EPC Class1과 C1G2 보안성 분석

김건우
한국전자통신연구원
wootopian@etri.re.kr

Analysis about EPC Class 1 and C1G2 Security

Keonwoo Kim
Electronics and Telecommunications Research Institute

요 약

최근들어 Radio Frequency Identification (RFID) 태그가 다수의 상품에 부착되고 여러 분야에 적용되기 시작했지만, 비용문제로 인해 인증이나 암호화 같은 보안기능은 고려하지 않고 있다. 보안 기능이 없는 RFID 시스템은 개인정보 노출, 불법 리더의 접근, 위조 태그의 남용과 같은 심각한 부작용을 초래하지만 현 단계에서는 보안기능을 적용하기가 쉽지않다. 여러 기술을 따르는 수동형 태그중 EPCglobal의 EPC Class 1과 Class 1 Generation 2(C1G2)는 산업계의 여러 분야에서 특히, supply-chain 모델에서 사실상 국제표준으로 여겨진다. EPC Class1 수준의 태그는 자체 밧데리를 가지지 않는 수동형 태그이고, 암호 프리미티브를 적용한 알고리즘이나 프로토콜은 제공하지 않는다. EPC Class1 과 EPC C1G2의 유일한 보안 대책으로는 태그를 영원히 동작하지 못하게 하는 Kill 기능이 있다. Kill을 수행한 태그는 RFID 태그로서의 의미가 사라진다. 본 논문에서는 Kill 기능에 대한 EPC Class1 시스템의 취약성을 보이고 또한, EPC C1G2 시스템에서 Kill 관점에서의 보안성을 분석한다.

1. 서 론

최근에 항만, 물류, 유통 등의 여러 분야에서 RFID가 적용되기 시작하고, 우리나라에서는 이동통신 시스템과 결합한 mobile RFID 서비스를 준비하고 있다. 아직까지는 능동형 RFID 보다 수동형 RFID를 적용한 분야가 많고 RFID 태그의 범용적인 사용을 위해서는 수동형 태그의 수요가 많을 것으로 예상된다 [1].

수동형 태그는 리더로부터 신호를 받아서 필요한 전력을 공급받고 리더의 명령에 응답한다. 하지만, 제한된 메모리 공간, 적은 게이트 수, 프로토콜 구동에 필요한 전력의 제한 등으로 강한 암호 프리미티브나 보안 요구사항을 만족시키기 어렵다. 즉, 안전한 리더-태그간 통신을 위한 프로토콜 설계에서 전자서명이나 공개키 기반 암호 뿐만 아니라 해쉬나 대칭키 기반 암호까지도 수동형 태그에 구현하기가 어렵다. 하지만, 인증, 접근제어, 데이터 암호화와 같은 보안 기능을 제공하지 않은 RFID 시스템에서는 태그 소유자의 위치추적, 프라이버시 보호, 태그 복제, 허가받지 않은 리더의 불법접근 등을 근본적으로 방지하기가 거의 불가능하다. 이런 기능이 수행되기 위해서는 산술 및 논리적 연산을 하는 마이크로칩과 대용량 메모리가 태그에 내장되어야 한다.

여러가지 기능을 수행할 수 있는 태그와 그 제작 비용과의 상관관계가 있어, 우리는 현재 널리 사용되는 수동형 태그에 연구의 초점을 맞춘다. 이 논문에서 우리는 여러 가지 타입의 수동형 태그 중 특히 EPC 태그의 보안성에 관하여 분석할 것이다.

RFID 사용을 위해 EPC 코드를 개발하고 산업계 위주의 표준화을 주도하는 EPCglobal[2]은 수동형 태그와 관련 RFID 시스템을 위해 860MHz ~ 930 MHz Class 1 RFID 태그와 태그-리더 간의 통신 인터페이스를 개발했다 [3]. 또한, 최근에는 Class1의 진화된 버전으로서 Class1과 동일한 주파수 대역에서 UHF RFID 프로토콜을 적용한 C1G2 태그[4]를 상용화하기 시작했다.

EPC 태그는 수동형이고 암호 프리미티브를 적용한 보안기능은 제공하지 않는다. 태그의 기능을 정지시켜 태그로서의 기능을 더 이상 없게하는 Kill 기능이 현재로서는 유일한 보안 기능이라고 할 수 있다. 그래서, EPC 시스템의 보안성을 살펴보기 위해서는 Kill 기능에 관한 면밀한 분석이 필요하다.

본 논문은 다음과 같이 구성된다. 2장에서는 RFID 시스템과 EPCglobal 시스템에 관하여 간략히 살펴본다. 3장에서 EPC Class1 시스템에서 Kill 기능에 대한 취약성을 살펴보고, 4장에서는 EPC C1G2 태그를 Kill 하기 위한 과정을 도출하고 EPC C1G2 보안성을 분석한다. 마지막으로 5장에서 결론을 내린다.

2. RFID와 EPCglobal 시스템

RFID 시스템은 태그, 리더, 백엔드 데이터베이스, 그리고 다른 부가적인 시스템으로 구성된다

리더는 Transceiver 혹은 Interrogator 라고도 하며, RF

인터페이스를 통하여 태그에 데이터를 보내거나 태그로부터 데이터를 읽는 장치이다. 리더는 태그와의 물리적인 접촉없이 다른 태그와의 충돌을 피하여 태그로부터 고유의 식별코드를 인식할 수 있어야 하고 태그에 정보를 기록할 수 있어야 한다. 또한, 태그의 로깅 정보나 암호키와 같은 데이터를 저장하는 백앤드 데이터베이스와 연결될 수 있다.

Transponder라고도 불리는 태그는 프로토콜 수행과 암호연산 등을 수행하기 위한 프로세서, 데이터를 저장하는 메모리, 그리고 RF 안테나로 구성된다. 태그는 각각 고유의 식별수단인 ID를 가지고 있고, RF 동작 범위 내에서 리더에게 ID를 전송한다. 태그는 두가지 종류가 있는데, 자체 밧데리를 내장한 능동형 태그와 자체 밧데리를 내장하지 않는 수동형 태그가 그것이다. 수동형 태그는 리더로부터 RF 신호를 받아서 태그 동작에 필요한 전력을 공급받는데, 능동형 태그에 비해 비싸지 않게 제조가 가능하고 현재 많은 응용분야에서 사용된다. 한편, 태그의 제한된 전력으로 인하여 태그-리더 사이의 하향 채널 통신거리는 리더-태그 사의의 상향 채널 통신거리 보다 훨씬 짧다. 또한, 수동형 태그에 tamper-resistant 메모리를 적용하기에는 비용이 많이 들어 태그 내부 데이터가 차분전력 공격, EM 공격과 같은 물리적 공격에 의하여 쉽게 노출될 수 있다.

RFID 시스템을 구성하는 요소로서 태그, 리더 외에 리더와 연결된 정보 서버, 미들웨어 시스템, 추적 관리 개체 등이 있다.

한편, EPCglobal은 supply-chain 모델에서 태그 정보의 실시간, 자동식별을 위한 국제 표준을 사실상 주도하는 기관으로, EPCglobal 네트워크를 구성하고 지원한다. EPCglobal 네트워크는 다음과 같은 요소로 구성된다[2].

- EPC(Electronic Product Code)
  - 각각의 태그를 식별하는 고유의 식별번호
  - 여러 코드 체계 중 태그 식별을 위한 사실상 표준
- ID System
  - EPC 태그와 EPC 리더로 구성
  - EPC는 EPC 태그에 저장되고, EPC 태그는 케이스, 팔레트, 컨테이너 등의 아이템에 부착됨
  - EPC 리더는 EPC Middleware를 사용하여 정보를 관리하고 EPC 태그와 통신
- EPC Middleware
  - EPC IS와의 통신을 위해서 실시간 read 이벤트와 정보를 관리하고 alert를 제공하며, EPC 리더와의 통신을 위해 기본적인 read 정보를 관리함
- EPC IS(EPC Information Service or Server)
  - EPC와 관련된 데이터를 EPCglobal 네트워트를 통하여 상대방과 교환가능하도록 하는 서비스
- EPC Discovery Service
  - 특정 EPC와 관련된 데이터를 찾을수 있게하고 그 데이터에 접근을 요청하도록 하는 서비스
  - Object Naming Service (ONS)

본 논문에서는 수동형 리더와 이것의 보안 시스템에 관심이 있기 때문에, EPCglobal의 EPC Class 0~5 중에서 EPC Class 1 과 Class1 Generation2(C1G2)에만 초점을 맞춘다.

3. EPC Class 1 취약성 분석

3장에서는 EPC Class1 태그는 합법적인 리더가 아니더라도 어떠한 리더로부터라도 Kill 명령을 받아서 기능이 정지될수 있음을 보인다.

EPC Class 1 태그는 내부 데이터 또는 저장 정보로서 고유의 식별자인 EPC, 그 식별자에 적용되는 에러 검출 및 정정 코드인 CRC, 그리고, 태그를 Kill 하기 위한 8 비트 Kill 패스워드만을 가진다[3]. 리더와 태그 사이의 통신은 리더가 먼저 태그에게 command를 보냄으로서 시작되고 태그는 리더의 command에 대한 reply 응답만 보낸다.

EPC Class1 시스템에서는 6개의 required command, 즉, *ScrollAllID*, *ScrollID*, *PingID*, *Quiet*, *Talk*, *Kill* command를 반드시 구현해야 하고, *ProgramID*, *VerifyID*, *LockID*, *EraseID* command 등의 identifier programming command 구현은 필수사항은 아니다.

다른 보안기능이 없는 EPC Class 1 시스템에서, 위의 command를 이용하여 공격자가 태그를 Kill 하는 것이 가능하다. required command와 identifier programming commands 중에서, 태그는 *ScrollAllID*, *ScrollID*, *PingID*, 그리고, *VerifyID* command에 해당하는 특정 reply를 보냄으로서 응답한다. 공격자가 특정 태그를 Kill 하기 위해서는 EPC와 패스워드가 필요한데, 이는 *VerifyID* command를 보냄으로서 획득될 수 있다. 그림 1은 공격자에 의해 EPC Class 1 태그를 Kill 하는 과정이다.

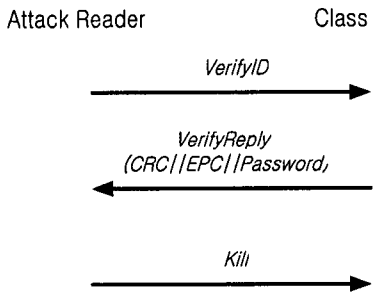

그림 1. EPC Class1 태그를 Kill 하는 절차

① 공격 리더는 태그에게 *VerifyID* command를 보냄으로서 태그 Kill 절차를 시작한다.

② 태그는 공격 리더의 Kill 시도에 *VerifyReply*로 응답한다. *VerifyReply*에는 EPC, CRC, 그리고, Kill 패스워드 정보가 들어있다.

③ 태그로부터 EPC와 Kill 패스워드를 획득한 공격리더는 태그에게 *Kill* command를 보낸다.

리더로부터 *Kill* command를 받은 태그는 영원히 작동이 불가능하다. EPC Class1 태그에 대한 공격은 태그 소유자의 의도와 관계없이 발생할 수 있고 모든 EPC Class1 태그는 항상 Kill 될 가능성이 있기 때문에 아주 심각한 문제이다. 이 공격은 리더와 태그 사이의 인증이나 접근제어 메커니즘 같은 어떠한 보안 인터페이스도 없기 때문에 발생하는데, 이는 EPC Class1 시스템에서는 불법적인 리더라도 태그를 엑세스 할수 있음을 의미한다.

4. EPC C1G2 보안 분석

4장에서는 EPC C1G2의 보안에 관하여 분석한다. C1G2 RFID 프로콜은 Class1보다 진화하고 많은 기능이 보강되었지만 전력, 계산능력 등의 수동형 태그 기준을 맞추기 위해서는 복잡한 보안 프로토콜이 사용되지 않는다. EPC Class1 과 마찬가지로 C1G2는 Kill 기능이 보안 기능으로서 작동한다. EPC C1G2 시스템은 32 비트의 Kill 패스워드를 사용는데, 이는 다시 2개의 16 비트 패스워드로 나뉘어진다 [4].

불법 리더에 의해 C1G2 태그를 Kill 하기 위한 공격은 두번의 연속적인 *Kill* command의 성공을 필요로 한다. 첫번째 *Kill* command에는 32 비트 Kill 패스워드 중 상위 16 비트가 사용되는데, 이 값은 난수 RN16과 EXOR 된값이다. 이때 RN16은 *Kill* command을 보내기 전에 리더가 태그에게 보낸 *Req_RN* command에 대한 태그의 응답이다. 마찬가지로 두번째 *Kill* command에는 32 비트 Kill 패스워드 중 하위 16 비트가 새로운 RN16과 EXOR 된다. 이때의 RN16은 첫번째 *Kill* command를 보내고 두번째 *Kill* command를 보내기 전에 리더가 난수값을 얻기 위해 태그에게 보내는 *Req_RN* command에 대한 태그의 응답이다. 즉, 리더는 보안을 위해 동일한 RN16을 재사용하지 않는다. 그림 2는 EPC C1G2 태그를 Kill 하기 위한 과정을 나타낸 것이다. Kill 하기전에 우선 리더는 inventory 과정을 거쳐 태그를 인식하게 된다. 그리고나서 리더는 Req_Rn → Kill → Req_Rn → Kill 과정을 반복한다.

그림 2에서 알수있듯이, 공격자는 $1/2^{16} \times 1/2^{16} = 1/2^{32}$ 의 확률을 가지고 Kill 패스워드를 추측해서 두번의 *Kill* command를 시도하는데, 이때 백워드 채널에서 RN16을 획득할 수 있다고 가정한다. EPC Class1에서는 공격자가 *VerifyID* command를 보냄으로서 태그의 Kill 패스워드를 획득할 수 있는 방법이 있었으나 C1G2에서는 이것이 불가능하다. 또한, 태그가 두번의 *Kill* command 사이에 *Req_RN* command를 제외한 다른 command를 수신하면 태그를 Kill 하려는 공격은 실패한다. 이것은 EPC Class1 태그와는 달리 불법 리더가 C1G2 태그를 Kill 하는 것은 매우 어렵다는 것을 의미한다.

즉, C1G2 태그에서는 보안을 위한 어떠한 암호학적인 알고리즘이나 프로토콜이 사용되지 않지만, Kill 관점에서는 수동형 태그에 적합한 보안을 제공한다고 보여진다.

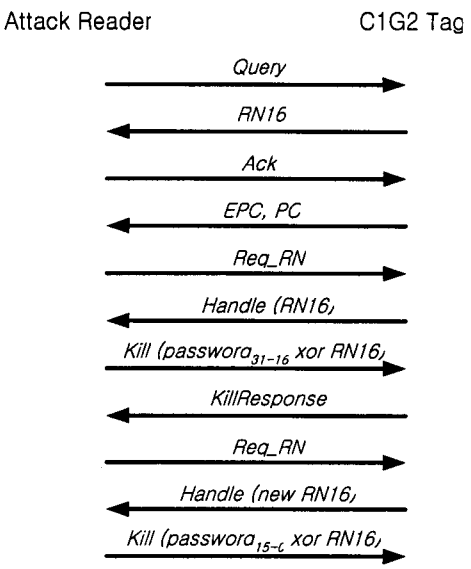

그림 2. EPC C1G2 태그를 Kill 하는 절차

5. 결 론

제한된 태그 리소스로 인하여 Class1 수준의 태그에 강력한 보안 기능을 적용하는 것은 현재로서는 거의 불가능하다. 하지만, Kill을 통해서 EPC 시스템의 최소한의 보안 기능에 관한 분석은 필요하다. 이에 EPC Class1은 어떠한 리더라도 태그 기능을 정지시킬 수 있어서 매우 심각한 문제가 됨을 보였다. 하지만, 불법리더라 하더라도 패스워드를 모르면 EPC C1G2를 Kill하는 것이 매우 어렵다는 것도 보였다.

향후 EPC Class2 이후에는 태그에 Kill 이외의 좀더 향상된 보안기능이 적용되리라 예상된다. 궁극적으로는 보안 프로토콜이 안전하고 신뢰성이 있음을 증명하려면 암호학적인 프리미티브가 사용되어야지만 가능하고 이는 EPC Class4 이상에서 적용되리라 예상된다.

참 고 문 헌

[1] Vince Stanford, " Pervasive Computing Goes the Last Hundred Feet with RFID Systems" , IEEE Pervasive Computing, Vol. 2, No. 2, 2003.

[2] http://www.epcglobalinc.com

[3] EPCglobal, " 860MHz - 930 MHz Class 1 Radio Frequency Identification Tag Radio Fre-quency & Logical Communication Interface Specification" , Technical Report, Candidate Recommendation, Version 1.0.1, 2002.

[4] EPCglobal, " Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz - 960MHz" , Version 1.0.9, 2005.