

RFID를 이용한 PC 보안 소프트웨어의 설계 및 구현

진병욱*

*청운대학교 멀티미디어 학과
e-mail:quddnr4515@naver.com

Design and Implementation of A PC Protection Software using RFID

Byung-wook Jin*

*Dept of Multimedia Science, Chungwoon University

요약

본 논문에서는 RFID를 이용하여 PC 보안 소프트웨어를 설계 및 구현을 하였다. 본 논문에서 연구한 PC 보안 소프트웨어는 송신기인 RFID Tag와 수신기인 RFID Reader에 연결된 안테나를 통해 서로 통신하여 PC에 설치된 S/W를 이용하여 사용자 인증을 받는 PC 보안 방법이다.

이는 위조 및 번조가 불가능하며, 스니핑 공격 및 스푸핑 공격에 대하여 기존의 PC 보안 시스템보다 안전성이 향상되었다.

1. 서론

오늘날 컴퓨터와 인터넷의 보급이 증대되면서 일반 가정, 회사, 소·대형마트 및 공공기관 등 사회 모든 분야에서 컴퓨터를 이용한 업무 즉 자료의 입력, 수집, 보관, 처리 및 출력 등의 일을 수행함으로써 인하여 컴퓨터의 활용이 점차 증가하며 정보 보안의 중요성 인식이 높아지고 있다.

이렇게 컴퓨터의 활용 증가와 컴퓨터 정보 보호의 인식이 높아짐에 따라 개인 정보 및 업무상 중요한 정보들이 저장 되어 있는 이러한 정보들을 보호하기 위해 최근 다양한 형태의 PC 보안 시스템들이 연구 개발되고 있다.

이에 본 논문에서는 바코드 시스템과 마그네틱 카드 시스템이 우리 생활에 밀접하게 이용되고 있으나 생산 방식의 변화, 소비자 의식의 변화, 문화 및 기술의 진보, 바코드와 마그네틱 카드의 단점 해소 요구에 의해 개발된 시스템인 즉, 무선으로 사람, 물건, 동물 등을 인식, 추적, 식별할 수 있는 기술인 RFID 기술을 적용시켜 PC 보안 시스템의 새로운 방법을 설계 및 검증 한다.

2. 기존 PC 보안 시스템 분석

2.1. Password를 이용한 PC 보안

Windows의 사용자 로그인이나 Screen Saver에서 Password 로그인 방식으로 기본적으로 제공되는 PC보안 시스템으로 쉽게 사용가능하고 무료로 사용할 수 있는 장점이 있지만, 키보드를 이용하여 Password를 입력하는 불편함이 있고 보안을 위해서 지속적으로 Password를 변경하여야한다. 그리고 Password를 입력할 때 정보가 누출될 가능성이 높음.

2.2. 생체인식을 이용한 PC 보안

지문을 이용하여 인증을 받는 방법으로 사용자는 지문을 인식할 수 있는 하드웨어에 손가락을 접촉하고 PC에 설치 되어있는 소프트웨어를 이용하여 인증 단계를 거쳐서 Password 대신에 로그인한다.

이 방법은 지문인식이 가능한 고가의 하드웨어를 구매해야하며 수동적으로 손가락을 접촉해야한다.

또 한 인식이 낮아서 여러 번의 접촉을 시도해야 하며, 지문 정보가 누출될 우려가 있다.

2.3. RFID를 이용한 PC 보안

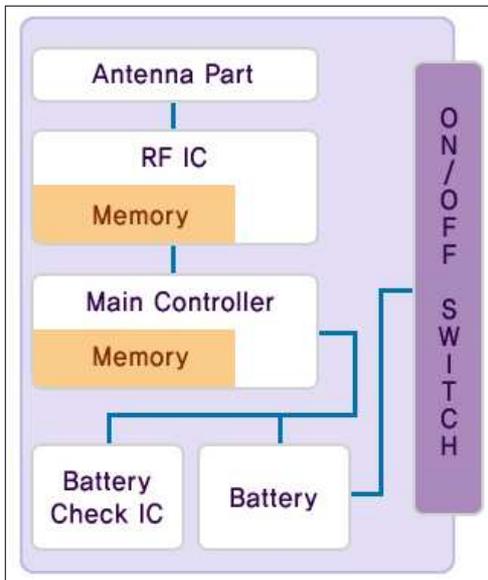
카드형의 RFID 태그를 사용하는 방법은 보통 13.56KHz 대역의 비접촉식 RFID Tag를 사용하며, USB 또는 Serial 방식의 리더기와 서로 양방향 통

신하는 방법이다. 사용자는 카드를 항상 소지해야 하며 PC에 연결된 리더기에 5cm 이내로 가까이 가서 인증을 받아야 되기 때문에 불편하다는 단점이 있다. 이는 13.56KHz RFID Tag가 Passive 태그이기 때문이며, 자체 전류가 없는 방식은 인식 거리가 짧다는 점과 항상 카드를 수동적으로 이용해야 한다. 그리고 카드 발급시 저용량의 메모리 한계 때문에 ID값이 제조시부터 내장되어 설계되며, 하드웨어 구조가 단순하여 복제 및 위조가 될 확률이 높다는 것이 특징이다.

3. PC 보안 시스템의 설계 및 구현

3.1. RFID 송신기의 설계

RFID 송신기의 크기는 휴대하기 편리하도록 소형으로 설계하며, 내부는 Antenna Part, RF IC, Main Controller, Battery, Battery Check IC, On/Off Switch로 구성된다.



[그림1] RF 송신기 H/W 구성도

[그림1]은 RF 송신기의 구성도로 태그의 스위치가 On 상태가 되면 전원을 공급 받고 이때의 태그는 RF 수신기로 데이터를 보내기 위한 내부의 모든 모듈을 초기화 한다.

태그는 RF 수신기에 데이터를 전달하게 될 값을 구성하며, 최초로 배터리의 전압이 이상한지를 판단하여 플래그 값을 '0' 또는 '1'로 설정하여 다음 흐름으로 넘어가게 된다.

태그는 용도에 따라 무선신호의 세기를 사전에 선택할 수 있으며, 이 설정 값은 RF IC의 내부 Regist

-er에 저장하여 RF 출력의 세기를 조정할 수 있다.

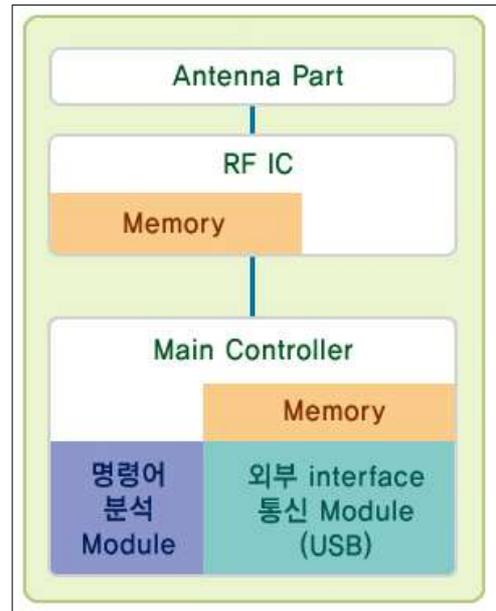
MCU에서는 배터리 체크 회로에서 전송받은 플래그의 값 및 RF 전파의 세기를 메모리에 저장되어 있는 태그 ID 값과 조합하여 RF 수신기로 전송할 데이터의 값을 생성한다.

이렇게 조합된 데이터를 태그는 리더로 송출하게 되며, 지정한 시간마다 이와 같은 작업을 반복하기 위해 지연시간을 두어 일정 시간이 지나게 되면 배터리 체크 회로의 단계부터 다시 시작하게 된다.

3.2. RFID 수신기의 설계

RF 수신기는 USB Type으로 PC에 부착하여 사용되며, 태그로부터 전송받은 데이터를 수신하며 RF 수신기는 PNP기능이 지원되도록 구현 되었다.

RF 수신기는 Tag로부터 전송받은 데이터를 순차적으로 저장, 분석을 통해 RF 수신기의 회로 안에 포함되어 있는 메모리의 값과 조합하여 RF 수신기의 메인 컨트롤러(MCU) 들어가게 되며, 태그로부터 들어온 명령어를 분석해 주는 모듈을 통하여 해석을 하게 되고, 그에 맞는 명령을 외부 인터페이스 통신 모듈인 USB 포트를 통하여 사용자 PC로 전송하는 기능을 담당한다.



[그림2] RF 수신기 H/W 구성도

3.3. PC 보안 시스템 소프트웨어의 설계

PC 보안 S/W는 RF 송신기가 보내주는 값을 실시간으로 처리하는 RF 수신기로부터 데이터를 전송 받으며, 태그로부터 수신되지 않거나 RF 수신기의 ID 값이 S/W로 전달되지 않으면 PC 보안을 구동

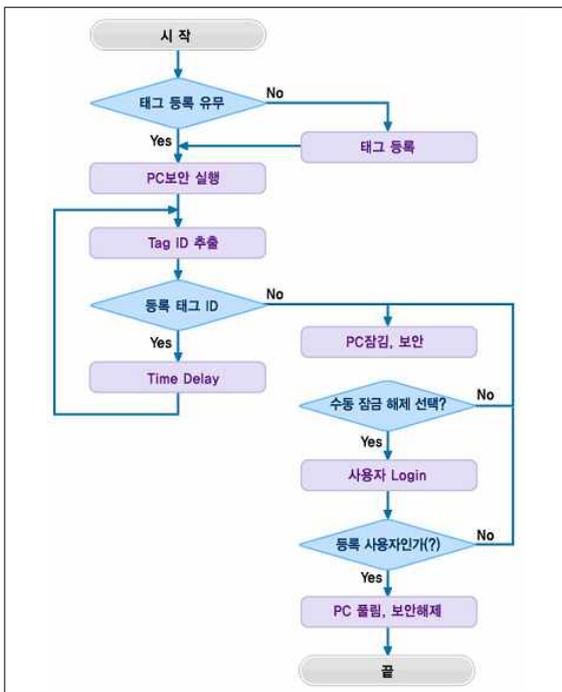
시킨다.

PC 보안 S/W는 설정해 놓은 키보드의 자판 이외의 키나 마우스 사용을 금지시킨다. 또 한 사용자가 휴대하고 있는 RF 송신기로부터 데이터가 수신되지 않으면 사용자가 RF 수신기로부터 전차거리를 벗어났다고 판단하게 되며, RF 수신기의 ID 값이 전송되지 않을 경우에는 누군가가 의도적으로 사용자 PC에서 RF 수신기를 탈거한 것으로 판단하여 PC 보안을 구동시켜 데이터를 보호하게 된다.

등록된 사용자의 정보와 다른 ID와 PASSWORD로 로그인을 시도하게 되면 일정시간 동안 사용자의 ID와 PASSWORD의 입력을 제한하도록 되어 있으며, 그 이전에 잠겨 있는 PC를 해제하기 위해서는 정당한 RF 태그의 수신이 필요하다.

허가된 ID와 PASSWORD 정보는 Hash 알고리즘으로 암호화된다.

[그림3]은 PC 보안 S/W의 전체 흐름도를 인증절차를 표현하였다.



[그림3] PC 보안 S/W의 전체 흐름도

3.4. PC 보안 시스템의 구현

본 논문에서 제안하는 RF송수신기를 이용한 암호화 방식의 PC보안 시스템은 Visual C++ 6.0을 이용하여 구현하였으며 사용자 및 설정 데이터를 저장하기 위해서 Access 2003을 사용하였다. 구현된 시스템은 최초 실행 시 Master 관리자를 등록해야 실행

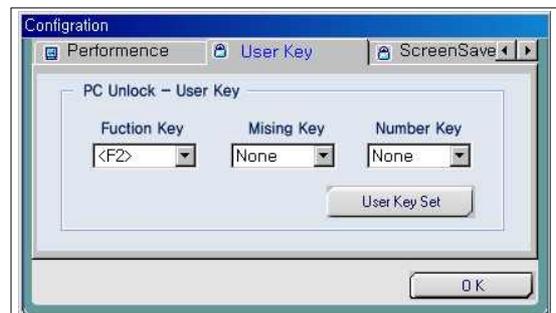
되며 PC에 Tray 아이콘을 등록하도록 구현하였다. 사용자를 등록하고 관리하며 PC보안 시스템의 환경을 설정한다. 그리고 등록된 사용자의 정보와 RF 송신기의 ID 값을 이용하여 자동으로 PC 보안을 실행하고 해제한다.

[그림4]는 태그를 등록하는 화면이며, 그림[5]는 용자의 PC에서 PC 잠금 모드로 바뀌었을 경우 마우스 및 키보드, Screen Saver의 Lock 상태를 해제하는 Key를 설정하는 화면이다.

[그림5]는 사용자의 PC가 잠금 모드로 바뀌었을 때 스크린에 보여주는 화면 보호기의 파일의 경로를 설정을 하는 화면으로 설정된 경로의 파일이 PC 보안이 작동되어 잠금 모드인 경우 스크린에 보여지게 된다.



[그림4] 태그 등록 화면



[그림5] User Key 환경설정 화면



[Fig 4-10] ScreenSaver 환경설정 화면

4. 결론

[표1]은 기존 PC 보안 시스템과 제안한 PC 보안 시스템과 비교 한 것으로 표에서 보는 것과 같이 보안 동작방법이 자동으로 기존의 시스템보다 편리하며 다른 시스템에서는 여러 공격에 보안이 해제될 우려가 있지만, 제안한 PC보안 시스템은 단 하나의 번호를 부여함으로써 복제가 불가능하다.

[표 1] 기존 PC 보안 시스템과의 비교

비교 항목	Password	지문 인식	스마트 카드	제안하는 보안 시스템
보안 동작 방법	수동	수동	수동	자동
보안 공격 방법	Dictionary 공격에 약함	비슷한 지문 인식	카드 복제	없음

또한, 본 논문에서 제안하는 방법은 Tag와 Reader 사이에 배열을 전송하며, 만약 공격자가 배열을 획득할 수가 있다고 하더라도 복호화에 필요한 키셋을 유추하지 못하기 때문에 스니핑 및 스푸핑 공격에 대해서도 안전하다.

참고문헌

[1] 안재명, “EPC GLOBAL NETWORK 기반의 RFID기술 및 활용”, 2007.
 [2] 이근우, 오동규, 곽진, 오수현, 김승주, 원동호, “분산 데이터베이스 환경에 적합한 Challenge-Response 기반의 안전한 RFID 인증 프로토콜”, 한국정보처리학회 논문지 C, 제12권-C 권, 제 3호, 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 Müller, 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. Kinoshita, “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.