한국산학기술학회논문지
Vol. 10, No. 2, pp. 287-293, 2009

RF 송수신기를 이용한 PC 보안 설계 및 구현

이근왕[1*], 박일호[2]

Design and Implementation of A PC Protection using RF Transmitter-Receiver

Keun-Wang Lee[1*] and Il-Ho Park[2]

요 약 본 논문에서는 RF송신기와 수신기를 통하여 데이터를 통신하고, 수신기에 연결된 PC에 설치된 S/W를 이용하여 사용자 인증을 받는 PC 보안 방법을 제안한다. 기존의 PC보안 방법들은 사용자의 수동적인 움직임을 요구하였지만, 제안하는 방법은 PC 가까이에 태그를 소지한 사용자가 있는지 유무 판단을 하여 자동으로 PC를 보호한다. 또한 위조 변조가 불가능하며, 스니핑 공격과 스푸핑 공격에 대해 안전하며, 오판정율도 다른 시스템에 비해 낮아서 안전하다.

Abstract This paper would suggest about data communicate using RF Transmitter-Receiver and about PC protection method authenticate using software of PC which Receiver is connected. Older PC protection system is demanded manual operation of the user but the suggesting method protect PC automatically with judge existing of the user who has Tag approaches the distance which gets near. And it is impossible about the forgery and it is safe about sniffing attack and spoofing

Key Words : RFID, Tag, Reader

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.

종래의 컴퓨터에 저장된 각종 정보의 유출을 막는 방법으로는 사용자 PC에 저장되어 있는 비밀번호를 입력하는 방법, 스마트카드를 이용하여 컴퓨터에 연결된 카드리더기에 카드를 인식하는 방법, 지문을 이용하여 컴퓨터에 부착된 지문인식기를 통하여 지문을 인식하는 생체인식기술 등이 있다.

하지만 상기된 기술 중 비밀번호를 입력하는 방식은 비밀번호를 주기적으로 변경해야 하며, 이를 분실했을 시에는 데이터를 복구하는데 상당한 노력이 필요하며, 스마트카드의 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 로그인시 항상 지문을 인식해야하며, 다른 기술에 비하여 인식률 또한 낮기 때문에 불편함이 많다.

2. RFID 개념과 기술

2.1 RFID 개념 및 동작

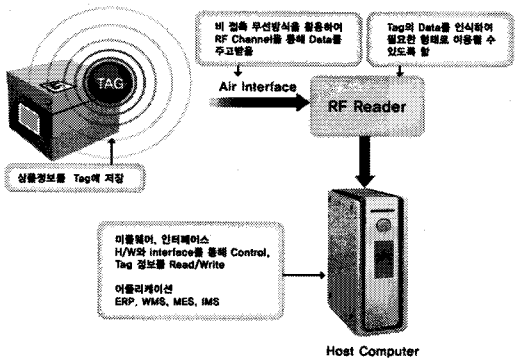
RFID 기술은 바코드 시스템과 마그네틱카드 시스템이 우리 생활에 밀접하게 이용되고 있으나 생산 방식의 변화, 소비자 의식의 변화, 문화 및 기술의 진보, 바코드

[1]청운대학교 멀티미디어학과
*교신저자:이근왕(kwlee@chungwoon.ac.kr)
[2](주)리테일테크 기술연구소
접수일 08년 10월 31일 수정일 09년 01월 19일 게재확정일 09년 2월 16일

와 마그네틱 카드의 단점 해소 요구에 의해 개발된 시스템이다. 즉, 무선으로 사람, 물건, 동물 등을 인식, 추적, 식별할 수 있는 기술이다[1].

RFID 시스템은 태그, 리더, 그리고 태그로부터 읽어들인 데이터를 처리할 수 있는 데이터 처리 시스템으로 구성된다. 태그와 리더 사이의 데이터 통신은 무선 통신 방식에 의해서 이루어진다[1].

기본적인 RFID 시스템은 [그림 1]과 같이 동작을 하며, 상품정보를 담고 있는 태그가 비 접촉 무선방식인 RF 채널을 통해 데이터를 전송 또는 수신 할 수 있는 에어 인터페이스(Air Interface)를 매체로 하여 RF 리더에서 상품의 정보를 인식하고 네트워크망이나 전용선을 이용하여 호스트 컴퓨터(또는 전용서버)의 미들웨어를 통하여 어플리케이션에서 활용할 수 있도록 하는 구조로 되어 있다. 에어 인터페이스란 무선 통신의 인터페이스 규약으로서 이동 단말과 기지국 간의 주파수, 통신 방식, 접속 방법 등 무선 접속 조건을 총칭하는 말이다. RFID 시스템은 RFID 리더가 질의를 하면 태그가 응답하는 구조를 갖고 있으며, 무선통신을 하기 때문에 태그나 리더에 안테나도 필요하다[1].



[그림 1] RFID 동작 원리

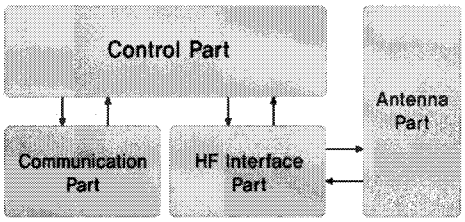
2.2 태그(Tag)

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

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

2.3 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 복호화 하는 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 2] RFID 리더

[그림 2]와 같이 RFID 리더의 구성 요소로는 태그에서 사용할 전력을 공급하고, 데이터를 송수신하기 위해서 무선으로 신호를 주고받을 수 있는 최종단의 안테나부, 안테나를 통해서 무선으로 데이터를 송수신하기 위한 HF 인터페이스부, HF 인터페이스 단을 제어하며 외부 인터페이스로부터 수신된 명령어에 대한 분석 및 태그로부터 수신된 데이터에 대한 전송을 하기 위한 제어부, 외부 인터페이스와 여러 가지 통신방법 (직렬통신(RS-232,RS-485 등), USB, Wire/Wireless LAN 등)을 사용하여 태그의 데이터를 전송하기 위한 통신부로 구성되어 있다[1].

2.4 암호학적 인증 프로토콜

현재 RFID 시스템에서는 암호학적인 방법을 이용한 인증기법을 주로 연구하고 있으며, 현재까지 해쉬-락 기법[2], 확장된 해쉬-락 기법[2], 해쉬-체인 기법[3], 해쉬 기반 ID 변형 기법[4], 개선된 해쉬 기반 ID 변형 기법[5], Challenge-Response 기반 안전한 RFID 인증 기법[6], 외부 재 암호화 기법[7] 등이 제안되었다.

2.4.1 해쉬-락 기법

이 기법은 태그가 적합한 값이 들어올 때 까지 ID를 표시하는 것을 거절하는 방법이다. 이는 단지 한 번의 해쉬 함수(Hash Function)만을 사용하기 때문에 저가로 구현될 수 있다.

2.4.2 확장된 해쉬-락 기법

이 방법은 위에 설명한 해쉬-락 기법의 확장된 기법으로 위치 추적 문제를 해결한 방법이며, 태그는 해쉬 함수와 의사난수 생성기(Random Number Generator)를 갖는다는 것을 가정한다.

2.4.3 Key를 주기적으로 변경하는 기법

리더와 태그간의 상호인증과정을 통하여 태그와 백 엔드 데이터베이스의 Key값을 주기적으로 갱신하여 해커가 Key를 탈취하였다 하더라도 다음 세션에서는 쓸모없는 Key가 되어 안전하게 통신할 수 있는 방법이다.

2.5 기존의 PC 보안 시스템

2.5.1 Password를 이용한 PC보안

Windows의 사용자 로그인이나 화면보호기에서 비밀번호 로그인 방식으로 기본적으로 제공되는 PC보안 시스템으로 쉽게 사용가능하고 무료로 사용할 수 있는 장점이 있지만, 비밀번호를 입력하기 위해서는 키보드를 이용해야 되는 불편함이 있고 보안을 위해서 지속적으로 비밀번호를 변경하여야한다. 그리고 비밀번호를 입력할 때 정보가 누출될 우려도 있으며, 비밀번호를 분실할 우려 또한 다분하다.

2.5.2 생체인식을 이용한 PC보안

지문을 이용하여 인증을 받는 방법으로 사용자는 지문을 인식할 수 있는 하드웨어에 손가락을 접촉하고 PC에 설치 되어있는 소프트웨어를 이용하여 인증 단계를 거쳐서 로그인한다. 이 방법은 지문인식이 가능한 고가의 하드웨어를 구매해야하며 수동적으로 손가락을 접촉해야한다. 그리고 손가락을 접촉해도 인식률이 낮아서 여러 번의 접촉을 시도해야 하며, 지문 정보가 누출될 우려가 있다.

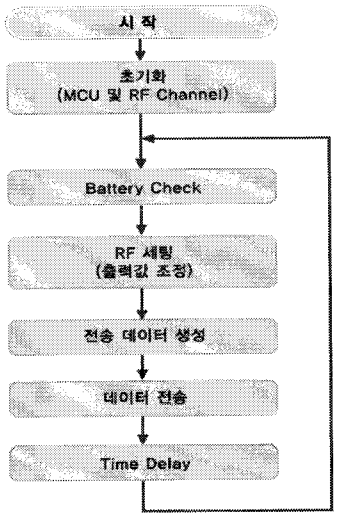
2.5.3 스마트카드 방식을 이용한 PC보안

카드형의 RFID 태그를 사용하여 리더기와 통신하는 방법으로 사용자는 카드를 소지해야하며 PC에 연결된 USB또는 Serial 리더기에 가까이 가져가서 인증을 받아야 된다. 이 방법은 카드형 태그와 리더기의 인식 거리가 짧다는 단점이 있으며, 수동적으로 카드를 이용해야 한다. 그리고 복제 및 위조가 가능하다는 단점이 있다.

3. RF 송수신기를 이용한 PC 보안 시스템 설계

3.1 RF 송신기(태그)의 설계

1) [그림 3]과 같이 태그는 리더로 데이터를 보내기 위한 최초단계인 내부의 모든 모듈의 초기화를 하게 된다.
2) 태그는 리더에게 데이터를 전달하게 될 값들을 구성하게 되는데 이 값들 중 가장 먼저 배터리의 전압을 체크하여 그 값이 일정량 이하로 떨어지면 배터리 체크 모듈에서 배터리의 전압 이상이 있다고 판단되면 플래그 값을 '0'으로 만들며, 이상이 없을 시에는 '1'로 설정하여 다음 흐름으로 넘어가게 된다.
3) 태그는 용도에 따라 무선신호의 세기를 사전에 선택할 수 있으며, 설정 값은 IC의 내부 Register에 저장하여 RF 출력의 세기를 조정할 수 있다.
4) MCU에서는 배터리 체크 회로에서 전송받은 플래그의 값 및 RF 전파의 세기를 메모리에 저장되어 있는 태그 ID 값과 조합하여 리더로 전송할 데이터의 값을 생성한다.
5) 지정한 시간마다 이와 같은 작업을 반복하기 위해 지연시간을 두어 잠시 기다리게 하는 모듈이며 일정 시간이 지나게 되면 배터리 체크 회로의 단계부터 다시 시작한다.



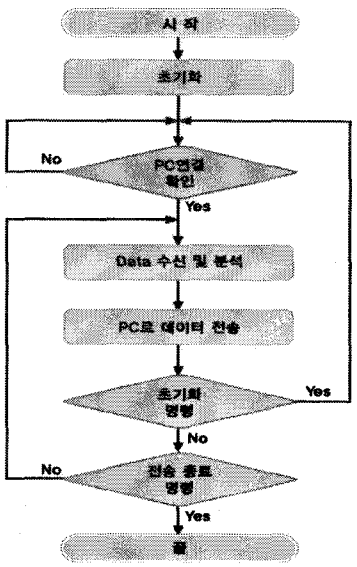
[그림 3] RF송신기의 흐름도

3.2 RF 수신기(리더)의 설계

1) RF 수신기를 사용자 PC의 USB 포트에 부착하게 되면 사용자 PC의 입출력 컨트롤러의 USB 포트에서 전원을 공급받아 사용하게 되며, RF 송신기로부터 전송받을 데이터 값을 사용자 PC의 PC 보안 소

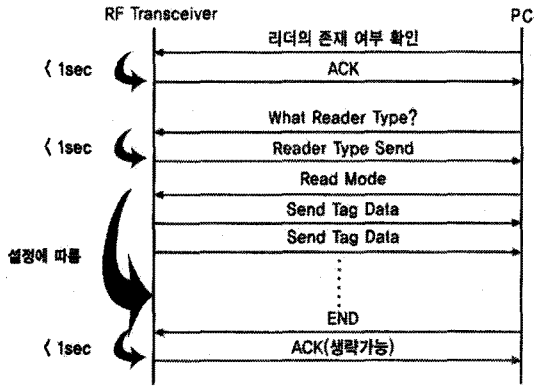
프트웨어에게 전달하기위해 [그림 4]와 같이 내부의 모든 모듈에 대하여 초기화를 진행한다.

2) 사용자 PC로부터 USB 포트를 통하여 데이터를 수신하였을 경우, 커넥션 체크 명령어인지 명령어 분석 모듈을 통하여 판별하게 되며, 커넥션 체크 명령어인지 확인이 되면 RF 송수신기와 사용자 PC에 연결되어 있기 때문에 ACK 신호를 사용자 PC로 전송하게 되며, 그렇지 않을 경우 사용자 PC로부터 전송될 명령에 대한 수신 대기 모드를 유지하게 된다.
3) 사용자 PC와 연결이 확인되면 PC 보안 소프트웨어에서 명령어를 전송하며, 이때 RF 송수신기에서 수신된 데이터를 명령어 분석 모듈을 통하여 해석하여 동작을 하게 된다.
4) 각각의 명령에 상응하는 동작은 RF 송신기에서 RF 선로를 통하여 수신된 데이터를 프로토콜에 맞도록 조합하거나 명령에 상응하는 데이터를 만들게 된다.
5) 이렇게 조합된 데이터를 사용자의 PC에게 전송하기 위하여 외부 인터페이스 통신 모듈을 통해 메인 컨트롤러에서 조합된 값을 전송하게 된다.
6) 리더는 사용자 PC로부터 전송 종료 명령어가 수신되기 전까지 RF 송신기로부터 수신되는 데이터를 지속적으로 전송하며, 데이터를 전송하는 도중 초기화 명령이 사용자 PC로부터 수신되면 PC 연결 확인부터 다시 시작하게 된다.



[그림 4] RF수신기의 흐름도

3.3 RF 송수신기의 프로토콜 설계



[그림 5] RF 송수신기의 통신 흐름도

[그림 5]은 태그로부터 리더로 수신된 데이터 또는 PC에 연결된 리더로부터 수신된 명령에 대한 응답 프로토콜이며, 태그로부터 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.

3.4 PC 보안 S/W 설계

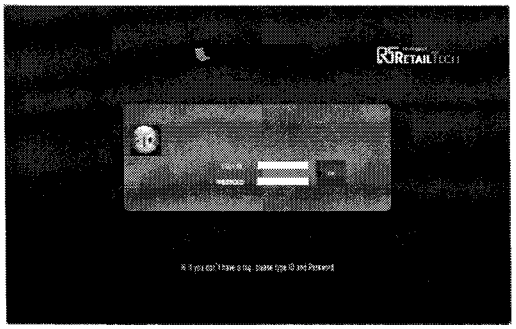
PC 보안 S/W는 RF 송신기(이하 태그로 명칭)가 보내주는 값을 실시간으로 처리하는 RF 수신기(이하 리더로 명칭)로부터 데이터를 전송 받으며, 태그로부터 수신되지 않거나 태그의 ID 값이 S/W로 전달되지 않으면 PC 보안이 구동된다.

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

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

4. 구현 및 성능평가

4.1 구현



[그림 6] PC 보안기 화면

PC 보안기에 등록된 태그를 소지한 사용자가 근접해 있지 않을 경우 PC 보안 실행되고 [그림 6]과 같은 화면이 보인다. 스크린 세이버와 PC 보안기의 잠김 기능을 통하여 1차 PC 보안이 되고 사용자의 특수키를 이용하지 않는 한 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 계정과 비밀번호를 입력하여 PC 로그인하여 보안을 해제할 수 있다.

4.2 성능평가

4.2.1 안전성에 대한 성능평가

스니핑 공격에 대한 안전성 : 제안하는 방법은 태그와 리더사이에 배열을 전송하며, 만약 공격자가 배열을 획득할 수가 있다고 하더라도 복호화에 필요한 키셋을 유추하지 못하기 때문에 안전하다.

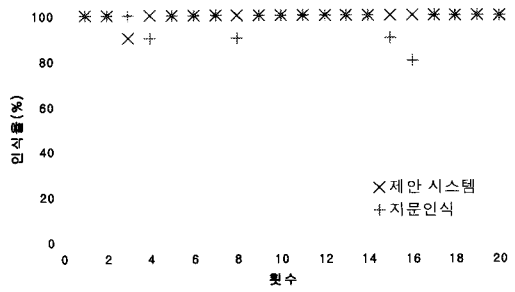
스푸핑 및 재전송 공격에 대한 안전성 : 상호인증을 위해서는 배열을 사용하며, 배열을 생성하고 복호화하기 위해서는 키셋이 필요하다. 키셋을 유추할 수 없다면, 키셋을 유추할 때 사용한 해쉬 알고리즘 역시 알 수가 없기 때문에 안전하다.

4.2.2 비교분석

Password 보안 방법은 사용자가 PC에 입력을 해야 되고, 지문인식 또한 사용자의 지문을 인식해야 되고, 스마트카드의 경우도 카드리더기에 카드를 꽂아야 되어 수동적이지만 제안하는 방법은 리더가 태그의 데이터를 받으면 보안이 해제되고 받지 못하면 보안이 실행기 때문에 자동적이다.

그리고 Password를 사용한 보안 방법은 무작위로 입력하거나, Dictionary 공격에 약하며 지문 인식의 경우는 사용자의 지문에 이물질 및 상처를 입었을 경우 인식을 못한다. 그리고 스마트카드는 카드 복제의 우려가 있지만, 제안하는 방법은 태그가 단 하나의 ID를 가지고 있어 복제가 불가능하다.

안전성 실험을 위해서 지문인식을 이용한 PC 보안 시스템의 인식율과 RF 송수신기를 이용한 PC 보안 시스템의 인식율을 비교분석하였다.

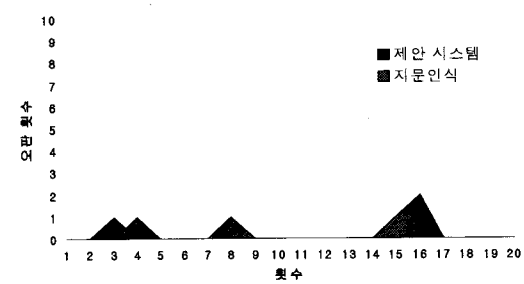


[그림 7] 제안 시스템과 지문인식의 인식율 실험

제안 시스템의 경우는 태그의 스위치를 On/Off하여 사용자의 PC에서 보안이 실행되고 해제되는 것을 실험하였고, 지문인식의 경우는 사용자의 PC에 연결된 지문인식기에 지문을 인식하여 Login되는 것을 실험하였다.

상기된 내용과 같은 실험 평가는 [그림 7]와 같다. 지문인식의 경우는 97.5%의 인식율을 나타내었지만 제안 시스템의 경우 99.5%의 인식율을 나타내었다.

[그림 8]는 제안 시스템의 오판정율과 지문인식의 오판정율을 비교분석한 실험 평가이다. 지문인식은 총 200회의 실험에서 5회의 오판을 하여 오판정율은 2.5%이지만 제안 시스템은 200회의 실험에서 1회의 오판을 하여 0.5%의 오판정율을 보여주었다.



[그림 8] 제안시스템과 지문인식의 오판정율 실험

5. 결 론

오늘날 컴퓨터와 인터넷의 보급이 증대되면서 모든 분야에 컴퓨터를 이용한 업무가 점차 증가하고 있다. 이렇게 활용이 증가함에 따라 컴퓨터에는 중요정보가 저장되어 있으며, 이러한 정보들을 보호하기 위해서 다양한 형태의 보안 시스템들이 연구 개발되고 있다.

기존의 PC 보안 방법 중에 비밀번호 입력방식은 P비밀번호를 주기적으로 바꾸어야 하며, 이를 분실했을 시에는 데이터를 복구하기 힘들고, 스마트카드의 경우 접촉식 카드를 카드리더기에 항상 꽂아야 하며, 비접촉식 스마트카드를 사용해도 인식거리가 매우 짧기 때문에 수신이 안 될 수 있어 불편하다. 또한 지문 인식 기술은 다른 기술에 비하여 인식률 또한 낮기 때문에 불편함이 많다.

본 논문에서는 RF 송수신기를 이용하여 암호화 방식의 PC 보안 시스템에 대하여 연구하였으며, PC 보안 시스템 설계 및 구현, 실험에 대한 내용을 기술하였다.

제안하는 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.

제안하는 PC 보안 시스템은 기존에 개발된 사용자의 수동적인 움직임을 요구하는 PC 보안 시스템들과는 다르게 RF 송신기와 RF수신기의 거리에 따라 PC보안이 잠기고 풀리기 때문에 사용자의 액션을 요구하지 않고 자동으로 로그인 되어 편리하며 리더기와 태그가 소형으로 제작되었으며, 목걸이형 태그를 사용하여 편리한 휴대 및 설치가 가능하다.

비밀번호를 사용하여 사용자의 정보를 보호하는 방식은 Dictionary 공격이 취약하고 생체인식 기술인 지문 인식 방식은 사용자의 지문에 이물질이 묻어서 잘못 인식할 수 있고, 비슷한 지문을 가지고 있는 비 인증 사용자도 인증을 받을 수 있어서 사용자의 PC의 정보가 유출될 우려가 있다. 그리고 스마트카드의 RFID 방식은 복제가 가능하며, 자기장에 의하여 파손될 수도 있지만, 본 논문에서 제안하는 PC 보안 시스템은 복제가 불가능하며, 태그를 소지하고 리더와의 통신을 통하여 PC의 잠금 상태를 해제하기 때문에 안전하며, 배터리를 교환하면 반영구적으로 사용이 가능하다.

PC 보안 시스템의 안전성을 실험하기 위해서 RF 송수신기를 이용한 PC 보안 방법과 지문인식을 이용한 PC 보안 방법을 비교 실험한 결과 지문 인식의 경우는 총 200회의 실험에서 5회의 오판을 하여 오판정율은 2.5% 이지만 RF 송수신기를 이용한 PC 보안 방법은 200회의 실험에서 1회의 오판을 하여 0.5%의 오판정율을 보여주었다.

참고문헌

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

[2] S. A. Weis, S. E. Sarma, R. L. Rivest, D. and W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Security in Pervasive Computing 2003, LNCS 2802, pp.201-212, Springer-Verlag, 2004.

[3] 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.

[4] D. Henrici, P. Muller, "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.

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

[6] 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.

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

이 근 왕(Keun-Wang Lee) **[종신회원]**

- 1993년 2월 : 한발대학교 전자계산학과 (공학사)
- 1996년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2000년 2월 : 숭실대학교 컴퓨터학과 (공학박사)
- 2001년~현재 : 청운대학교 멀티미디어학과 부교수

<관심분야>
멀티미디어 통신, 멀티미디어 응용, 교육 콘텐츠

박 일 호(Il-Ho Park) **[정회원]**

- 2007년 2월 : 청운대학교 멀티미디어학과(공학사)
- 2007년 2월 ~ 현재 : (주)리테일테크 기술연구소 연구원

<관심분야>
RFID