RFID를 이용한 신분 인증 시스템 설계

김대유, 김정태

목원대학교

Analyses of Encryption Method of Quantum Communication for High-speed communication

Design of Identification Authentication Scheme Using RFID

Dae-Yoo Kim ,Jung-Tae Kim

Mokwon University

E-mail : kr_sua@nate.com

요 약

유비쿼터스의 대중화가 되고 있는 지금의 보안체제는 너무 취약하다고 볼 수 있다. 공공기관이나 사무 공간에서의 보안은 더욱 필요한 실정이지만 사용자의 가치인식의 부족으로 최소한의 보안도 이루워지지 않고 있다. 현재 시스템에서 정보가 도용되었을 경우 언제, 누가, 어떻게 무엇을 했는지 알 수 없기다 하지만 유비쿼터스 생활 속에서 아용되는 RF카드에 있는 정보를 이용하여 최소한의 보안을 지킬 수 있다. 따라서 본 논문에서는 RFID를 이용한 개인 신분 인증을 위한 인증 시스템을 설계하였다.

Ⅰ. 서론

유비쿼터스는 원래 라틴어에서 유래된 단어로, 언제, 어디에나 존재한다는 의미이다. 유비쿼터스가 IT용어로 사용되기 시작한 것 미국 Zerox PARC의 마크 와이저(Mark Weiser)박사가 '어디에서든지 컴퓨터에 접근할 수 있는 세계'를 지칭하는 말로 '유비쿼터스 컴퓨팅'을 사용하였다. 사람과 컴퓨터, 그리고 사물이 연결되는 유비쿼터스 라이프(Ubiquitous Life)는 우리 생활 속에 깊숙이 파고 들었다. 교통카드로 버스를 타거나 전철 개찰구를 통과할 때 카드 속에 들어있는 정보는 물리공간의 현금으로 전환시킨다. 위치정보를 자동으로 발신하는 태그를 넣어 절대 잃어버리지 않는 골프공도 나왔으며, 고급 승용차에 장착되는 자동감지 와이퍼는 빗물의 양을 스스로 감지해 와이퍼의 작동속도를 자동으로 조절한다. 이러한 시나리오 중 일부는 우리생활에서 사용되지만 미래 유비쿼터스 사회에서 전개될 시나리오 중 일부일 것이다. 유비쿼터스 컴퓨팅을 구축하기 위해서는 네트워크 고도화가 전제되어야 한다. 즉 네트워크에 연결되지 않은 컴퓨터는 유비쿼터스 컴퓨팅이 아니다. 컨버전스(Convergence)기술의 일반화, 광대역화, 정보기기의 저가격화 등이 없이는 모든 기기에 통신 능력을 부여하는 것이 어렵기 때문이다.

Ⅱ. RFID의 개념

전자 TAG를 사물에 부착하여, 사물이 주위 상황을 인지하고 기존 IT 시스템과 실시간으로 정보교환/처리할 수 있는 기술이다. 학교 건물 곳곳에 센서나 칩셋트 형태로 태그가 심어져 학생, 교사, 방문자 등 모두가 언제 어디서나 어떤 단말기로도 필요한 정보를 수집하고 교환할 수 있는 유비쿼터스 캠퍼스(u-Campus)의 구현도 눈앞에 다가왔다. 도서관에서 책을 대출하고 반납하면서도 직원과 한 번도 얼굴을 마주할 필요가 없는 유비쿼터스 도서관(u-Library)도 전국으로 확산되고 있다. 서울시가 '공무원 전자카드 1단계 사업' 제안 요청서를 공개하였으며 1단계에서는 출-퇴근 근태관리를 비롯해 출입통제, 교통카드, 전자화폐 등의 기능이 카드에

삽입될 예정이며 2단계에서는 PC접근 제어와 전자서명 기능이 추가 된다고 보도되었다.

• RFID 기술적 특징

바코드나 Smart Card에 비하여 우수한 특성에 의해 다양한 응용이 가능하며, 향후 900MHZ 대역 제품이 현재의 13.56MHZ 대역을 대신하여 주력 제품이 될 것임

• RFID TAG 기술의 원리

안테나는 태그에 전력을 공급하며 태그는 그 응답으로 데이터를 되돌려 주며, 자기장을 이용하는 방식과 전파를 이용하는 방식이 주로 이용됨

리더기와 Tag의 수신거리는 태그마다 차이가 있고, 현재 13.56MHZ(약 5cm) 통신이 가능하다.

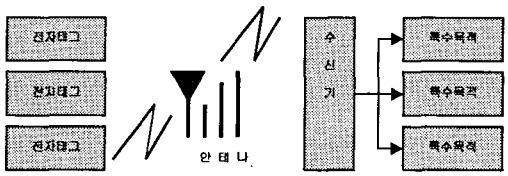

그림1. RFID 시스템의 개요

• RF SecureWARM 시나리오

공공의 장소인 학교는 여러 사용자가 한대의 PC를 사용한다. 그러나 보안에 많은 노출이 되어 있고 개인정보의 유출이 걱정됨에도 아무런 관리를 하기 힘들다. 그래서secure WARM을 가지고 간단히 보안을 할 수 있음을 전개해 보았다. 학생은 RFID 학생증을 소지하고 다니며, 학교의 컴퓨터는 많은 사용자가 사용한다. 미희 학생은 누가 도용했는지는 모르지만 자신의 과제문서가 지켜졌다는 사실로도 많은 즐거움을 느낄 것이다. 이 시나리오는 일부분의 상황 설정이다. 하지만 이것이 대규모의 사업장과 치열해지는 경쟁사회에서 개인의 정보는 개인의 경쟁력이며, 자산과 동일 시 된다. 최소한의 자신의 정보에 접근하는 사용자를 미연에 차단하여야 한다는 개념과 동시에 나중에 어떤 사용자가 접근했냐는 것조차도 공신된 기관으로부터 사전승인을 받아 확인을 할 수 있겠다.

III. RF SecureWARM 동작과정

시스템이 시작되면 윈도우로 부팅되고 나서 시스템운영체제는 SecureWarm을 실행하게 된다. SecureWarm에서는 시스템을 사용할 수 없게 보안모드를 띄우게 되며, 이때 사용자는 시스템을 사용하기 위해서 카드를 단말기에 올려놓아야 한다. 사용자가 단말장치에 카드를 올려놓았을 경우, SecureWarm은 카드의 정보를 읽어와 서버에 그 정보를 보내고 시스템 접근권한이 있는 사용자인지 판단한다. 만약 카드의 소유자가 인가된 사용자일 경우 보안모드가 해제되며 시스템을 사용할 수 있게 되며, 비 인가된 사용자일 경우 다시 보안모드로 돌아가 비 인가된 사용자는 시스템을 사용할 수 없도록 제한한다.

• RF SecureWarm Base Architecture & User Interface

시스템을 제어하기 위한 입력장치(키보드와 마우스)로 통해서 운영체제로 전달해주는 역할을 하게 되는데, 이 메시지를 가로채서 인증된 사용자만 시스템을 사용할 수 있게 도와주는 S/W가 RF Secure 이다.

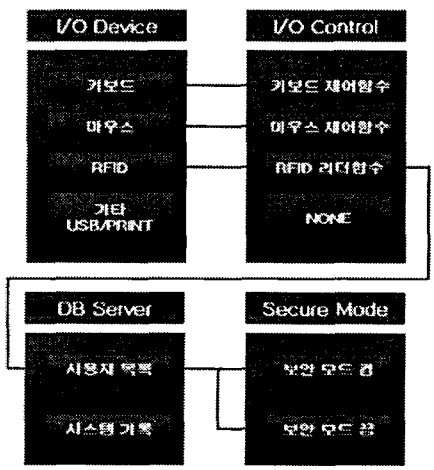

그림2. RF Secure Warm Base Architecture

• **보안모드(Secure Mode)**

인증되지 않은 사용자가 시스템을 사용할 수 없도록 제어하는 프로그램의 화면이다, 사용자에게 인증해야만 사용 할 수 있다는 간단한 화면이 표시되며, RFID카드를 리더기에 올려놓았을 경우 그 카드의 정보를 읽어 DB서버에 인증을 요구하며 해당시각과 카드의 정보를 기록하고 인증된 사용자는 보안모드가 해제되며 인증되지 않은 사용자는 보안모드가 해제 되지 않으며 인증에 실패했다는 사실을 알려준다

그림3. UI 보안화면-UI 시스템화면

• 사용자 인터페이스 (User Interface)

일반 사용자의 UI는 보안화면밖에 없으며, 관리자만이 환경설정 메뉴를 관리할 수 있다.

• 환결설정메뉴(RF SecureWARM)

관리자가 환경을 설정하는 방법은 관리자의 카드를 수신기에 올려놓고, 트래이 아이콘에 있는 설정(관리자)메뉴로 들어가면 된다. (일반 카드로 접근이 불가능함)

• RF ScureMode

사용자의 환경에 맞게 설정해주기 위한 관리자 메뉴이다

- Skip Card : 카드를 수신기에 올려져 있을 때만 보안모드를 해제함
- Check Card : 카드를 수신기에 올려놓았을 경우 보안모드가 해제되며, Time Rate 시간(분)이 지나도록 시스템을 사용하지 않을 경우 자동으로 보안모드가 됨

• **Database Setting**

데이터베이스에 시스템의 사용을 기록하기 위한 환경설정

- DBSelect : 데이터 베이스의 버전을 체크해주면된다. 이하(mSQL,MySQL,Oracle)설정가능
- ServerIP : DB서버의 IP주소를 입력한다.
- Account : DB서버의 계정을 적는다.
- Password : DB서버의 계정과 일치하는 패스워드를 적는다.

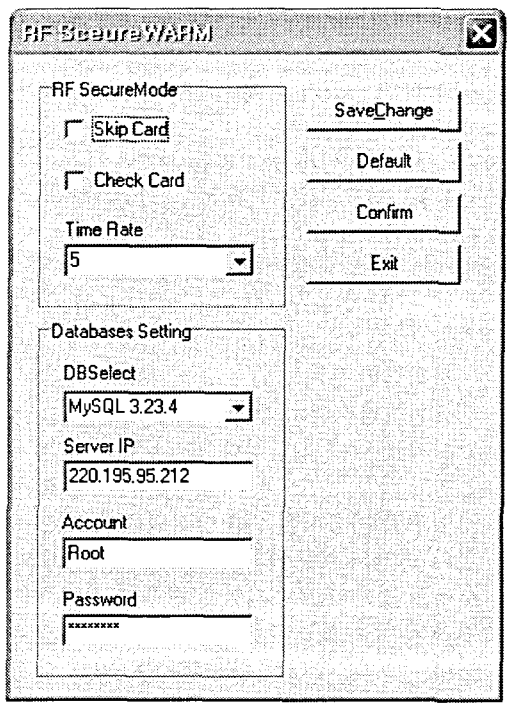

그림4. UI - RF SecureWarm 관리자 메뉴

IV. Secure Warm 문제

• 사회적인 문제

- 시장형성이 제대로 갖추어진 곳이 없다.
- 문서나 정보의 보안의식이 부족하다.
- 수신기와 카드를 구입해야 사용이 가능함으로, 경제적인 부담감이 크다.

• 사용자 문제

- 카드를 분실했을 경우 카드의 도용이 매우 쉽다.
- 해당 기업의 카드는 해당기업에서만 사용이 가능하다.

- 수신기의 고장이나 도난 시 시스템을 사용할 수 없게 된다.
- 유지보수가 관리자가 필요로 한다.

• 기술적 문제
- Secure Warm 프로그램이 해커로부터 중단될 가능성이 있다.
- DB서버가 다운되었을 때, 모든 시스템을 사용할 수 없게 된다.
- RFID 표준화가 되지 않아, H/W선택이 까다롭다.
- 모든 H/W에서 동작하는 모듈(S/W)을 개발해야 한다.
- CPU점유율이 높다.

V. Secure Warm 해결방안

• 사회적인 문제

유비쿼터스의 대중화가 되고 있는 지금의 보안체제는 너무 취약하다고 볼 수 있다. 공공기관이나 사무 공간에서의 보안은 더욱 필요한 실정이지만 사용자의 가치인식의 부족으로 최소한의 보안도 이루워지지 않고 있다. 현재 시스템에서 정보가 도용되었을 경우 언제, 누가, 어떻게 무엇을 했는지 알 수 없기다 하지만 유비쿼터스 생활 속에서 아용되는 RF카드에 있는 정보를 이용하여 최소한의 보안을 지킬 수 있다

• 사용자 문제

카드의 분실 도용을 막기 위해서 MD5 암호화를 하며, 타 기업에서 사용할 수 있도록 S/W를 기획하고 있으며 시스템 이벤트 로그를 기록하므로 유지보수를 편리하게 할 수 있다. 카드의 분실은 관리자에게 재발급 아 사용이 가능하다

• 기술적 문제

올바른 코드 작성과 최소한의 코드로 프로그램을 작성과 시작과 동시에 서버로부터 시스템 인증키를 발급하여 해커나 크래커로부터 보호하게 제작할 것이며, DB서버가 다운되지 않도록 로컬에 서버를 설치하는 방향으로 코드를 작성할 것이다. RFID의 표준화가 되기 전 모듈을 작성하서 사용하고, 이후에 모듈을 변경하여도 S/W가 동작하도록 설계되어 있다.

VI. 결론

현재 국내 RFID분야는 도입단계 이므로 전체시장의 흐름과 어느 정도 보조를 맞추면서 선점할 수 있는 시장을 엿보아야 한다고 본다. 그리하여 미들웨어 수준의 소프트웨어는 아니지만 하드웨어와 소프트웨어의 접목에서 소프트웨어가 큰 비중을 차지하면서 높은 효율적 측면을 나타 낼 수 있다는 아이디어를 제안함으로서 향후 사업비중의 변화가 생길 수 있다고 보여진다. RFID 분야의 하드웨어에 국한 되었던 것이 소프트웨어 분야와도 많은 결합을 하게 되면서 또 다른 시장의 형성 될 것으로 예상되며, Open Source의 개념을 개발당시부터 염두하고 개발하여 타 사용자가 용이하게 이 Source를 사용가능하게 개발하였다. 국내 RFID S/W 시장에 발전을 기대 할 수 있을 것이다

참고문헌

[1] Tilmann H, "On/off phase shoft keying for chaos encrypted communication using external cavity semiconductor lasers". IEEE J. of QE, v.38, n.9, sep. 2002, pp.1162-1170

[2] Shuo T, "Effects of message encoding and decoding on synchronized chaotic optical communication", IEEE J. QE, v.39,n.11, Nov, 1003, pp1468-1474