2 세대 EPCglobal RFID 규격의 보안 취약성 검토 및 개선 방안 연구

한국정보통신대학교, 국제정보보호기술연구소
박재민, Dang Nguyen Duc, Vo Duc Liem, 서영준, 김광조

A Study on the Improvement and Risk Analysis of Security in EPCglobal RFID Gen2

Jaemin Park, Dang Nguyen Duc, Vo Duc Liem, Youngjoon Seo, and Kwangjo Kim
International Research Center for Information Security (IRIS),
Information and Communication University (ICU), Korea

요 약

차세대 IT혁명을 이끌 기술로 평가되는 전파식별(RFID) 태그의 글로벌 표준으로 EPC 클래스-1 Generation-2 UHF-RFID 규격을 토대로 한 `ISO18000-6 타입 C'가 사실상 확정됐다. 이로써 국내외에서 RFID 표준의 혼선문제가 해소돼 RFID 시스템 시장이 일대 전기를 맞게 될 전망이다. 하지만 제안된 Gen2 규격은 복제 공격, 도청 공격 등 다양한 보안 공격에 취약하다. 본 논문에서는 Gen2 규격의 보안 취약성을 알아보고, 그 해결 방안을 알아보도록 한다.

1. 서론

RFID(Radio Frequency Identification)는 초소형 반도체에 식별정보를 넣고 무선주파수를 이용해 이 칩을 지닌 객체를 판독·추적·관리할 수 있는 기술을 말한다. 지금까지의 RFID 시스템은 국제 표준 부재로 인해 시스템 오류 및 업무 혼선의 문제를 야기하였다. 하지만 지난 6월 싱가포르에서 개최된 ISO 국제표준화회의에서 `EPC 클래스-1 Generation-2 UHF-RFID[1](이하 Gen2)' 규격에 기초한 ISO 18000-6의 신규타입(타입 C)이 사실상의

RFID 국제 표준으로 확정됨으로써 RFID 시스템 시장이 일대 전기를 맞게 될 전망이다.

그러나 Gen2 규격은 저가형 태그에 초점을 두어 RFID 시스템에서 필요한 보안 요구사항들을 충분히 만족시키지 못하고 있다. Kill 및 Access 패스워드를 이용하여 태그 기능을 영구 정지시키거나 태그의 특정 메모리 영역 쓰기 기능을 제한(Lock)하여 고객 프라이버시 보호 및 안전성이 향상되었다고 분석하고 있지만, 실제 Gen2 규격은 복제 공격·도청 공격·고객 프라이버시 침해·중간자 공격·서비스 거부 공격 등의 공격에 매우 취약하다. 또한 Gen2 규격의 태그는 기존에 제안된 RFID 보안 기법에서 사용한 대칭키 암호 알고리즘 및 암호학적 해쉬함수가 지원되지 않아, Gen2 규격 기반의 RFID 시스템에 직접 사용하는 것은 불가능하다.

이에 Ari Juels는 Gen2 규격에서 명시하고 있는 Kill 및 Access 패스워드를 이용한 태그-리더 간의 인증 기법을 제안하여 복제 공격을 방지하고자 하였다[2]. 하지만 이 기법 역시 도청 공격 등에 취약하다는 문제점이 있다. 따라서 Gen2 규격 기반 RFID 시스템의 성공적인 산업화를 위해 Gen2 규격이 내재한 보안 취약성의 해결방안 모색이 우선 과제가 되고 있다.

본 논문에서는 Gen2 규격에 명시되어 있는 태그-리더 간의 Air-Interface에서 나타날 수 있는 보안 취약성을 살펴본다. 특히, 리더가 태그를 식별한 후 태그의 메모리 뱅크 접근을 하는 과정에서 도청 공격 및 규격의 허점을 이용함으로써 발생할 수 있는 보안 취약성 그리고 악의적인 목적으로 획득한 EPC 코드를 이용한 태그 복제에 대해서 중점적으로 알아볼 것이다. 그리고 지금까지 제안된 Gen2 규격 기반의 보안 기법과 그 문제점에 대해서 알아보고, 앞으로 Gen2 규격 기반의 보안 기법 연구가 나아가야할 방향을 제시한다.

본 논문의 2장에서는 Gen2 규격에 대한 일반적인 소개하도록 한다. 3장에서는 Gen2 규격이 내재하고 있는 보안 취약성에 대해서 알아본다. 4장에서 Ari Juels에 의해 처음으로 제안된 Gen2 규격 기반의 보안기법을 조사하고, 제안 기법의 보안 취약성 및 구현 시 고려사항에 대해서 분석한다. 끝으로 5장에서 결론 및 향후 연구 방향을 제시한다.

2. EPC 클래스-1 Generation-2 UHF-RFID(Gen2) 규격 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 사용자 중심의 EPCglobal 네트워크 표준을 개발/보급함으로써 공급체인을 이동하는 상품의 가시성을 높여 기업의 효

율성 제고에 이바지함을 목적으로 하고 있다. EPCglobal은 작년 12월 UHF 대역의 태그-리더 간 통신 프로토콜 버전 2인 Gen2 규격을 제정하였다. 초창기 개발되었던 버전 1(Gen1)과는 기능 및 성능 면에서 크게 개선되었기 때문에 2세대(Gen2)라는 별칭이 붙게 되었다. 다음 표를 통해 Gen1과 Gen2의 차이점에 대해서 알아보자.

비교 항목	Gen1		Gen2
표준	Class-0 및 Class-1, 18000-6A 및 18000-6B로 총 네 개의 UHF 표준 존재		단일 국제 표준 프로토콜
리더 모드	Single-reader mode		Single-reader mode, Multi-reader mode, Dense-reader mode
세션	무		유
태그 메모리	클래스-0	칩 생산 시 프로그램 됨	필드에서 프로그램 가능
	클래스-1	사용자 프로그램 가능	
데이터 전송 속도	클래스-0	80kb/s	640kb/s
	클래스-1	140kb/s	
패스워드 길이	클래스-0	24비트	32비트
	클래스-1	8비트	

<표 1> Gen1 및 Gen2 규격 비교

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 ISO(International Organization for Standardization)가 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 규격에서 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 태그

를 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 향상된 고객 프라이버시 및 보안을 기대할 수 있다. 표에서 보는 것과 같이 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.

3. Gen2 규격의 보안 취약성 및 해결방안

본 장에서는 Gen2 규격의 RFID 시스템에서 나타날 수 있는 보안 취약성을 살펴본다. 앞에서 언급했듯이 Gen2 규격의 RFID 태그에서는 기존 RFID 정보보호 기법에서 사용하고 있는 암호학적 알고리즘 및 함수들을 구현하는 것이 불가능하여, 기존 기법을 Gen2 기반의 RFID 시스템에 사용하는 것은 불가능하다. 기존 기법들을 살펴보면, Weis 등은 프라이버시 보호를 위한 인증 기법을 제안하였고[6,7], Ohkubo 등은 암호학적 해쉬함수를 이용하여 태그의 EPC 코드를 리더가 태그를 식별할 때마다 변경시킴으로써 태그 추적 문제를 해결하고자 하였다[9]. 하지만 언급된 기법들은 Gen2 규격에는 적합하지 않은 암호학적 해쉬함수를 필요로 하기 때문에 실제 Gen2 기반의 RFID 시스템에서는 사용할 수 없다. [8]에서는 RFID 시스템에 사용하기 적합한 AES 대칭키 암호 알고리즘을 제안하였지만, 이 역시 클래스-1 EPC 태그에서 사용하기에는 계산 량이 많으며, Gen2 규격에서는 지원하지 않고 있다.

이와 같이 일반적인 RFID 보안 기법들에서 사용되어온 암호학적 해쉬함수, 대칭키 암호 알고리즘 등이 Gen2 규격에서는 지원되지 않기 때문에 Gen2 규격 기반의 RFID 시스템에서는 여러 가지 보안 취약성이 발견될 수 있다. 이미 [2]에서 Gen2 규격이 태그-리더 간의 상호 인증 메커니즘 부재로 인해 복제 공격에 취약하다는 것이 밝혀졌다. 상호 인증 기법 부재로 인해 복제 및 도청 공격 이외에도 중간자 공격 및 서비스 거부 공격이 가능하다. 또한 태그의 EPC 코드가 식별 이후 불변하기 때문에 고객 위치 추적과 같은 고객 프라이버시 침해를 야기할 수 있다. 그럼 Gen2 규격에서 나타날 수 있는 보안 취약성과 그 해결방안에 대해서 자세히 알아보도록 하자.

3.1 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.

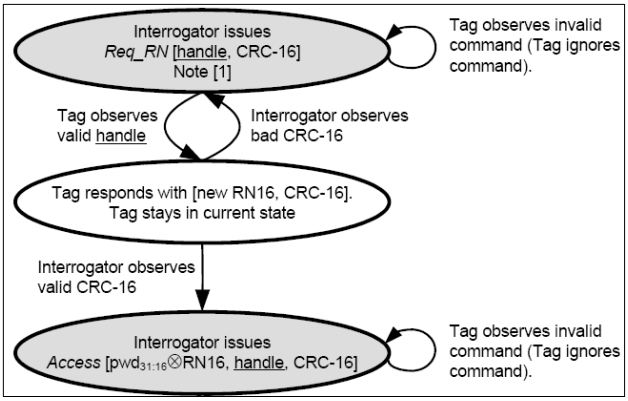
이를 해결하기 위해 Ari Juels는 Gen2 규격 상의 패스워드를 이용하여 복제 태그를 탐지하는 기법을 제안하였다[2]. 리더가 태그의 진위 여부를 Kill 패스워드를 이용한 태그 인증을 통해 확인함으로써, 리더는 태그의 복제 여부를 확인할 수 있다.

3.2 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 16비트를 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.

이는 태그-리더 간에 교환되는 메시지를 암호화함으로써 해결할 수 있다. Gen2 규격의 태그는 암호학적 해쉬함수 및 대칭키 암호화 알고리즘을 지원하지 않기 때문에, Gen2 규격에 명시된 PRNG(Pseudo Random Number Generator)와 태그-리더 간에 공유된 Seed 값을 이용하여 메시지 암호화를 수행한다. 태그 T_x와 리더 사이의 통신을 위해, T_x와 신뢰개체 E는 세션키 $PRN_i^x = PRNG(PRN_{i-1}^x)$을 계산한다($x \geq 1$, $y \geq 1$, $i > 1$, $PRN_1^x = Seed_x$). 여기서, $Seed_x$은 T_x의 Seed 값을 의미하며, 태그가 실제 필드에 배치되기 전에 E와 공유된다. 또한, E는 일반적으로 RFID 시스템에서 백-앤드 서버를 의미하며, 태그 및 리더에 관

한 모든 정보를 가지고 있으며 리더와 안전한 통신 채널을 통해 연결되어 있다. 리더는 T_x와의 통신을 위해 E에게 PRN_i^x을 요청하며, 해당 세션키는 안전한 통신 채널을 통해 리더에게 전송된다. 리더와 T_x은 세션키를 이용하여 보내고자 하는 메시지 M을 $M \otimes PRN_i$을 통해 암호화한다. 해당 세션키 PRN_i^x는 사용 후, 다음 통신 세션의 메시지 암호화를 위해 PRN_{i+1}^x로 업데이트된다. 하지만 이 방안은 동일 세션키 생성을 위해 태그와 서버 간의 완벽한 동기화가 유지되어야 한다는 문제점이 존재한다.



<그림 1> 태그 Access 과정

3.3 프라이버시 침해

Gen2 규격 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.

이는 Gen2 규격에서 명시하고 있는 PRNG을 이용하여 태그 및 신뢰개체가 해당 태그의 식별 정보를 EPC와 가명(Pseudonym)의 쌍으로 보유함으로써 해결할 수 있다. 태그는 리더의 EPC 코드 요청에 대해서 가명인 PRN(Pseudo Random Number)으로 응답하고, 리더는 이 PRN값을 신뢰개체에게 전송함으로써 해당 태그에 대한 필요 정보를 얻을 수 있다. 그 후 태그와 신뢰개체는 PRN값을 새로운 가명으로 업데이트한다. 이와 같은 과정을 통해 EPC 코드 불변으로 인한 고객 프라이버시 침해를 방지할 수 있다. 하지만 이 방안 도청 공격 방지 방안과 마찬가지로 동일 PRN 생성을 위해 태그와 서버 간의 완벽한 동기화가 유지되어야 한다는 문제점이 존재한다.

3.4 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.

이는 태그-리더 간의 상호 인증 기법을 사용함으로써 해결될 수 있다. 지금까지 알려진 Gen2 규격 기반의 상호 인증 기법은 [2]에서 제안한 EnhancedTagAuth가 전부이다. 이를 위해서는 태그가 반드시 Access 패스워드를 구현해야 하며, 기법 자체가 도청 공격에 취약하다는 문제점이 있다. 그래서 앞 절에서 언급한 도청 공격 방지 기법과 제안 기법을 함께 사용함으로써 태그-리더 간의 상호 인증을 제공할 수 있다. 이를 통해 중간자 공격 및 서비스 거부 공격을 방지할 수 있다.

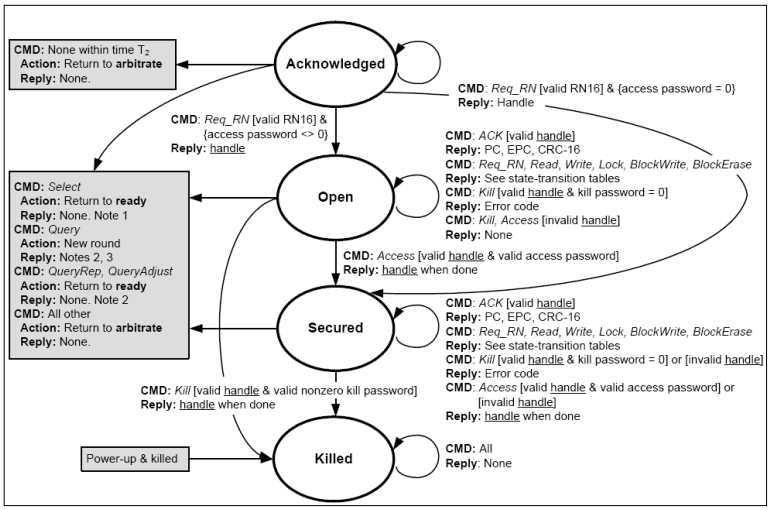
3.5 불법적인 메모리 읽기-쓰기

Gen2 규격에서 명시하고 있는 태그 상태 전이도에 의하면, Gen2 규격 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>은 Gen2 규격의 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 16비트 난수(handle)를 후방 산란하고 Secured 상태로 전이한다. Secured 상태에서 공격자는 Read/Write 등의 명령을 통해 태그의 메모리 뱅크를 읽고 쓰게 된다.

이는 모든 태그로 하여금 Access 패스워드를 구현하도록 하여 Secured 상태로의 전이 이전에 Access 명령을 통한 접근 제어 과정을 거치도록 함으로써 어느 정도 해결될 수 있다. 하지만 이 메커니즘 역시 도청 공격에 취약하기 때문에 앞 절에서 언급한 도청 공격 방지 기법과 함께 사용되어야 한다. 하지만 Access 패스워드의 구현은 Gen2 규격에서 필수 사항이 아니므로 RFID 태그 제조업체는 가격 문제로 인해 강제성이 없다면 Access 패스워드를

구현하려고 하지 않을 것이다. 따라서 Access 패스워드에 대한 표준 개정이 동반되어야 한다.



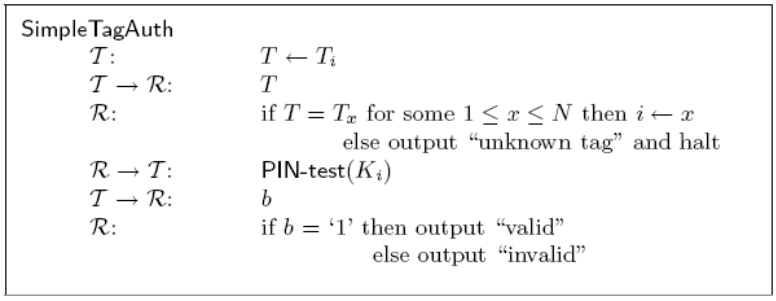
<그림 2> EPC Gen2 태그의 상태 전이도

4. Juels의 패스워드 기반의 인증 기법

본 장에서는 Gen2 규격의 보안 취약성 중 하나인 복제 공격 방지를 위해 Ari Juels가 제안한 패스워드 기반의 인증 기법을 알아본다[2]. 제안 기법에서 태그는 Basic EPC 태그와 Enhanced EPC 태그로 분류되며, 전자는 Kill 패스워드가 후자는 Kill 및 Access 패스워드가 구현되어 있는 EPC 태그를 의미한다. 리더(또는 신뢰개체)는 모든 EPC 태그의 Kill/Access 패스워드를 보유하고 있으며, 인증을 위해 사용되는 (메타) 명령인 PIN-test(·)가 구현되어 있다고 가정한다. 그리고 EPC 태그는 PIN-test 명령에 대한 응답을 하도록 구현되어 있다고 가정한다.

4.1 SimpleTagAuth 기법

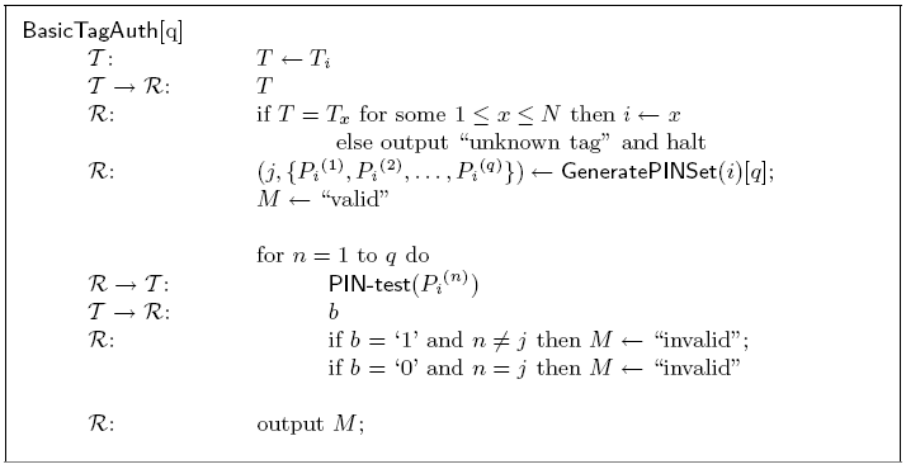
리더가 복제 태그 탐지를 위해 Basic EPC 태그를 인증하는 기법이다. 리더가 PIN-test를 통해 정당한 Kill 패스워드를 태그에게 전송하고, 태그는 전송 받은 Kill 패스워드를 자신의 것과 비교하여 일치 여부를 리더에게 알림으로써 태그 인증을 수행하게 된다. <그림 3>을 통해 SimpleTagAuth 기법의 진행 과정 및 교환되는 메시지를 확인할 수 있다.



<그림 3> SimpleTagAuth 프로토콜

4.2 BasicTagAuth 기법

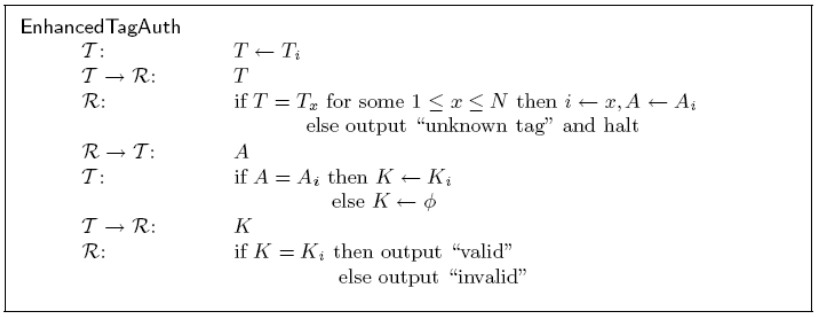
Gen2 규격과 비호환인 복제 태그의 경우, SimpleTagAuth 기법을 이용한 태그 인증이 불가능하다. 즉, 리더의 PIN-test 명령에 대해서 태그는 정당한 Kill 패스워드라고 응답할 수 있다. 이를 해결하기 위해 리더는 GeneratePINSet 함수를 통해 임의의 허위 Kill 패스워드 집합을 생성하고, 이 집합에 실제 정당한 Kill 패스워드를 임의의 위치에 위치시킨다. 리더는 집합 내의 Kill 패스워드에 대해서 PIN-test 명령을 수행하고, 정당한 Kill 패스워드에 대해서 태그가 정확하게 응답했을 때만 태그를 정당한 태그로 인증하게 된다. <그림 4>을 통해 BasicTagAuth 기법의 진행 과정 및 교환되는 메시지를 확인할 수 있다.



<그림 4> BasicTagAuth 프로토콜

4.3 EnhancedTagAuth 기법

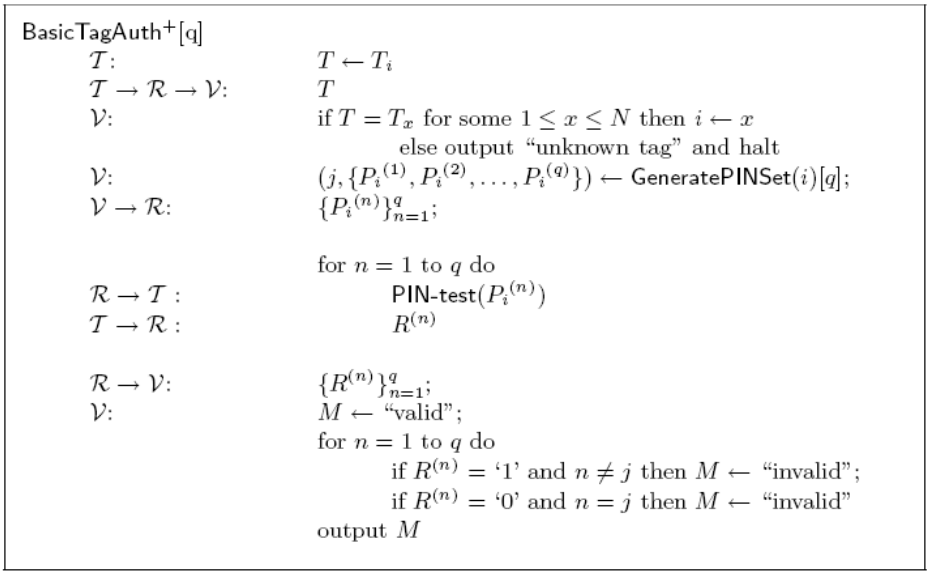
Enhanced EPC 태그에 대해서 Kill 및 Access 패스워드를 이용하여 태그-리더 간의 상호 인증을 수행하는 기법이다. 이 기법에서 Access 패스워드는 태그가 리더를 인증하는데 Kill 패스워드는 리더가 태그를 인증하는데 사용된다. <그림 5>을 통해 EnhancedTagAuth 기법의 진행 과정 및 교환되는 메시지를 확인할 수 있다.



<그림 5> EnhancedTagAuth 프로토콜

4.4 BasicTagAuth+ 기법

리더를 신뢰할 수 경우에 신뢰개체가 EPC 태그 인증을 수행하는 기법이다. 신뢰개체는 BasicTagAuth 기법에 있었던 태그 인증을 위한 임의의 허위 Kill 패스워드 생성, 태그 응답에 대한 평가와 같은 모든 절차를 수행한다. 이 기법에서 리더는 일종의 통신 매개체 역할만을 수행한다. 이 기법은 리더가 쉽게 공격자의 공격을 받는 경우에 유용하다. 일반적으로 리더는 태그의 Kill 패스워드를 자유롭게 접근할 수 있으며, 만약 공격자가 리더를 공격하여 EPC 태그의 Kill 패스워드를 획득할 수 있다면, 완벽한 태그 복제 공격을 수행할 수 있다. 따라서 이 기법에서는 각 리더의 Kill 패스워드에 대한 소유 또는 접근을 원천적으로 불가함으로써 이 문제를 해결하였다. <그림 6>을 통해 BasicTagAuth+ 기법의 진행 과정 및 교환되는 메시지를 확인할 수 있다.



<그림 6> BasicTagAuth+ 프로토콜

4.5 제안 기법의 보안 취약성

앞에서 언급한 기법들은 태그의 복제 방지를 위한 기법들이다. 하지만 EPC 태그의 극심한 자원 제약 사항으로 인해 제안 기법은 복제 공격 이외의 공격에 대해서 취약하다. 각 제안 기법들에서 나타날 수 있는 보안 취약성을 알아보도록 한다.

- SimpleTagAuth 기법에 대한 스푸핑(Spoofing) 공격: Gen2 규격 비호환인 태그는 리더가 PIN-test 명령을 통해 전송하는 모든 PIN에 대해서 태그 자신이 가지고 있는 값과 일치한다고 응답하여 리더를 속일 수 있다. 이는 BasicTagAuth 기법을 통해 해결될 수 있다.
- BasicTagAuth 기법에 대한 도청 공격: 공격자가 특정 태그의 EPC 코드를 획득한 후, 정당한 리더를 도청하면서 허위로 생성된 패스워드 집합을 얻어낼 수 있다. 공격자는 도청 공격을 통해 획득한 패스워드 집합을 복제 태그에 대해서 테스트함으로써 해당 태그에 적합한 Kill 패스워드 값을 알아낼 수 있다.
- EnhancedTagAuth 기법에 대한 도청 공격: 태그-리더 간의 상호 인증을 위해 해당 태그의 Kill 및 Access 패스워드가 평문의 형태로 공격자에게 노출된다. 공격자는 쉽게 Kill 및 Access 패스워드를 획득할 수 있으며, 이를 통해 태그를 완벽하게 복제하거나 악의적으로 태그의 동작을 정지(Kill)할 수 있다. 또한, 획득한 Access 패스워드를 통해 태그의 메모리 뱅크에 접근하여 임의로 EPC, TID 등을 수정함으로써 RFID 시스템의 장애를 초래할 수 있다.
- BasicTagAuth/BasicTagAuth+ 기법에서 리더는 무작위로 생성된 패스워드 집합에 포함된 모든 패스워드를 한 태그에 대해서 테스트해야하기 때문에 태그 및 리더 측면에서 시간 및 자원을 낭비하게 된다.

앞에서 언급한 복제 방지 기법은 복제 공격은 어느 정도 방지할 수 있으나, 기법 자체가 도청 공격에 취약하여 Kill 및 Access 패스워드 값들을 공격자가 쉽게 획득할 수 있어 더욱 심각한 태그 복제 문제를 야기할 수 있다. 태그가 보유하고 있는 패스워드 값을 검증하기 위해 사용되는 PIN-test 명령 역시 Gen2 규격에서 명시하고 있는 다른 명령들과 유사한 형태의 명령이기 때문에, 공격자는 리더가 보내는 PIN-test 명령을 도청함으로써 명령과 함께 전달되는 패스워드 값을 획득할 수 있다. 또한 완벽하지 않은 상호 인증 기법으로 인해 중간자 공격 및 서비스 거부 공격에 무방비한 상태이다.

이를 해결하기 위해 앞 장에서 언급한 도청 공격 방지 기법을 사용함으로써 제안 기법의 도청 공격에 대한 보안 취약성을 어느 정도 해결할 수 있다. 또한 EnhancedTagAuth와 도

청 공격 방지 기법의 조합을 통해 태그-리더 간의 상호 인증을 제공할 수 있으므로 중간자 공격 및 서비스 거부 공격을 방지할 수 있다.

4.6 제안 기법 구현 시 고려 사항

제안 기법을 실제 RFID 시스템에서 사용하기 위해서는 Gen2 규격에서 명시하고 있는 규격에서 기법과 관련된 사항을 수정해야 한다. 규격 수정으로 인해 가장 큰 영향을 받는 것은 태그이다. 인증 기법 수행에 필요한 명령 및 검증 프로시저를 구현하는 것은 태그 가격의 상승을 의미한다. 태그 가격 상승은 RFID 시스템의 보급 및 상용화 정도와 매우 밀접한 관계가 있어 기법 제안 시 최우선적으로 고려되어야할 사항이다. 제안 기법 구현에 있어 고려해야할 사항은 다음과 같다:

- 태그 및 리더는 특정 명령에 포함된 Kill 패스워드의 유효성 검증을 위해 Gen2 규격에서 정의하지 않은 유효성 검증 프로시저를 추가해야 한다. 이때, 태그의 응답 메시지에는 검증 결과를 전송하기 위한 1-비트가 추가되어야 한다.
- Kill 명령을 이용한 Kill 패스워드 검증을 위해 태그가 정당한 Kill 명령에 대해 태그 자신을 정지시키기에 불충분한 전력을 보유하도록 해야 한다.

위에서 언급한 제안 기법 구현의 고려 사항들은 RFID 시스템의 호환성과 직접적으로 연관된 문제이기 때문에 반드시 고려되어야 한다. 또한 제안 기법에 대한 표준화 작업이 진행되어 표준 호환성 문제를 해결할 수 있어야 한다. 따라서 앞으로 제안될 보안 기법들은 규격에서 명시하고 있는 명령, 메시지 포맷 등을 최대한 준수하면서 개발 대상인 RFID 시스템의 보안 요구사항들을 만족시킬 수 있어야 한다.

5. 결론 및 향후 연구과제

차세대 IT혁명을 이끌 기술로 평가되는 RFID 태그의 글로벌 표준이 EPC 클래스-1 Generation-2 UHF-RFID 규격을 토대로 한 `ISO18000-6 타입 C'로 사실상 확정됨에 따라 해당 규격의 보안 취약성 및 이를 극복하기 위한 보안 기법에 관한 연구가 활발하게 진행될 것으로 예상된다.

본 논문에서는 지금까지 연구된 Gen2 규격이 내재한 복제 공격의 취약성에 대해서 알아보았다. 이를 해결하기 위한 Ari Juels의 기법에 대해서 조사하고, 해당 기법의 보안 취약성 및 구현 시 고려 사항에 대해서 알아보았다. 즉, Ari Juels의 기법은 도청 공격 등에 취약하

며 안전하지 않은 인증 기법으로 인해 더 큰 복제 공격을 야기할 수 있는 문제점을 내재하고 있다는 것을 알 수 있었다. 또한 실제 Gen2 규격 기반의 RFID 시스템 개발 및 구현 시, 규격에서 명시하고 있는 것 이외의 추가적인 명령이 구현되어야 하고, 메시지 포맷이 변경되어야 하기 때문에 현실성과 호환성에 있어 문제가 발생할 수 있다.

복제 공격 이외에도 프라이버시 침해, 중간자 공격, 서비스 거부 공격, 불법적인 메모리 읽기/쓰기와 같은 보안 취약성이 Gen2 규격에 내재되어 있음을 확인할 수 있었으며, 각각에 대한 해결 방안을 간략하게 알아보았다. 본 논문에서 제시한 해결 방안은 리더-신뢰개체 간의 추가적인 메시지 교환이 필요하지만 이는 Gen2 규격과는 무관하며, 태그의 경우 Gen2 규격에 명시된 바를 최대한 준수하였기 때문에 현실성이 있는 접근법이라고 판단된다.

따라서 Gen2 환경에서의 RFID 정보보호에 대한 핵심 연구과제 중 하나는 규격에서 명시하고 있는 사항들을 최대한 준수하면서 저비용으로 필요한 보안 요구사항들을 충족하는 RFID 시스템을 개발하는 것이다. 즉, 제안 보안 기법이 Gen2 규격을 준수하는 대부분의 RFID 시스템에서 호환성의 문제없이 유연성 있게 사용될 수 있는 것이 중요하다. 이와 동시에 제안 보안 기법은 Gen2 규격에서 나타난 복제 공격, 도청 공격, 고객 프라이버시 침해, 중간자 공격, 서비스 거부 공격 등과 같은 보안 취약성을 해결할 수 있어야 한다. 앞으로 이와 같은 요구사항들을 만족하는 Gen2 규격에 적합한 보안 기법에 대한 연구가 활발하게 진행될 전망이다. 그리고 Gen2 규격에 메시지 암호화, 태그-리더 간의 상호 인증 등과 같은 보안 메커니즘을 포함하기 위한 표준화 활동이 활발하게 진행되어야 한다.

[참고문헌]

[1] 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

[2] A. Juels, "Strengthening EPC Tags Against Cloning" , In submission, Available at http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/

[3] EPCglobal, Inc., http://www.epcglobalinc.org/

[4] RFID 산업 활성화 지원센터, http://www.rfidepc.or.kr/

[5] Mark Roberti, "Understanding the EPC Gen 2 Protocol", RFID Journal Special Report, Mar. 28, 2005

[6] S. E. Sarma, S. A. Weis, and D. W. Engels, "Radio-frequency-identification security risks and challenges", RSA Laboratories, CryptoBytes, 6(1), 2003

[7] S. A. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems", In First International Conference on

Security in Pervasive Computing, 2003

[8] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm", Cryptographic Hardware and Embedded Systems (CHES), p.357-370, Springer-Verlag, 2004, LNCS no.3156

[9] S. Kinoshita, F. Hoshino, T. Komuko, A. Fujimura and M. Ohkubo, “Nonidentifiable Anonymous-ID Scheme for RFID Privacy Protection”, Proc. of CSS 2003 pp.497-502, IPSJ, 2003 Oct. (in Japanese)

[10] 양정규, 김광조, 표철식, "저가의 RFID에 관한 정보보호 기법연구", 2004년도 한국정보보호학회 하계정보보호학술대회, Vol.14, No.1, pp.605-609, 2004.6.24~26, 경동대학교, 속초