의 서명시간 정보를 이용하기 위해서는 ONS 끼리의 시간이 동기화되어 있어야 한다.

· DNSSEC[7]

TSIG는 리더와 서버간의 통신을 안전하게 하는 용도로 적합하다. 그러나 리더와 서버 중 하나가 해킹을 당해 TSIG 키가 누출된다면 더 이상 안전하지 못

하다. 또한 TSIG는 공유 비밀키 방식을 이용하기 때문에 키 배포 문제로 TSIG를 여러 ONS간에 이용하도록 설정하는 것은 현실성이 없다. 이를 해결하기 위해 공개키 암호방식을 사용할 수 있다. RFC 2535에 기술된 DNSSEC(DNS Security)은 DNS 메시지에 공개키 기반의 전자서명 기능을 제공한다. 이는 ONS 데이터에 대한 응답이 누구로부터 왔는가에 관련한 인증 메커니즘을 제공한다. DNSSEC은 디지털 서명을 이용한 데이터 기반 인증과 DNS Zone내의 데이터 무결성, 그리고 트랜잭션 보안을 제공한다. DNS 응답은 속임수를 쓰기 쉬운 비연결 프로토콜인 UDP 패킷이며, DNS 트래픽은 일반적으로 방화벽을 통과할 수 있도록 설정되어 있어 공격자는 이를 이용해서 DNSSpoof 공격을 할 수 있다. 하지만 DNSSEC을 사용하면 스푸핑 공격시 사용되는 위장 패킷은 서명에 필요한 키를 가지고 있지 않으므로 무시하여 방어할 수 있다.

3) 정보서버 보안

정보 서버는 데이터를 기업 내부 혹은 기업 간에 공유함으로써 RFID 네트워크에 유용성을 더해 주기 위한 다른 차원의 애플리케이션이다. 정보 서버가 다루는 영역은 데이터가 수집되고, 서비스 구동과 그에 연관된 데이터 표준을 사용하여 질의된다. 정보 서버는 낮은 계층보다 더욱 복잡하고 다양한 국면을 가진 기업 IT 환경 내부에서 동작한다. 이는 서로 다른 기업들 간에 비슷한 업무를 수행하기 위한 해결책은 서로 다르기 마련이며, 정보 서버는 이러한 기업 사이에 RFID 데이터를 주고받는 것을 목적으로 하는 것이 가장 큰 이유이다. 마지막으로 정보 서버는 RFID 네트워크 구조들 중 가장 최상의 위치를 차지하도록 구성되었고, 따라서 기업들 간에 서로 다른 기업 시스템에 접근하는 자연스러운 접속점이 된다. 따라서 이 접속점들, 즉 정보 서버를 잘 관리하여 보안을 처리한다는 것이 정보 서버의 보안시스템 이다. 그렇기 때문에 정보 서버는 웹서버 해킹, NFS · FTP · telnet · mail등 통신 애플리케이션을 이용한 공격 등 인터넷에 연결된 서버들이 기본적으로 받을 수 있는 각종 공격에 대비해야 한다.

다. RFID 멀티도메인 보안

RFID Network가 단일 도메인에서 멀티 도메인으로 발전함에 따라 보안 요구사항도 단일 도메인에서는 고려하지 않았던 사항들이 생기게 된다. 그 중 가장 고려해야 할 것이 인증 및 접근제어이다. 인증 및 접근제어를 효과적으로 수행하기 위해서는 네트워크 내에 공개키(Public key) 기반의 인프라를 갖추고 전자서명 및 공인인증을 이용하는 방법으로 접근해야 할 필요가 있다. 이런 환경을 구성하기 위해서는 정부나 다른 기관에서 TTP(Trusted Third Party)가 되어 리더나 애플리케이션의 인증을 수행할 수 있는 구조를 갖추어야 한다. 이외에 서로 다른 RFID Network에서는 RFID 도메인 간에 서로 인증 및 접근제어의 판단은 서비스를 제공하는 RFID 도메인에 위임할 필요성이 있다.

RFID 멀티 도메인에서 인증 및 접근 제어를 담당하는 부분은 정보 서버 혹은 미들웨어가 될 것으로 예상된다. EPCglobal과 Verisign은 인증, 접근제어, 연합의 필요성을 소개하고 있으며, 정보 서버가 그 역할을 담당할 것으로 보고 있다. 한편, 현재의 RFID 도메인을 구축할 때에 정보서버(Information Server, ID)가 없는 경우가 있으며, 이때 일반적으로 미들웨어(Middleware)가 정보서버가 담당하는 역할을 포함하게 되므로 미들웨어에 인증 및 접근 제어의 기능을 수행할 수도 있다.

인증 및 접근제어의 기존 보안 기술로는 RFID 관리와 유사한 개념인 ID 관리, 이종 환경에서 VO

(Virtual Organization)의 형태로 Proxy를 사용하여 인증 및 접근 제어를 수행하고 자원을 공유하는 그리드 보안 기술[3], 또한 웹 서비스 간에 인증 및 접근 제어를 다루는 웹 서비스 보안 기술[4], 마지막으로 이들 요소에 공통으로 사용될 수 있는 OASIS의 표준인 SAML[20]과 XACML[23] 등이 있다. 이런 보안 기술 중 XML 보안 기술이 RFID Network에 적용하기에 가장 알맞다. 이러한 내용은 EPCglobal Inc 및 Auto-ID Center 문서에도 명시되어 있다. XML 보안 기술 중 XML 전자서명과 XML 암호화를 통해서 무결성, 기밀성이 보장되는 통신 환경이 구축될 수 있으며 두 도메인 간에 키 교환을 위해 XKMS[24]가 기반구조로 사용될 수 있다.

현재 학계나 산업계에서 RFID 멀티 도메인에서의 인증 및 접근 제어에 대한 방안은 뚜렷이 제안된 방법이 없는 실정이다. 또한 앞서 언급한 것처럼 인증과 접근 제어 기술이 RFID 멀티 도메인의 구성 요소 중에서 미들웨어와 정보 서버에서 구현될지도 결정되지 않은 상황이다. 따라서 RFID 멀티 도메인에서의 보안 기술은 EPCglobal Network와 uID 센터와 같은 산업계의 표준을 비롯하여, 이러한 표준들이 반영되는 ISO 표준도 더불어 살펴보면서 점진적으로 방안을 구현하는 것이 현명할 것이다.

III. 결 론

RFID 시스템은 기존의 바코드를 대체하여 각종 응용 분야에서 혁신적인 변화를 가져올 것으로 기대된다. 그러나 이러한 RFID 기술의 확산은 개인 신상정보노출에 따른 개인의 사생활 침해와 같은 역기능의 새로운 문제를 야기할 것으로 우려되고 있다. 이것은 RFID 기술이 정보접근의 매개역할을 하는 태그식별정보가 개인이 알지 못하는 사이에 당사자의 허가 없이 사용될 가능성을 내재하고 있기 때문이다. 이러한 보안 위협으로 크게 프라이버시 보호와 네트워크 보호가 필요하다.

RFID 시스템 보안 위협으로는 크게 프라이버시 침해와 위변조 문제로 나누어 볼 수 있으며 이에 대한 보안 대책이 시급한 실정이다. 본 문서에서는 RFID 시스템에 대한 보안 기술의 최신 동향을 살펴보고 Active Tag에 적용될 수 있는 보안 기술을 고려해보았다.

먼저 RFID 시스템 보안 기술을 네트워크 구간별로 포핸드 보안, 백엔드 보안, 멀티 도메인 보안으로 분류하였다. 포핸드 보안은 RFID 태그와 리더 사이의 보안 기술을 다루며, 인증 및 접근 제어 기술, 도청 방지 기술, 물리적 보안 기술 등으로 나누어볼 수 있다.

인증 및 접근 제어를 위해 일방향 해쉬 함수를 이용하여 해쉬 락, 랜덤화된 해쉬락, 해쉬 기반, 상태 기반, 시도-응답, 상태기반, 위치추적 및 서비스 거부 공격에 강한 프로토콜 등이 있다. 그리고 도청 방지를 위해 고요한 트리워킹(Silent Tree-Walking), 재암호화(Re-encryption), Noisy Tag 기술 등이 있다. 마지막으로 물리적 보안을 위해서 킬 태그, 패러데이 케이지, Active Jamming, Blocking 태그, Noisy Tag 등이 있다. 이러한 포핸드 보안 기술은 태그의 기능과 RFID 태그가 사용되는 환경의 보안 위협 정도에 따라 본 문서에서 소개한 보안 기술을 적용할 수 있다.

백엔드 보안 기술은 RFID 리더 뒷단의 미들웨어를 비롯하여, 정보서버, ONS 서버 등의 RFID 시스템을 구성하는 구성요소들과 이들 구성 요소간의 안전한 통신을 제공하기 위한 기반 기술들이다. 미들웨어는 Fault Tolerant 한 미들웨어, DoS 공격에 대한 보안 기술을 인터넷 서버(웹 서버, FTP 서버 등)에 사용하고 있는 기존 기술을 적용 시킬 수 있다. 정보

서버의 경우에는 보안 위협을 줄일 수 있도록 최대한 서비스를 줄여서 RFID 네트워크 서비스 이외의 다른 서비스는 제공하지 않고 정보 서버 전용으로 운용하는 방침으로 운용 되어야 한다. 마지막으로 ONS 서버의 경우에는 기존의 DNS 서버와 매우 유사하므로 DNSSec을 RFID 네트워크 시스템에 맞게 수정하여 사용할 수 있다. 이들 각 구성 요소간의 안정한 통신은 현재 사용하고 있는 IPSec, SSL/TSL 등을 적용시킬 수 있다.

멀티 도메인 보안 기술은 서로 다른 도메인 간에 안전한 정보의 교환을 위해 필요한 보안 기술로 ID management, 웹 서비스 보안 기술, SSO 기술, 그리드 보안 기술과 관련성이 있다. 이들 기술에서 공통적으로 사용되는 기술로 SAML과 XACML 기반의 인증 및 접근제어 기술이 적용될 수 있을 것으로 사료된다.

이상에서 RFID 네트워크 구간별 보안 방안에 관한 최근 동향과 향후 연구 방향을 살펴보았다. 본 논문에서 제시한 내용은 앞서 언급하였듯이 RFID 시스템이 사용되는 환경과 보안 위협에 따라 적정한 수준의 보안을 제공할 것인지 완벽한 보안 기술을 적용할 것인지에 차후에 고려되어야 할 것이다.

[참 고 문 헌]

[1] 김완석, "유비쿼터스코드 RFID 객체와 u응용 모델",2004.11.10

[2] 유승화, "유비쿼터스 사회의 RFID", 2005.03.10

[3] 이재광, "그리드 보안기술 동향", KETI, pp. 3, 6, 2004년 12월

[4] 이재승, "웹 어플리케이션 보안 기술 동향", ETRI, pp. 22-36, 2005. 04. 19

[5] 주학수, "RFID 시스템의 보안 및 프라이버시 보호를 위한 기술 분석", 전자정보센터 IT리포트

[6] 한국전산원, "RFID 도입방법론 기초 연구", 2005.10.27

[7] Giuseppe Ateniese, Stefan Mangard, "A New Approach to DNS Security (DNSSEC)"

[8] Juels, A.; Pappu, R.: Squealing Euros: Privacy Protection in RFID-Enabled Banknotes, Financial Cryptography, 2002

[9] Juels, A. et al.: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, 10th ACM Conference on Computer and Communications Security, 2003

[10] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost?RFID", Proceedings of the SCIS 2004, 2004

[11] Miyako Ohkubo, Koutarou Suzuki and Shingo Kinoshita, Cryptographic Approach to "Privacy-Friendly" Tags, submitted 2003.

[12] S. A. Weis, S. Sarma, R. Rivest, and D. Engels. Security and privacy aspects of low-cost radio frequency identication systems. In First International Conference on Security in Pervasive Computing, 2003.

[13] David J. Wheeler and Robert M. Needham. TEA, a Tiny Encryption Algorithm. Technical report, Computer Laboratory, University of Cambridge, 1995.

[14] Vixie, P., Gudmundsson, O., Eastlake, D. and B. Wellington, " Secret Key Transaction Signatures for DNS(TSIG)", RFC 2845, May 2000.

[15] Yojiro UO, Shigeya Suzuki, Osamu Nakamura, Jun Murai, "Name service on the EPC network", Auto-ID Labs Workshop, 2004

[16] CRYPTOREC reports, published 2002 (in Japanese)

[17] NTRU. GenuID. http://www.ntru.com/products/genuid.htm

[18] "Auto-ID Object Name Service (ONS) 1.0", 2003.08.12, http://www.autoidlabs.org

[19] "Auto-ID Savant Specification 1.0", 2003.09.01, http://www.autoidlabs.org

[20] "Technical Overview of the OASIS Security Assertion Markup Language (SAML) V1.1", 2004.05.04, http://www.oasis-open.org

[21] "The Application Level Events(ALE) Specification", 2005.09.15, http://www.epcglobalinc.org

[22] "The EPCglobal Architecture Framework EPCglobal Final Version", 2005.07.01, EPCglobal, http://www.epcglobalinc.org

[23] "XACML 2.0 Access Control Markup Language Approved as OASIS Standard", 2005.03.02, http://www.oasis-open.org

[24] "XML Key Management Specification", 2001.03.30, http://www.oasis-open.org

신택현

2005년 한국항공대학교 항공통신정보공학과 졸업 (공학사)
2005년 ~ 현재 한국항공대학교 컴퓨터공학과 석사과정
관심분야 : RFID 보안, 임베디드 시스템, 하드웨어 디자인

김동성

2001년 한국항공대학교 전자공학과 졸업(공학사)
2003년 한국항공대학교 컴퓨터공학과 졸업 (공학석사)
2003년 ~ 현재 한국항공대학교 컴퓨터공학과 박사과정
관심분야 : 정보보호, 유비쿼터스 컴퓨팅 보안

박종서

1983년 한국항공대학교 항공통신공학과 (공학사)
1986년 North Carolina State Univ. 대학원 졸업 (공학석사)
1994년 Pennsylvania State Univ. 대학원 졸업 (공학박사)
1996년 ~ 현재 한국항공대학교 컴퓨터공학과 교수
관심분야 : 정보보안, Embedded system, 하드웨어디자인, 컴퓨터구조