RFID 통신 프로토콜을 이용한 암호화 방법에 대한 연구

박일호*
*(주)리테일테크
e-mail: kwlee@chungwoon.ac.kr

A Study For Cryptographic Method using RFID Communication Protocol

Il-Ho Park*
*RetailTech Co.,Ltd

요 약

본 논문에서는 RF 송수신기를 이용하여 데이터를 전송하고, 전송받은 데이터를 이용하는 가운데 안전하게 통신하기 위한 방법으로 RFID 통신 프로토콜을 이용한 암호화 방법을 연구한다. 그리고 이러한 통신 프로토콜을 이용하여 안전하고 편리한 PC 보안 방법을 연구한다. 이러한 PC 보안 방법은 PC 가까이에 Tag를 소지한 사용자가 있는지 유무 판단을 하여 자동으로 PC를 보호한다. 또한 위조 변조가 불가능하며, 스니핑 공격과 스푸핑 공격에 대해 안전하다.

1. 서론

오늘날 컴퓨터와 인터넷의 보급이 증대되면서 모든 분야에 컴퓨터를 이용한 업무가 점차 증가하고 있다. 이렇게 컴퓨터의 활용이 증가함에 따라 중요 정보를 보호하기 위해 최근 다양한 형태의 보안 시스템들이 연구 개발되고 있다.

기존의 컴퓨터에 저장된 각종 정보의 유출을 막는 방법으로는 사용자 PC에 저장되어 있는 Password를 입력하는 방법, Smart 카드를 이용하여 컴퓨터에 연결된 카드 리더기에 카드를 인식하는 방법, 지문을 이용하여 컴퓨터에 부착된 지문인식기를 통하여 지문을 인식하는 생체인식 기술 등이 있다.

하지만 상기된 기술 중 Password 입력방식은 비밀번호를 주기적으로 변경해야 하며, 이를 분실했을 시에는 데이터를 복구하는데 상당한 노력이 필요하며, Smart 카드의 경우 접촉식 카드는 카드리더기에 항상 꽂아야 하는 불편함이 있으며, 비접촉식 Smart 카드를 사용해도 그 인식거리가 매우 짧기 때문에 수신이 안 될 수 있어 불편하다. 또한 지문 인식과 같은 생체인식 기술은 Login시 항상 지문을 인식해야하며, 다른 기술에 비하여 인식률 또한 낮기 때문에 불편함이 많다.

2. RFID 기술과 프로토콜

2.1 RFID 기술

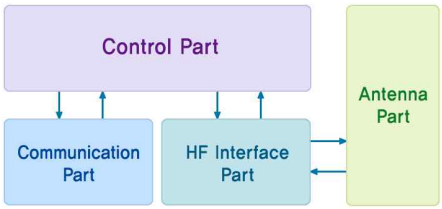
2.1.1 태그(Teg)

RFID 태그는 리더로부터 전원을 공급받거나, 데이터를 수신 또는 송신하기 위한 안테나, 태그의 ID 및 사용자가가 임의로 읽고 저장할 수 있는 메모리를 포함하고 있는 장비를 말하며, 사물에 부착하여 리더기를 통하여 인식되어지는 과정이 필요하다[1].

태그의 경우 크게 두 가지로 구분되어 지는데, 자체의 전원을 가지고 있는 능동형 태그(Active Tag)와 리더로부터 자기장을 통하여 전원을 공급받아 동작하는 수동형 태그(Passive Tag)가 있다[1].

2.1.2 리더 (Reader)

RFID 리더는 소프트웨어 애플리케이션이 비접촉식의 RFID 태그로부터 데이터를 읽거나 쓰기위해 설계된 디바이스이다. RFID 리더는 HF 인터페이스 파트를 통하여 능동형 태그로 명령어를 전송하며, 태그로부터 응답 데이터를 수신하여 디지털 데이터로 복호화하는 기능을 한다. 또한 능동형 태그로는 수동형 태그와 동일하게 명령어 및 응답 데이터를 송수신하는 기능 이외에 태그가 동작할 수 있는 전력을 함께 전달하는 기능을 한다[1].



[그림 1] RFID 리더의 전체 블럭다이어그램

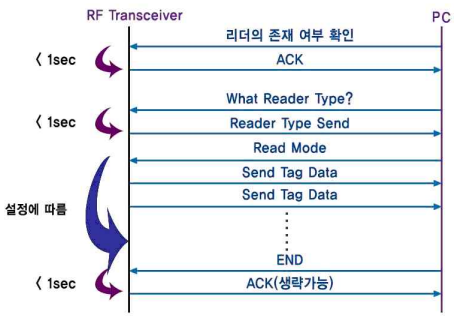
RFID 리더의 구성 요소로는 태그에서 사용할 전력을 공급하고, 데이터를 송·수신하기 위해서 무선으로 신호를 주고받을 수 있는 최종단의 안테나부, 안테나를 통해서 무선으로 데이터를 송·수신하기 위한 HF 인터페이스부, HF 인터페이스 단을 제어하며 외부 인터페이스로부터 수신된 명령어에 대한 분석 및 태그로부터 수신된 데이터에 대한 전송을 하기 위한 제어부, 외부 인터페이스와 여러가지 통신 방법을 사용하여 태그의 데이터를 전송하기 위한 통신부로 구성되어 있다[4].

2.2 암호학적 인증 프로토콜

현재 RFID 시스템에서는 암호학적인 방법을 이용한 인증기법을 주로 연구하고 있으며, 현재까지 해쉬-락 기법[8], 확장된 해쉬-락 기법[8], 해쉬-체인 기법[7], 해쉬 기반 ID 변형 기법[5], 개선된 해쉬 기반 ID 변형 기법[3], Challenge-Response 기반 안전한 RFID 인증 기법[2], 외부 재암호화 기법[6] 등이 있다.

3. RF 송수신기를 이용한 통신 프로토콜

3.1 RF 송수신기의 프로토콜 설계



[그림 2] RF 송수신기의 통신 흐름도

[그림 2]는 Tag로부터 Reader로 수신된 데이터 또는 PC에 연결된 리더로부터 수신된 명령에 대한 응답 프로토콜이며, 태그로부터는 각각의 태그에 대한 ID 및 정보를 수신하여 PC에 연결된 리더로 전달하거나, 리더로부터 전달되는 명령에 따라 그에 대한 동작을 취한 후 그 결과에 따른 응답을 한다.

3.1.1 Connection Check

최초 PC에서 리더의 장착 여부를 검사하기 위한 명령으로 5byte의 데이터를 PC에 연결된 리더기로부터 태그로 전송한다.

[표 1] Connection Check Protocol

STX	Length	Command	Check-Sum	ETX
1 byte	1 byte	1byte	1 byte	1 byte

- STX : 데이터의 시작을 알림
- Length : 데이터 길이
- Command : 데이터 Type
- Check-Sum : 데이터가 정확한지 체크
- ETX : 데이터의 끝을 알림

3.1.2 ACK

리더로부터 Connection Check, Reader Type 및 END Mode 명령에 대한 응답으로 명령을 수신 한 이후 1초 이내에 응답하여야만 한다. Reader Type에 대한 응답일 경우에는 통신 채널 데이터를 포함하여 송신한다.

[표 2] ACK Protocol

STX	Length	Command	Response	Check-Sum	ETX
1byte	1byte	1byte	1byte	1byte	1byte

- STX : 데이터의 시작을 알림
- Length : 데이터 길이
- Command : 데이터 Type
- Response : 리더로부터 받은 데이터의 응답
- Check-Sum : 데이터가 정확한지 체크
- ETX : 데이터의 끝을 알림

3.1.3 Send Tag Data

태그로부터 수신된 데이터를 PC에 부착된 리더로 전달하기 위한 protocol로 총 12 Byte이며 PC로부터 Read Mode에 대한 명령어를 수신하였을 때부터 END Mode라는 명령을 받을 때까지 태그 데이터를 전송한다.

[표 3] Send Teg Protocol

STX	Length	Command 1	Command 2	Tag Type		
TID1	TID2	TID3	TID4	Tag Status	Check -Sum	ETX

- STX : 데이터의 시작을 알림
- Length : 데이터 길이
- Command1 : 데이터 Type1
- Command2 : 데이터 Type2
- Tag Type : 주파수 별 Tag의 channel
- TID1~TID4 : 태그의 ID
- Tag Status : 태그의 전파세기, 태그 배터리 상태, 태그의 신호 Mode
- Check-Sum : 데이터가 정확한지 체크
- ETX : 데이터의 끝을 알림

3.1.4 Reader Type

PC와 연동할 RF Transceiver의 채널에 대한 질의 명령으로, Tag와 리더의 채널이 동일해야 등록 및 사용이 가능하며 프로토콜은 Connection Check와 동일하다.

3.1.5 Read Mode

리더의 장착 여부를 확인한 이후 태그의 정보를 수집하기 위한 명령으로, 리더는 END Mode 명령이 올 때까지 태그의 정보들을 송신한다. 프로토콜은 Connection Check와 동일하다.

3.1.6 End Mode

태그의 데이터 수집이 완료되었을 경우 리더에서 소비하는 전류를 최소화하기 위하여 태그 데이터의 수신을 종료하며, 다시 'Read Mode' 명령을 수신하기 전에는 태그의 데이터를 전송하지 않는다. 프로토콜은 Connection Check와 동일하다.

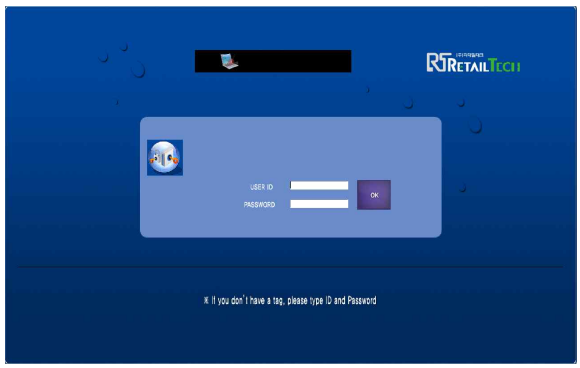
3.2 PC 보안 S/W 설계

PC 보안 S/W는 RF 송신기(이하 Tag로 명칭)가 보내주는 값을 실시간으로 처리하는 RF 수신기(이하 Reader로 명칭)로부터 데이터를 전송 받으며, Tag로부터 수신되지 않거나 Tag의 ID 값이 S/W로 전달되지 않으면 PC 보안이 구동된다.

PC 보안 S/W는 프로그램으로 설정해 놓은 키보드의 자판 이외의 키 및 마우스 사용을 금지시켜 주는 기능을 하고 있다. 이때 사용자가 휴대하고 있는 Tag로 부터의 데이터가 수신이 되지 않는 것은 사용자가 Reader로부터 전파거리를 벗어났다고 판단하고, Reader의 ID 값이 전송되지 않는것은 누군가에 의해 의도적으로 사용자 PC에서 RF 수신기를 탈거한 것이므로 PC 보안 소프트웨어에 의해 데이터를 보호한다.

허가된 ID 및 패스워드 정보는 Hash 알고리즘으로 암호화되기 때문에 어떠한 방법으로도 해독되지 않는다. 사용하는 Hash 알고리즘의 특징은 단방향 함수만을 제공하기 때문에 시스템에서 불필요한 복호화과정에 의한 시스템 자원 사용을 최소화 하였고 악의적으로 정보를 해킹하고자 하는 침입자로부터 데이터를 보호한다.

4. 구현



[그림 3] PC 보안기 화면

PC 보안기에 등록된 태그를 소지한 사용자가 근접해 있지 않을 경우 PC 보안 실행되고 [그림 3]과 같은 화면이 보인다. 스크린 세이버와 PC 보안기의 잠김 기능을 통하여 1차 PC 보안이 되고 사용자의 특수키를 이용하지 않는한 마우스 및 키보드는 동작하지 않는다. PC 보안기에 등록된 태그를 소지하고 있는 사용자가 PC에 접근할 경우는 자동으로 보안이 해제되며 사용자가 태그를 분실했을 경우는 사용자 특수키를 이용하여 스크린 세이버를 해제하고 등록된 ID와 Password를 입력하여 PC 로그인하여 보안을 해제할 수 있다.

5. 결 론

오늘날 컴퓨터와 인터넷의 보급이 증대되면서 모든 분야에 컴퓨터를 이용한 업무가 점차 증가하고 컴퓨터의 중요한 정보들을 보호하기 위해서 다양한 형태의 보안 시스템들이 연구 개발되고 있다.

본 논문에서는 RF 송수신기를 이용하여 통신 프로토콜을 설계하였으며, 암호화 방식의 PC 보안 시스템에 대하여 연구하였다.

PC 보안 시스템은 RF 송신기와 수신기를 이용하여 해쉬 데이터로 암호화하여 통신하고 수신기로부터 받은 데이터를 PC에서 실행되고 있는 PC 보안 시스템을 통하여 기존에 등록되어 있는 RF 송신기의 ID가 있는지 체크하여 인증을 받는다.

수동적인 움직임을 요구하는 PC 보안 시스템들과는 다르게 RF 송신기와 RF 수신기의 거리에 따라 PC보안이 잠기고 풀리기 때문에 사용자의 움직임을 요구하지 않고 자동으로 로그인 되어 편리하다. 그리고 RFID 통신 프로토콜을 이용하여 데이터를 전송하기 때문에 스니핑 및 스푸핑 공격에 안전하다.

참고문헌

[1] 안재명, “EPC GLOBAL NETWORK 기반의 RFID기술 및 활용”, 2007.

[2] 이근우, 오동규, 곽 진, 오수현, 김승주, 원동호, “분산 데이터베이스 환경에 적합한 Challenge-Response 기반의 안전한 RFID 인증 프로토콜”, 한국정보처리학회 논문지 C, 제12권-C권, 제3호, pp.309-316, 2006 6.

[3] 황영주, 이수미, 이동훈, 임종인, “유비쿼터스 환경의 Low-Cost RFID 인증 프로토콜”, 한국정보보호학회 하계정보보호학술대회 논문집 Vol.14, NO1, pp.109-114, 2004.

[4] 정행섭 “퍼지 추론을 이용한 지문인식에 관한 연구”, 석사학위논문, 2003

[5] Henrich, D. and M?ller, P., “Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers”, Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshop (PERCOMW'04), pp. 149-153, IEEE, 2004.

[6] A.Juels, R.Pappu, “ Squealing Euros : “Privacy protection in RFID -enabled banknotes", Financial Cryptography '03 LNCS 2742, pp.103-121, Springer-Verlag Heidelberg, 2003.

[7] M. Ohkubo, K. Suzuki, and S. Kinosita, “Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID", Proceedings of the SCIS 2004, pp.719-724, 2004.

[8] Weis, S. et al., “Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Security Pervasive Computing, 2003 LNCS 2802, pp.201-212, Springer-Verlag Heidelberg. 2004.