적외선 기반 피기백킹 방지 기법을 적용한 네트워크 그룹 접근통제 시스템★

김종민* · 최경호** · 이동휘***

요 약

오늘날과 같은 정보화사회에서는 비인가자의 조직 내 출입 시, 중요 정보자산에 접근이 용이해지기 때문에 통제 상의 어려움이 있다. 비인가자는 고도의 기술을 활용하지 않더라도, 뒤따름(Piggy-backing)과 어깨 너머로 훔쳐보기(Shoulder surfing) 등의 방법을 통해 중요 정보를 획득 할 수 있다. 그러므로 본 연구에서는 비인가자가 조직 내 주요 공간에 위치 시 연관된 정보통신기기의 네트워크 접속을 차단하여 내부 정보를 열람할 수 있는 권한을 적절히 통제하는 방법을 제시하고자 한다. 제시된 방법은 RFID와 적외선 센서를 결합하여 네트워크 접근통제 시스템에 적용시킨 것으로, 이를 통해 비인가자 출입으로 인한 내부 정보 유출 위협을 차단하여, 인원 보안 측면을 강화한 보다 안전한 내부 네트워크 환경을 제공할 수 있다. 또한 내부 사용자의 보안인식 제고를 위한 수단으로 활용할 수 있는 장점도 있다.

Network Group Access Control system using piggy-backing prevention technique based on Infrared-Ray

JongMin Kim* · KyongHo Choi** · DongHwi Lee***

ABSTRACT

Information society in recent times, lots of important information have been stored in information systems. In this situation, unauthorized person can obtains important information by piggy-backing and shoulder surfing in specific area of organization. Therefore, in this study, we proposed network group access control system by combining RFID and infrared-ray for blocking information leakage due to unauthorized access by internal threats and enhancing personnel security. So it can provides a more secure internal network environment.

Key words : RFID, NAC, 정보보호, 적외선, piggy-backing, shoulder surfing

접수일(2012년 8월 27일), 수정일(1차: 2012년 9월 6일), 게재확정일(2012년 9월 7일)

★ 본 연구는 지식경제부 지역혁신센터사업인 산업기술보호특화센터 지원으로 수행되었음.

* 경기대학교 산업보안학과
** 경기대학교 산업기술보호특화센터
*** 경기대학교 산업보안학과 (교신저자)

1. 서 론

정보통신기술은 사회 전반에 자동화의 이점과 편리성을 제공하며 발전하고 있다. 이에 따라 개인 또는 조직이 수집, 저장 및 분석하고 있는 정보의 양도 함께 증가하고 있다. 정보통신기기를 이용하여 더욱 많은 정보를 빠르게 가치 있는 자산으로 전환시킬 수 있는 것이다. 이렇게 축적된 정보라는 자산은 개인과 조직의 활동 속에서 유용하게 사용되고 있다. 이때, 정보자산이 안전하게 활용될 수 있도록 기밀성(Confidentiality), 무결성(Integrity) 및 가용성(Availability)을 보장해야 한다[1].

정보자산은 다양한 내·외부의 위협에 직면해있다[2]. 이 위협들은 지능화 및 고도화하며 계속 발전하고 있으므로[3], 개별적으로 대처하기 보다는 통합적인 대응 프로세스를 제공할 수 있는 프레임워크를 구축하고 운영하는 것이 중요하다[4]. 사이버 위협에 대한 통합관리 노력은 최근 융합보안의 개념이 정립되면서 기술적인 부분 뿐만 아니라 물리적, 관리적 영역 가지 포함하며 발전하고 있다[5][6].

하지만 여전히 발생하고 있는 침해사고는 더욱 더 보안 강화를 위한 노력을 추진해야 함을 보여주고 있다. 특히, 내부자로 인한 정보 유출과 관리 상의 문제로 인한 시스템 중지 사례는 인적 보안 강화를 시급히 요구하고 있다[7][8][9]. 내·외부의 사용자에게 정당한 권한을 부여하여 허가된 정보자산에만 접근을 허용함으로써 기밀성, 무결성 및 가용성을 보장해야 하는 것이다.

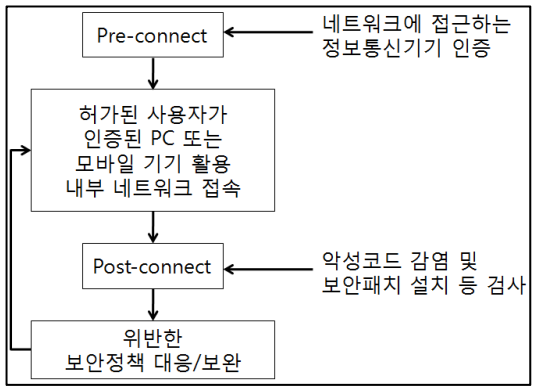
그러나 외부 사용자의 경우, 조직 내 출입이 가능하면 중요한 정보자산 접근이 용이해지기 때문에 통제 상의 어려움이 있다. 고도의 기술을 활용하지 않더라도, 뒤따름(Piggy-backing)과 어깨 너머로 훔쳐보기(Shoulder surfing) 등의 방법을 통해 중요 정보 획득을 할 수 있기 때문이다[10][11]. 따라서 비인가자의 물리적 접근 시 해당 공간에서 네트워크를 통한 정보 열람을 차단하는 방식을 적용하면, 정보자산 보호와 인적 보안 관리를 동시에 추진할 수 있다. 또한 이 방법은 내부 사용자들이 보안정책 위배 시, 직접적인 통제 상황에 직면하게 되기 때문에 보안인식 제고에도 기여할 수 있다.

그러므로 본 연구에서는 비인가자가 조직 내 주요 공간에 위치 시 연관된 정보통신기기의 네트워크 접속을 차단하여 정보를 열람할 수 있는 권한을 적절히 통제하는 방법을 제시하고자 한다. 이를 위해 다음의 2장에서는 정보통신기기의 네트워크 접근통제와 적외선을 이용한 내·외부 인원 출입통제에 관해 살펴보고, 3장에서 제안되는 시스템을 설계한다. 이후 4장에서 성능 분석을 실시하며 이를 토대로 5장에서 결론을 맺는다.

2. 관련연구

2.1 네트워크 접근통제 시스템

네트워크 접근통제 시스템(NAC : Network Access Control system)은 내부 네트워크에 접속하는 정보통신기기의 보안성을 확보할 수 있게 해주는 인프라이다. 내부 네트워크에서 허가된 PC 또는 모바일 기기의 접속만을 허용하거나, 보안 정책 준수를 유도할 수 있으며, 장애 탐지를 통한 가용성 확보도 가능하다.[12][13][14].



(그림 1) 네트워크 접근통제시스템 운영절차

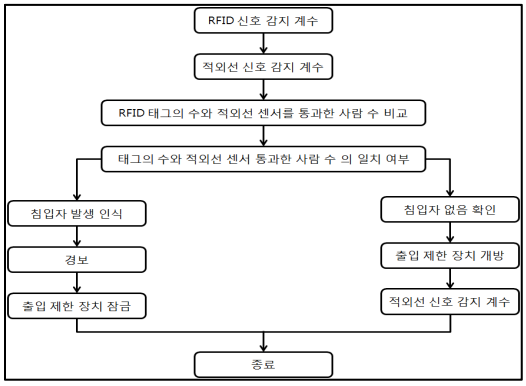
이와 같이 유용한 네트워크 접근통제 시스템을 안전하게 활용하기 위해, 발생 가능한 문제점과 위협들은 계속 식별 및 관리되고 있다[15][16][17]. 그러나 인가된 사용자의 내부 네트워크 접속 이후 동일한 물리 공간 내에서는, 비인가자의 모니터 화면 내용 인식

또는 직접적으로 허가된 정보통신기기의 사용이 가능하다는 문제점이 있다. 따라서 중요 정보의 대외 유출을 방지하기 위해서는 기술적으로 네트워크 접근을 차단하는 방법 외에도 물리적으로 비인가자에 대한 통제를 수행할 필요가 있다.

2.2 적외선 기반 출입통제

특정 물리 공간에서 비인가자를 식별하고 출입을 통제하는 방법은 적외선과 RFID(Radio Frequency ID entification) 등이 이용된다[18][19]. 여기서 적외선은 보행자의 수를 확인할 수 있기 때문에 출입통제에 활용할 수 있는 정보를 제공한다[20].

적외선은 센서와 감지장치로 구성되며, 출입 인원수를 계수한다. 따라서, RFID를 이용한 허가된 인원의 출입 시, 적외선으로 실제 출입 인원을 확인하여, 뒤따름을 통한 비인가자 접근 여부를 실시간으로 파악할 수 있다. 뒤따름 방지의 인증절차를 보게 되면 (그림 2)와 같다[21].



(그림 2) 뒤따름 방지 인증 절차[21]

3. 제안 시스템 설계

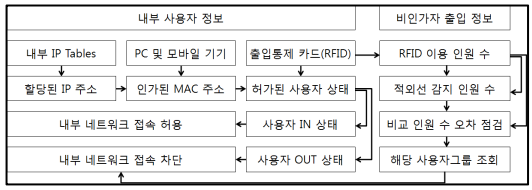
제안하는 시스템은 RFID 태그를 소지한 허가된 사용자 출입 시, 해당 인원에게 승인된 정보통신기기의 내부 네트워크 접근을 허용하는 이중 인증 구조를 가지고 있다. 따라서, 각 사용자가 소지한 RFID 태그 정보와 해당자에게 허용된 정보통신기기 정보는 통합 관리된다.

또한 하나의 물리적 공간 내에서 정보통신기기를 이용한 내부 정보 열람을 하는 사용자들은 하나의 그룹으로 분류하여 관리한다. 이는 비인가자 출입이 발생한 공간에서의 내부 정보 열람을 차단하기 위함이다. 그러므로 제안하는 시스템을 운영하기 위한 데이터베이스 테이블 구조는 다음 <표 1>과 같이 구성된다.

<표 1> 사용자별 RFID 및 정보통신기기 정보

그룹 번호	RFID Tag ID	사용자명	할당 IP	허용 MAC
01	0048	최OO	192.168.5.3	00-00-00…
01	0076	변OO	192.168.5.7	00-00-00…
02	0107	김OO	192.168.8.4	00-00-00…
02	0707	김OO	192.168.8.6	00-00-00…

다음 (그림 3)은 제안 시스템의 보안정책 적용구조를 보여준다. RFID 카드를 이용한 허가된 인원의 출입 정보를 기준으로 내부 네트워크에 해당 인원에게 인가된 정보통신기기의 접속 및 해제 정책을 실행한다. 이때, 하나의 물리 공간으로 진입하는 RFID 이용 인원 수는 적외선 센서 및 감지장치에서 계수된 인원수와 비교되며, 비인가자의 접근 확인 시, 해당 공간 내 정보통신기기 모두에게 네트워크 접근차단정책이 적용된다.

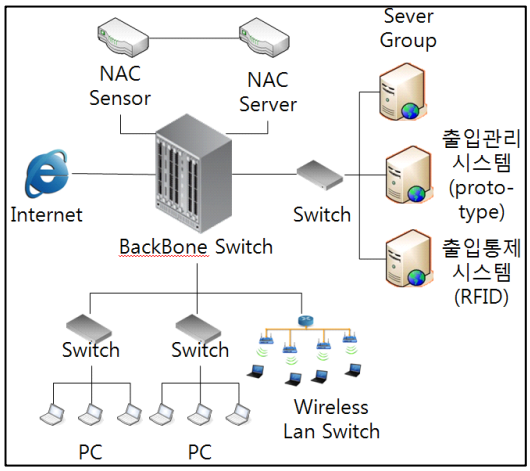


(그림 3) 제안 시스템의 보안정책 적용구조

4. 제안 시스템 구현 및 평가

제안된 시스템은 50여 명의 내부 사용자가 10여 개의 분리된 공간에 분산되어 있는 S社에 적용 및 실험

되었다. 제안된 시스템이 적용된 네트워크 구조는 다음과 같다.

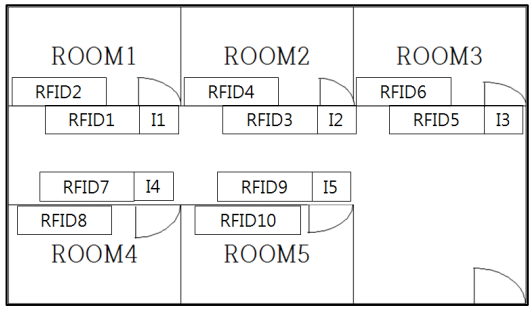


(그림 4) 제안된 시스템이 적용된 네트워크 구조

물리적으로는 각 사무실 출입문에 RFID 센서를 부착하여, 내부 사용자 출입 시 네트워크 접근통제를 실행한다. 허용 및 차단정책을 실행하기 위한 정보는 사용자 진입 및 진출 상태를 확인할 수 있는 RFID 상태 정의 목록에서 추출한다.

그리고 허가된 사용자의 특정 공간 진입 시, 비인가자의 접근을 확인하는 적외선 센서가 5초간 동작한다. RFID 센서에 인식된 인원 수 보다 초과한 보행자 수가 확인되면, 해당 공간에 인가된 정보통신기기의 목록을 조회하여, 네트워크 차단정책을 자동 적용한다. 이 과정을 통해 특정 공간 내 비인가자 접근 시 허가된 사용자라 하더라도 네트워크를 통한 정보 열람을 통제할 수 있다.

(그림 5)는 물리 공간에 배치된 RFID와 적외선 센서를 보여주며, <표 2>는 인가자와 비인가자의 진입 및 진출 상태를 확인할 수 있는 목록이다. 비인가자의 특정 공간 진입 시, 해당 공간 내 모든 사용자의 정보통신기기에 네트워크 접근차단을 요청하는 패킷이 <표 3>과 같이 생성된다.



(그림 5) RFID와 적외선 센서 배치환경

<표 2> 사용자별 진입 및 진출 상태 정의 목록

구분	1	2	3	4	5
인가자 진입	RFID1	RFID3	RFID5	RFID7	RFID9
비인가자 진입	I1	I2	I3	I4	I5
인가자 진출	RFID2	RFID4	RFID6	RFID8	RFID10

<표 3> 네트워크 접근차단 요청 패킷 내용 예

그룹 번호	RFID Tag ID	사용자명	허용 MAC	정책
02	0107	김OO	00-00-00…	차단
02	0707	김OO	00-00-00…	차단

상기와 같이 구현된 제안 시스템의 성능을 측정하기 위해 각각의 물리공간별로 10회씩 내부 사용자 진입 후 비인가자가 동행하는 상황을 실험하였다. <표 4>에서 볼 수 있는 바와 같이, 제안된 시스템을 이용한 비인가자 진입 시 내부 네트워크 차단 정책은 약 5초 정도의 시차를 두고 정상적으로 동작하는 것을 보여주고 있다. 이 결과는 내부 사용자의 RFID 태그 인식 후 비인가자의 진입 시까지 약 2초 정도의 격차가 있다는 점을 감안하면, 실제 정책적용을 위해 소요되는 시간은 약 3초 정도 임을 알 수 있게 해준다.

<표 4> 실험결과(10회 평균)

구분	RFID 태그 인식 후 비인가자 진입 소요시간(초)	네트워크 그룹 차단정책	
		적용율(%)	소요시간(초)
1	1.816	100	4.585
2	2.015	100	4.691
3	2.342	100	5.406
4	1.981	100	5.215
5	2.693	100	5.695
평균	2.169	100	5.118

따라서 본 연구에서 설계하고 구현한 적외선 기반 피기백킹 방지 기법을 적용한 네트워크 그룹 접근통제 시스템은 비인가자 출입 시 네트워크를 이용한 내부 정보열람을 차단하도록 하는 보안정책을 집행하기에 효과적이다.

5. 결 론

본 연구에서는 RFID와 적외선 센서를 결합하여 네트워크 접근통제 시스템에 적용시킴으로써 비인가자 출입으로 인한 내부 정보 유출 위협을 차단할 수 있다. 이에 따라 인원 보안 측면을 강화한 보다 안전한 내부 네트워크 환경을 제공할 수 있다.

그리고 이 방법은 사용자의 보안인식 제고에도 기여할 수 있는 장점이 있다. 내부 사용자들이 비인가자의 출입으로 인해 네트워크를 통한 정보 열람을 차단받을 수 있기 때문에, 보안정책을 준수해야 하는 의식수준과 당위성을 높일 수 있다. 따라서, 네트워크 접근통제시스템 에이전트를 활용한 사용자 보안인식 제고 등의 교육 관련 연구로도 활용 가능할 것으로 판단된다.

참고문헌

[1] Jason Andress, The Basics of Information Security, Elsevier, 2011.

[2] Won Kim, Ok-Ran Jeong, Chulyun Kim and Jungmin So, "The dark side of the Internet: Attacks, costs and responses", Information Systems, Vol. 36, Issue 3, Pages 675 - 705, May 2011.

[3] 이동휘, 최경호, 이동춘, 김귀남, 박상민, "사회공학기법을 이용한 피싱 공격 분석 및 대응기술", 정보·보안 논문지, 제6권, 제4호, pages 171 - 177, 2006.

[4] 김진섭, "「위험관리 기반 침해사고 조기 대응 체계」 구축 사례", 정보보호학회지, 한국정보보호학회, 제20권, 제6호, pp. 73 - 87, 2010. 12.

[5] 김정덕, 김건우, 이용덕, "융합보안의 개념 정립과 접근방법", 정보보호학회지, 제19권, 제6호, pages 68 - 74, 2009.

[6] 강구홍, 강동호, 나중찬, 김익균, "계층분석과정을 이용한 융합보안을 위한 물리 보안 이벤트 활용: 정보 보안 중심", 정보보호학회논문지, 제22권, 제3호, pages 553 - 564, 2012.

[7] Carl Colwill, "Human factors in information security: The insider threat - Who can you trust these days?", Information Security Technical Report, Vol. 14, Issue 4, Pages 186 - 196, November 2009.

[8] 천우성, 박대우, "농협 사태를 통한 관리보안의 문제점 연구", 한국전자통신학회 2011 춘계종합학술대회지, 제5권, 제1호, 2011.

[9] 차인환, 김정덕, "정보보호를 위한 인적자산 관리 지표 실증 연구", 정보보호학회논문지, 제19권, 제6호, 2009.

[10] Wendy Goucher, "Look behind you: the dangers of shoulder surfing", Computer Fraud & Security, Vol. 2011, Issue 11, Pages 17 - 20, November 2011.

[11] Johnny Long, Scott Pinzon, Jack Wiles, and Kevin D. Mitnick, No Tech Hacking,

SYNGRESS, 2008.
[12] 김영진, 권헌영, 임종인, "U-정보사회에서의 포괄적 네트워크 보안관리 방안", 정보보호학회지, 한국정보보호학회, 제18권 제3호, pp. 74 - 80, 2008. 6.
[13] 이원진, 김기원, 부기동, 우종정, "u-Campus의 네트워크 신뢰성 보장을 위한 NAC 도입에 대한 연구", 한국정보기술학회논문지, 한국정보기술학회, 제7권, 제4호, pp. 252 - 258, 2009. 8.
[14] Lawrence Orans and Mark Nicolett, "Gartner's Network Access Control Model", Gartner IT Security Summit 2005, June, 2005.
[15] 선종현, 한명묵, "인트라넷에서 호스트의 행위정보를 통한 악성코드 감염 호스트 탐지 시스템", 2010년도 한국인터넷정보학회 정기총회 및 추계학술발표대회 논문집, 한국인터넷정보학회, 제11권, 제2호, pp. 61 - 62, 2010. 10.
[16] 최경호, 김종민, 이대성, "RFID 출입통제시스템과 연동한 네트워크 이중 접근통제 시스템", 정보·보안 논문지, 제12권, 제3호, pages 53 - 58, 2012.
[17] 선종현, 김주혁, 한명묵, "NAC의 Post- connect에서 상관관계 분석을 통한 악성코드 탐지 시스템", 한국인터넷정보학회 2010년도 학술발표대회, 한국인터넷정보학회, pp. 459 - 464, 2010. 6.
[18] 강성철, 강민성, 김형찬, 도양회, 이광만, 김도현, "RFID 미들웨어 기반의 출입문 제어 에이전트 설계 및 구현", 한국멀티미디어학회 추계발표대회논문집, pages 650 - 653, 2006.
[19] 박승환, 구자일, "RFID를 이용한 교도소의 온라인 통제 시스템 개발", 전자공학회 논문지, 제45권, IE편, 제4호, pages 74 - 79, 2008.
[20] 김형기, 이광국, 윤자영, 김재준, 김회율, "적외선 라인 레이저를 이용한 보행자 수 측정", 대한전자공학회 하계종합학술대회, 제31권, 제1호, pages 1023 - 1024, 2008.
[21] 주식회사 에스원, 출입 관리 시스템 및 그 방법, KR-A-10-2009-0034068, 대한민국 특허청, 2009. 4.

[저 자 소 개]

김 종 민 (Jong-Min Kim)

2012년 현재 경기대학교
산업보안학과
박사과정

email : dyuo1004@gmail.com

최 경 호 (KyongHo Choi)

2002년 경기대학교 경제학사
2005년 경기대학교 경제학석사
2008년 경기대학교 정보보호학박사
2012년 경기대학교 연구교수
(산업기술보호특화센터)

email : cyberckh@gmail.com

이 동 휘(DongHwi Lee)

2000년 경기대학교 컴퓨터과학과
(이학사)
2003년 경기대학교 정보보호기술공학과
(공학석사)
2006년 경기대학교 정보보호학과
(정보보호학박사)
2011년~2012년 University of Colorado Denver, Dept. of Computer Science and Engineering, Researcher
2012년 ~ 현재 경기대학교
산업보안학과

email : dhclub@naver.com