RFID 출입통제시스템과 연동한 네트워크 이중 접근통제 시스템★

최경호* · 김종민** · 이대성***

요 약

내부에 있는 정보를 보호하기 위한 노력들 중 하나인 네트워크 접근통제 시스템의 적용은 내부 사용자들의 효과적 제어 및 자동적인 네트워크 관리와 보안을 가능하게 한다. 그러나 이미 허가된 PC 또는 모바일 기기로 위장하거나 자리를 비운 사용자의 인가된 시스템을 이용하여 내부 네트워크에 접속할 수 있는 문제점이 있다. 또한 허가된 PC 또는 모바일 기기의 악성코드 감염으로 인해 사용자가 직접 사용하는 시간 이외에도 동작하여 비의도적인 정보유출 및 내부 네트워크 공격 등이 발생할 수 있다. 따라서 내부 네트워크에 접속을 허가 받은 이가 인가된 장비를 이용하여 접근정책에 따른 통신을 수행하고 있는지를 확인해야 한다. 이를 위해 본 연구에서는 RFID 출입통제시스템과 연동한 네트워크 이중 접근통제 시스템을 제안한다. 제안된 시스템은 내부 네트워크 접속 시 이중인증을 수행함으로써 허가된 사용자가 인가된 장비를 이용하여 통신을 수행하는 환경을 제공한다.

Network 2-Factor Access Control system based on RFID security control system

KyongHo Choi* · JongMin Kim** · Daesung Lee***

ABSTRACT

Network Access Control System that is one of the efforts to protect the information of internal applies to effectively control of insider and automatic network management and security. However, it has some problems : spoofing the authorized PC or mobile devices, connect to the internal network using a system that authorized users are away. In addition, information leakage due to malicious code in the same system. So in this paper, Network 2-Factor Access Control System based on RFID security control system is proposed for safety communication environment that performing a two-factor authentication using authorized user and devices to connect to the internal network.

Key words : RFID, NAC, 정보보호, 이중 인증, 악성코드 차단

접수일(2012년 5월 29일), 수정일(1차: 2012년 6월 10일), 게재확정일(2012년 6월 11일)

★ 본 연구는 지식경제부 지역혁신센터사업인 산업기술보호 특화센터 지원으로 수행되었음

* 경기대학교 산업기술보호특화센터
** 경기대학교 산업보안학과
*** 부산가톨릭대학교 컴퓨터공학과 (교신저자)

1. 서 론

오늘날의 현실에서는 정보화 사회가 진전될수록 PC 또는 서버에 저장되는 정보의 양 또한 증가하고 있다. 이렇게 집적되는 정보들은 그 자체로 활용 또는 다른 업무에 이용되면서 부가가치를 창출할 수 있는 원동력이 되고, 조직의 생존과 경쟁력을 결정짓는 척도로 사용되기도 한다. 따라서 각종 정보보호제품의 적용, 기술 개발 및 보안인식 교육 등과 같은 노력들이 내부에 있는 정보를 보호하기 위해 다각적으로 꾸준히 추진되고 있다[1, 2, 3].

이러한 노력들 중 하나인 네트워크 접근통제 시스템의 적용은 내부 사용자들의 효과적 제어 및 자동적인 네트워크 관리와 보안을 가능하게 한다[4]. 그러나 이미 허가된 PC 또는 모바일 기기로 위장하거나 자리를 비운 사용자의 인가된 시스템을 이용하여 내부 네트워크에 접속할 수 있는 문제점이 있다. 또한 허가된 PC 또는 모바일 기기의 악성코드 감염으로 인해 사용자가 직접 사용하는 시간 이외에도 동작하여 비의도적인 정보유출 및 내부 네트워크 공격 등이 발생할 수 있다[5]. 따라서 내부 네트워크에 접속을 허가 받은 이가 인가된 장비를 이용하여 접근정책에 따른 통신을 수행하고 있는지를 확인해야 한다.

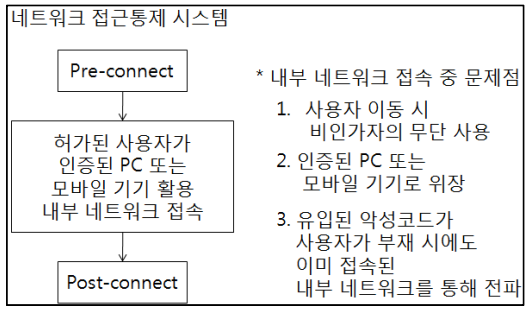
이를 위해 본 연구에서는 RFID 출입통제시스템과 연동한 네트워크 이중 접근통제 시스템을 제안한다. 다음의 2장에서 네트워크 접근통제 시스템, 이중 인증 및 RFID에 대해 살펴보고, 3장에서 제안된 시스템을 설계한다. 4장에서는 설계된 구조를 가지는 프로토타입의 성능을 시험해보고 이를 토대로 5장에서 결론을 맺는다.

2. 관련연구

2.1 네트워크 접근통제 시스템

네트워크 접근통제 시스템은 사용자가 이용하는 PC 또는 모바일 기기의 보안정책 준수 여부를 검사해 보안 위협에 노출된 단말기 및 비인가 사용자의 내부 네트워크 접속을 통제하는 역할을 수행한다[6, 7]. 가트너 社는 네트워크 접근통제 시스템의 절차, 기능 및 기술을 정의하였으며, 동 시스템을 적용하지 않을 경우 네트워크, PC 및 서버의 휴지시간(downtime)이 1.5배 - 3배 더 많아지고, 정보절취도 발생할 것이라 하였다[8]. 이러한 맥락에서 다수의 공공/민간기관들은 네트워크 접근통제 시스템을 이용해 내부 네트워크 보호를 수행하고 있다.

그러나 네트워크 접근통제 시스템을 이용 보안인프라를 구축하더라도 여전히 발생 가능한 위협을 정의하고 관리해야할 필요성은 존재한다[9]. PC 또는 모바일 기기 등이 인증(pre-connect)을 통해 내부 네트워크에 접속했다 하더라도, 보안정책을 위반할 시 즉시적 격리(post-connect)가 가능하도록 지속적으로 위협을 탐지 및 차단하는 노력을 추진해야 하는 것이다[10, 11].



(그림 1) 네트워크 접근통제 시스템을 이용한 내부 네트워크 접속 중 문제점

(그림 1)과 같이 PC 또는 모바일 기기 등의 인증 이후 허가된 사용자가 내부 네트워크에 접속할 때 비의도적으로 보안정책을 위반하게 되는 경우를 차단하기 위해서는 RFID 출입통제시스템 등과 연동한 이중 인증이 필요하다.

2.2 이중 인증

이중 인증은 보안 수준의 향상을 위한 효과적인 방법으로 응용된다[12]. 인증의 수단은 ID/PW부터 생체인증까지 다양한 방법들이 있다[13]. 그러나 각각의 수단들은 취약 요인들을 가지고 있기 때문에 이를 보완하도록 2가지 이상의 방법을 병행 운영하는 것이 권장되는 것이다[14].

네트워크 접근통제 시스템에 이중 인증을 적용한

예는 대학교와 같은 개방형 네트워크에서 ID/PW를 이용, L7 계층인 Application에서 URL Redirection을 통해 사용자 인증을 하는 것이다[15]. 이 방법은 사용자가 많은 개방형 구조에서는 적합하나, 고정적 사용자들은 별도의 ID/PW를 입력하는 과정을 거쳐야 하며, 여전히 허가된 사용자의 부재 시 연결된 세션으로 인한 문제점은 존재한다.

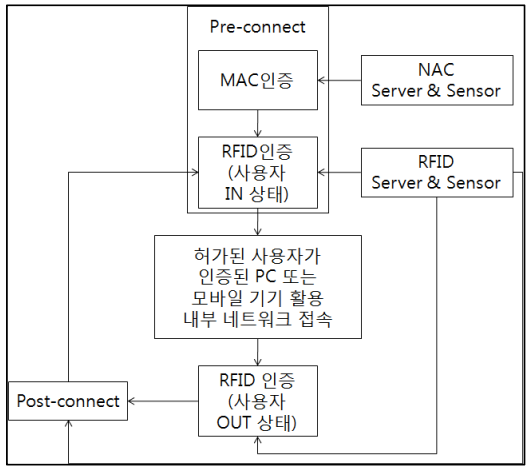
2.3 RFID

RFID (Radio Frequency Identification) 시스템은 특정 객체(item)에 부착되어 추적 가능한 전자적 인증 장치인 태그(Tag)와 태그에서 데이터를 감지하고 추출할 수 있는 장치인 리더(Reader)로 구성된다[16]. 리더는 태그를 식별하기 위해 질의(Query) 명령을 전송하며, 해당 태그가 반응하는 방식으로 동작한다[17]. 이러한 RFID는 위치를 관리하는 프레임워크와 같이 동작하여 객체의 식별 및 위치 추적 시스템을 구축하기에 용이하다[18].

3. 제안 시스템 설계

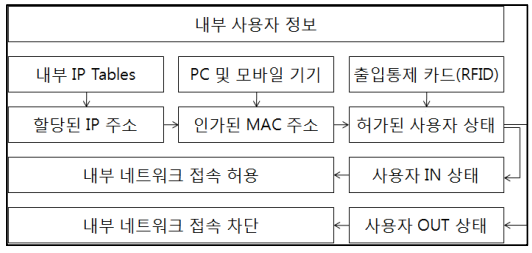
제안하는 시스템은 RFID 태그를 소지한 내부 사용자가 인가된 PC 또는 모바일 기기를 이용하여 내부 네트워크에 접속할 시 미리 수립된 보안정책에 따라 허용 여부를 결정해준다.

다음 (그림 2)는 제안하는 시스템의 이중 인증 구조를 보여준다. PC 또는 모바일 기기는 MAC 주소를 이용한 물리적 인증을 통해 인가된 것임을 증명한다[19]. 이에 더해, RFID를 소지한 사용자가 사무실 내에 위치하고 있다는 것을 인증하여 내부 네트워크에 접속을 허용하게 된다.



(그림 2) 제안 시스템의 이중 인증 구조

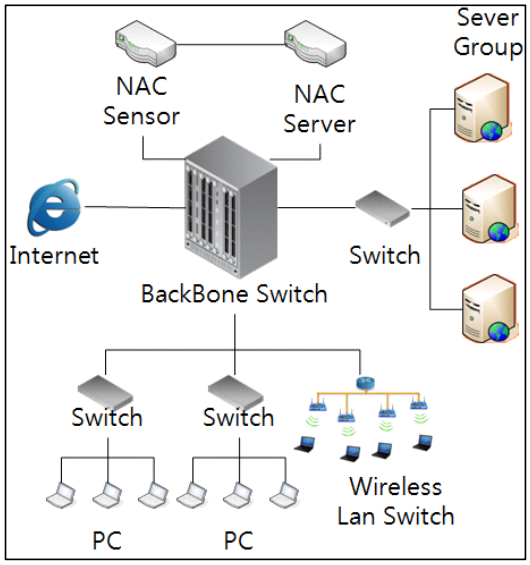
여기서 RFID 시스템은 IN, OUT 상태가 정의된 정책 기반 하에서 내부 사용자의 상태 정보를 지속 모니터링하며, 상태 변동 발생 시 이를 네트워크 접근통제 시스템에 통보하는 역할을 수행한다. 네트워크 접근통제 시스템은 해당 내용을 바탕으로 접근 및 차단 정책을 적용하게 된다.



(그림 3) 제안 시스템의 보안정책 적용구조

4. 제안 시스템 구현 및 평가

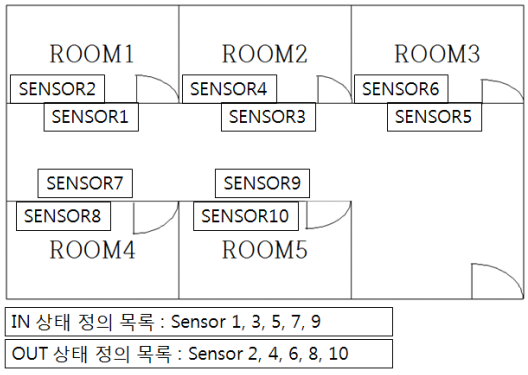
제안된 시스템은 단일층으로 약 1,000㎡의 공간을 가지고 있는 S社에 적용되었다. 10여 개의 분리된 공간을 중심으로 별도의 서버실이 구성되어 있으며, 제안된 시스템이 적용된 네트워크 구조도는 다음과 같다.



(그림 4) 제안된 시스템이 적용된 네트워크 구조

물리적 공간에서는 각 사무실 출입문에 RFID 센서를 배치하여, 내부 사용자의 IN, OUT 상태를 확인하며, IN 또는 OUT 상태를 정의하기 위해 태그를 인식하는 센서의 번호를 목록화한다. 다음 (그림 5)에서 보는 바와 같이, 내부 사용자의 IN 상태는 센서 1, 3, 5, 7, 9에서 특정 태그를 인식한 경우, OUT 상태는 2, 4, 6, 8, 10에서 사용자 이동을 확인한 경우이다.

내부 사용자의 상태 인식 결과에 변화가 생길 시, RFID 시스템은 네트워크 접근통제 시스템에 해당 정책의 변동을 요청하는 패킷을 전송하며, 내용은 <표 1>과 같이 표현된다.



(그림 5) 내부 사용자 상태 정의 센서 배치도

<표 1> RFID 기반 NAC 정책연동 패킷 내용

순번	시간	태그번호	상태	정책
1	201203021130	EMP048	IN	허용
2	201203021152	EMP112	OUT	차단

상기 표에 제시된 내용의 패킷을 통해 RFID 기반 네트워크 접근통제 시스템에 보안정책이 갱신되는 소요시간은 <표 2>와 같이 나타난다.

<표 2> RFID 기반 NAC 정책연동 소요시간

구분	정책연동 소요시간	
	허용 정책	차단 정책
20회 평균	3.046초	3.021초

내부 사용자 부재 시의 네트워크 접속 차단으로 악성코드 확산이 방지되는 기능은 성인광고 메일을 발송하는 바이러스를 이용 테스트하였으며, 해당 PC의 인터넷 접속은 방화벽에서 거부되도록 설정 후 진행하였다. 결과는 다음 <표 3>과 같다.

<표 3> RFID 기반 NAC 악성코드 차단결과

구분	스팸메일 전파건수	
	허용 정책	차단 정책
10회 평균	12	0

따라서 본 연구에서 설계하고 구현한 RFID 기반의 네트워크 접근통제 시스템은 허가된 사용자가 인가된 PC 또는 모바일 기기를 이용하여 내부 네트워크에 접속을 하도록 하는 보안정책을 준수하도록 유도하기에 효과적이며, 악성코드로 인한 비의도적인 정보유출을 방지할 수 있다.

5. 결 론

본 연구에서 제안한 시스템은 내부 네트워크 접속 시 이중 인증을 수행함으로써 허가된 사용자가 인가

된 장비를 이용하여 통신을 수행하는 안전한 환경을 제공한다. 특히 이중 인증 과정에서 사용자의 별도 입력을 요구하는 일이 없는 것이 편리한 점이다.

그러나 현재는 고정 IP 주소를 사용하는 네트워크를 기준으로 설계되어 있고, RFID 카드를 미소지한 사용자의 경우 네트워크를 사용할 수 없는 단점이 있다. 따라서 보다 더 다양한 방식으로 이중 인증을 수행하여 안전하면서도 사용자도 편리한 방식을 제공해야 한다. 또한 정보통신기술의 발전 속도를 감안하여, 보다 개방적이고 다양한 모바일 기기들이 활용되는 네트워크 구조 하에서도 응용될 수 있도록 확장되어야 한다.

참고문헌

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

[2] Jinhyung Kim and Hyung-jong Kim, "Design and Implementation of Data Leakage Prevention System Considering the Level of Privacy Protection and Violation", Information - An International Interdisciplinary Journal, Vol. 14, No. 11, pp. 3691 - 3698, November, 2011.

[3] 임채호, "효과적인 정보보호인식제고 방안", 정보보호학회지, 한국정보보호학회, 제16권, 제2호, pp. 30 - 36, 2006. 4.

[4] 백승현, 김승광, 박홍배, "사내 네트워크 보안을 위한 네트워크 접근제어시스템 설계 및 구현", 전자공학회 논문지-TC, 대한전자공학회, 제47권, TC편, 제12호, pp. 90-96, 2010. 12.

[5] Kyong-Ho Choi, Won Hyung Park and Kuinam J. Kim, "A Study of ESMTC (Enterprise Security Management system based on Threshold Classification)", 2012 International Conference on Information Science and Applications - ICISA 2012, pp. 156 - 161, May, 2012.

[6] 김영진, 권헌영, 임종인, "U-정보사회에서의 포괄적 네트워크 보안관리 방안", 정보보호학회지, 한국정보보호학회, 제18권 제3호, pp. 74 - 80, 2008. 6.

[7] 이원진, 김기원, 부기동, 우종정, "u-Campus의 네트워크 신뢰성 보장을 위한 NAC 도입에 대한 연구", 한국정보기술학회논문지, 한국정보기술학회, 제7권, 제4호, pp. 252 - 258, 2009. 8.

[8] Lawrence Orans and Mark Nicolett, "Gartner's Network Access Control Model", Gartner IT Security Summit 2005, June, 2005.

[9] 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.

[10] 선종현, 한명묵, "NAC의 pre-connect에서 행위정보를 통한 Group-Decision", 한국인터넷정보학회 2009 제20차 정기총회 및 추계학술발표대회, 한국인터넷정보학회, pp. 55 - 58, 2009. 10.

[11] 선종현, 김주혁, 한명묵, "NAC의 Post-connect에서 상관관계 분석을 통한 악성코드 탐지 시스템", 한국인터넷정보학회 2010년도 학술발표대회, 한국인터넷정보학회, pp. 459 - 464, 2010. 6.

[12] 이극, 지재원, 천현우, 이규원, "하이브리드 클라우드 컴퓨팅 환경에 적합한 인증시스템 설계", 정보·보안 논문지, 한국융합보안학회, 제11권, 제6호, pp. 31 - 36, 2011. 12.

[13] Ross Anderson, "Security Engineering : A Guide to Building Dependable Distributed Systems", WILEY, Second Edition, 2008. 4.

[14] 김현승, 박춘식, "클라우드 컴퓨팅과 개인 인증서비스", 정보보호학회지, 한국정보보호학회, 제20권, 제2호, pp. 11 - 19, 2010. 4.

[15] 이춘재, 조기량, "네트워크 이중 인증을 통한 역할 기반 개방형 네트워크 접근 통제 시스템의 구현", 한국통신학회논문지 '07-8, 한국통신학회, Vol. 32, No. 8, pp. 502 - 508, 2007. 8.

[16] Chia-Chen Chen and Tien-Chi Huang, "Learning in a u-Museum: Developing a context-aware ubiquitous learning environ-

ment", Computers & Education, Vol. 59, Issue 3, pp. 873 - 883, November 2012.

[17] 박영재, 김영범, "캡쳐 효과를 고려한 RFID 태그 인식 프로토콜", 전자공학회 논문지-TC, 대한전자공학회, 제49권, TC편, 제1호, pp. 19-25, 2012. 1.

[18] 박용민, 이준혁, "유비쿼터스 컴퓨팅 환경을 위한 RFID/WSN 통합 관리 시스템에 관한 연구", 전자공학회 논문지-TC, 대한전자공학회, 제49권, TC편, 제1호, pp. 31-46, 2012. 1.

[19] 노철우, 강경태, 이지웅, 전재현, "NAC(Network Access Control)을 이용한 컴퓨터 네트워크 보안 플랫폼 구성", 한국콘텐츠학회 2009 춘계 종합학술대회 논문집, 한국콘텐츠학회, 제7권, 제1호(상), pp. 8 - 11, 2009. 5.

[저 자 소 개]

최 경 호 (KyongHo Choi)

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

email : cyberckh@gmail.com

김 종 민 (JongMin Kim)

2012년 경기대학교 산업보안학과
박사과정

email : dyuo1004@gmail.com

이 대 성 (Daesung Lee)

1999년 2월 인하대학교
전자계산공학과 학사
2001년 2월 인하대학교
전자계산공학과 석사
2008년 2월 인하대학교
정보공학과 박사
현재 부산가톨릭대학교
컴퓨터공학과 조교수

email : xdilemma@naver.com