SLRRP 기반의 안전한 RFID 리더 프로토콜 연구

이 현 록*, 서 영 준*, 김 완 식**, 김 광 조*

*한국정보통신대학교, 국제정보보호기술연구소

**케이티주식회사 미래기술연구소 USN 플랫폼 연구부

A Study on Secure RFID Reader Protocol based on SLRRP

Hyunrok Lee*, Youngjoon Seo*, Woan-Sik Kim**, Kwangjo Kim*

*International Research Center for Information Security, ICU.

** USN Research Department, Future Technology Laboratory, KT.

요 약

최근 RFID(Radio Frequency Identification) 기술에 대한 관심의 증대로 해당 기술에 대한 활발한 연구가 수행 중에 있다. 특히 RFID와 리더 사이의 인증프로토콜에 대한 많은 연구들이 선행되었으며, 괄목할만한 연구 성과들이 제시된 상황이다. 하지만 이에 비해 RFID 리더와 서버간의 보안통신을 위한 안전한 RFID 리더 프로토콜에 대한 연구는 매우 부족한 실정이다. 본 논문에서는 대표적인 RFID 리더 프로토콜인 EPCglobal 리더 프로토콜과 IETF SLRRP(Simple Lightweight RFID Reader Protocol)에 대해 소개하고 해당 리더 프로토콜의 문제점을 제시한다. 그리고 리더 프로토콜의 보안요구사항을 만족하는 안전한 SLRRP 기반의 RFID 리더 프로토콜을 제안하였으며, 기존의 프로토콜과의 비교분석을 통해 제안 프로토콜이 SLRRP의 장점을 수용하면서 기존 프로토콜이 가졌던 문제점들은 해결한 것을 보인다.

I. 서론

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 산업 분야로 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, 요즘 징수, 위조지폐방지, 홈 네트워크 등에 유용하게 쓰일 것이다.

하지만 이러한 기술의 발전 이면에는 정보화에 따른 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 암호 기술 개발과 해당 환경에 적합한 종합적인 보안기술 개발이 요구되고 있다. 이를 반영하듯 RFID와 리더 사이의 인증프로토콜에 대한 많은 선행 연구들이 있어 왔으며, 현재까지 프라이버시 보호 및 인증을 위해 Kill, Sleeping, Blocker, 프록시, 해쉬기반, 재암호화, PUF 등을 사용한 기법[1][2][3[4][5][6][7]들과 같은 괄목할만한 많은 연구 성과들이 제시된 상황이다.

하지만 이에 비해 RFID 리더와 서버간의 보안통신을 위한 안전한 RFID 리더 프로토콜에 대한 연구는 매우 부족한 실정이다. 실제 리더 프로토콜의 대표적인 표준인 EPCglobal의 리더 프로토콜 v1.1(이하 EPCRP)[8]과 IETF에서 표준화가 진행 중인 SLRRP(Simple Lightweight RFID Reader Protocol, 이하 SLRRP)[9]는 단순히 HTTPS[10]와 TLS[11]의 사용을 권고하여 보안성을 확보한다고 언급하고 있지만, 리더가 설치되는 다양한 환경과 통신 환경, 계산능력, 하드웨어 등의 특성을 고려하지 않거나 다양한 환경을 고려하더라도 특정 통신 프로토콜 상에서만 보안을 제공하고 있어서 이런 리더 프로토콜에

일련의 인증프로토콜, 키 합의, 메시지 포맷 등의 보안기술을 포함하여 작성된 표준이 절실하다. 본 논문에서는 대표적인 RFID 리더 프로토콜인 EPCRP와 IETF SLRRP에 대해 간략히 소개하고 해당 리더 프로토콜의 문제점을 제시한다. 그리고 리더 프로토콜이 만족해야할 보안요구사항과 기존 프로토콜의 문제점을 해결할 수 있는 안전한 SLRRP 기반의 RFID 리더 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 먼저 Ⅱ장에서는 기존 RFID 리더 프로토콜의 소개와 문제점들을 살펴보고, Ⅲ장에서는 리더 프로토콜의 보안요구사항을 제시하고 안전한 RFID 리더 프로토콜을 제시한다. Ⅳ장에서는 제안프로토콜을 비교분석하고, Ⅴ장에서 본 논문의 결론을 내리도록 한다.

II. RFID 리더 프로토콜

RFID 리더 프로토콜은 리더 기기와 백엔드 서버 사이의 통신 규약으로 본 장에서는 대표적인 RFID 리더 프로토콜인 EPCRP와 SLRRP를 소개하고 해당 프로토콜의 문제점을 도출하며 대략적인 해결방안을 살펴보도록 한다.

1. EPCRP

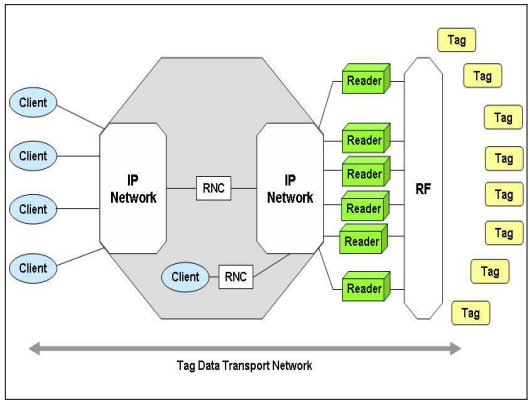
EPCglobal에서는 현재 많은 RFID 시스템에서 국제표준으로 사용되고 있는 EPC 프레임워크와 호환되는 리더 프로토콜의 표준을 정의하였다. 해당 표준은 모든 RF 프로토콜과 리더의 지원하도록 작성되었으며, 바코드와 같은 다른 형식을 가진 태그도 표준의 범위에 포함 시켰다. 해당 프로토콜은 아래와 같이 리더, 메시징, 트랜스포트 레이어의 세 부분으로 나누어 기술되어 있다.

- ⊙리더 레이어 : 리더 프로토콜의 핵심이라 할 수 있는 부분으로 리더와 호스트 사이에 교환되는 메시지의 추상문법과 내용이 기술되어 있다.
- ⊙메세징 레이어 : 리더 레이어상의 메시지가 어떻게 정의되며, 형식과 프레임에 대한 정의, 트랜스포트 레이어로 어떻게 전송되어지는가에 대한 것이 자세히 기술되어 있다.
- ⊙트랜스포트 레이어 : 리더 운영체제에서 지원되는 통신장치에 대응되는 레이어에 대한 표준이 정리되어 있다.

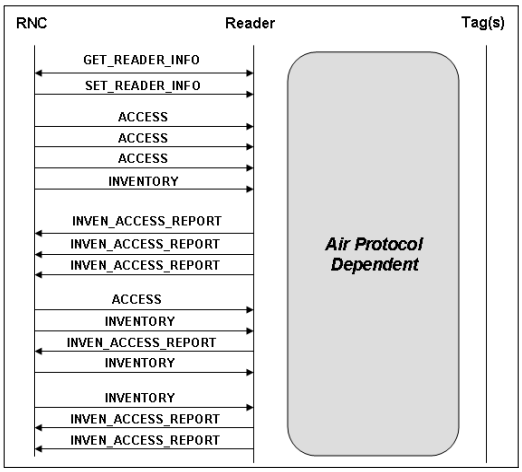
또한 EPCRP 표준은 메시징과 트랜스포트 레이어 사이의 바인딩(Messaging/Transport Binding, MTB)을 제공하여 TCP, Bluetooth, 시리얼 통신과 같은 다양한 통신채널을 리더에서 지원할 수 있는 방법을 가상코드 API 수준까지 상세히 제시하고 있으며, XML로 표기할 수 있도록 스키마까지 방대하게 정의하고 있다. 하지만, 이런 상세한 표준문서상에 보안에 대한 고려는 HTTPS를 사용하고, EPCglobal의 인증서 프로파일 표준[12]을 이용하여 인증서를 발급받는 것으로 규정하고 있어서 다양한 바인딩을 제공하여 통신채널의 다변화를 장점으로 내세우고 있는 해당 표준에서 한계로 작용할 수 있다. 따라서 리더 프로토콜 표준에 자체 보안 메커니즘을 포함시켜야만 특정 통신채널을 사용할 때만 보안이 되는 단점을 해결할 수 있다.

2. SLRRP

IETF에서는 리더와 백엔드 서버간의 통신을 IP 네트워크만을 사용 하는, 즉 WLAN을 기본으로 한 SLRRP 리더 프로토콜 표준을 심의하고 있다. 해당 프로토콜은 하나의 표준으로 대규모 RFID 플랫폼을 WLAN을 기반으로 하는 기업망을 통해 관리할 수 있다는 것을 장점으로 내세우고 있으며, 특히 모든 RF 프로토콜과의 호환 및 간단한 구조를 통해 구현하기 쉽고 편리한 것을 최대 강점으로 기술하고 있다. 해당 표준에서는 [그림 1]과 같은 RFID 기반구조상에서 RNC(RFID Network Controller)와 리더간의 프로토콜을 [그림 2]와 같이 정의하고 있으며, 리더 설정 명령, 데이터 수집 명령, 리더 상태 전송 명령, 태그 데이터 전송 명령 등의 상세 메시지 포맷을 정의하고 있다.



[그림 1] SLRRP에서 사용되는 RFID 시스템 구조



[그림 2] SLRRP 리더 프로토콜

해당 프로토콜에서는 TLS기반으로 보안채널을 설정하는 보안 메커니즘으로 리더 프로토콜에서 고려해야 하는 보안 취약점을 해결할 수 있다고 기술하고 있으나, 리더가 설치되는 실제 산업현장에서는 IP

네트워크가 아닌 다양한 통신환경을 고려해야 하기 때문에 IP 기반의 TLS로는 한계가 있다. 따라서 해당 표준 역시 자체 보안 메커니즘을 포함시켜야만 특정 통신채널을 사용할 때만 보안이 되는 단점을 해결할 수 있다.

III. 안전한 RFID 리더 프로토콜

이 장에서는 리더 프로토콜이 가져야하는 보안요구사항과 제안하는 SLRRP기반의 리더 인증프로토콜, 키 합의, 메시지 포맷에 대하여 기술하도록 한다.

1. RFID 리더 프로토콜의 보안요구사항

RFID 리더 프로토콜 상에서 발생할 수 있는 대표적인 보안 취약점을 살펴보면 다음과 같이 정리될 수 있다.

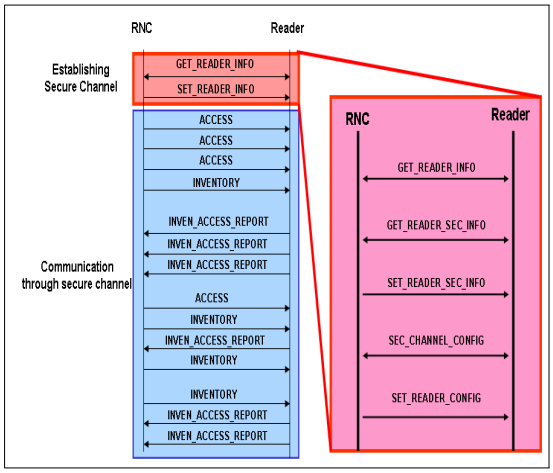
- ⊙악의적인 리더 : 리더와 서버 간에 악의적인 리더가 참여하여 스푸핑 공격, 데이터 수집 등을 할 수 있다.
- ⊙리더의 탈취 : 정상적이고 합법적인 리더가 공격자에게 탈취되어 도청, 데이터 수집 등을 수행할 수 있다.
- ⊙통신채널 도청 : 공격자는 리더와 서버 간의 다양한 유무선 통신채널을 통해 수동 혹은 능동적인 도청으로 주요 데이터를 수집 할 수 있다.
- ⊙재전송공격 : 공격자는 리더와 서버 간의 통신 메시지를 재전송하여 리더의 정보, 태그 데이터 등 원하는 정보를 얻을 수 있다.

위와 같은 보안 취약점을 보호하기 위하여 다음과 같은 RFID 리더 프로토콜의 보안요구사항을 정의할 수 있다.

- ⊙인증 : 악의적인 리더의 참여, 리더의 탈취 등으로 발생할 수 있는 보안취약점을 방지하기위해 리더와 서버 간에 주기적인 기기인증이 필요하며 암호학적 인증프로토콜을 리더 프로토콜에 포함시켜야 한다.
- ⊙무결성 : 스푸핑 공격, 능동적인 도청 등을 방지하기 위해 리더 프로토콜은 무결성을 제공하여야 한다.
- ⊙기밀성 : 수동적인 도청 등의 공격을 방지하기 위해 리더 프로토콜을 통해 전송되는 메시지는 기밀성이 유지되어야 한다.
- ⊙재전송공격 방지 : 리더와 서버 간에 전송되었던 메시지를 다시 전송했을 때 원하는 정보를 얻을 수 없도록 세션 키의 주기적 갱신과 같은 방법으로 방지할 수 있어야 한다.

2. SLRRP 기반의 안전한 리더 프로토콜

기본적인 SLRRP 리더 프로토콜에 보안 메커니즘을 추가하기 위해서는 [그림 3]과 같이 먼저 리더 설정 단계에서 보안 채널을 설정하는 단계가 필요하다.



[그림 3] SLRRP에서 보안 채널 설정 메시지

이때 SLRRP 메시지 식별방식은 [그림 4]처럼 정의하며, 상세 메시지 형식은 SLRRP 표준 형식을 따른다. [그림 5]에서는 기본적인 암호모듈과 채널설정 정보 교환용 GET_READER_SEC_INFO 메시지, GET_READER__SEC_INFO_RESPONSE 메시지의 실례를 나타낸다.

Type	Message Name
0x00	(reserved by IETF)
0x01	GET_READER_INFO
0x02	GET_READER_INFO_RESPONSE
0x03	SET_READER_CONFIG
0x04	SET_READER_RESPONSE
0x10	INVENTORY
0x11	INVENTORY_RESPONSE
0x12	STOP_INVENTORY
0x13	STOP_INVENTORY_RESPONSE
0x18	ACCESS
0x19	ACCESS_RESPONSE
0x1A	STOP_ACCESS
0x1B	STOP_ACCESS_RESPONSE
0x20	INVENTORY_ACCESS_REPORT
0x30	GET_READER_SEC_INFO
0x31	GET_READER_SEC_INFO_RESPONSE
0x32	SET_READER_SEC_INFO
0x33	SET_READER_SEC_INFO_RESPONSE
0x34	SEC_CHANNEL_CONFIG
0x35	SEC_CHANNEL_CONFIG_RESPONSE

[그림 4] SLRRP 메시지 식별 방식의 확장

GET_READER_SEC_INFO

x	x	x	x	x	Ver	Type = 0x30	Message Length = 0xB	
Message Seq Num							x x x x x x x x x x x x x x x x	
Requested Data								

GET_READER_SEC_INFO_RESPONSE

x	x	x	x	x	Ver	Type = 0x31	Message Length = Variable	
Message Seq Num							x x x x x x x x x x x x x x x x	
Requested Parameters or Operation Error Parameters								

[그림 5] 추가적인 SLRRP 메시지 형식의 예

보안 채널 설정 단계에서 인증은 리더가 속해 있

는 도메인의 백엔드 서버 공개키로 서명된 대리 인증서(Proxy certificate)[13]방식의 인증프로토콜을 통해 수행하게 되며, 모든 리더가 공인인증기관에서 인증서를 발급받고 관리하는 것은 비효율적이므로 각 리더들을 관리하는 해당 도메인의 백엔드 서버가 CA 역할을 하게 된다. 안전한 리더 프로토콜을 위한 인증프로토콜과 키 합의 프로토콜에서 사용된 표기법과 상세한 동작방식은 다음과 같다.

⊙ 사용된 표기법

- BS : 해당 도메인의 서버
- R : 해당 도메인에 속한 리더
- $Cert_x$: 공인인증기관에서 발급받은 BS x의 인증서
- $PCert_y$: 해당 도메인의 서버의 공개키로 서명된 리더 y의 대리 인증서
- EN_k : 키 k로 블록 암호화
- E_x : x의 공개키로 암호화, (x=R 혹은 BS)
- S_x : x의 비밀키로 생성된 전자서명, (x=R 혹은 BS)
- t_x : x의 타임 스탬프 (x=R 혹은 BS)
- $h(m)$: m의 해쉬 값
- $MAC_k(m)$: 키 k를 가지는 메시지 인증 코드
- MK : Diffie-Hellman 기법으로 생성된 마스터 키, $MK = g^{ab}$
- SK : BS와 R 사이에 사용되는 세션 키, $SK = MAC_{MK}(t_{BS}, t_R)$

⊙ 인증프로토콜

1. $BS \rightarrow R$: t_{BS}
2. $BS \leftarrow R$: $PCert_R$, t_R, BS, $S_R(t_R, t_{BS}, BS)$
3. $BS \rightarrow R$: $Cert_{BS}$, R, $S_{BS}(t_{BS}, t_R, R)$

⊙ 키 합의 프로토콜

1. $BS \rightarrow R$: t_{BS}
2. $BS \leftarrow R$: t_R
3. $BS \rightarrow R$: $S_{BS}(h(t_{BS}, t_R))$, $EN_{SK}(h(t_{BS}, t_R, S_{BS}(h(t_{BS}, t_R))))$
4. $BS \leftarrow R$: $EN_{SK}(h(t_{BS}, t_R, S_{BS}(h(t_{BS}, t_R))))$

위에서 기술한 인증, 키 합의 프로토콜의 단계가 종료되고 사용될 블록암호 알고리즘 협상단계를 거치게 되면 SEC_CHANNEL_CONFIG이 종료되고 보안채널이 형성되어 리더와 서버간의 안전한 통신이 가능하게 되며, 이런 자체 보안 메커니즘을 SLRRP 표준에 포함시켜서 다양한 통신채널을 사용할 때에도 제안 리더 프로토콜로 보안요구사항을 만족하는 안전한 통신이 가능하다.

IV. 비교분석

[표 1] 기존 리더 프로토콜과 제안 프로토콜의 비교

구 분	EPCRP	SLRRP	제안 프로토콜
다양한 RF 프로토콜 지원 및 확장성	GEN2 Class0/1 지원	모든 RF 프로토콜 지원	모든 RF 프로토콜 지원
태그 인벤토리 제어	읽기 과정에서만 지원	모든 단계에서 지원	모든 단계에서 지원
TID 지원	없음	지원	지원
다양한 통신 채널 지원	지원	WLAN	지원
인증서 관리 효율성	비효율적	비효율적	효율적
보안요구사항	일부 만족	일부 만족	모두 만족

[표 1]에서 기존의 리더 프로토콜들과 비교를 하였으며, 해당 표는 제안 프로토콜이 하나의 표준으로 대규모 RFID 플랫폼을 기업망을 통해 관리할 수 있으며, 모든 RF 프로토콜과의 호환 및 간단한 구조를 통해 구현하고 쉽고 편리한 SLRRP의 장점을 수용하면서도 해당 프로토콜의 문제점, 즉 리더가 설치되는 다양한 환경과 통신 환경, 계산능력, 하드웨어 등의 특성을 고려하지 않거나 다양한 환경을 고려하더라도 특정 통신 프로토콜 상에서만 보안을 제공하고 있는 단점을 해결한 프로토콜임을 보여준다.

V. 결 론

RFID와 리더 사이의 인증프로토콜에 대한 많은 연구들이 선행되었으며, 괄목할만한 연구 성과들이 제시된 상황이다. 하지만 이에 비해 RFID 리더와 서버간의 보안통신을 위한 안전한 RFID 리더 프로토콜에 대한 연구는 매우 부족한 실정이다.

본 논문을 통해서 대표적인 RFID 리더 프로토콜인 EPCglobal의 리더 프로토콜과 IETF SLRRP에 대해 소개하였고 해당 리더 프로토콜의 문제점을 제시였으며, 리더 프로토콜이 만족해야할 보안요구사항과 기존 프로토콜의 문제점을 해결할 수 있는 안전한 SLRRP 기반의 RFID 리더 프로토콜을 제안하였다. 또한, 기존의 두 리더 프로토콜과의 비교를 통해 제안 프로토콜이 SLRRP의 장점을 수용하면서 문제점들은 해결한 것을 알 수 있었다.

향후 진행되어야 할 연구로 해당 제안 리더 프로토콜의 상세 설계를 통해 좀 더 명확한 표준문서로 다듬어 나갈 필요가 있으며, 또한 실제 구현을 통한 검증이 필요하다. 나아가서 제안한 안전한 리더 프로토콜이 EPCglobal, IETF와 같은 국제 표준화 기구에서 채택될 수 있도록 노력해 나갈 예정이다.

참 고 문 헌

[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] Ari Juels, Ronald Rivest, and Michael Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. ACM CCS, Oct. 2003

[3] Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels. Security and privacy aspects of low-cost radio frequency identification systems. International Conference on Security in Pervasive Computing, Mar. 2003

[4] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita. Cryptographic Approach to ''Privacy-Friendly'' Tags. RFID Privacy Workshop, Nov. 2003

[5] Dirk Henrici and Paul Müller. Hash-Based Enhancement of Location Privacy For Radio-Frequency Identification Devices Using Varying Identifiers. PerSec, Mar. 2004

[6] Philippe Golle, Markus Jakobsson, Ari Juels, and Paul Syverson. Universal Re-Encryption for Mixnets, CT-RSA, Feb. 2004

[7] Pim Tuyls and Lejla Batina. RFID-Tags for Anti-Counterfeiting. CT-RSA, Feb. 2006

[8] Reader Protocol(RP) Standard, Version 1.1, EPCglobal
http://www.epcglobalinc.org/standards

[9] Simple Lightweight RFID Reader Protocol, IETF
http://www.ietf.org/ietf/05mar/slrrp.txt

[10] HTTP over TLS standard, IETF
http://www.ietf.org/rfc/rfc2818.txt

[11] Transport Layer Security standard, IETF
http://www.ietf.org/rfc/rfc2246.txt

[12] EPCglobal Certificate Profile Standard, Ratified Specification 1.0, Mar. 8 , 2006 ,EPCglobal
http://www.epcglobalinc.org/standards

[13] X.509 Public Key Infrastructure-Proxy Certificate Profile, IETF
http://www.ietf.org/rfc/rfc3820.txt