수동형 RFID 보안태그와 리더의 인증 및 데이터 보호 프로토콜 보안 취약점 분석1)

추상호*, 김성윤*, 김호원*
*부산대학교 컴퓨터공학과
e-mail:sanghochu@gmail.com

Vulnerabilities Analysis for Authentication Protocol of Passive RFID Security Tag

Sangho Chu*, Seongyun Kim*, Howon Kim*
*Dept of Computer Engineering, Pusan National University

요 약

RFID는 태그가 부착된 사물의 정보를 무선통신을 통해 인식하는 기술로써 바코드를 대체하는 등 다양한 영역으로 응용 범위가 확대되고 있다. 따라서 각 응용에 필요한 보안 문제도 중요시 되고 있다.

본 논문에서는 지금까지 RFID시스템의 보안 취약성을 해결하기 위해 제안된 많은 인증 프로토콜들 중 한국정보통신기술협회에서 제정한 잠정표준인 "수동형 RFID 보안태그와 리더의 인증 및 데이터 보호 프로토콜"에 대하여 프라이버시 침해, 위치추적, 비동기화 공격 가능 및 전방향 안전성을 만족하지 못하는 등의 보안 취약점이 있음을 보이고, 이에 대한 분석을 하였다.

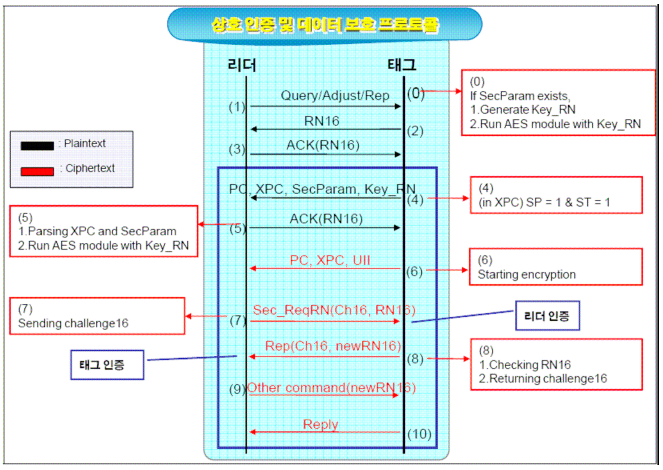
1. 서론

RFID기술은 유비쿼터스 사회의 핵심 기술 중 하나로써 주목 받고 있다. RFID 시스템을 구성하는 요소에는 태그, 리더, 인증서버가 있는데, 이 중 태그-리더 간 통신 시 RF무선 신호를 이용하기 때문에 보안 프로토콜을 적용하지 않을 경우 여러 가지 보안 문제가 생길 수 있다. 이러한 보안 문제들에 대한 해결을 위해 제안된 기존의 프로토콜들 중 본 논문에서 다루고자 하는 것은 한국정보통신기술협회에서 제정한 잠정표준(TTAI.KO-12.0091)인 "수동형 RFID보안태그와 리더의 인증 및 데이터 보호 프로토콜"이다. 이 표준은 수동형 RFID 태그와 리더 간 인증 및 데이터 통신채널 보호를 보장하기 위한 프로토콜 규격으로서, ISO/IEC 18000-6 타입 C 규격의 수동형 RFID 태그에 추가적으로 AES 보안 모듈을 장착시키고, 추가적인 명령/응답 메시지, 메모리맵 정보 및 보안 프로토콜을 정의하여 보안 기능 향상 및 호환성을 제공한다[1].

본 논문에서는 표준에서 기술하고 있는 두 가지 프로토콜들에서 나타나는 보안 문제들에 대한 분석을 하였다.

2. 상호 인증 및 데이터 보호 프로토콜

본 장에서는 [1]의 상호 인증 및 데이터 보호 프로토콜에 대한 설명을 한다. (그림 1)은 프로토콜의 동작을 나타내고 있다.



(그림 1) 상호 인증 및 데이터 보호 프로토콜

2.1 사전 가정 및 특징

상호 인증 및 데이터 보호 프로토콜의 사전 가정 및 그에 따른 특징은 다음과 같다[1].

(1) UII를 암호화하여 전송한다. 따라서 임의의 리더로부터 UII정보를 감출 수 있다.

(2) 태그와 리더는 마스터 키를 서로 알고 있다고 가정한다.

(3) 태그와 리더는 매 inventory과정 마다 세션 키를 유도하여 사용한다고 가정한다.

1) "이 논문 또는 저서는 2010년 교육과학기술부로부터 지원받아 수행된 연구임" (지역거점연구단육성사업/차세대물류IT기술연구사업단)

2.2 프로토콜 단계별 설명

본 프로토콜 절차의 단계별 설명은 다음과 같다[1].

(0) SecParam을 가진 보안태그는 Key_RN을 생성하고, Key_RN과 마스터 키를 이용하여 AES 모듈을 구동시켜 세션 키를 생성한다.

(1) 리더가 태그에게 쿼리 메시지를 전송한다.

(2) 쿼리 메시지를 받은 태그는 랜덤넘버를 회신한다.

(3) 랜덤넘버를 받은 리더는 ACK 메시지를 전송한다.

(4) ACK메시지를 받은 태그는 PC, XPC, SecParam 및 Key_RN을 전송한다.

(5) 리더는 Key_RN과 마스터 키를 이용하여 AES 모듈을 구동시켜 세션 키를 생성한다. 그리고 다시 ACK 명령을 전송한다.

(6) 단계(6) 이후부터는 암호화되어 전송된다. 태그는 PC, XPC, UII를 현재 세션 키로 암호화하여 회신한다.

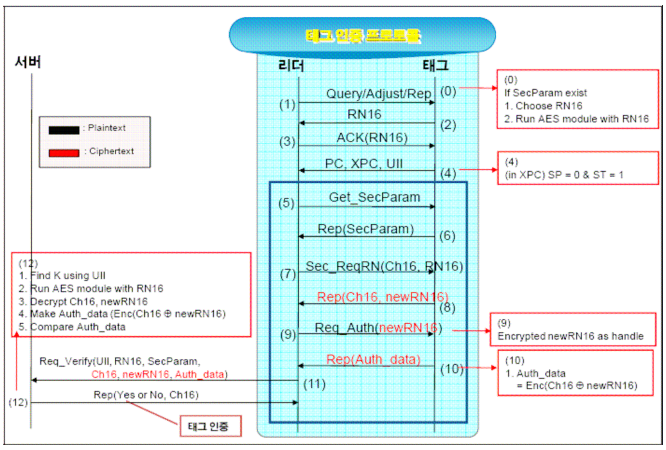
(7) 리더는 상호 인증을 위하여 Challenge로 사용할 랜덤넘버 Ch16을 포함한 Sec_ReqRN 명령을 전송한다.

(8) 태그는 Challenge 랜덤넘버 Ch16과 새로운 랜덤넘버 newRN16을 암호화하여 회신한다.

이후 단계는 사용자 메모리 영역에 대한 읽기/쓰기 동작이다. newRN16을 handle로 사용하며 암호화된 통신을 수행 가능하다.

3. 태그 인증 프로토콜

본 장에서는 [1]의 태그 인증 프로토콜에 대한 설명을 한다. (그림 2)은 태그 인증 프로토콜의 동작을 나타내고 있다.



(그림 2) 태그 인증 프로토콜

3.1 사전 가정 및 특징

본 프로토콜의 사전 가정 및 그에 따른 특징은 다음과 같다[1].

(1) 리더의 inventory 과정은 기존 18000-6C와 동일하다. 즉, UII가 평문으로 전달된다.

(2) 리더는 마스터 키를 알지 못한다. 따라서 양주나 명품의 정품인증 등 리더가 마스터 키를 알 경우 이를 악용할 여지가 있는 진품 확인 서비스와 같은 응용에 적합하다.

(3) 별도로 존재하는 인증서버가 태그의 마스터 키를 알고 있다. 즉 임의의 리더가 인증서버로부터 태그의 인증여부를 확인 받을 수 있다.

3.2 프로토콜 단계별 설명

본 프로토콜 절차의 단계별 설명은 다음과 같다[1].

(0) SecParam을 가진 보안태그는 RN16을 생성하고, RN16과 마스터 키를 이용하여 AES 모듈을 구동시켜 세션 키를 생성한다.

(1) 리더가 태그에게 쿼리 메시지를 전송한다.

(2) 쿼리 메시지를 받은 태그는 랜덤넘버를 회신한다.

(3) 랜덤넘버를 받은 리더는 ACK 메시지를 전송한다.

(4) ACK메시지를 받은 태그는 PC, XPC, UII를 전송한다.

(5) 태그 인증을 수행하려는 리더는 Get_SecParam을 평문으로 전송한다.

(6) 태그는 SecParam을 회신한다.

(7) 리더는 Challenge로 사용할 랜덤넘버 Ch16을 생성하고, 이를 태그에게 전송한다.

(8) 태그는 Challenge 랜덤넘버 Ch16과 새로운 랜덤넘버 newRN16을 암호화하여 회신한다.

(9) 리더는 Auth_data를 얻기 위해 Req_Auth 메시지를 태그에게 전달하는데 이때는 파라미터에 (8)에서 수신한 암호화된 newRN16을 그대로 사용한다.

(10) 태그는 Ch16과 newRN16을 XOR한 값을 암호화하여 Auth_data를 생성한 후 이를 회신한다.

(11) 리더는 인증서버와의 통신을 통해 태그가 보내온 값들을 검증한다. 이 때, 리더와 인증서버 사이의 통신은 안전한 채널을 통해 수행된다고 가정한다.

인증서버는 UII와 관련된 마스터 키를 찾고, RN16과 마스터 키로부터 세션 키를 유도한다. 이후 세션 키를 사용하여 암호화된 Ch16과 newRN16을 복호화 한 후 XOR하여 Auth_data를 구한다. 인증서버가 구한 Auth_data값과 리더로부터 수신한 Auth_data 값을 비교하여 인증 성공, 실패를 판단하여 리더에게 회신한다.

3. 보안 취약점 분석

본 장에서는 [1]의 두 프로토콜에 대한 보안 취약점을 분석한다. <표 1>은 본 논문에서 다루고 있는 [1]과 [2]의 프로토콜들에 대한 보안 취약점을 비교한 것이다.

알려진 취약점 중 하나는, 악의적인 태그가 세션 키 생성을 위해 사용되는 랜덤넘버를 재전송하게 되면 이전 세션과 같은 세션 키 스트림이 사용되는 문제가 있다[1][2]. 이 문제에 대해서는 [2]에서 스푸핑 공격 모델을 세우고 이를 해결 하는 프로토콜을 제시하고 있으므로 자세한 설명은 생략한다. 본 논문에서 다루고자 하는 취약점들은 아래 소단원들에서 설명한다.

<표 1> 프로토콜 보안 취약점 비교

	상호 인증 및 데이터 보호 프로토콜[1]	태그 인증 프로토콜[1]	개선된 상호 인증 및 데이터 보호 프로토콜[2]	개선된 태그 인증 프로토콜[2]
태그인증	O	O	O	O
리더 인증	O	X	O	X
데이터 보호	O	X	O	X
스푸핑 공격 방지	X	X	O	O
프라이버시 보호	O	X	O	X
위치추적 방지	O	X	O	X
비동기화 공격 방지	X	X	X	X
전방향 안전성	X	X	X	X

3.1 태그 소지자의 프라이버시 침해 문제

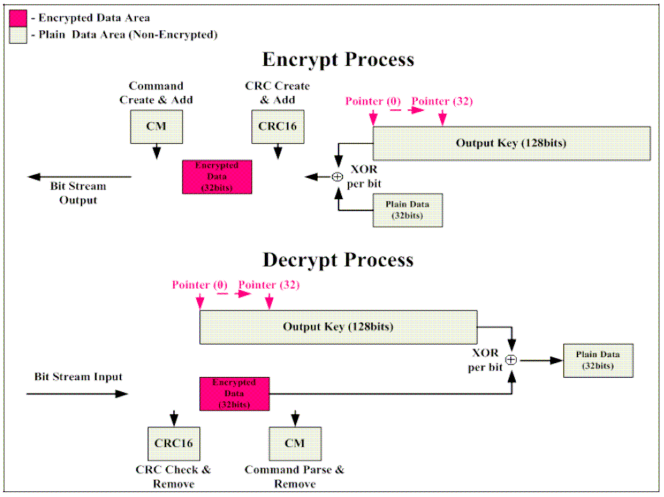
단방향 태그 인증 프로토콜에서 보이는 문제점으로 태그에서 리더로 PC, XPC, UII를 전달하는 과정에서 메시지가 암호화 되지 않으므로, UII값이 노출된다. UII값은 일반적으로 특정 형식이나 국제 규격을 따르므로 노출 될 경우 태그 소지자가 어떠한 물품을 가지고 있는지 등에 대한 프라이버시 침해 문제가 있다. 이러한 문제는 UII를 암호화하여 전달하는 방식으로 해결 할 수 있다. 리더는 태그의 마스터 키를 알지 못하여 UII정보를 알 수 없지만, 태그가 사용한 마스터 키의 index 정보를 SecParam정보로부터 획득하여 인증서버로 알려주게 되면 인증서버에서 복호화 가능하므로 문제가 되지 않는다.

3.2 위치 추적 문제

위치 추적 문제 또한 단방향 태그 인증 프로토콜에서만 보이는 문제점으로 태그는 항상 동일한 UII값을 회신하기 때문에 악의적 리더는 원하는 태그에 주기적으로 쿼리를 전송함으로써 위치를 추적 할 수 있다. 이러한 문제는 UII를 매번 바꿈으로써 해결 할 수 있는데, 본 논문에서는 UII값이 고정된 RFID 시스템이므로, UII값 자체를 바꿀 수는 없고, UII를 암호화하게 되면 매번 다른 세션키를 사용하게 되므로 해결 할 수 있다.

3.3 비동기화 문제

비동기화 문제는 리더가 태그와 마스터 키를 공유하고 있는 프로토콜에서 보이는 문제점이다. 태그나 리더는 암호화된 메시지가 오면 세션 키를 이용해 복호화하고 다음 세션 키를 사용할 준비를 하게 되는데, 만약 악의적 리더나 태그가 아무 메시지나 전송하게 되면 이를 복호화하기 위해 세션 키를 사용하게 되어 정당한 상대방과의 세션 키가 비동기화 되어 더 이상 현재 세션을 유지 할 수 없게 된다. (그림 3)은 본 논문에서 다루는 프로토콜들의 암호화/복호화 방법이다.



(그림 3) 암호화/복호화 방법

암호화나 복호화 후 현재 세션 키의 위치를 알리는 Pointer가 바뀌기 때문으로, 이러한 문제를 해결하기 위한 세션 키 관리 정책이 필요 하다.

3.4 전방향 안전성 문제

전방향 안전성이란, 현재 세션에서 공격자가 원하는 정보(마스터 키 등)를 얻어냈을 때, 이전 세션들에 대한 안전성을 만족하여야 한다는 것이다. 본 논문에서 다루고 있는 프로토콜들은 모두 항상 동일한 마스터키를 사용하기 때문에 전방향 안전성을 만족하지 못한다. 따라서 매 세션마다 마스터 키를 바꿀 수 있는 마스터 키 관리 정책이 필요하다.

4. 결론

본 논문에서는 수동형 RFID 보안태그와 리더의 인증 및 데이터 보호 프로토콜에 관한 국내 잠정표준[1]의 보안 취약점에 대해 분석하였다. 각 취약점들에 대한 해결책 및 개선된 프로토콜에 대한 제시하여 태그 소지자에 대한 프라이버시 보호, 위치추적 방지, 비동기화 공격 방지 및 전방향 안전성을 제공하는 개선된 태그 인증 프로토콜에 대한 연구는 향후 계획으로 남겨둔다.

참고문헌

[1] 정보통신단체표준(잠정표준) TTAI.KO-12.0091, “수동형 RFID 보안태그와 리더의 인증 및 데이터 보호 프로토콜,” 2008년12월.

[2] 양연형, 김선영, 이필중, “개선된 수동형 RFID 보안태그와 리더의 인증 및 데이터 보호 프로토콜,” 정보보호학회논문지, 20(1), pp. 85-94, 2010년2월.