제27회 한국정보처리학회 춘계학술발표대회 논문집 제14권 제1호 (2007. 5)

RFID 를 이용한 복합기 보안 시스템

김철우
고려대학교 컴퓨터정보통신대학원 미디어공학과
e-mail : neos21@empal.com

A Multi-Function Printer Security System using RFID

Chul-Woo Kim
Dept. of Media Engineering, Korea University

요 약

오늘날 우리 사회는 정보 유출에 따른 심각한 현상들을 겪고 있으며 기업들은 정보 유출을 막기위해 많은 비용을 들이고 있는 실정이다. 정보 유출 중 문서 및 팩스를 이용한 1 차적인 문서 유출을 막기 위해 과거 기업들은 여러 방법들을 사용하여 왔다. 특히 기업은 보안과 동시에 업무 효율 그리고 비용 문제까지 고려 해야만 하는 실정이다. 본 고에서는 그러한 문제점들을 고려해서 현재 사용되어 지고 있는 보안 시스템의 개념과 운영 방법들을 논하고 그에 따른 개선점등을 바탕으로 새로운 RFID 을 이용한 복합기 보안 시스템을 제안하고자 한다. RFID 를 통해서 서버 인증을 실시하고 복합기에서 이를 바탕으로 사용 허가를 주는 방법으로 출입문에서 시작하여 주변기기로 이어지는 통합적인 시스템이다. 이는 보안성 및 경제성을 고려할 때 기업의 새로운 복합기 보안 시스템으로 정보 보안 및 기업의 경쟁력을 향상 시킬 수 있을 것으로 기대된다.

1. 서론

현재의 기업 환경에서는 기술의 발전과 경쟁이 날로 심해지면서 정보가 기업의 승패를 좌우하게 되었다. 기업들은 저마다 경쟁에서 이기려고 정보를 획득하고 정보를 방어하기 위해 모든 방법을 동원하고 있는 실정이다. 그러한 맥락에서 기업에서 사용하고 있는 사무기기에서의 정보 관리는 매우 중요하게 받아들여 지고 있는 게 사실이며 현재 모든 기업들은 저마다 보안 시스템을 사용하고 있고 그에 따라 소요되는 비용도 막대하게 증가하고 있다.

특히 기업의 보안 시스템의 최전방에 위치하고 있는 주변기기는 과거 아나로그로 운영되어지다 현재는 통합 운영되어 프린터, 복사기, 팩스, 스캔이 같이 이루어 지면서 보안 부분에 있어서 그 중요성이 대두되어 지고 있는 실정이다. 과거 기업들은 복합기를 사용함에 있어 단순히 패스워드를 사용하거나 사용자 IP 의 구분으로 보안을 적용 시켜 왔다. 하지만 보안 유출이 본 고에서 보여 주듯이 사람에 의해서 가장 많이 이루어 지기에 출입문 통제에서부터 이루어지는 인적 보안이 복합기로 연계되어 이어져야 함은 현재 복합기 보안 시스템의 화두로 여겨지고 있다.

복합기 업체들도 현 시점을 반영하듯 가장 앞선 기술로 IC 카드를 이용한 보안 시스템을 적용하고 있다. 그러나 IC 카드를 이용함에 따라 있을 수 있는 보안의 문제점과 불편함에 있어서 본 고에서는 RFID 를 이용한 복합기 보안 시스템을 제안하고 이를 이용함에 있어서의 경제적인 효과 등을 설명하려고 한다.

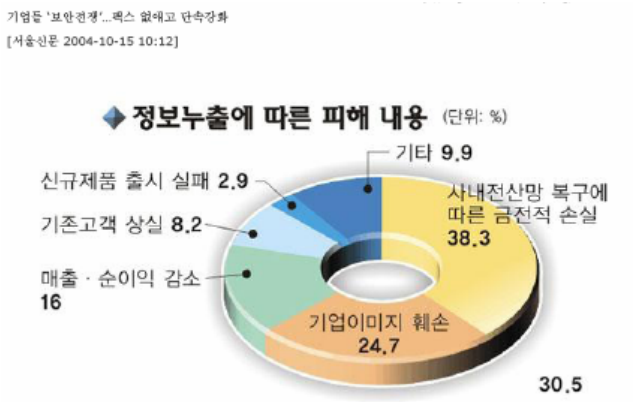
본 논문의 구성은 다음과 같다. 제 2 절에서는 기업의 보안 유출 실태와 심각성을 기술하고 기존 복합기 보안 방법을 기술한다. 제 3 절에서는 RFID 를 이용한 복합기 보안 시스템을 제안하고 그 구현 방법 및 실용성을 평가한다. 제 4 절은 결론과 시사점을 기술하고 참고문헌 언급으로 마무리 하겠다.

2. 정보 유출 실태 및 복합기 보안 방법

2.1 기업의 정보 유출 실태

기업의 정보 유출로 인한 피해는 금전적인 손실 뿐만 아니라 (그림 1)와 같이 다양한 방법으로 많은 손실을 끼치고 있다. 이와 같이 기업들은 막대한 손실을 방어 하기위한 보안의 방법으로 과거 1 세대보안인

Physical Group 보안에서부터 Network, Server 보안을 강조하였으나 현재는 4 세대 보안인 사용자 정보 보안에까지 필요성과 역할에 대해서 강조하고 있다.



(그림 1) 정보누출에 따른 피해 내용

즉 과거 자체 보안 규정을 수립하고 외부 해킹으로부터의 정보 보호나 방법에 편중했으나 기밀 정보 유출의 80%이상이 내부자에 의해 발생되면서 내부 정보 유출을 막기 위한 내부 보안 및 내부 사용자들이 접근 할 수 있는 PC, 주변기기에 대한 보안이 강화되고 있다. 기업들은 이러한 보안을 위해서 (그림 2) 와 같이 노력을 기울이고있다.

(그림 2) 기밀유출 대응 사례

하지만 이러한 기업의 노력에도 불구하고 유출 경로유출을 막기 위 방어를 위한 간접 비용이 날로 늘어나는 게 사실이다. 또한 주요 유출 경로가 (표 1) 에서 보듯이 단순 Copy 가 정보 유출의 대부분을 차지 하면서 적은 비용으로 가장 많은 정보 유출을 막을 수 있는 방법으로 복합기 보안이 기업에 있어서는 필수 환경으로 나타나게 된다.

정보유출경로	구성비	비고
인력이동(스카우트)	38.5%	디지털 Copy
복사	30.8%	Soft / Hard Copy
내부전산망(e-mail)	15.4%	
외부인력시찰/견학	15.4%	

<표 1> 정보유출 경로

복합기 보안은 기업이 내부자로부터 정보 유출을 막기 위해 선행 되어야 할 방법인 것이다.

2.2 복합기 보안 방법

복합기는 Copy, Scan, Print, Fax 등을 같이 사용할 수 있는 것으로 사무기기를 하나로 통합 했다고 할 수 있다. 그러므로 복합기 보안은 <표 2> 에서 보여지듯이 다양한 분야의 보안이 같이 이루어져 운영되는 방식이다.

복합기 기능	보안방법	보안 적용 법
COPY	워터마크	복사 문서에 특정 글자 인쇄
PRINT	사용자인증	비번 입력후 인쇄 실시
FAX	사용자인증 및 로그	비번 입력후 송수신 로그 보관
SCAN	사용자인증 및 PC 전송	비번 입력후 스캔 및 PC 이동

<표 2> 복합기 보안방법

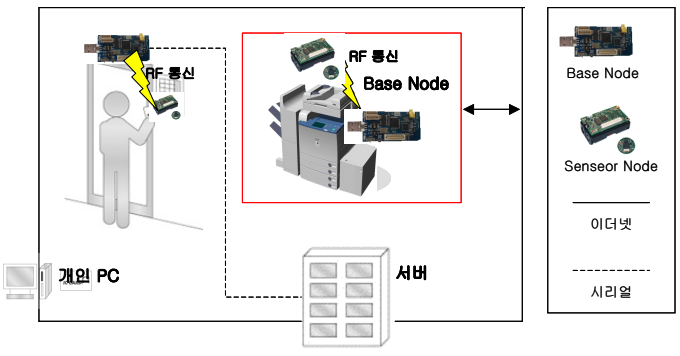
복합기는 각각의 정보 보안 방법을 적용하고 있으며 그 중 대표적인 보안 방법은 사용자 인증이다. 사용자 인증은 복합기 내부에 단순히 사용자 인증을 하여 사용하기 전 복합기에 로그인 하는 방법과 IC 카드를 이용하여 사내 네트워크로 사용자를 인증하는 방법으로 나눌 수 있다.

IC 카드로 인증하는 방법은 IC 카드를 사용하여 사내 네트워크에서의 서버 인증을 받아 PC 및 E-mail, 복사, 프린터 등을 통합하여 쓰는 시스템이다. 기존의 각각의 보안 시스템에서 이루어지는 사용자 인증을 하나로 통합하여 네트워크로 실제 근무자의 사용인증을 실시하지만 IC 카드를 복사기에 직접 접촉해야 한다는 점에서 개선점이 필요하다.

3. RFID 를 이용한 복합기 보안 모델

3.1 RFID 복합기 보안 모델 시나리오 및 개요

복합기 보안에 있어서 단순 복합기만을 보안하는 것은 전체적인 사용자 관리상 문제를 들어 낼 수 있다.

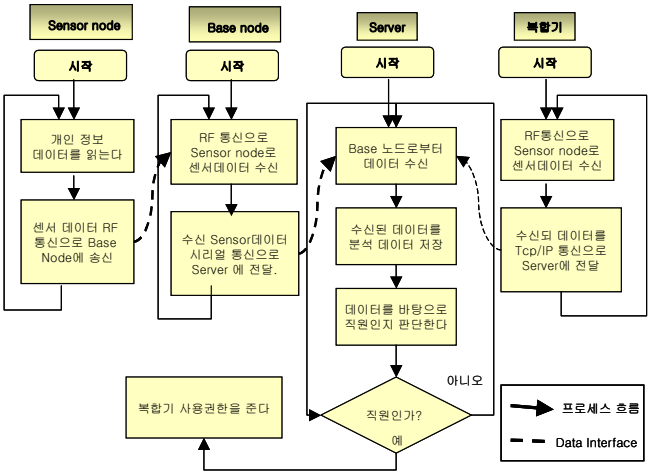


(그림 3) 시스템구성도

본 논문에서는 RFID 를 이용함으로 출입 통제에서부터 복합기 보안까지 연계하여 이루어져 단순 복합

기 보안이 아닌 실제적인 사용자 인증을 가능하게 하는 모델이다.

RFID 을 이용한 복합기 보안은 출입 시 사용자 정보를 가지고 있는 센서노드가 출입문에 고정되어 있는 Base 노드와 RF 통신을 통해서 개인정보를 전달하고 시리얼 통신으로 서버에 전달된 개인정보로 출입 인증을 실시한다. 인증된 사용자 정보는 복합기를 사용하기 위해 복합기 앞으로 접근 시 사용자가 가지고 있는 센서 노드와 복합기의 Base 노드 사이에 RF 통신을 통하여 사용자를 확인하고 사용자 인증을 실시하기 위해 서버로 UTP 케이블을 통해 정보를 보내고 서버에서 사용자 확인 후 로그인 된다. RFID 를 이용한 보안 시스템은 (그림 3) 에서 보듯이 사용자가 출입 시 사용자가 가지고 있는 사원 증 또는 사원 배지를 통해서 자동 체크되며 사용자가 복합기로 접근 시 출입 정보와 비교하여 자동 로그인 된다. 이때 복합기는 개인 PC 에서 보내는 프린터 출력 명령까지 수행 할 수 있으므로 PC 와 주변기기에서 중요시 되는 출력 보안을 이룰 수 있는 것이다.



(그림 4) RFID 복합기 보안 시나리오

RFID 복합기 보안에서 가장 중요한 것은 출입 통제의 일반적인 보안에 RFID 를 적용하고 이를 복합기 보안으로 까지 연동해서 적용한다는 것이다. (그림 4) 의 시나리오가 보여주듯이 복합기 보안 시스템이 출입통제 시스템에 RFID 라는 같은 인터페이스로 존재한다.

3.2 RFID 보안 복합기 구현

RFID 를 이용한 복합기를 구현하고 실제 테스트를 함으로 해서 RFID 를 적용한 복합기 보안이 일반적인 복합기 보안과의 차이점을 알고 이를 평가 할 수 있다.

실제 구현을 바탕으로 평가하기 위해 RFID 세팅한다. RFID 의 Mote 는 TI 사의 Hmote 을 사용하고 Mote 을 프로그래밍 하기 위해 TinyOS 을 사용한다. TinyOs 는 Hmote 의 전용 OS 로 사용되는 OS 이다. 서버는 윈도우 XP 를 OS 로 사용하고 복합기로는 캐논 IR4570 복합기를 사용하여 구현한다.

Sensor node 는 무선 통신으로 데이터를 송신하기 위해 InrToRfm 컴포넌트를 사용한다. IntToRfm 은 인터페이스 IntOutput 을 통해 출력값을 받고 이것을 무선으로 broacasting 하는 컴포넌트이다. 이때 주의할 점은 보내는 데이터를 기술하는 것, 받은 노드를 기술하는 것, 송출되는 메시지와 관련 메모리가 재 사용될 수 있는 때를 결정하는 것, 메시지를 버퍼에 저장하고 처리하는 것이다. Sensor Node 를 세팅한 다음 Base node 와의 통신을 위해 Base node 를 세팅한다.

Base node 는 Sensor node 로부터 송신된 데이터를 수신하는 기능이다. 데이터의 송수신은 RF 통신을 사용하는데 무선통신 데이터를 수신하기위해서 RfmTolnt 컴포넌트를 사용한다. RfmTolnt 는 메시지를 수신하기 위해 내부에서 GenericComm 을 사용한다. 다음은 RfmTolnt module 의 코드이다.

```
event Tos_msgPtr ReceiveIntMsg.receive(TOS_MsgPtr m)
   { IntMsg*message=(IntMsg *)m->data;
    Call IntOutput output(message->val);
    Return m; }
```

Base node 를 세팅한 다음은 Server 를 세팅하고 서버에 저장된 직원들의 이름과 Sensor 에서 가져온 데이터를 비교하여 인증을 시켜준다. 이때 Server 는 windows XP 을 기반으로 개발하며 Base node 로부터 전달되는 데이터를 분석해서 복합기에서 사용자 인증을 할 수 있도록 파일로 저장하는 기능을 한다.

복합기의 RF 통신 구현은 출입문에서의 통신 방법과 동일하게 구현되며 복합기에서 서버로 인증을 받을 수 있는 방법은 기존 캐논 IR4570 의 IC 카드 인증 컴포넌트를 사용한다.

3.3 실험 및 평가

RFID 을 구현한 시스템에서 RF 통신과 출입문 인증 및 복합기 인증 구현을 실험한다.

회차	출입문			복합기		
	센서거리	성공여부	개폐시간	센서거리	성공여부	인증시간
1	1M	실패	실패	1M	실패	실패
2	1M	실패	실패	1M	실패	실패
3	0.8M	성공	2.06 초	0.8M	실패	실패
4	0.8M	성공	2 초	0.8M	성공	2.3 초
5	0.5M	성공	1.8 초	0.5M	성공	2.1 초
6	0.5M	성공	1.7 초	0.5M	성공	2.1 초
7	0.2M	성공	1.5 초	0.2M	성공	1.8 초
8	0.2M	성공	1.6 초	0.2M	성공	1.7 초
9	0.1M	성공	1.3 초	0.1M	성공	1.5 초
10	0.1M	성공	1.5 초	0.1M	성공	1.3 초

<표 2> RFID 을 이용한 사용자 인증 실험결과

실험은 총 10 회를 실시하며 출입문 개폐 시간 및 복합기 로그인 시간 , 출입문 개폐 및 복합기 인증 성공 여부를 실험한다.

실험은 총 10 회에 걸쳐서 실시하고 실험에 있어서 센서와의 거리에 차이를 두어 각 2 번씩 실시하여 시간 및 성공여부를 체크 한다.

<표 2> 에서 보여지듯 센서의 거리에 따라서 성공여부가 차이가 난다. 센서가 가까울수록 출입문 및 복합기 인증이 빠르며 성공률도 높다. 즉 RFID 의 통신거리 및 인증 시 인증자의 위치에 따라서 RFID 의 성공률과 반응시간이 결정이 난다. 이 실험에서 보여지듯 RFID 의 통신이 안정화 된다면 복합기 보안은 안정적으로 이루어 질 수 있다는 것이다.

기존의 각각의 복합기 보안 시스템과 비교하면 복합기 RFID 를 이용한 복합기 보안을 평가 할 수 있다.

기존 복합기 보안 시 사용자 인증 방법만을 가지고 비교 평가 할 경우 출입문 개폐 인증이 수반 되므로 복합기 사용 인증만을 가지고 비교 평가 하겠다.

<표 3> 은 ID/PW 인증 및 IC 카드 인증으로 RFID 을 이용한 복합기 인증을 평가하는 표이다. 평가의 기준은 총 10 회의 평균으로 이루어지며 인증 시 진행되는 복합기 작동 절차와 작동 절차 전 기준선에서 복합기 앞 기준선에서 시작하기까지 걸리는 시간 그리고 인증 시간이다.

인증방법	인증절차	인증평균시간	인증전소요시간	비고
RFID	0	1.5 초	0 초	
PW/ID	3	15 초	2 초	홍길동/0
IC card	0	1.2 초	3 초	

<표 3> 인증 방법에 따른 비교

여기서 볼 수 있듯이 RFID 을 이용한 복합기 사용자 인증은 인증 속도에서는 ID/PW 인증보다 월등이 빠르지만 IC 카드 인증과는 인증 자체에 걸리는 시간은 비슷하다. 하지만 IC 카드가 인증을 하기 위한 사용자 패널 접근 시간이 필요한 반면 RFID 는 단순히 복합기 접근 만으로 인증 절차에 들어가기 때문에 시간 및 절차를 단축 할 수 있다.

4. 결 론

기업의 정보 유출을 막기 위한 방법으로 다양한 보안 방법론이 거론되고 있다. 그 중 4 세대에 해당하는 인적 보안이야 말로 기업들이 오늘날 보안에 가장 중점을 두는 분야이다. 이 인적 보안 중 가장 기초적인 것이 바로 출입 통제 및 PC 주변기기 보안이다. 그러한 의미에서 앞에서 거론한 RFID 복합기 보안이야 말로 출입 통제와 주변기기인 복합기의 사용자 인증을 연계한 효율적인 보안 방법이라고 하겠다. 특히 기존의 PW/ID 복합기 인증에 비해서 인증 속도 및 절차가 많이 개선되었으며 IC 인증에서 불편함으로 다가왔던 IC 패널 접근성 문제도 제거하는 방법이라고 할 수 있다. 단 RFID 의 종류 및 성능에 따라 거리에 따른 인증 실패도 일어나지만 이러한 문제는 H/W 의 성능 개선 및 인터페이스 위치 개선으로 충분히 개선 될 수 있는 것이다.

또한 RFID 의 특성상 사용자의 동선에 따른 위치 파악이 가능하며 층간 이동에 따른 복합기 연계 인증도 가능하여 그 확장성 또한 우수하다고 하겠다. 마지막으로 RFID 을 이용한 복합기 보안은 기존의 출입 통제 시스템과 디지털 복합기를 그대로 이용할 수 있으므로 초기 구축 비용마저 IC 카드 인증과 비슷하여 앞으로 기업들이 추구 할 정보 유출 방지 및 복합기 보안 방법으로 본 논문을 통해서 제안한다.

참고문헌

[1] MS Chen, D.Kandlur, and P. S. Yu. Storage and retrieval nethods to support fully interactive playout in a disk-array-vased video server. Multimedia Systems, 3(3):126-135, July 1995

[2] 최정무, 정보보호시스템 기준, 아주대학교 산업대학원 컴퓨터공학과, 2002.

[3] 이훈재, 이상곤 외, “스마트카드 비밀채널 평가/분석기술 연구”, 한국전자통신연구원 부설 국가보안기술연구소, 최종보고서, 2002

[4] E. Bihan and A. Shamir, “Differential Fault Analysis of Secret Key Cryptosystems” , Advanced in Cryptology CRYPTO ’97, LNCS 1294. pp.513-525, Springer-verlag, 1997

[5] EMV2000, “Integrated Circuit Card Specification for Payment Systems Book2” .

[6] Uyless Black(2000), “Internet Security Protocols Protecring IP Traffic” , Prentice Hall

[7] 권창영, 김경신, 원동호, “ID 를 이용한 암호시스템에 관한 고찰” , 한국통신정보보호학회지. 제 4 권, 제 1 호, 1994. 3.

[8] M.Girault, “An identity-based identification scheme based on discrete logarithms modulo a composite number”, Eurocrypt’90, pp. 481-486, 1990.

[9] Real Networks. Inc. Helix producer user’s guide, June 2002.