情 報 保 護 學 會 誌
第 14 卷 第 6 號, 2004. 12

RFID 시스템에서의 프라이버시 보호기술

강 전 일*, 박 주 성*, 양 대 헌*

요 약

유비쿼터스로 대변되는 현재, 그리고 미래의 사회에서는 정보는 무시할 수 없는 가치를 가지게 될 것이다. 타인의 정보를 악용하는 사례가 빈번이 이어지면서 정보를 정당한 권리를 가진 개체가 소유해야한다는 인식이 널리 퍼지게 되었지만, 불행히도 유비쿼터스의 한 부분을 차지하는 RFID 시스템 또한 이러한 부분에 대해서 면역이 존재하는 것은 아니다. 이 글에서는 RFID 시스템에서 정보라는 무형의 자원을 안전하게 지키기 위해 필요한 여러 가지 기술에 대해서 설명할 것이다.

Ⅰ. 서 론

1998년 미국 제록스 팔로앨토 연구소의 마크 와이저 소장이 처음 이 용어를 사용함으로써 유명해진 유비쿼터스(Ubiquitous)란 단어는 라틴어로 '언제 어디서나 있는'이라는 의미로 시간과 장소에 구애 받지 않는 컴퓨팅 환경을 이야기한다. 컴퓨팅 역사의 첫 번째 패러다임이 메인프레임이었고 두 번째 패러다임은 PC였다. 현재 말하고 있는 세 번째 패러다임은 과거 '일대다', '일대일'의 관계를 뛰어 넘어 컴퓨터와 인간의 관계가 '다대일'로, 현실 세계를 모방하여 구성되었던 사이버공간이 아니라 현실에 인간을 위한 컴퓨팅 환경이 구현되는 것이다.

유비쿼터스의 기반 기술들은 실로 다양해서 각 분야에서 서로 유기적인 협력이 필요한 상황이지만 분야별로 자신들이 유비쿼터스의 핵심이라고 주장하고 있는 것이 사실이다. RFID(Radio Frequency Identification; 무선인식) 시스템 또한 그러한 분야 중에 하나이다. 데이터베이스라든지 인프라 네트워크 분야는 유비쿼터스를 지탱하는 기반이 될 것이다. 하지만 일반적으로 이러한 부분에 대해서 모르는 사용자들은 이러한 것에 대해서 전혀 신경 쓰지 않으며 쓰지도 말아야 한다. 그렇다면 무엇이 사용자와 유비쿼터스 환경을 연결할 것인가. 혹자는 생체인식이나 광학 인식 등을 말할지도 모르겠지만 가격과 성능, 그리고 유연성 등을 생각해보면 RFID 시스템보다 뛰어나지는 않다.

쇼핑을 하고 계산을 하기 위해 까마득한 줄에 서서 자신의 차례를 기다릴 필요가 없어지는 세상을 유비쿼터스 세상에서는 보장한다. 짧은 통로를 지나가기만 하는 것으로 물품에 대한 계산은 자동으로 이루어지며 온라인으로 자동 지불될 것이다. 이 예는 RFID 시스템이 이끄는 유비쿼터스 세상의 아주 작은 하나의 예일 뿐이다.

정보는 이제 무시할 수 없는 가치를 가진다. 이를 악용하는 사례가 빈번이 이어지면서 정보를 정당한 권리를 가진 개체가 소유해야한다는 인식이 널리 퍼지게 되었지만, 불행히도 RFID 시스템 또한 이러한 공격에 대해 안전한 것은 아니다. 이 글에서는 RFID 시스템에서 정보라는 무형의 자원을 안전하게 지키기 위해 필요한 여러 가지 기술에 대해서 설명할 것이다.

Ⅱ. RFID 시스템 개요

1. 자동 인식

현재 자동 인식(Automatic Identification) 부분은 광학 문자 인식기(Optical Character Reader, OCR/OMR), 자기인식기(Magnetic Stripe Reader, MSR), 바코드(Barcode)등이 있으며, 그 외에도 음성인식이나 지문인식 같은 생체인식(Biometrics)이 있다. 그리고 주파수를 이용하는 RFID 시스템이 있다.

다른 자동 인식 시스템에 비교하여 RFID 시스템이 가

* 인하대학교 정보통신대학원 정보보호연구실({dreamx, security77}@seclab.inha.ac.kr, nyang@inha.ac.kr)

지고 있는 단점은, 가격이 바코드나 광학 문자 인식 등에 비해서 높다는 것이다. 그에 반해 장점은 8천 비트 이상의 정보를 담을 수 있으며, 기계적 인식률이 좋고, 오염물질에 대해 매우 강하다는 것이다. 주파수를 사용하여 광학 방식에서 사용하는 시야 가림 등의 영향도 없을뿐더러 방향과 위치에 대한 영향도 없다. 바코드 시스템의 최대 인식 거리가 약 50cm인 것에 비하면 RFID 시스템의 경우 멀리는 수십 미터에 이를 수 있는 것도 커다란 장점이라 하겠다.

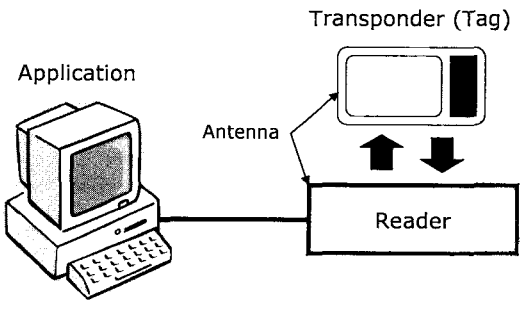
2. 구성 요소

RFID 시스템은 크게 두 가지 부분으로 나눌 수 있다. '리더-태그 시스템'과 '백엔드 시스템'이 바로 그것이다.

2.1 리더-태그 시스템 구성 요소

리더-태그 시스템은 태그에 기록되어 있는 비트로 표시된 정보를 리더가 읽어와 응용프로그램에게 넘겨주고 응용프로그램이 리더에게 명령하여 태그에 새로운 비트로 표시된 정보를 기록하는 부분을 의미한다. 보통 [그림 1]과 같은 구성 요소를 가지고 있다.

태그(Tag)는 실제 물체에 부착하는 것으로 칩과 안테나를 가지고 있다. 적게는 64 비트에서 많게는 8천 비트 정도까지 정보를 담을 수 있다. 값싼 RFID 시스템 구현을 위해서 이 태그를 얼마나 저렴하게 만들 수 있는가가 중요하며, 그렇기 때문에 태그는 하드웨어적으로 상당히 제한적일 수밖에 없으며 간단한 몇 가지 명령을 수행할 수 있을 정도이다. 리더(Reader)는 태그의 정보를 읽어들이는 장치로 정보를 응용프로그램에게 전송하는 역할과 응용프로그램에게 명령을 받아 태그에 정보를 기록하기 위하여 명령어를 주파수 형태로 변환하여 전송하는 역할을 한다. 응용프로그램(Application)은 리더에서 전송된 비트로 표현된 정보를 받아 로컬 데이터베이스를 뒤져 비트의 의미를 재인식하고 필요한 일련의 작업을 수행하는 역할을 한다.



[그림 1] RFID 시스템의 리더-태그 시스템

리더-태그 시스템에서 몇 가지 주목해야할 부분은 사용하는 주파수 대역, 배터리 내장여부, 사용하는 메모리와 충돌방지 알고리즘 등에 대한 것이 있다.

RFID 시스템에서 사용하는 주파수의 경우 크게 세 가지 정도로 나눌 수 있다. 각각의 용도에 따라 100-500kHz, 10-15MHz, 850-950MHz/2.4-5.8GHz로 나눌 수 있는데 그 중 일찍부터 관심을 끌었던 주파수는 125kHz, 13.56MHz, 2.45GHz이다. 그러나 ITU-R에 의해 전 세계는 그 쓰임에 따라 유럽 및 아프리카(지역1), 북남 아메리카(지역2), 극동 및 오스트리아(지역3), 세 지역으로 나뉘었지만 국가나 지역 별로 사용하는 RFID의 주요 관심분야라든지 요구사항이 다른 관계로 특정한 주파수를 할당하는데 어려움이 있다. 그런 이유로 현재 전 세계에서는 8개의 주파수를 사용하고 있고 특별히는 13.56 MHz의 경우 주요 RFID 제조회사들이 자신들의 태그에 이를 채택하고 있고 ISO 15693에 지정되어 있는 등, 전 세계적으로 표준화가 진행 중에 있다. 주파수의 특성에 따라 태그의 데이터를 읽어 들이는 속도나 거리, 그리고 가격의 차이가 발생하며 주파수가 높을 수록 이 세 가지 특성이 모두 높아진다.

RFID 태그는 전원 공급 방법에 따라서 액티브(Active) 타입과 패시브(Passive) 타입으로 크게 나눌 수 있다. 액티브 타입은 전원을 내장한 것이 특징으로 배터리를 내장하고 있어 패시브 타입에 비해 더 긴 거리를 데이터 전송거리로 갖는 것이 특징이지만 비싼 것이 단점이다. 패시브 타입은 리더로부터 전원을 공급받아 사용하는 타입으로 현재 가장 경쟁적으로 개발하고 있는 타입이다. 아주 약한 전력을 사용하기 때문에 전송거리가 20cm-1m 내외로 짧지만 가격이 저렴한 것이 특징이다. 그 외에, 압전(piezo-electric) 효과와 느린 속도에서 탄성파(음향파)의 표면 관련분산(dispersion)에 기반을 한 표면 음향파(SAW; Surface Acoustic Wave) 타입이 있다.

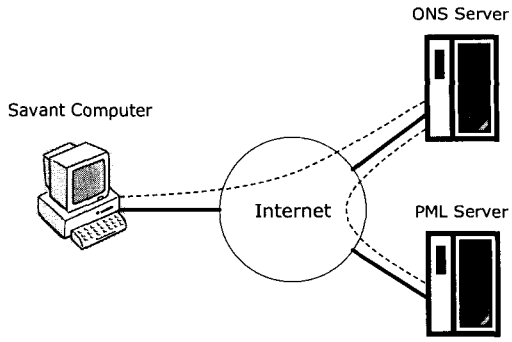
RFID 시스템에서 사용하는 메모리는 RAM, OTP (One Time Programmable user memory), EEP-ROM, FRAM 등이 있다. RAM은 임시 데이터를 저장하기 위해 사용할 수 있다. 전원공급이 끊어지게 되면 저장되지 않은 데이터는 영원히 잃어버리게 되는데, 태그에서는 RAM은 데이터 통신 중 일시적으로 존재하는 데이터의 임시 저장을 위해 사용된다. 액티브 타입의 태그의 경우 RAM을 장기 데이터 저장에 사용할 수도 있다. EEP-ROM의 경우 커패시터가 오랫동안 전하를 저장할 수 있는 능력에 기초하고 있는데, 셀을 하나를 충전하는데 높은 전력이 필요하며, 시간도 5-10ms 정도 소요된다. 메모리 용

량이 클 경우 쓰기 속도가 그에 비례하여 느려지게 되는 단점이 있기 때문에 RAM 같은 임시 저장소로 사용할 수는 없다. 100,000번에서 1,000,000번 정도의 쓰기 횟수가 지원된다. FRAM 셀의 기본 원리는 전계가 없는 경우에도 전기적 극성을 유지할 수 있는 물질의 능력이다. FRAM 셀의 쓰기 동작은 0.1μs정도로 굉장히 빨라 버스 주기 또는 상태 머신의 주기 시간 안에 데이터를 쓸 수 있다. 전력 소모 면에서도 EEPROM과 몇 배나 차이가 나며 사실상 RFID에서는 FRAM을 사용할 것으로 결정되었다. 그러나 다른 회로와의 결합에 문제가 있어 현재 사용하고 있지 못한 상황이다. 쓰기 가능 횟수는 10^{10}번 정도로 EEPROM보다 최대 10^5번 정도 더 많다.

RFID 시스템에서 리더의 필드 안에 여러 개의 태그가 자신의 고유 번호를 송신할 경우 데이터의 충돌이 발생하게 된다. 유용성과 편리함을 위해서는 반드시 이러한 충돌을 방지할 수 있는 알고리즘이 필요하다. RFID 시스템에서 많이 사용하는 충돌 방지 알고리즘은 시간 분할 다중 접속(TDMA) 방식으로 태그에서 구현되고 리더에 의해서 제어되는 방식이다. 이러한 충돌 방지 알고리즘은 다시 크게 두 가지로 나눌 수 있는데, 첫 번째가 ALOHA 방식이다.

ALOHA 방식에서 태그들은 자신이 데이터를 보내고 싶을 때 보내면 되는데 충돌이 일어날 경우 재전송을 요구하기 위한 방법이 추가적으로 필요하다. 이 방법은 고유 번호가 매우 적을 때 사용할 수 있다. 확률적으로 ALOHA 방법은 18%정도의 전송 성공률을 보이기 때문에 이를 보안하기 위해서 슬롯(Slotted) ALOHA를 사용한다. 슬롯 ALOHA의 경우 태그들이 동기화된 시간의 시작점에서만 전송을 시도하는 것으로 성공률은 38%정도로 ALOHA에 비하면 2배 정도 높은 수치이다. 슬롯 ALOHA에서 모든 태그를 검색하기 위해서 주어지는 슬롯을 무한정 늘릴 수는 없기 때문에 이를 동적으로 조절하는 것이 바로 동적(Dynamic) 슬롯 ALOHA이다. 이 방법은 매 전송요구 명령 전송 시 태그가 이용할 수 있는 슬롯의 수를 하나의 파라미터로 전송하는 것이다. 리더가 제시한 슬롯의 수보다 많은 태그가 전송을 위해 경쟁한다면 이후에 이용할 수 있는 슬롯의 수를 늘리는 식으로 작동한다. 이러한 ALOHA 구조를 이용하기 위해서는 태그들에 RNG (Random Number Generator)가 탑재되어야 하며 확률적이긴 하지만 태그가 전송되지 않을 가능성도 배제할 수 없다.

또 다른 방식으로는 이진 탐색 기법(Binary Tree-walking)이 있다. 이 알고리즘을 이용하기 위해서는 충돌의 정확한 비트 위치가 리더 내에 파악되어야 한다. 리더는 태그에게 정해진 양의 비트의 전송을 요구하고 충돌이 발생하지 않았을 경우 다음 정해진 양의 비트의 전송을 요구한다. 충돌이 발생할 경우 충돌한 위치를 기록하여 서브 트리를 검색하게 된다. 태그가 많으면 많을수록 비트의 충돌 확률은 커짐으로 이를 완화하기 위하여 정해진 양을 줄이면 되지만 리더는 초기에 태그의 개수를 알 수 없기 때문에 안전을 위해서는 1 비트씩 처리해야 한다.



〔그림 2〕 백엔드 시스템의 예. EPC Network

2.2 백엔드 시스템 구성 요소

백엔드 시스템은 어떻게 구성하느냐에 따라 시스템에 따라 많은 차이점을 보일 수 있으며 딱히 정형화된 틀이 있는 것은 아니다. 그래서 여기서는 EPCglobal의 EPC 네트워크를 예를 들어 백엔드 시스템에 대한 구성에 대해서 알아보기로 한다. EPC(Electronic Product Code)는 EPCgloabl에서 만든 RFID 태그의 코드 체계를 뜻한다.

Savant는 잘못 읽은 태그의 데이터를 수정(Data smoothing), 오버랩된 리더에 의해 중복되어 읽힌 태그를 제거(Reader coordination), 위로 올리고 내릴 필요가 있는 정보가 무엇인지 결정(Data forwarding), 시간으로 생성된 EPC 데이터를 가져오고 지능적으로 저장(Data storage), 조정된 작업을 통하여 데이터를 관리하고 모니터링(Task management) 등의 일을 하는 장치로 EPC를 사용하는 태그를 직접 EPC Network에 연결하는 역할을 한다.

ONS(Object Name Service)는 EPC에 대한 비트 정보를 URI 형태로 변환하여 EPC에 대한 상세한 정보가 담긴 PML 서버를 찾아내고 이를 연결해주는 역할을 한다. ONS는 기본적으로 현재 인터넷에서 사용되는 DNS (Domain Name Service)를 사용하기로 결정되었으며 질의와 응답에 있어서 DNS 표준을 따른다.

PML(Physical Markup Language) 서버는 PML 형식으로 EPC에 대한 정보를 저장하는 서버를 의미하지는 않는다. EPC에 대한 정보를 저장하는 방식에는 제한이

없으며, PML은 Savant와 ONS, Savant와 RFID 리더 등에서 데이터를 교환할 때 사용하는 XML 기반 프레임워크를 정의한다. 현재 EPC 1.1에서는 EPC의 제조번호(serial number)에 대한 데이터의 저장과 관리에 대하여 정의하지 않고 있다.

III. RFID 보안 문제

1. 보안 문제의 인식

RFID 시스템은 그 편리함에도 불구하고 개인 정보나 보안에 대해 취약한 것이 사실이다. 바코드 시스템과 비교하여 시야가림에 대한 문제가 없어졌지만 그 시야가림의 문제로 인하여 RFID의 태그는 항상 읽혀질 준비를 하고 있는 것도 사실이다. 2005년부터 유럽 중앙은행은 유럽에서 사용하는 유로에 RFID 태그를 내장한다고 밝히고 있다. 만약의 경우이긴 하지만 아무런 보안 대책을 세우지 않았다면 악의적인 사람이 길거리에 지나가는 사람들을 모니터링 할 수 있다. 보이지 않지만 그 사람은 누가 현금을 더 많이 가지고 다니는지 알 수 있으며 그는 범죄의 피해자가 될 수도 있다.

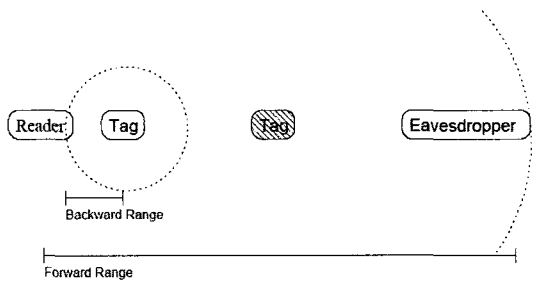
다른 예로 들 수 있는 것은 개인 정보에 관한 문제이다. 만약, 옷(물론 속옷도 포함해서)에 붙인 태그가 악의적인 사람의 물음에 자신의 고유 번호를 가르쳐 준다면 이는 심각한 사회 문제가 될 것이다. 만약 사람에게 RFID 태그와 고유한 번호를 부여한다고 가정해보자. RFID 태그에는 너무 많은 정보가 들어 있을 것이고 개인의 정보란 더 이상 존재하지 않을 수도 있다. 이러한 보안 문제를 고려한다면 RFID 시스템에서 태그에 부여하는 정보의 양은 충분히 고려하여 결정 하여야 한다.

불행하게도 태그에는 자체적인 네트워킹 기능이 있어 신뢰할 수 있는 CA(Certificate Authority) 같은 곳에 접속하여 리더를 신뢰할 수 있는지 알아낼 방법이 없다. 고기능의 태그의 경우 나름대로의 인증과 암호화 시스템을 탑재할 수 있지만 그렇지 않을 경우 태그는 어떠한 리더의 요구에도 응답하게 된다.

이러한 이유로, RFID의 보안의 취약성이 사회적으로 문제가 될 수 있음을 인식하는 일은 매우 중요하다. RFID 시스템의 보안 문제에 대해서도 역시나 두 가지 부분으로 나누어 생각할 수 있을 것이다.

2. 리더-태그 보안 문제

리더-태그에서의 보안 문제가 심각한 것은 태그에 탑재



〔그림 3〕 Forward Range와 Backward Range

될 수 있는 하드웨어적 기술의 한계는 지나치게 낮고, 태그에 담겨진 정보를 불법적으로 엿듣거나 정보에 대한 변조를 시도할 수 있는 가장 빠르고 손쉬운 부분이기 때문이다.

2.1 Forward and Backward Range (Sniffing Model)

Forward Range와 Backward Range의 모델은 한 태그 보안 기술에 대하여 설명하기 위해 제시되었다. 엿듣기를 목적으로 하는 소극적인 공격자가 있을 때 태그를 공격하는 방법에 대한 예시이다.

Forward Range는 리더가 태그에게 질의를 보낼 수 있는 물리적 범위를 의미한다. 반대로 Backward Range는 태그가 리더에게 질의에 대한 응답을 보낼 수 있는 물리적 범위를 의미한다. 태그에 배터리를 내장하지 않는 RFID 시스템의 경우 리더는 태그에게 에너지를 전달해야 하는 필요성에 의하여 필드의 범위가 넓어질 수밖에 없고, 태그는 리더에게 전달받은 에너지를 이용하여 리더에게 응답하기 때문에 범위가 작을 수밖에 없다. 따라서 Forward Range는 Backward Range보다 범위가 크다고 말할 수 있다.

만약, 이진 탐색 기법을 충돌 방지 알고리즘으로 사용하는 값싼 RFID 시스템에서 도청자(Eavesdropper)가 태그의 정보를 얻고자 한다고 가정하자. 도청자가 Forward Range 안에 있을 때, 이진 탐색 기법을 사용하는 RFID 시스템의 리더는 태그에서 태그의 정보를 계속 전송하게 되며 도청자를 이를 성공적으로 도청할 수 있을 것이다.

이 모델은 기본적으로 ALOHA 방식을 사용하는 RFID 시스템에는 해당되지 않지만 설계한 RFID 시스템에서 이러한 문제가 발생하지 않는지 확인해봐야 할 것이다.

2.2 Re-Writable Tag

EEPROM을 사용하는 태그와 같이 재기록(Re- Write) 가능한 태그의 경우 이 데이터는 안전하지 않을뿐더러 언

제나 다른 사람에 의해서 수정되거나 바뀔 가능성이 존재하게 된다.

가령, EEPROM을 채택한 태그를 사용하는 RFID 시스템으로 운영중인 대형 슈퍼마켓이 있다고 생각해보자. 어떠한 보안 수단이 존재할 수 있지만, 이를 무력화 시키고 태그의 정보를 값싼 다른 물건의 정보로 바꿔치기 할 수 있을지도 모른다. 이러한 사실을 깨닫지 못한다면 슈퍼마켓은 맞지 않는 재고 품목으로 물품 확보에 차질을 빚을 것이고, 아무런 문제가 없는 전산시스템의 오류를 의심하여 이를 수정하기 위해 인력과 시간을 낭비할 지도 모를 일이다.

2.3 서비스 거부 공격(Denial of Service)

RFID 시스템에 대한 가장 강력한 공격은 RFID 시스템을 부분 또는 전체를 마비시킬 수 있는 서비스 거부 공격(Denial of Service)이라고 말할 수 있다. 무의미한 비트를 무작위로 생성하여 연속적으로 공중에 뿌리는 특수하게 개조된 태그가 있을 때 리더가 다른 태그를 읽으려고 한다면 리더는 이로 인하여 발생하는 수많은 충돌과 상황에 맞지 않는 데이터에 끝없이 재시도를 할지도 모른다. 물론, 이 공격은 충분히 검색 가능하며 리더는 상황에 맞게 읽기를 포기할 수도 있다. 하지만 이 공격을 검색 가능하다 하다고 하더라도 이 태그를 찾아 물리적으로 제거하기 전까지 리더는 쓸 수없는 상태가 되어 버린다.

2.4 그 외 다른 공격 방법

RFID 태그에 대한 공격은 이처럼 고차원적인 방법이외에도 아주 단순하면서도 강력한 방법도 존재할 수 있다. 전자기적 쇼크를 태그에 주어 태그를 침묵시키는 방법은 쇼크에 면역이 있는 태그를 생산하는 것 이외에는 현재로서는 딱히 막을 방법이 존재하지 않는다. 슈퍼마켓에서 태그가 침묵한 상품은 공짜와 다를 바 아니다.

3. 백엔드 시스템 보안 문제

RFID 시스템을 자립(Stand Alone) 시스템으로 운영할 수도 있을 것이다. 공개된 회선이 아니라 비싼 회선 설치비를 지불하고 독자적인 네트워크를 이용한 백엔드 시스템을 구성할 수도 있다. 하지만 만약 전 세계적으로 공통된 백엔드 시스템을 사용하거나 VPN을 구성하듯 인터넷을 이용하는 백엔드 시스템을 구성할 경우 RFID 백엔드 시스템의 보안은 순전히 사용하는 인터넷 보안 기술에 의존하게 된다.

3.1 스푸핑(Spoofing)

스푸핑(Spoofing) 공격은 자격조건이 없는 호스트로부터 올바르지 않은 정보를 수용하거나 사용할 때 일어난다. 위조 공격은 이러한 공격에 대해 취약한 DNS 서버에게 치명적일 수 있다. 이런 공격은 인터넷 사이트나 전자우편에 대하여 자격이 없는 호스트로 전달해 주게 된다. 이 문제는 당사자가 사용하는 서버를 위조할 수 없다고 하더라도 다른 호스트를 위조함으로서 당사자에게 직간접적으로 피해를 입힐 수 있다. 이 공격은 자신이 공격을 당하고 있는지 알지도 못한 채 오랜 시간을 보낼 수도 있기 때문에 더욱 위험할 수 있다.

EPC 네트워크의 예로 본다면 ONS 서버와 PML 서버가 이 위협에 노출되어 있다고 볼 수 있다.

3.2 서비스 거부 공격(Denial of Service)

서비스 거부 공격을 대상이 되는 서버에 실행할 경우 RFID 시스템은 타격을 받을 수밖에 없다. 물론 EPC 네트워크에서의 ONS 서버와 PML 서버는 이러한 공격으로부터 자신을 안전하게 보호할 수 있지만 회선 용량이나 라우터의 처리 용량은 한정되어 있다는 것을 유의해야 한다. 이런 의미에서 서비스 거부 공격은 그 시도만으로도 충분히 성공했다고 할 수도 있을 것이다.

3.3 데이터베이스 공격

암호화된 정보를 송출하는 태그의 경우 암호화된 정보가 담긴 데이터베이스를 공격하여 그 내용을 얻어 올 필요는 없다. 또한 암호화되지 않은 정보라고 해도 마찬가지이다. 암호화되거나 되지 않은 정보를 바로 태그의 아이디로 사용하여 독자적인 데이터베이스를 구축할 수도 있기 때문이다. 물론, 이를 구축하는 것이 절대로 쉬운 일은 아니지만 결코 불가능하지도 않다. 현재의 EPC 네트워크와 같이 상품번호(product number)만 제공하는 백엔드 시스템이라면 이러한 공격에 대해서는 태그의 정보를 읽을 수 없도록 원천 봉쇄하거나 예측 불가능하고 사용할 때마다 다른 키로 암호화 하는 방법이외에는 이를 막을 수 있는 방법이 없어 보인다.

IV. RFID 보안 기술

이 장에서는 RFID 리더-태그 보안 기술에 대하여 살펴보기로 한다. (백엔드 시스템의 보안 기술은 사실상 DNS와 XML 관련 보안 기술이 사용될 것이며 DNS의 보안과 관련해서는 DNSSEC이 나와 있고 XML관련해서

는 W3C의 XML Signature, XML Encryption 등과 OASIS의 SAML, XACML 등의 기술들이 나와 있다. 또한 IPSec나 SSL/TLS 같은 기술을 사용할 수 있을 것이다.)

1. Faraday Cage

무선 주파수가 침투하지 못하도록 하는 방법으로 금속성의 그물(Mesh)나 박막(Foil)을 입히는 방법이다. 실제로 2005년 유로화의 RFID 시스템의 도입에 대비하여 돈 봉투에 그물을 입힌 상품을 나오기도 하였다. 그러나 이 경우도 사용 범위가 극히 제한적이라는 것이 문제로 생물 인식에 쓰인 태그 같은 경우 사용할 수 없다.

또한, 이 방법은 거꾸로 침묵하지 말아야할 태그를 침묵시키는 데에 역으로 사용될 수 있다는 것은 우려되는 일이 아닐 수 없다. 상품에 태그가 삽입된 위치를 알고 있다면 태그 크기의 박막을 붙이는 것만으로도 이 상품은 공짜가 되어버린다.

2. Active Jamming

리더기가 제품을 읽지 못하도록 방해 신호를 보내는 물건을 소비자가 들고 다니자는 것인데, 불법적으로 이용할 소지가 크고 오히려 방해 신호에 의해 다른 RFID 시스템이 손상될 수 있기 때문에 특별한 경우가 아니면 사용할 수 없는 방법이다.

3. 'Kill' Tag

이 방법은 MIT의 Auto-ID Center(현 EPCglobal)에서 제안한 방법으로 태그의 설계에 8-bit의 패스워드를 포함하고 태그가 이 패스워드와 'Kill' 명령을 받을 경우 태그가 비활성화 되는 방식이다. 태그는 내부에 단락회로가 있기 때문에 이를 끊음으로서 '자살 명령'을 실행하게 되는데 이렇기 때문에 한 번 죽은 태그는 다시 살릴 수 있는 방법이 없게 된다. 이런 경우 태그를 재사용할 필요가 있는 분야에서는 사용이 불가능하다. 아주 간단한 예로 반품이 가능한 물건에 붙어 있는 태그의 경우 이런 Kill Tag 명령 방식을 사용할 수 없다.

물론, Read/Write로 설계된 태그의 경우 플래그(Flag) 비트를 이용하여 태그를 죽였다 다시 살릴 수도 있을 것이다. 하지만, 이 경우 또한 여전히 태그에 사용하는 8-bit 암호에 대한 문제가 남는다. 수많은 제품에 사용될 태그라는 것을 감안하고 보안을 생각한다면 128-bit 이상을 암호로 사용해야 하지만 이는 태그에 상당한 부담이 된다. 태그마다 다른 암호를 사용한다면 이를 저장하는 것도 문제이다.

실제로 이 방법은 EPCglobal의 EPC Class1 태그에 내장하도록 되어 있다.

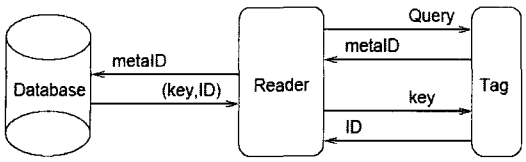
4. Blocker Tag

Juels, Rivest, Szydlo는 개인 정보 보호를 위하여 "블로커 태그(Blocker Tag)"라고 부르는 특별한 툴에 대하여 기술하였다. 블로커 태그는 모든 질문 메시지에 대해서 '그렇다'라고 대답하는 태그를 말한다. 이 방식은 이진 탐색 트리 기법이나 ALOHA 기법을 충돌 방지 알고리즘으로 사용하는 RFID 시스템에서 사용할 수 있다. 모든 질문 메시지에 응답하기 때문에 이진 탐색 기법을 사용하여 태그를 읽어 들이는 방식에서는 탐색의 모든 영역을 검색하게 되는 결과를 가져오고 ALOHA 기법을 사용하는 태그에서는 태그를 전혀 읽을 수 없도록 만든다. 태그의 고유번호 길이가 길어지면 길어질수록 리더는 리더의 용량을 초과하는 개수의 태그를 찾기 위해 시도할 것이고 이는 리더에게 치명적인 결과를 가져올 것이다. 이를 조금만 응용한다면 리더에 대한 서비스 거부 공격을 실행할 수 있다는 것을 쉽게 알 수 있을 것이다. 이를 해결하기 위해서 리더 친화적인(Reader friendly) 방법이 강구되기도 하였는데, 우선 리더는 자신이 읽으려는 태그 그룹에게 블로커 태그가 있는지 물어보고 블로커 태그는 이 물음에 대답한다. 만약 블로커 태그가 있다면 리더는 탐색을 포기한다.

블로커 태그를 조금 더 유용하게 사용하는 방법은 자신이 비밀을 지키고자 의도 태그들의 비트에 맞춰 처음 비트들을 제어함으로서 비밀 구역(Privacy Zone)을 만드는 것이다. 블로커 태그와 동일한 시작 비트를 갖는 태그들은 블로커 태그가 만드는 비밀 구역 안에서 안전하게 보호될 수 있다.

5. Silent Tree-walking

앞서 기술 하였던 Forward and Backward Range 모델에 따르면 이진 탐색 기법으로 태그를 읽어 들일 경우 리더는 도청자에게 태그에 대한 정보를 말해주게 된다. 그래서 제시된 고요한 이진 탐색 기법(Silent Tree-walking)은 태그가 리더에게 보내는 데이터는 도청자가 직접 들을 수 없다는 점에 착안하여 리더가 태그의 정보를 부르지만 태그가 리더에게 보낸 마지막 데이터와 부르고 리더가 태그에게 보내고 싶은 데이터를 XOR하는 방식으로 이루어지게 된다. 여러 개의 태그에서 충돌이 일어나면 일어나는 횟수만큼 1/2의 확률로 원래 태그들의 정보와 멀



〔그림 4〕 해쉬 기반 접근 제어 : 풀기과정

어지게 되는 것이다. 이 탐색 기법의 장점은 리더가 부르는 데이터를 도청자로부터 보호할 수 있다는 것이고, 실행 시간 측면에 있어서도 일반 이진 탐색 기법과 동일하다.

이와 유사한 방식으로 태그가 난수를 생성하여 이를 리더에 보내고 이를 기초(Portion)로 하여 탐색을 시도하는 방식(Randomized Tree-walking)이다. 태그는 반드시 자신이 생성했던 난수를 기억하고 있어야 하며, RNG를 가지고 있고 전원이 끊어지지 않도록 해야 한다는 제약 사항이 있다.

6. Hash-Lock Access Control

해쉬 기반 접근 제어(Hash-Lock Access Control)은 태그에 대한 접근 제어 기술이다. 접근 제어는 허가된 사용자만이 태그를 접근할 수 있도록 하기 위한 방법을 말한다. 태그를 잠그기 위하여, 리더는 난수 형태의 키를 해쉬하여 데이터베이스에 저장하고 이를 태그의 메타 아이디로 사용한다. 그리고 리더는 태그에게 메타 아이디를 보내고 태그는 이를 저장하고 잠김 상태가 된다.

태그를 풀기 위하여, 리더는 태그에게 잠김을 풀려고 한다는 메시지(또는 쿼리, Query)를 보낸다. 태그는 자신이 저장했던 메타 ID를 리더에게 보내고 리더는 데이터베이스에서 메타 ID에 해당하는 ID와 자신이 생성했던 키를 가져온다. 리더는 태그에게 키를 보내고 태그는 이 키를 해쉬해서 나온 값이 자신의 메타 ID와 동일하다면 태그는 잠김 상태에서 빠져나와 주위의 리더에게 반응하게 된다.

이와는 조금 다른 방법으로는 랜덤 접근 제어가 있다. 랜덤(Randomized) 접근 제어의 태그를 잠그는 방법은 위의 해쉬 기반 접근 제어와 동일하며 잠겨 있는 태그를 풀기 위해서는 리더가 태그에게 메시지를 보낸다. 태그를 랜덤한 nonce, R을 생성하여 자신의 메타 ID와 R의 해쉬를 계산하고 R과 함께 리더에게 보낸다. 리더는 데이터베이스에게 모든 ID를 줄 것을 요구한 뒤 모든 ID를 검색하여 ID와 R을 해쉬한 것과 동일한 ID를 찾아 태그에게 보낸다. 만약 자신의 메타 ID와 동일한 ID를 받게 되면 태그는 잠김 상태를 풀고 주위의 리더에게 반응한다. 이 방법의 문제는 리더가 자신이 잠궜던 태그가 많으면 많을수록 태그를 해제하는 데 걸리는 시간이 늘어난다는 것이다.

조금 다른 문제로 위의 일련의 과정을 수행하기 위해서는 태그는 반드시 해쉬 값을 계산할 수 있어야 한다. 문제는 NTRU나 TEA 같이 효율적인 알고리즘이라고 할지라도 보안을 위하여 태그가 포함할 수 있는 최소 200개에서 최대 2000개의 게이트를 가지고는 구현할 수 없다는 것이다. 때문에 아주 가벼운 해쉬 함수가 필요하며 암호학적으로 충분한 안전성을 가져야 한다. 이러한 성질을 만족하기 위해 NLFSR (Non-Linear Feedback Shift Registers) 기반 해쉬 함수의 사용이 제안되고 있다.

7. 재암호화(Re-Encryption)

재암호화(Re-Encryption)은 RSA 연구소에서 Euro에 내장하기 위하여 개발한 보안 기술로, 공개키 암호화 시스템을 사용하여 암호화한 고유 번호를 태그에 덮어 쓰는 방식으로 이루어진다. 태그에는 하드웨어적 제약사항 때문에 신뢰할 수 있는 비밀키 암호화 시스템도 내장할 수 없다. 하물며 공개키 암호화 시스템을 태그 안에 절대로 불가능하다고 말할 수도 있을 것이다. 이런 이유로 '믿을 수 있는 외부 계산기'가 필요하다는 단점이 있다.

재암호화 방식은 ElGamal 공개키 암호화 시스템에 기반하고 있으며 다음과 같은 절차를 따른다.

위 과정에서 보다시피 재암호화를 위해서는 비밀키를 몰라도 되지만 공개키는 반드시 알아야 한다. 이 이야기를 외부 계산기를 통해 재암호화를 수행할 때마다 공개키를 외부 계산기에게 가르쳐 주어야 한다는 것과 같다. 때문에 RSA연구소는 2004년에 보편적인 재암호화(Universal Re-Encryption) 방식을 발표했다.

이 방식은 기본적인 ElGamal 암호화 시스템에서 사용하는 암호화된 문장(ciphertext)의 길이나 계산 비용(computational costs)의 두 배를 소요하게 되지만 재암호화를 위해서 공개키를 알고 있을 필요는 없다.

P, Q are prim, P = 2Q+1
G_Q is subgroup of Z_P^* of order Q
g is generator of G_Q
x is private key, $x \in G_Q$
y is public key, $y = g^x \bmod P$
Encryption $E(m) = (G,M) = (g^r, my^r)$
where $r \in G_Q$ and random
Decryption $D(G,M) = M/G^x = my^r/g^{xr} = m$

Re-Encryption $R(G,M) = (G',M') = (Gg^{r'}, My^{r'})$
Decryption $D(G',M') = M'/G'^x = my^{xr'}/g^{xrr'} = m$

〔그림 5〕 ElGamal 암호화 시스템을 사용한 재암호화

P, Q are prim, P = 2Q+1
G_Q is subgroup of Z_P^* of order Q
g is generator of G_Q
x is private key, $x \in G_Q$
y is public key, $y = g^x \bmod P$
r is random encryption factor, $(k_1, k_2) \in G_Q$
Encryption
$E(m,r) = [(\alpha_1, \beta_1); (\alpha_2, \beta_2)] = (my^{k_1}, g^{k_1}); (y^{k_2}, g^{k_2})]$
Decryption
$D(E(m,r)) = (m_1, m_2) = (\alpha_1/\beta_2^x, \alpha_2/\beta_2^x)$
$= (my^{k_1}/g^{k_2 x}, y^{k_2}/g^{k_2 x}) = (m, 1)$
if m_1 is not 1, the decryption fails.
Re-Encryption
$R(E(m,r)) = [(\alpha'_1, \beta'_1); (\alpha'_2, \beta'_2)]$
$= [(\alpha\alpha_1^{k_3}, \beta\beta_2^{k_3}); (\alpha_2^{k_3}, \beta_2^{k_3})]$

〔그림 6〕 Universal Re-Encryption

8. One-Time Pad

One-Time Pad는 현재까지 암호학에서 만든 가장 단순하면서도 강력한 암호화 시스템이다. 오로지 XOR 연산 하나만을 하기 때문에 연산 능력에 대한 제한이 거의 없고, 다른 어떠한 암호화 시스템보다도 강력한 것이 장점이다. 하지만 키의 길이가 평문 길이와 같아야 하고 복호화 작업을 해서 얻어낸 평문이 정말로 맞는 지 알 수 없기 때문에 현실과는 전혀 맞지 않는 암호화 시스템이었다. 하지만 RSA 연구소의 Ari Juels은 이 One-Time Pad를 이용하는 RFID 전용 암호화 시스템을 고안해 냈다.

우선 RFID 태그와 이를 확인하는 검증자(Verifier) 사이에만 알고 있는 어떤 값 $\kappa \in \{\alpha i\} \cup \{\beta i\} \cup \{\gamma i\}$를 구성하는 익명(pseudonym)들이 존재한다. 어떠한 d가 결정되었을 때 태그는 αd를 전송한다. 검증자는 자신이 알고 있는 익명들에서 αd와 같은 익명이 있는지 검색하여 그에 해당하는 βd를 태그에게 전송한다. 이것이 올바르다면 태그는 그에 해당하는 γd를 검증자에게 전송하여 서로를 인증한다. 필요하다면 검증자는 새로운 부분 One-Time Pad를 태그에게 전송한다. 태그는 이 새로운 부분 One-Time Pad를 κ의 앞에 붙이고 나머지를 뒤로 쉬프트 하여 κ'를 구성한다. 태그는 기본적으로 자신의 정보와 이러한 패드 값 κ를 XOR 연산한 결과를 알려준다.

V. 결 론

RFID 시스템은 지금까지 몇 년에 걸친 준비기간을 가졌고 수년 내에 우리의 생활 속에 깊이 뿌리 내릴 것이다. RFID의 도입으로 지금까지의 프라이버시와는 다른 수준의 침해가 가능해질 것으로 예상되며, 이에 따라 이를 보완할 수 있는 프라이버시 보호기술의 개발이 시급하다. 이 글에서는 주로 RFID의 프라이버시 보호에 대해 기술적인 면에 대한 설명을 주로 했으나, 사용자의 프라이버시 보호를 위해서는 기술적인 접근 이외에도 정책, 제도, 법 정비를 통한 접근 방법도 연구되어야 한다.

참 고 문 헌

〔1〕 Klaus Finkenzeller, 이근호 외 3명 공역 "*RFID HANDBOOK*", 2nd Edition in Korea , 2004, ISBN 89-314-2769-7

〔2〕 Stephen A. Weis, "Security and Privacy in Radio-Frequency Identification Devices", MIT, May 2003

〔3〕 Ari Juels and Ronald L. Rivest and Michael Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", RSA Laboratory, MIT

〔4〕 Ari Juels, John Brainard, "Soft Blocking: Flexible Blocker Tags on the Cheap", RSA Laboratory

〔5〕 Stephen A. Weiss, Sanjay E. Sarma, Ronald L. Rivest, Daniel W. Engels, "Security and Privacy Aspect of Low-Cost Radio Frequency Identification Systems", Laboratory for Computer Science, Auto-ID Center MIT

〔6〕 Philippe Golle, Markus Jakobsson, Ari Juels, Paul Syverson, "Universal Re-encryption for Mixnets", RSA Laboratory, 2004

〔7〕 Ari Juels, "Minimalist Cryptography for Low-Cost RFID Tags", RSA Laboratory

〔8〕 Ari Juels, Ravikanth Pappu, "Squealing Euros: Privacy Protection in RFID-Enabled Banknotes", RSA Laboratoty, ThingMagic, LLC

〔9〕 "Radio Frequency Identification Basic Primer", AIM, Inc. AIM WP-98/002R(White Paper), 1999

〔10〕 Roy Want, Daniel M. Russell, "Ubiquitous Electronic Tagging", Xerox PARC, IBM Almaden Research Center

〔11〕 Tom Ahlkvist Scharfeld, "An Analysis of the Fundamental Constraints on Low Cost

Passive Radio-Frequency Identification System Design", MIT, Aug 2001
[12] Ching Law, Kay Lee, Kai-Yeung Siu, "Efficient Memoyless Protocol for Tag Identification", Proceeding of the 4th International Workshop on Discret Algorithms and Method for Mobile Computing and Communication, MIT-AUTOID-TR-003, Aug 2000
[13] David L. Brock, "The Physical Markup Language", MIT-AUTOID-WH-003, Feb 2001
[14] Christian Floerkemeier, Robin Koh, "Physical Mark-up Language Update", MIT, technical memo, June 2002
[15] "The Object Name Service Version 0.5 (Beta)", Oat System & MIT Auto-ID Center, Feb 2002
[16] "PML Core Specification 1.0", Auto-ID Center Recommendation, Sept 2003
[17] "Auto-ID Object Name Service (ONS) 1.0", Auto-ID Center Working Draft, Aug 2003
[18] Armit Goyal, "SavantTM Guide", MIT Auto-ID Center, technical report, Apr 2003
[19] "Auto-ID Savant Specification 1.0", MIT Auto-ID Center, Sept 2003
[20] "Auto-ID Reader Protocol 1.0", MIT Auto-ID Center, Working Draft Version of 5, Sept 2003
[21] "Draft protocol specification for a 900 MHz Class 0 Radio Frequency Identification Tag", MIT Auto-ID Center, Feb 2003
[22] "860MHz-930MHz Class 1 Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommandation, Version 1.0.0", MIT Auto-ID Center, Nov 2002
[23] "13.56MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification: Candidate Recommendation, Version 1.0.0", MIT Auto-ID Center, Feb 2003
[24] "EPCTM Tag Data Standard 1.1 Rev.1.24", Standard Specification, MIT Auto-ID Center, Apr 2004
[25] "I·CODE1 System Design Guide", Philips Semiconductors, Revision 1.1 public, Application Note, Apr 2002
[26] "Passive RFID Basics", Pete Sorrells, Microchip Technology Inc., AN680, 1998
[27] "125kHz microIDTM Passive RFID Device with Anti-Collision", MCRF250,Microchip Technology Inc., 2003
[28] 이근호, "무선식별(RFID) 기술", TTA 저널 제89호, pp124~129
[29] 유스문, 조은희, "유비쿼터스 환경에서 RFID의 보안", (주) 니츠, 2004
[30] http://www.epcglobalinc.org
[31] http://www.rsasecurity.com
[32] http://www.oasis-open.org
[33] http://www.w3c.org

〈著 者 紹 介〉

강 전 일 (Jeon-il Kang)

2003년 2월 : 인하대학교 컴퓨터 공학과 졸업
2004년 3월~현재 : 인하대학교 정보통신대학원 석사과정
〈관심분야〉 RFID 보안

박 주 성 (Ju-sung Park)

2004년 2월 : 인하대학교 컴퓨터 공학과 졸업
2004년 3월~현재 : 인하대학교 정보통신대학원 석사과정
〈관심분야〉 RFID 보안

양 대 헌 (DaeHun Nyang)

1994년 2월 : 한국과학기술원 과학기술 대학 전기 및 전자 공학과 졸업
1996년 2월 : 연세대학교 컴퓨터 과학과 석사
2000년 8월 : 연세대학교 컴퓨터 과학과 박사
2000년 9월~2003년 2월 : 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재 : 인하대학교 정보통신대학원 전임강사
〈관심분야〉 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안