

RFID를 이용한 오피스 보안 및 자동화 시스템의 설계 및 구현

이승철⁰, 고명철¹, 김정환², 한덕수³, 양권우⁴
건국대학교 컴퓨터소프트웨어학과⁰¹²
육군3사관학교 전산정보처리학과³
공주교육대학교 컴퓨터교육학과⁴

whitepoem@lycos.co.kr⁰, (cheol¹, jhkim²)@kku.ac.kr, dshan123@hanmail.net³, kwyang@gju.ac.kr⁴

Design and Implementation of Office Security and Automation System Using RFID

Seungcheol Lee⁰, Myeong-Cheol Ko¹, Junghwan Kim²
Dept. of Computer Science, Konkuk University
Deok-Soo Han³
Dept. of Computer Science, Korea Third Military Academy
KwonWoo Yang⁴

Dept. of Computer Education, Gongju National University of Education

요 약

최근 보안에 대한 사회적인 관심이 높아지면서 RFID는 기존의 스마트카드와 바코드 시스템이 갖는 여러 기능적인 한계점들을 극복함으로써 향후 이를 대체할 보안 신기술로서 인식되고 있다. 현재 사무실 출입의 보안을 위해 대표적으로 사용되고 있는 출입문 인증시스템은 일단 출입문을 통과한 사용자들에 대해서는 사무실 내부의 모든 요소들이 무방비 상태로 노출되어 보안상의 허점이 발생한다. 또한 사무실 내 개개의 PC에 단말기를 설치하여 사용하는 스마트카드 인증시스템 역시도 빈번한 자리 이동에 따른 카드 인증 절차의 번거로움으로 인해 근거리 이동시 PC를 잠그지 않는 경우가 빈번하게 발생함으로써 사용자 PC에 저장된 보안이 필요한 데이터들에 대한 침해 우려가 발생한다. 본 논문에서는 다중사용자 환경에서 각각의 사용자가 소지한 RFID 태그를 이용하여 기존 카드시스템과 같이 복잡한 인증절차가 필요 없고 빈번한 자리 이동이 발생하더라도 추가적인 인증작업이 없이 매번 자동으로 컴퓨터 시스템을 잠금 및 해제시킴으로써 인증과정에 따른 사용자의 부담을 줄일 수 있는 보안시스템을 제시한다. 또한 사용자가 출근과 동시에 매일 일상적으로 반복되는 사무실에서의 컴퓨터 작업에 대한 효율을 높이기 위한 사무 자동화 시스템을 구현한다.

1. 서 론

최근 사회적으로 보안에 대한 중요성이 인식되면서 컴퓨터시스템의 정보 보호를 위한 다양한 보안 기술들이 등장하였다. 현재 규모 있는 상당 수 회사에는 대부분 건물, 층 혹은 사무실 단위로 보안을 위한 출입문 인증시스템이 설치되어 있다. 출입문 통과를 위한 인증방식도 스마트카드나 생체인식 기술을 이용할 정도로 현재의 보안 기술은 매우 발달되어 있다[1]. 그러나 이러한 생체인식 시스템이나 스마트카드와 같은 진보된 보안 기술을 이용하더라도 일단 출입문을 통과하고 나면 사무실 내부의 보안을 요하는 모든 컴퓨터 시스템들이 출입자들에게 무방비 상태로 노출되게 된다. 대한상공회의소가 2006년 국내 기업 400개사를 대상으로 실시한 '국내기업의 산업기밀 유출실태' 조사에 따르면 20.5%가 회사기밀정보로 인한 피해를 경험했다고 응답했다[2]. 미국의 경우 2006년 CSI/FBI Computer Crime and Security Survey에 따르면 1999년부터 2006년 사이의 모든 조사대상의 50%이

상이 사용하는 컴퓨터 시스템에 인증되지 않은 접근이 있었다고 응답하였다[3]. 이러한 결과는 컴퓨터시스템에 대한 현재의 보안 기술 수준이 아직도 매우 낮다는 사실을 단적으로 보여준다고 할 수 있다.

대부분의 사무실에서 일단 출입문 인증시스템을 통과한 사용자들에 대해서는 사무실 내의 모든 컴퓨터시스템들이 거의 무방비 상태로 노출되게 된다. 물론 허가되지 않은 사용자로부터 시스템을 차단하기 위해 운영체제에서 지원하는 화면보호기 같은 프로그램을 이용 할 수 있다. 그러나 짧은 시간 동안 근거리 이동이 빈번하게 발생할 경우 시스템을 잠그지 않게 되어 일시적으로 보안에 구멍이 생길 수 있으며 화면보호기가 작동되는 시간 간격을 짧게 설정하더라도 매번 수동으로 로그인 과정을 거쳐야하므로 많은 번거로움을 초래할 수 있다. 보안이 좀 더 중요시 되는 곳에서는 컴퓨터시스템에 스마트카드 인증시스템을 직접 장착하여 키보드에서 발생하는 Keystroke 해킹 등으로부터 시스템을 보호하기도 한다[4]. 그러나 스마트카드 인증시스템 역시도 빈번한 자리 이동으로 인한 카드 인증 절차의 번거로움을 유발한다.

본 연구에서는 사무실 내 개인 컴퓨터시스템 단위로 보안기능을 처리하기 위한 오피스 보안 시스템에 대해 연구한다. 제안하는 보안 시스템은 개인이 소지한 RFID 태그를 이용함으로써 기존 스마트카드 인증시스템이 갖는 장점을 살리면서도 복잡한 인증절차가 필요 없고 빈번한 자리 이동이 발생하더라도 추가적인 인증작업이 없이 매번 자동으로 컴퓨터시스템을 잠금 및 해제시킴으로써 인증과정에 따른 사용자의 부담을 줄일 수 있다. 제안하는 시스템은 다중 사용자환경 하에서 서로 다른 권한을 갖는 다수의 사용자가 동시에 컴퓨터시스템에 접근했을 때에도 이를 구분하여 처리해 줌으로써 보다 수준 높은 보안 기능을 제공한다. 또한 사용자가 출근과 동시에 매일 일상적으로 반복되는 사무실에서의 컴퓨터 작업에 대한 효율을 높이기 위해 인증과정이 끝남과 동시에 사용자의 권한에 따라 일련의 프로그램들을 자동으로 실행시키는 사무실 자동화 시스템을 구현한다.

2. 관련 연구

RFID(Radio Frequency Identification)란 마이크로 칩이 내장된 TAG, Label, Card 등의 장치와 리더기간에 무선주파수를 이용하여 데이터를 송수신하는 자동인식 기술을 의미한다. RFID태그는 일반 바코드와 같이 고유 ID를 가질 수 있으면서 무선으로 수 미터까지 인식이 가능하다. 또한 고속으로 이동하는 여러 개의 태그 인식이 동시에 가능하며 대용량 데이터의 저장이 가능하다[5]. 이 외에도 기존 바코드(Barcode)와 비교하여 RFID가 가지는 장점은 <그림-1>과 같으며[6] 이러한 특징들로 인해 바코드 시스템이 갖는 여러 한계점들을 극복함으로써 향후 이를 대체할 신기술로서 인식되고 있다. 비록 태그의 저가격·저전력·소형화 문제, 효율적 인식문제, 사용자의 보안 및 프라이버시 문제, 태그 식별자의 코드 표준화 문제, 다중 태그 식별 문제 등의 해결되어야 할 과제들이 남아있지만 이와 관련된 연구가 현재 활발히 진행되고 있다[7][8].

구분	Barcode	RFID
인식거리	0-50cm	0-5M
인식속도	4초	0.01-0.1초
투과력	불가능	투과가능(금속제외)
재사용여부	불가능	가능
보안능력	거의없음	복제 불가능
데이터 쓰기	불가능	가능

<그림-1> 바코드와 RFID 비교

RFID가 USN의 핵심기술로 대두되기 전에는 암호화를 통한 보안 기능이 뛰어나고 위조카드 제작이 어려운 안정성으로 인해 스마트카드가 각광을 받았었다[9]. 스마트카드는 IC Card, Chip Card, Microprocess Card, CPU Card 등의 이름을 가지고 있으나 일반적으로 마이크로프로세서, 카드운영체제, 보안 모듈, 메모리 등을 갖추으로써 특정 트랜잭션을 처리할 수 있는 능력을 가진 집적회

로 칩(Integrated Circuit Chip)을 내장한 신용카드 크기의 플라스틱 카드를 지칭한다[10]. 스마트카드는 <표-1>과 같이 인터페이스에 따라 크게 접촉식과 비접촉식으로 구분할 수 있으며 메모리의 공유 형태에 따라 하이브리드 및 콤비 카드로 나눌 수 있다[11].

<표-1> 스마트카드의 종류

인터페이스 방식에 따른 분류	
접촉식(Contact)	비접촉식(Contactless)
관독기와 스마트카드 칩 사이에 물리적인 접촉을 통해 작동하는 카드	카드 내에 내장되어 있는 안테나를 이용한 무선주파수를 통하여 통신하는 카드

메모리 공유 형태에 따른 분류	
하이브리드(Hybrid)	콤비(Combi)
하나의 카드 내에 물리적으로 접촉식 카드와 비접촉식 카드가 독립된 형태로 존재(메모리 공유 불가능)	하나의 카드 내에서 접촉·비접촉식 카드가 공유하는 결합형 카드(메모리 공유 가능)

이중 <그림-2>에서처럼 Contactless 방식의 스마트카드가 13.56MHz 주파수 대역을 이용하는 RFID 기술을 사용한다. 이러한 특성으로 인해 스마트카드와 RFID의 개념이 종종 혼용되기도 한다.

주파수 구분	특징	적용 가능분야
저주파수 대역 (125kHz & 134kHz)	- 짧은 인식거리(1m이하) - 저가형 - 느린 인식속도	- 출입통제 - 동물식별 - 재고 관리
중간주파수 대역 (13.56MHz)	- 동적개발 - 상호호환성 적용 - 비금속 장애편의 투과성 우수	- 출입통제 - 스마트카드
고주파수 대역 (433MHz)	- 고가형 - 동종방출 - 긴 인식거리	- 컨테이너 식별 및 추적
고주파수 대역 (860-960MHz)	- 저가형, 장거리 인식(~10m) - 금속 및 액체 인식률 저조 - 수동형	- 동물동물류 분야
마이크로파 대역 (Microwave, 2.45GHz)	- 장거리(~27m) - 빠른 인식속도 - 차폐물이 있는 경우 인식 불가 - 고가형	- 자동차 운반 효율 모니터링 - 텔레마트 시스템

<그림-2> 주파수 종류별 특성[12]

스마트카드에 대한 상호 운용성 문제를 해결하고자 PC/SC Workgroup이 설립되었고[13], 그중에서도 Microsoft사에서는 클라이언트 인증, 코드 서명 및 전자메일 보안, Microsoft® Windows Server 2003 제품군 도메인에 로그인 등의 작업에 보안 솔루션을 제공하는 휴대용 부정 조작 방지 수단으로 접촉식 스마트카드를 사용하고 있다[14]. 그러나 기본적으로 접촉방식의 스마트카드는 복잡한 인증과정과 수동 조작의 번거로움으로 인해 실용성이 떨어진다.

따라서 본 논문에서는 이러한 기존 보안방식이 갖는

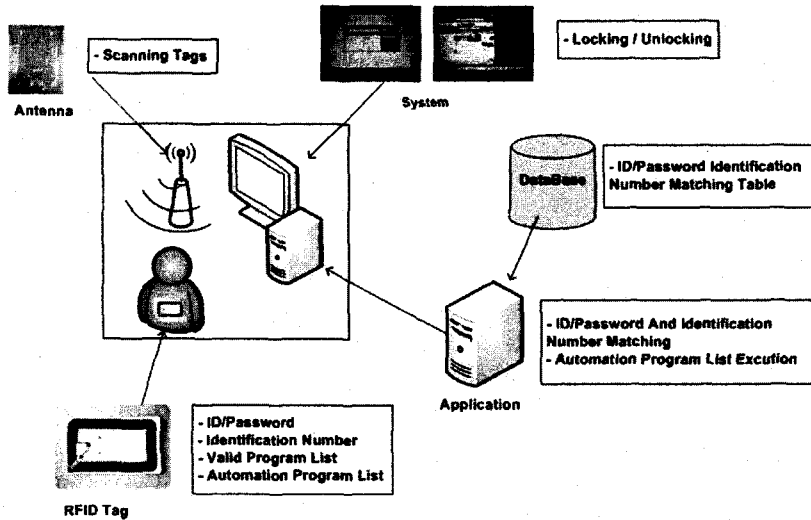
단점을 해결할 수 있는 RFID 기술을 이용한 자동 보안 인증시스템을 제시하고자 한다.

3. 시스템 설계

본 시스템은 내부적으로 오피스 보안시스템 및 오피스 자동화시스템으로 구성되어 있다. 본 절에서는 RFID를 기반으로 하는 오피스 보안 및 자동화 시스템의 전체적인 구성과 제어흐름에 대해 설명한다.

시스템을 사용할 수 있으므로 각 사용자의 권한 정보를 소지한 태그 내에 기록함으로써 이에 따라 유동적인 PC사용을 제공하게 된다.

RFID Reader에서 태그로 신호를 보내고 태그가 응답하는 Passive 방식은 태그가 여러 개 일 경우 충돌이 발생하는데 이러한 충돌은 대역폭의 낭비나 태그 인식을 저하시킨다. 이와 같은 다중 태그 식별 문제(Multiple Tag Identification Problem)에 관해서는 Bit-arbitration Algorithm, Splitting Tree Algorithm, Tree-walking Algorithm, Query Tree Algorithm 등 다양한 알고리즘



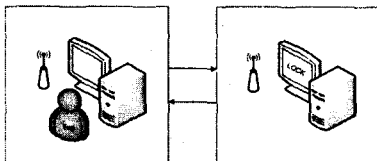
<그림-3> 시스템 구성도

<그림-3>은 본 논문에서 구현하고자 하는 시스템의 전체적인 구성도이다.

이 연구 되고 있다[15][16][17]. 본 논문에서는 Anti-Collision 프로토콜을 내장하고 있는 RFID Reader를 사용한다.

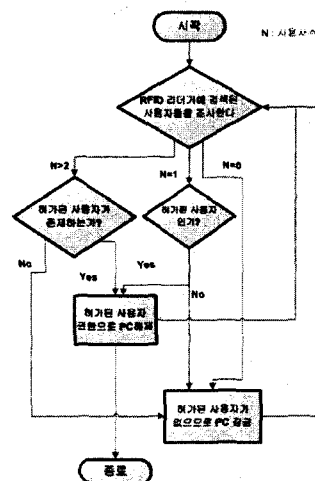
● RFID 기반 오피스 보안시스템

본 논문에서는 빈번한 자리 이동시 컴퓨터를 잠그기 위한 자동인증 도구로서 RFID 태그를 사용한다. RFID는 비접촉식이면서 이동 중에도 인식이 가능하므로 <그림-4>와 같이 태그를 소지하고 있는 사용자가 급하게 자리를 비우더라도 리더가 이를 순간적으로 인식하여 사용중이던 PC를 잠그게 된다.



<그림-4> RFID 기반 보안시스템

<그림-5>와 같이 2명 이상의 사용자가 PC에 동시에 접근할 경우 이를 구분하여 사용자의 PC를 잠그는 유동적인 처리로 보다 수준 높은 보안기능을 제공한다. 다중 사용자환경에서는 여러 명의 사용자가 하나의 컴퓨터시



<그림-5> 시스템 제어흐름도

이상과 같이 RFID의 무선 인식기능에 의한 자동 인증 방법을 사용함으로써 기존의 스마트카드와 같은 수동식 인증 방법이 갖는 불편함을 크게 해소하게 된다.

● RFID 기반 오피스 자동화시스템

오피스 자동화 시스템은 크게 두 가지 기능을 가진다. 첫 번째는 태그를 소지한 사용자가 PC를 처음 부팅했을 때 매번 실행하는 프로그램이나 정해진 시간에 꼭 실행되어야 할 프로그램 등을 선택하여 태그에 기록 하는 기능이다. 두 번째는 이렇게 사용자의 태그에 기록된 정보를 감지하고 정해진 프로그램을 실행하는 기능이다.

이러한 기능들을 지원하기 위해 오피스 자동화 시스템은 <그림-6>과 같이 시작상태(PC를 처음 부팅 시켰을 경우), 실행상태(허가된 사용자가 PC를 사용 중인 경우), 종료상태(PC 사용을 마친 경우) 등 세 가지 상태를 가지게 된다.

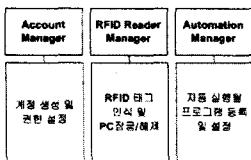
시작 상태	실행 상태	종료 상태
태그 인식에 관련 시 작 프로그램 실행	태그 인식에 관련 시 작된 보안 모듈 / 지정된 시간에 프 로그램 자동 실행	시작상태 시에 자 동으로 실행될 프 로그램을 태그에 저장

<그림-6> 상태에 따른 기능

시작 상태에서는 사용자가 기존에 태그에 저장해 놓은 정보에 따라 자동으로 일련의 프로그램들을 실행하는 기능을 수행하게 된다. 실행 상태에서는 항상 실행되어야 하는 프로그램의 정보를 태그에 기록하며 앞서 3장에서 언급한 오피스 보안시스템에 의한 구동이 함께 이루어지게 된다. 마지막으로 종료 상태에서는 다음 실행 시에 자동으로 실행될 프로그램 목록 등 태그에 저장되어야 할 정보들이 자동으로 저장되게 된다.

4. 시스템 구현

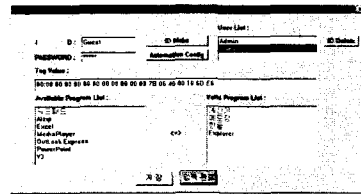
본 논문에서 구현한 시스템은 <그림-7>과 같이 Account Manager, RFID Reader Manager, Automation Manager 등 크게 세 개의 모듈로 구성된다.



<그림-7> 시스템 모듈과 기능

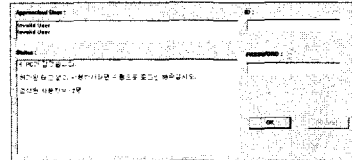
먼저 Account Manager는 시스템 사용권한이 있는 사용자가 RFID 태그가 없을 때에도 시스템의 잠금 상태를 수동으로 해제 할 수 있도록 해당 사용자의 계정을 생성하고 권한을 부여하는 기능을 담당한다. <그림-8>과 같이 접근을 허가하고자 하는 사용자의 계정을 신규로 생

성할 수 있으며 각각의 사용자에 대한 오피스 자동화 기능을 지원하기 위해 프로그램의 사용권한을 목록으로부터 지정해 줄 수 있다.



<그림-8> Account Manager Interface

다음으로 RFID Reader Manager는 RFID Reader에서 보내온 태그 정보를 인식하여 시스템의 잠금 및 해제 여부를 판단하여 처리한다. 각각 서로 상이한 권한을 갖는 여러 명의 사용자가 동시에 시스템에 접근하는 경우 RFID Reader로부터 보내오는 정보에는 이러한 내용들이 포함되어 RFID Reader Manager는 이러한 정보를 바탕으로 적절한 인증처리를 수행하게 된다. <그림-9>는 시스템에 접근하는 여러 태그들을 <그림-10>에 따라 식별하여 사용자의 수 혹은 권한의 정도에 따라 구분하여 처리한 결과를 보여주고 있다. RFID Reader Manager Interface에는 RFID태그를 소지 하지는 않았지만 시스템 사용이 허가된 사용자가 수동으로 로그인하기 위한 기능이 포함되어 있다.



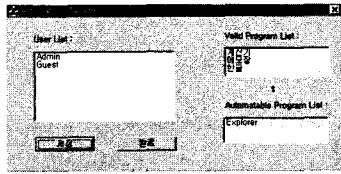
<그림-9> RFID Reader Manager Interface

		N>1	N=1	N=0
허가된 태그	있다	Unlock	Unlock	Lock
소지 여부	없다	Lock	Lock	

<그림-10> 검색된 태그에 따른 시스템 잠금 및 해제(N: 검색된 태그의 수)

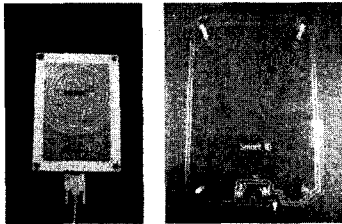
마지막으로 Automation Manager는 오피스 자동화 기능을 처리하기 위한 모듈로서 각 사용자가 인증절차 이후에 자동으로 실행하고자 하는 프로그램을 등록하고 처리하는 기능을 담당한다. Account Manager는 PC에 접근이 허가된 RFID 태그를 소지하지 않은 사용자의 컴퓨터 사용을 허가 할 수 있는 계정을 생성 하고 권한을 부여한다. Automation Manager를 통하여 설정할 수 있는 프로그램은 Account Manager에서 계정을 등록할 때 사용이 허가되었던 목록들에 대해서만 선택이 가능하다.

<그림-11>은 Automation Manager에서 각각의 사용자 계정에 따라 자동 실행할 프로그램 리스트를 추가하기 위한 인터페이스를 보인 것이다.



<그림-11> Automation Manager Interface

본 시스템의 구현은 Microsoft Windows XP 환경에서 Microsoft Visual C++ 6.0을 사용하였다. RFID Reader로는 EPCGlobal Inc.에서 제정한 EPC HF(13.56MHz Band) Class-1 Air Interface Protocol과 ISO 15693(ISO 18000-3 Model) 등 13.56MHz 기반의 다양한 프로토콜을 지원하는 eco사의 Multi-Protocol RFID Reader ER200을 사용하였다<그림-12>. 본 Reader는 Anti-collision 알고리즘을 바탕으로 태그의 동시인식 속도가 빠르면서 안정적인 장점을 가지고 있다.



<그림-12> Multi-Protocol RFID Reader

<그림-13>은 본 시스템에서 RFID 기반 시스템 보안을 처리하기 위한 세 가지 화면 형태를 보여주고 있다. 각각 검색된 사용자가 없는 경우와 검색된 사용자가 있지만 시스템이 잠긴 경우 그리고 허가된 사용자가 검색되어 시스템 잠금이 해제된 경우의 상태를 보여주는 화면이다.



<그림-13> 검색된 사용자가 없는 경우(좌), 검색된 사용자가 있는 경우(중), 허가된 사용자인 경우(우)

5. 실험 및 분석

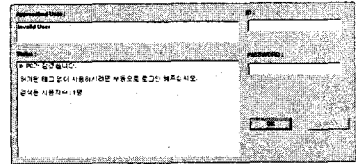
본 절에서는 제안하는 시스템을 다양한 사용자 접근 상황에 적용시켜 제안하는 시스템의 실용성에 대해 실험한다.

● 오피스 보안 시스템

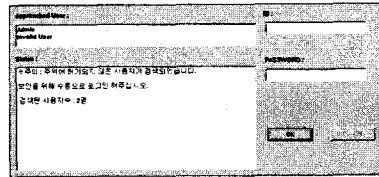
오피스 보안시스템은 허가받지 않은 사용자만 검색된 경우, 허가받지 않은 사용자와 허가된 사용자가 동시에 검색된 경우, 그리고 검색된 사용자가 전혀 없는 경우

등 세 가지 경우에 시스템을 잠그게 되어있다.

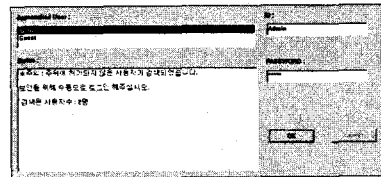
<그림-14>는 허가 받지 않은 사용자가 검색 되었을 때 이를 화면에 출력하고 시스템을 잠그는 과정을 보여 주고 있다. <그림-15>의 경우는 검색된 사용자가 두 명 이상이며 그중 허가된 사용자가 있는 경우이다. 이와 같은 경우 검색된 사용자가 기 설정해 놓은 잠금해제 기능에 따라 잠금을 해제시키거나 권한이 없는 사용자와 같이 있으므로 계속적으로 잠금을 유지하는 등의 처리가 가능하다. 또한 <그림-16>과같이 수동으로 잠금을 해제시킬 수도 있다.



<그림-14> 허가받지 않은 사용자



<그림-15> 2명 이상이고 그중 허가된 사용자가 있는 경우



<그림-16> ID/PASSWORD를 통한 수동식 로그인

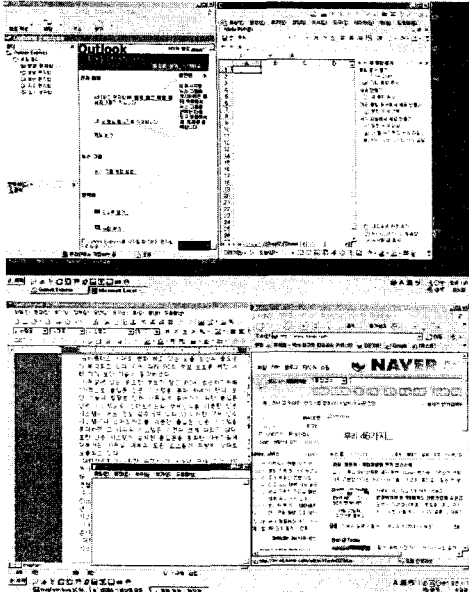
위와 같은 일련의 잠금 및 해제 처리는 매순간 매우 짧은 시간 동안에 자동으로 처리되는 작업으로서 기존 스마트카드 인증 시스템이 가지는 수동식 인증 방식의 번거로움을 해결하여 사용자가 짧은 시간동안 급하게 자리를 비우는 경우가 빈번히 발생하더라도 보안 공백이 생기지 않게 된다.

태그를 소지한 여러 명의 사용자가 동시에 접근했을 때 발생할 수 있는 다중태그 식별문제는 본 논문에서 사용한 RFID Reader 자체에서 Anti-Collision 프로토콜을 지원하기 때문에 문제가 발생하지 않았다. 하지만 현재 이 분야의 다양한 연구가 진행되고 있는 만큼 태그의 인식률을 높이기 위한 보다 효율적인 알고리즘을 향후 개발하고자 한다.

● 오피스 자동화 시스템

오피스 자동화 시스템은 사용자가 컴퓨터를 처음 켜고 동시에 검색된 사용자의 태그에 기록된 정보를 읽어 들여 해당 사용자가 설정해 놓은 일련의 프로그램들을 자동으로 실행시키게 된다. 여기서 본 시스템은 다중 사용

자환경을 지원하므로 해당 사용자가 실행권한을 가지고 있는 프로그램들에 대해서만 자동 실행이 가능하다. <그림-17>은 다중 사용자환경 하에서 여러 명의 사용자가 각각 설정한 서로 상이한 자동 실행 환경에 따라 오피스 자동화 시스템이 처리한 결과를 보인 것이다.



<그림-17> 사용자에 따른 프로그램 자동 실행

6. 결론 및 향후 과제

본 논문에서는 기존 스마트카드가 가지는 수동 인증작업의 번거로움을 해결하기 위해 RFID의 자동 인증 기능을 활용한 오피스 보안 및 자동화 시스템을 제안하고 구현해 보았다. 태그에 정보를 효과적으로 저장하는 기술이나 다중사용자의 처리문제, 수동식 로그인의 인증 기간 문제 등 몇 가지 보완해야 할 부분들이 남아있으나 다양한 테스트를 통해 본 논문에서 제안하는 RFID 기반 자동인식 기술은 기존 수동식 인증의 불편함을 크게 줄여 줄 수 있을 것으로 기대된다. 또한, 다중 사용자 환경 하에서 하나의 시스템을 공유하는 서로 권한의 정도가 다른 여러 사용자들의 동시 접근 시 이에 대한 적절한 처리 방법을 제안함으로써 제안하는 시스템이 실제 보안 관련 분야에 충분히 활용이 가능함을 확인 할 수 있었다. 향후 연구로서 태그에 다양한 정보를 효과적으로 저장하고 액세스하기 위한 알고리즘의 개발을 계획하고 있다.

참고 문헌

[1] 한재중, 윤용운, HF/UHF RFID와 화상처리를 이용한 Hybrid 출입통제 시스템 사례, 한국정보처리학회 학회지,

Vol.12, No.5, pp.106-112, 2005

[2] 국내기업의 산업기밀 유출 실태조사, 대한상공회의소 (<http://www.korcham.net>)

[3] CSI (Computer Security Institute), 2006 CSI/FBI Computer Crime and Security Survey(<http://GoCSI.com>), 2006

[4] 박종원, 이궁해, 스마트카드를 이용한 사용자 인증 및 관리, 한국정보과학회 춘계학술대회, Vol.31, No.1 pp.514-516, 2004

[5] 정민화, RFID 국제·국가 표준화 동향, 한국정보처리학회 학회지, Vol.12, No.5, pp.27-33, 2005

[6] 강진석, RFID 기반의 혈액 유통 시스템 설계 및 구현, 한국정보처리학회 논문지, Vol.12-A, No.5, pp.405-412, 2005

[7] 권성호, 홍원기, 이용두, 김희철, RFID 시스템에서의 트리 기반 메모리래스 충돌방지 알고리즘에 관한 연구, 한국정보처리학회 논문지, Vol.11-C, No.6, pp.851-862, 2004

[8] 최재귀, 박지환, 효율적인 식별 기능을 가진 위조 불가 RFID Tag 가변 ID 방식, 한국정보처리학회 논문지, Vol.11, No.4, pp.447-454, 2004

[9] 김효식, 김석우, PC 액세스 제어와 암호화 기능의 프로토타입 구현, 한국정보처리학회 추계학술대회, Vol.4, No.2, pp.1393-1399

[10] KEBTechnology: http://www.kebt.co.kr/kebt2004/board/pds/board_read.asp?table=PDS&subclass=pds_smart&num=2&page=3

[11] Smavis: <http://smavis.ye.ro/tech/tech1.php>

[12] 무선인식(RFID) 산업 활성화 지원센터, http://www.rfidepc.or.kr/sub.asp?s_m=3&s=3_02

[13] Microsoft: <http://www.microsoft.com/korea/technet/win2000/smtcard.asp>

[14] Microsoft: <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/ko/library/ServerHelp/0e3a4f1c-8b17-4e04-9e3b-33ea42591796.mspx?mfr=true>

[15] L. Bolotnyy and G. Robins, Randomized Pseudo-Random Function Tree Walking Algorithm for Secure Radio Frequency Identification, Automatic Identification Advanced Technologies, 2005

[16] Marcel Jacomet, Adrian Ehram, Urs Gehrig, Contactless Identification Device With Anticollision Algorithm, University of Applied Sciences Berne, Biel School of Engineering and Architecture

[17] Jeongkeun Lee, Taekyoung Kwon, Yanghee Choi, Sajal K. Das, Kyung-ah Kim, Analysis of RFID anti-collision algorithms using smart antennas, Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, 2004