情 報 保 護 學 會
영남지부 2006년도 정보보호 학술논문 발표회

Auto-ID Lab을 통한 RFID 보안기술 연구동향

이 현 록*, 김 광 조*

요 약

최근 RFID(Radio Frequency Identification) 기술은 유비쿼터스(Ubiquitous) 환경에서의 공장 자동화, 물류·유통 관리, 보안, 출입통제, 인물·동물 추적, 요금 징수, 위조지폐방지, 홈 네트워크 등에 유용하게 쓰일 수 있는 기술로 인식되면서 그에 대한 관심이 증대되고 있으며 이에 대한 활발한 연구가 수행 중이다. 본 논문에서는 RFID 관련 세계 최고 수준의 연구기관인 Auto-ID Lab에 대해 소개하고, EPCglobal의 RFID 표준인 Gen2 규격에 대한 소개와 보안에 대한 고려 없이 작성된 해당 규격에서 발생할 수 있는 보안 취약성을 살펴보도록 한다. 그리고 현재 Auto-ID Lab에서 작성 중에 있는 RFID의 위조방지(Anti-Counterfeiting)와 제품의 프라이버시를 위한 백서(White Paper)의 안에 대한 구조와 그 내용에 대해 알아보고 한국 Auto-ID Lab에서 추진 중인 위조방지기술을 비롯한 RFID 보안기술에 대한 향후 연구방향과 역할에 대해 살펴보도록 한다.

Ⅰ. 서 론

RFID(Radio Frequency Identification, 전파식별, 이하 RFID)는 초소형 반도체에 식별정보를 넣고 무선주파수를 이용해 이 칩을 지닌 물체나 동물, 사람 등을 판독·추적·관리할 수 있는 기술로, 현재 물류·유통뿐 아니라 전자지불·보안 등 다양한 분야에도 적용되고 있다. RFID 기술은 2차 세계대전 당시 레이더에서 발산되는 신호로 적과 아군을 식별할 목적으로 연합군에 의해서 처음으로 사용된 것으로 알려져 있다. 아직까지는 RFID 칩의 높은 가격으로 인해 RFID 기술의 사용이 보편화되지 못하고 있지만, 칩 가격이 급속한 속도로 낮아지고 있어 현재의 추세라면 2, 3년 내에 RFID 기술의 사용이 전 산업분야로 확대되어 나갈 것으로 보인다. 이러한 많은 애플리케이션들과 낮은 비용으로 인해 RFID 태그는 유비쿼터스 컴퓨팅의 핵심기술이 될 수 있으며 공장 자동화, 물류·유통 관리, 보안, 출입통제, 인물·동물 추적, 요금 징수, 위조지폐방지, 홈 네트워크 등에 유용하게 쓰일 것이다.

하지만 이러한 기술의 발전이 가져다주는 생활의 편익 및 사회·경제적 효율성의 이면에는 정보의 불법적인 도청, 위장, 변조 등과 같은 정보화의 역기능이 심각한 문제로 존재한다. 이러한 역기능은 기존 정보화 사회의 많은 역기능 사례에서 볼 수 있는 것처럼 개인은 물론 국가·사회적으로 엄청난 손실을 가져올 수 있으며, 특히 유비쿼터스 시대에는 기존의 환경과는 또 다른 형태의 역기능 즉, 구매 내역, 기호 내역, 소유 정보 등 개인의 프라이버시가 자신도 모르게 유출되던가, 개인의 위치 정보가 노출되는 등 새로운 보안 취약점이 발생하고 있으며 이를 대비한 소형, 경량 암

* 한국정보통신대학교(Information and Communications University, ICU)
국제정보보호기술연구소(International Research Center for Information Security, IRIS)
({tank,kkj}@icu.ac.kr)

호 기술 개발과 해당 환경에 적합한 종합적인 보안기술 개발이 요구되고 있다.

본 논문에서는 국제적인 RFID 연구기관인 Auto-ID Lab에 대해 살펴보고 한국 Auto-ID Lab의 역할과 EPCglobal[2]의 RFID 기술 국제표준인 Gen2규격[3]에 대한 소개 및 해당 규격에서 간과하고 있는 보안 취약점들을 알아본다. 또한 RFID 기술에 필요한 보안 기술 중 최우선적으로 고려되고 중점적으로 연구해야 하는 기술인 RFID 위조방지(Anti-Counterfeiting)에 대해 Auto-ID Lab에서 작성 중인 백서(White Paper)[4]의 구조와 내용을 살펴보며 앞으로 한국 Auto-ID Lab에서 추진 중인 위조방지기술을 비롯한 RFID 보안기술에 대한 향후 연구방향과 역할에 대해 살펴보도록 한다.

본 논문의 구성은 다음과 같다. 먼저 Ⅱ장에서는 Auto-ID Lab의 소개와 한국 Auto-ID Lab에 대해 살펴보고, Ⅲ장에서는 EPCglobal의 Gen2 표준과 보안 취약점을 밝혀 향후 보안기술 연구와 국제 표준화 활동에 보안기술 채택을 위한 연구에 도움을 주고자 한다. Ⅳ장에서는 위조방지 백서에 대한 구조와 내용을 알아보고 한국 Auto-ID Lab에서 추진 중인 RFID 보안기술에 대한 향후 연구방향과 역할에 대해 살펴보도록 하며, Ⅴ장에서 본 논문의 결론을 내리도록 한다.

Ⅱ. Auto-ID Lab 소개

물리적인 객체의 글로벌 네트워크의 구조에 대한 공개 규격을 개발하기 위해 1999년 최초로 설립된 오토 아이디 센터는 현재 연구대학들의 연합체로 구성된 Auto-ID Lab으로 발전되었다. 미국의 MIT에서의 설립을 근간으로 영국(켐브리지대), 호주(아델레이드대), 스위스(세인트갤런대), 일본(게이오대), 중국(푸단대) 등의 전세계 유명대학에 설치된 6개의 Auto-ID Lab들로 이루어진 RFID 관련 세계 최고 수준의 연구기관으로서, RFID 분야의 기술개발과 표준화를 주도하고 국제적인 감각을 가진 우수 인력을 배출하는 세계 최고의 연구 네트워크이다.

6개 기존 랩의 디렉터들로 구성된 Auto-ID Lab 이사회는 한국정부의 동북아 IT 허브계획, 우수한 IT 인프라 및 인력자원, RFID 관련한 각종 파일럿 프로젝트 수행 및 테스트베드 구축, 모바일 RFID 분야 주도적인 표준화 활동, ICU의 RFID 분야 연구 역량 및 영향력 등을 고려하여 인도, 싱가포르, 대만 등의 경쟁국에 앞서 한국 Auto-ID Lab ICU를 선정했다. Auto-ID Lab의 ICU 유치로 인해 한국은 아시아에서 중국, 일본에 이어 3번째로 Auto-ID Lab 유치국이 되었으며, 이는 그간 국내 RFID개발 성과와 정부의 정책의지, ICU의 적극적인 유치노력의 결실이다.

Auto-ID Lab ICU는 보안, 안테나, RF 송수신기, 모뎀, 센서네트워크, IT경영 등의 관련분야 ICU 교수 5명이 참여하고 있으며 그동안 미진했던 RFID 관련 해외 연구기관과의 공동연구 촉진 및 보다 적극적인 국제적인 표준화 활동에 참여하는 계기를 마련하게 되었다. 이와 같은 결정에 따라 ICU는 국내 RFID 관련 산업체, 학계 및 연구기관들과 관계를 맺는 Auto-ID Lab ICU를 학내에 설립하고, 기술개발 및 표준화 과제를 발굴하여 해외 Auto-ID Lab들과 공동연구 등의 협력을 적극 추진할 계획이다. 현재 한국 Auto-ID Lab은 한국전자통신연구원(ETRI)의 텔레매틱스-USN 연구단, 한국전산원, 한국인터넷진흥원, 한국정보보호진흥원, EPC글로벌코리아 등의 국책 연구 기관과 협약을 체결하였으며, 삼성종합기술원, LG전자, SK텔레콤 등의 대기업, RFID와 센서네트워크 관련 중소기업인 옥타컴(주), 메타비즈(주), 한맥 ENG(주) 등과도 협력을 체결하였다. 또한 정보통신부는 Auto-ID Lab의 ICU 유치를 계기로 RFID/USN 관련 국내 기업 및 연구기관이 해외 연구기관과 전략적 제휴를 통해 기술을 확보하고 국제적인 표준화 활동에 참여할 수 있는 장이 마련됨에 따라 국제공동연구를 지원하는 등 다각적인 노력을 하고 있다.

Ⅲ. EPCglobal Gen2 표준

1. EPCglobal RFID Gen2 표준 소개

EPCglobal은 상품코드의 국제표준 개발/관리 기구인 EAN(European Article Number)과 UCC(Uniform Code Council)의 통합으로 탄생한 GS1이 2003년 11월에 설립한 자회사로써 EPC(Electronic Product Code) 코드와 EPCglobal 네트워크의 전 세계 보급을 총괄하고 있는 국제 민간 기구이다. 이 기구는 EAN 인터내셔널과 UCC가 지난 30년간 바코드 및 전자문서 표준 보급을 통해 구축한 업계와의 협력 관계를 바탕으로 사

용자 중심의 EPCglobal 네트워크 표준을 개발/보급함으로써 공급체인을 이동하는 상품의 가시성을 높여 기업의 효율성 제고에 이바지함을 목적으로 하고 있다. EPCglobal은 작년 12월 UHF 대역의 태그-리더 간 통신 프로토콜 버전 2인 Gen2 표준을 제정하였다. 초창기 개발되었던 버전 1(Gen1)과는 기능 및 성능 면에서 크게 개선되었기 때문에 2세대(Gen2)라는 별칭이 붙게 되었다.

Gen1과 Gen2의 가장 큰 차이점은 Gen2는 단일 국제 프로토콜이라는 것이다. Gen1의 경우, 리더가 클래스-0과 클래스-1을 모두 지원하지 않으면 서로 다른 클래스의 태그를 식별할 수 없었다. 게다가 ISO가 국제 표준으로 2가지 UHF Air-Interface 프로토콜인 18000-6A 및 18000-6B를 승인하여 표준이 서로 상이한 경우 태그를 식별할 수 없었다. 하지만 Gen2가 단일 국제 프로토콜로 제정됨에 따라 기존의 RFID 표준 문제가 해소될 전망이다.

Gen2에서는 리더 충돌 문제를 해결하기 위해 다양한 리더 모드를 제공한다. Gen1에서는 Single-reader mode만을 제공하여, 동시에 여러 개의 리더가 태그를 식별할 때 간섭 문제가 발생하였다. 하지만 Gen2에서는 3가지의 리더 모드를 제공하여, 제한된 범위 내에 존재하는 여러 개의 리더가 충돌 없이 태그를 식별할 수 있다. 이는 Gen2 표준에서 명시하고 있는 세션(session)의 개념과도 연관된다. 각 태그는 4가지의 세션에서 동작할 수 있으며, 각 리더는 특정 세션의 태그만을 선택하여 식별함으로써 리더 간의 충돌을 방지한다.

태그 메모리의 경우, Gen1 클래스-0은 칩 생산 시 공장에서 프로그램이 되고, 클래스-1은 사용자가 프로그램 된다. 하지만 Gen2 태그는 실제 태그가 사용되는 필드에서 프로그램 될 수 있다. 즉, 태그가 케이스나 팔레트에 부착되어 있어도 정보를 입력할 수 있다.

데이터 전송 속도에 있어 Gen2는 Gen1에 비해 크게 향상되어 리더가 빠른 속도로 태그를 식별한다. 표에서 보는 것과 같이 Gen1의 클래스-0은 초당 80 킬로비트 그리고 클래스-1은 140 킬로비트의 데이터 전송을 지원하는 반면, Gen2는 초당 640 킬로비트까지 지원한다. 따라서 Gen2 리더는 Gen1 리더에 비해 보다 빠른 태그 판독률을 기대할 수 있다.

마지막으로 Gen2의 확장된 패스워드 길이로 인해 Gen1에 비해 향상된 고객 프라이버시 및 보안을 기대할 수 있다. Gen1의 클래스-0이 24비트 그리고 클래스-1이 8비트의 Kill 패스워드를 지원하는 반면, Gen2는 32비트의 Kill 및 Access 패스워드를 지원한다. 특히, Gen2에서는 리더의 태그 메모리 접근을 위한 인증에 사용되는 별도의 Access 패스워드를 명시하였다.

2. Gen2 표준의 정보보호 취약성

본 절에서는 Gen2 표준규격의 RFID 시스템에서 나타날 수 있는 보안 취약성을 살펴보고, 이를 바탕으로 향후 RFID 국제 표준규격에 보안기술 채택의 필연성을 설명하고자 한다.

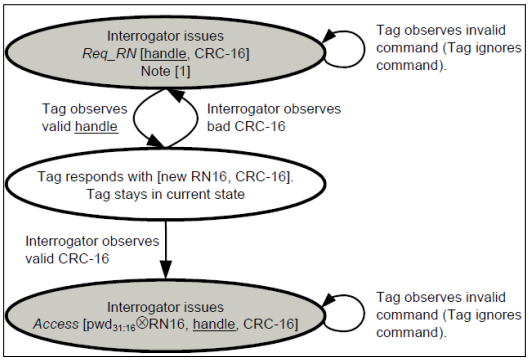
2.1 복제 공격

리더의 태그 식별 과정에서 EPC 코드는 평문 형태로 공격자에게 노출되어, 이를 이용한 공격자의 태그 복제 공격이 가능하다. 즉, 공격자는 이미 지불된 상품의 RFID 태그를 복제하여 지불되지 않은 상품에 부착시킴으로써 정당한 리더를 속이고 지불되지 않은 상품을 가져갈 수 있다. 이를 해결하기 위해, 계산 이후 태그 동작을 정지(Kill)시킬 수 있지만, 품질 보증 및 반품의 목적으로 태그 재사용이 필요한 경우에는 적용하기 힘들다는 단점이 있다.

2.2 도청 공격

태그-리더 간의 무선통신 특성 상 단거리 도청이 가능하여, 공격자는 태그의 Kill/Access 패스워드를 쉽게 도청할 수 있다. Kill 패스워드는 각 태그 당 한 번씩만 사용되므로 도청 가능성이 높지 않다. 하지만 Access 패스워드는 사용 빈도가 높고 상대적으로 신호의 세기가 강한 리더의 메시지에 Access 패스워드가 포함되어 있으므로 쉽게 도청될 수 있다. (그림 1)은 태그 Access 과정의 일부이다. 태그-리더 간의 통신 범위가 2~10m 정도이므로, 공격자는 이 범위 내에서 태그-리더 간의 모든 메시지를 도청할 수 있다. 공격자는 도청 공격을 통해 정당한 리더의 Reg_RN 명령에 대한 태그 응답 RN16를 획득할 수 있다. 그 다음 리더가 전송하는 Access 명령에 포함된 [pwd31:16⊕RN16]을 획득한 후, 이전에 획득한 RN16을 이용하여 Access 패스워드의 하위 16비트

를 알아낼 수 있다. 동일한 과정을 통해 공격자는 해당 EPC 태그의 나머지 상위 16비트를 알아낼 수 있다. Access 패스워드가 노출되면 태그의 메모리 뱅크 접근을 통해 Kill 패스워드를 획득하여 공격자가 태그의 동작을 정지(Kill)하고 복제 태그로 대체하는 것을 가능하게 한다. 또한 태그의 EPC 코드를 악의적으로 변경하여 리더가 태그를 식별할 수 없도록 함으로써 전체 RFID 시스템의 서비스 장애를 초래할 수 있다.



[그림 1] 태그 Access 과정

2.3 프라이버시 침해

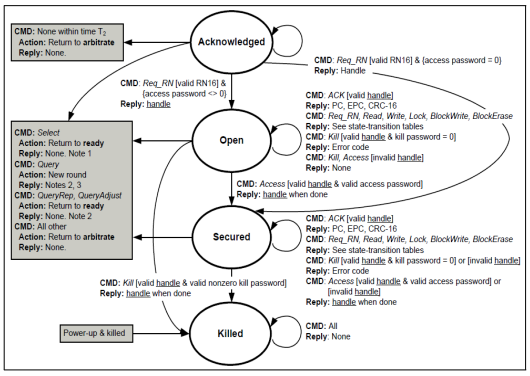
Gen2 표준 호환 리더는 모든 태그의 EPC 코드를 읽을 수 있다. 공격자가 EPC 네트워크의 데이터베이스에 접근할 수 있다면, 획득한 EPC 코드를 통해 태그가 부착된 제품을 구매한 고객의 프라이버시를 침해할 수 있다. 즉. 공격자는 어떤 종류의 제품을 고객이 구매하였는지 알 수 있으며, 상점, 주차장, 극장 등의 공공장소에서 고객 주위를 걸어 다니면서 고객의 소지품이 무엇인지 알아낼 수 있다. 데이터베이스에 접근할 수 없더라도 불변하는 EPC 코드의 특성으로 인해 특정 제품을 구매한 고객의 위치를 추적하여 고객의 프라이버시 침해를 야기할 수 있다.

2.4 중간자 공격 및 서비스 거부 공격

태그-리더 간의 상호 인증 기법 부재로 인해 중간자 공격 및 서비스 거부 공격이 가능하다. 공격자는 태그-리더 중간에서 마치 자신이 태그인 것처럼 위장하여, 원거리에서 리더가 보내는 메시지를 도청할 수 있다. 이 메시지를 중간에서 가로채서 태그에게 다시 전송함으로써 공격자는 마치 자신이 정당한 리더인 것처럼 태그와 통신할 수 있다. 즉, 공격자는 가로챈 메시지를 수정함으로써 태그를 악의적으로 읽고 수정할 수 있게 된다. 그리고 공격자는 매우 많은 수의 인가되지 않은 질의를 태그에게 요청함으로써 RFID 시스템 전체의 마비 현상을 야기할 수 있다. 또한 전파 방해를 유도하는 신호를 전송하여 리더 시스템을 방해할 수 있다.

2.5 불법적인 메모리 읽기-쓰기

Gen2 표준에서 명시하고 있는 태그 상태 전이도에 의하면, Gen2 표준 호환 리더는 쉽게 Access 패스워드가 구현되어 있지 않은 태그의 메모리 뱅크를 읽고 쓸 수 있다. 즉, 공격자가 악의적인 의도로 EPC 태그 메모리 뱅크의 Reserved, EPC, TID (Tag-Identification) 정보 등을 읽고 쓸 수 있게 된다.



[그림 2] EPC Gen2 태그의 상태 전이도

(그림 2)는 Gen2 표준의 EPC 태그 상태 전이도의 일부이다. 공격자가 자신의 리더를 이용하여 태그를 식별한 후(Acknowledged 상태), Access 패스워드가 구현되어 있지 않은 태그(Access 패스워드=0)는 Req_RN 명령에 대해서 새로 생성한 핸들(handle)이라 불리는 16비트 난수를 후방산란(Back scattering)하고 Secured 상태로 전이한다. Secured 상태에서 공격자는 Read/Write 등의 명령을 통해 태그의 메모리 뱅크를 읽고 쓰게 된다.

IV. RFID 보안

1. Auto-ID Lab의 위조방지에 관한 백서

Auto-ID Lab에서는 RFID, 특히 EPC 태그에 대한 여러 백서들을 작성하여 해당 기술의 발전과 보

급을 위한 지침과 학문적인 토대를 마련하는 노력을 하고 있다. 최근에는 의약품, 자동차·항공기 부품, 귀금속 등의 고가상품을 취급하는 물류시스템에서 위조상품의 방지에 대한 요구와 필요성이 높아져 위조방지에 대한 선도적인 기술을 확보하기 위한 백서의 안을 작성하고 있다. 해당 문서는 다음과 같은 구조와 내용으로 구성되어 있으나 전체적으로 추가적인 보완작업이 필요하며, 올해 내로 해당 백서를 완성하는 것을 목표로 하고 있다.

1.1 서론

해당 절에서는 상품의 위조에 대한 문제점과 분석을 통해 향후 RFID가 장착되는 상품의 위조방지를 위한 노력이 얼마나 중요한지를 기술하고 있으며, 아래와 같은 내용을 다루고 있다.

⊙ 상품들의 위조 규모가 얼마나 큰지에 대한 세계 각국의 통계
⊙ 저작물을 다루는 산업, 자동차 산업, 의약 산업에서의 위조에 의한 피해규모
⊙ 기술의 발전, 국제교역의 증가, 시장 및 상품의 다양화, 귀금속 및 브랜드 상품의 요구, 복잡한 공급망 등의 다양한 측면에서의 위조에 대한 분석
⊙ 각 산업계에서 일어나는 실제사례에 대한 검토

1.2 비즈니스 처리과정과 응용

해당 절에서는 비즈니스 관점에서 응용을 중심으로 위조 상품 시장과 현재 사용되고 있는 위조방지 기술 및 개발 중인 기술에 대해 기술하고 있으며, 기술적, 경제적, 사회적 요구사항에 대해 아래와 같은 내용으로 작성되고 있다.

⊙ 불법 시장의 구조와 운영절차
⊙ 위조방지 절차와 응용에 대한 현재의 기술 및 전략
⊙ 기존 위조방지 방법의 문제점
⊙ 안전한 상품을 위한 보안기술, 절차, 전략, 서비스에 대한 기술
⊙ 기술적, 경제적, 사회적 관점에서의 요구사항 분석

1.3 소프트웨어와 네트워크에 관련된 연구

해당 절에서는 기존의 EPC 태그와 해당 태그의 네트워크에 보안을 고려하였을 때 필요한 소프트웨어와 네트워크 기술에 대하여 서술하고 있으며 그 내용은 아래와 같다.

⊙ EPC 네트워크의 현재 상황
⊙ 보안을 지원하기 위한 확장된 EPC 구조에 추가적으로 요구되는 기능들
⊙ 보안 상품 인증 서비스, 센서통합을 위한 소프트웨어 지원
⊙ 설계 및 시뮬레이션
⊙ EPC 상품인증 서비스 (EPC-PAS: EPC Product Authentication Service)
⊙ 기존 EPC 정보서비스 (EPC-IS: EPC Information Service)와의 호환
⊙ 사용자 인증 개념과 데이터 교환 명세
⊙ 키 관리 및 시스템 관리

1.4. 하드웨어와 관련된 연구

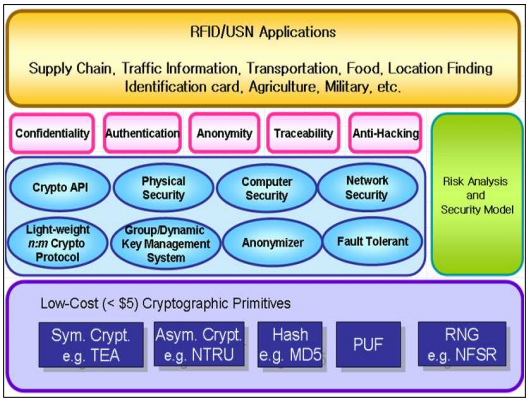
해당 절에서는 보안을 지원하기 위해 태그 칩에 하드웨어적으로 추가되어야 하는 보안기술 및 설계와 관련된 연구에 대해 언급하고 있으며, 다음과 같은 내용을 포함하고 있다.

⊙ 현재 RFID 태그와 리더의 하드웨어 기술 상황
⊙ 보안기능을 위해 하드웨어적으로 요구되는 추가적인 기능들
⊙ EPC-PAS 기능을 위한 태그 설계
⊙ 리더와 시스템 통합을 위한 리더 자체 및 프로토콜의 설계

2. 한국 Auto-ID Lab의 RFID 보안 연구

한국 Auto-ID Lab의 보안연구는 국제정보보호기술연구소(IRIS, 이하 IRIS)[5]를 중심으로 진행되고 있으며, IRIS에서는 이미 RFID 보안과 관련하여 경량암호원천기술, 경량 인증 프로토콜, 키 관리 기술, 보안 API, 보안 프레임워크, 보안관련 표준화 활동 등 많은 연구결과물들[6,7,8,9,10,11,12,13]과 과제들을 성공적으로 수행한 결과를 바탕으로 RFID/USN에 대해 (그림-3)에 나타나 있는 로드맵을 기초로 한 연구를 수행 중이다. 특히 RFID 위조방지를 위해 CRC 기반/Hash기반 경량 인증 프로토콜과 네트워크 구조

에 대한 연구를 수행하였으며, 향후 리더의 환경까지 고려한 경량 인증 프로토콜에 대한 연구로 확대하여 수행할 계획이고, RFID 하드웨어/소프트웨어의 설계와 구현에 있어 필요한 랜덤넘버생성기(RNG - Random Number Generator)의 게이트 수준에서의 최적화, 물리적인 복사방지 함수 (PUF - Physically Unclonable Function)에 대한 연구와 부 채널 공격(Side Channel Attack)에 대한 연구도 병행하고 있다. 앞으로는 안전한 RFID/USN 테스트 베드를 설계하고 구축하는 목표를 가지고 있으며, 해당 연구 결과들을 국제 표준규격으로 채택하기 위한 노력을 해 나갈 것이다.



[그림 3] RFID 보안 연구 로드맵

V. 결 론

본 논문을 통해서 RFID 기술에 대한 대표적인 국제적 연구기관인 Auto-ID Lab과 한국 Auto-ID Lab을 소개하고 EPCglobal의 RFID 표준규격인 Gen2 규격과 보안에 대한 고려 없이 작성된 해당 규격에서 발생할 수 있는 보안 취약성을 살펴보았다. 그리고 현재 Auto-ID Lab에서 작성 중에 있는 RFID의 위조방지와 제품의 프라이버시를 위한 백서의 구조와 그 내용에 대해 알아보았으며, 한국 Auto-ID Lab에서 추진 중인 위조방지기술을 비롯한 RFID 보안기술에 대한 향후 연구방향과 역할에 대해 살펴보았다.

가까운 장래에 RFID 기술은 유비쿼터스 시대의 하부구조를 형성하고 사물의 식별을 매체로써 중요한 역할을 할 것으로 기대되고 있다. RFID는 사물의 대량 식별을 위해 사용될 것이며 기존의 바코드 시스템을 대체하기 위한 차세대 기술로써 각광받고 있다. 하지만 이러한 RFID 기술의 긍정적인 이면에, RFID 시스템을 이루는 기본 요소 및 특성으로 인하여 보안위협에 노출되게 됨으로 인하여 역기능이 발생하게 된다. 이런 역기능들을 방지할 수 있는 보안기술개발 및 표준화는 시급히 개발하여야 하며, 향후 한국 Auto-ID Lab의 보안기술 연구를 담당하고 있는 ICU IRIS에서는 국내외 관련 연구기관과 협력하여 선도적인 역할을 수행할 수 있도록 노력해 나갈 것이다.

참 고 문 헌

[1] Auto-ID Labs
http://www.autoidlabs.org/

[2] EPCglobal
http://www.epcglobalinc.org/

[3] EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960 MHz Version 1.1.0 Draft 1

[4] Auto-ID Labs, "Flagship Project Anti-Countfeiting White Paper Structure" - Under discussion

[5] 한국정보통신대학교 국제정보보호기술연구소 IRIS, International Research Center for Information Security
http://www.iris.re.kr

[6] Jaemin Park, Zeen Kim and Kwangjo Kim, "State-Based Key Management Scheme for Wireless Sensor Networks", *Proc. of WSNS2005*, Nov.07~10, 2005, Washington DC, USA.

[7] Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren and Kwangjo Kim , "Mutual Authentication Protocol for Low-cost RFID", *Proc. of Workshop on RFID and Lightweight Crypto*, Jul.14~15, 2005, Graz, Austria.

[8] Divyan M. Konidala, Dang N. Duc and Kwangjo Kim, "A Capability-based

Privacy-preserving Scheme for Pervasive Computing Environments", *Proc. of IEEE PerSec2005*, Mar.8~12, 2005, Hawaii, USA.

[9] Jeongkyu Yang and Kwangjo Kim, "Security and Privacy on Authentication for Low-cost RFID", *Proc. of SCIS 2005*, Jan.25~28 Maiko Kobe, Japan.

[10] SungJun Min, Go Yamamoto and Kwangjo Kim, "Weak Property of Malleability in NTRUSign", *Proc. of ACISP04*, July 13-15, Sydney, Australia, *LNCS 3108*, pp.379-390, Springer-Verlag, 2004.

[11] Dang Nguyen Duc, Jaemin Park, Hyunrok Lee and Kwangjo Kim, "Enhancing Secrity of EPCGlobal Gen-2 RFID Tag against Traceability and Cloning ", *Proc. of SCIS 2006*, Jan.17~20, Hiroshima, Japan.

[12] Sangshin Lee, Tomoyuki Asano and Kwangjo Kim, "RFID Mutual Authentication Scheme based on Synchronized Secret Information", *Proc. of SCIS 2006*, Jan.17~20, Hiroshima, Japan.

[13] Divyan M. Konidala and Kwangjo Kim, "Mobile RFID Security Issues", *Proc. of SCIS 2006*, Jan.17~20, Hiroshima, Japan.