네트워크 접근제어 기반의 보안강화 시스템 구현

오승헌*
*고려대학교 컴퓨터정보통신공학과
e-mail:coomdory@korea.ac.kr

Implementation of Enhancement Security System based on Network Access Control

Seung-Heon Oh*
*Dept of Computer & Information Technology, Korea University

요 약

오늘날 사이버보안침해 위협의 증가에 따른 기업 내의 중요자료 유출을 방지할 수 있는 방안에 대한 연구의 필요성이 증대되고 있다. 본 논문에서는 비인가자의 네트워크 접속을 차단하는 네트워크 통제(NAC) 시스템과 개인 PC의 저장매체관리 시스템을 연계하여 정보보안의 핵심요소인 기밀성을 강화할 수 있는 모델을 제안하였다. 필수 SW(저장매체제어)를 설치하지 않을 경우 네트워크를 차단함으로서, 비인가자의 네트워크 차단과 동시에 중요자료 유출을 미연에 방지하여 보안을 강화할 수 있다.

Ⅰ. 서론

오늘날 정보보안의 중요성은 점차 커지고 있다. 특히 비인가된 접속자에 의한 기업내부 정보유출 문제는 해당 기업뿐만이 아니라 더 나아가 국가 전체의 큰 피해를 일으킬 수 있다. 비인가자의 네트워크 차단을 통해 정보보안의 기밀성을 향상시키는 방법으로 네트워크 접근제어(NAC)가 활용되고 있다. NAC는 네트워크로 접근을 요청하는 호스트의 인증 및 보안정책을 준수 여부를 판단하여 네트워크 접근을 제어하는 시스템을 의미한다.[1]

NAC 구축환경을 통하여 비인가 호스트의 네트워크 접속을 차단하고, 인가된 호스트의 경우 보안정책 준수 여부에 따라 내부, 외부 네트워크 접속을 구분하고, 선택적으로 허용하도록 하여, 내부 정보의 유출을 예방하고, 외부로부터의 해킹, 바이러스 침투 등을 방지할 수 있다.[2]

본 논문에서 제안하고자 하는 모델은 기존 NAC 시스템을 기반으로 하여 보안강화를 위한 필수 SW를 반드시 설치할 수 있도록 개선하였다. 즉, 호스트에 필수 SW 미설치 시 네트워크 접근을 차단되게 되며, 네트워크를 사용하고자 하는 호스트는 반드시 필수 설치 SW를 설치해야만 한다. 네트워크 접근통제 시스템과 보안강화 필수 SW 설치 시스템의 연계를 통하여, 내·외부의 보안위협으로 부터의 사내의 중요한 정보자산을 보호할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구에 대하여 기술하고, 3장에서는 제안하고자 하는 모델에 대해 기술한다. 4장에서는 이 논문의 결론과 향후 연구과제에 대해 기술한다.

Ⅱ. 관련 연구

2.1 네트워크 접근제어(NAC)

NAC는 네트워크상의 특정자원을 사용하고자 접근하는 장비에 일정 수준의 보안 정책을 부여하며, 보안 및 사용자 인증 된 노드(node)만을 접속 가능하게 하는 접근제어 역할을 수행하게 된다.[3]

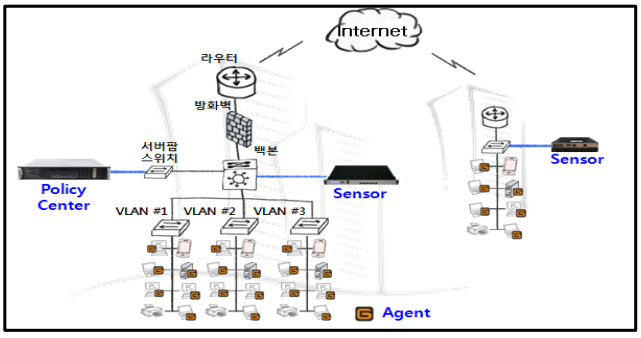
NAC을 통하여 비인가자의 네트워크 접근을 차단 한다. 인가자의 경우는 보안 정책에 따른 내부직원, 협력업체 직원, 혹은 임시사용자 등으로 구분하여, 사용이 허용된 네트워크만을 접속할 수 있도록 한다.

NAC 시스템의 구성요소는 아래와 같다.(그림1)

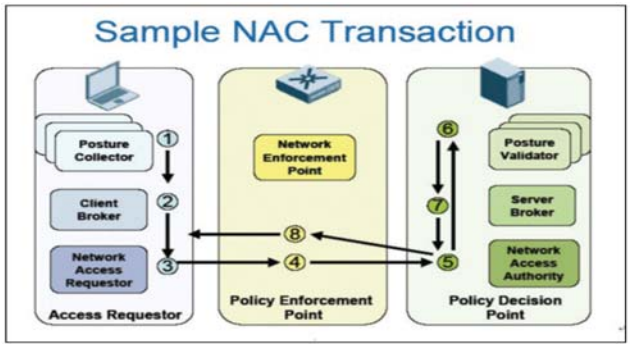
① 정책관리서버(Policy Center) : NAC 센서와 Agent에 대한 정책 관리를 수행한다.

② 센서(Sensor) : 네트워크상의 장비 및 사용자 통제 기능 수행하고, 노드정보(IP, MAC, OS등)를 관리한다.

③ Agent : 단말(PC)의 보안 정책 준수 여부 점검 하고, 사용자 PC 취약성 점검 및 정보 확인 기능을 수행한다.



<그림 1> NAC 시스템 구성도



<그림2> NAC 동작 순서도

NAC의 동작원리를 살펴보면(그림2) ① 네트워크 접속 사용자에 대한 인증을 수행한다. ② 사용자의 컴퓨터에 대한 무결성 검사를 수행한다. (OS패치 및 구성정보, 개인방화벽 유무 등의 검사) ③ 인증 및 무결성 검사 결과를 정책 관리서버의 정책과 비교한다. ④ 네트워크 접근 사용자에 대한 정책결정을 수행한다. ⑤ 사용자의 네트워크 접근 인증을 수행한다.[4]

2.2 저장매체제어

저장매체제어 시스템은 저장매체 관리 에이전트 SW가 설치된 사용자를 대상으로 저장매체(이동식디스크, 광학식 디스크, 플로피디스크 등)를 통제할 수 있다. 저장매체를 일반등급, 보안등급으로 구분하여 등록 후 사용하게 된다. 일반등급의 저장매체는 읽기 기능만 활성화 되어 있으며, 보안등급은 읽기, 쓰기 기능이 모두 활성화 되어있다. [5]

정보보안 강화를 위하여 비인가된 보조기억매체는 원칙적으로 사용을 금지하게 되며, 특별한 사유에 의하여 저장매체의 사용이 필요한 경우 보안모듈이 탑재된 보안 USB만을 사용하도록 강제할 수 있다. 이 경우 보안 USB의 사용자 등록, 인증, 사용승인 과정을 수행 되어야만 이용이 가능하다. 보안 USB 사용을 강제하는 저장매체 통제 시스템은 내부사용자의 저장매체를 통한 중요자료 유출 등의 보안사고를 미연에 방지할 수 있다.

저장매체제어 시스템은 통합매체제어관리서버, PC 에이전트, 보안USB 에이전트, 보안USB 메모리 등 4개의 구성요소로 이루어져 있다.[6]

① 통합매체제어관리서버 : PC 에이전트와 보안USB 에이전트의 요청을 처리하고 관리하는 기능을 제공한다.

② PC 에이전트 : 사용자 PC에 설치되는 프로그램으로 외부 보조저장장치를 제어하는 기능을 제공하고 관리서버와 통신하여 사용자 인증을 수행한다.

③ 보안USB 에이전트 : 보안USB 메모리에 저장되어 실행되는 보안 프로그램이며, 사용자 인증, 저장장치 인증, 파일 암호화, 원격소거 기능을 수행한다.

④ 보안USB 메모리 : 보안USB 에이전트가 탑재되는 USB 메모리 장치로 데이터가 암호화되어 안전한 저장기능을 가지도록 설계되어 있다.

Ⅲ. 시스템 구현

3.1 구현방법

본 논문에서는 네트워크 접근제어 시스템으로 Genian NAC 제품을 사용하였다. 방화벽 기술과 역할기반 접근제어 기술을 이용하여 기존 네트워크의 구성 변경 없이 비인가자의 네트워크 연결을 차단할 수 있다. 또한 네트워크 상에 존재하는 모든 장비들의 IP, MAC, OS, Platform 정보들을 자동으로 탐지하고 관리할 수 있다.

필수 설치 SW는 저장매체제어 시스템의 한 종류인 통합PC보안 SW를 선정하였다. 통합PC보안 SW를 통하여 비인가된 저장매체의 사용을 차단하고, 인가된 보안USB를 저장매체로 사용하도록 하여 내부 자료의 유출 및 바이러스 감염 등 보안위협 요소를 미연에 방지할 수 있다.

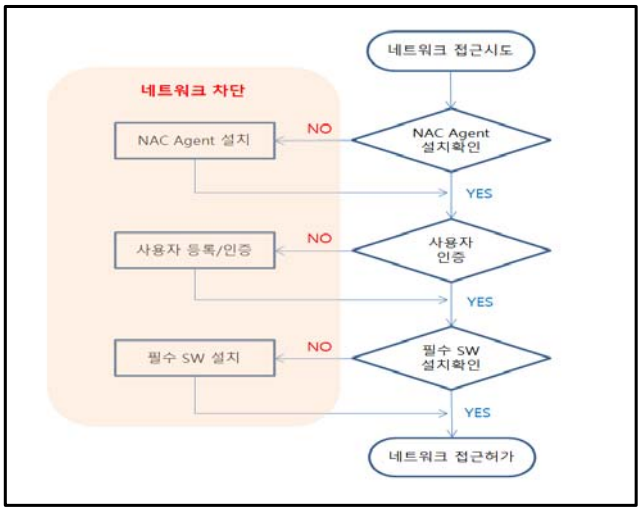
3.2 모델제안

제안된 모델은 내부 네트워크 보안 위협 요소를 제거하기 위해 비인가 사용자들의 네트워크 연결을 원천적으로 차단하며, 보안패치 및 필수 SW 설치 여부에 따라 네트워크 접근통제를 하게 된다. 만일 PC에 반드시 설치되어야 할 SW가 미설치 되었을 경우네트워크 접속을 차단하고, 필수 SW 설치 페이지로 유도하게 되며, 필수 SW가 설치가 완료 되어야만 네트워크 접속이 가능하다. 또한 사용자 PC의 패치여부를 검증하여 최신의 패치를 자동으로 배포/설치함으로써 보안을 강화할 수 있다.(표1)

<표 1> 필수 SW 및 패치 파일 리스트

구분	내 용	비고
필수 SW	통합 PC보안, 백신 등	
패치 관리	윈도우 OS 보안업데이트 등	

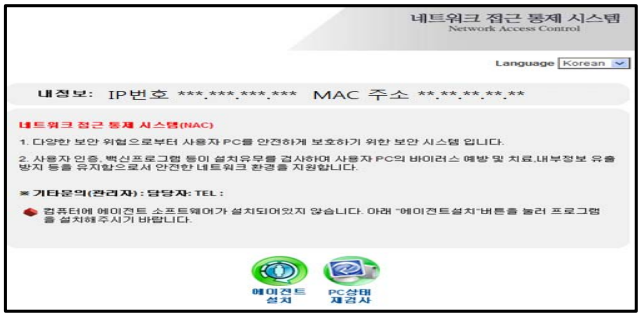
본 논문에서 제안한 NAC을 이용한 보안강화 모델의 상세한 과정은 그림3의 흐름도에 나타내었다.



<그림 3> 제안 모델 흐름도

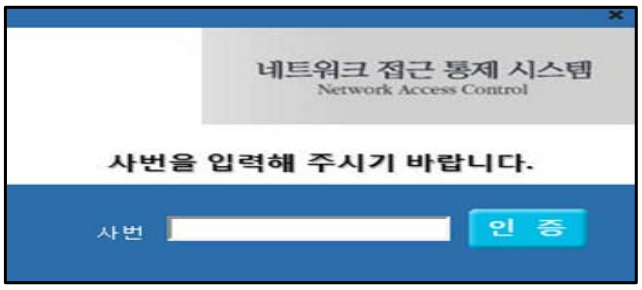
3.3 구현결과

본 장에서는 본 논문에서 제안한 NAC을 보안강화 모델을 실제 구현하고 이에 대한 결과를 제시한다.



<그림 4> NAC 에이전트 설치 화면

그림4은 NAC 에이전트 미설치 사용자의 네트워크 접근 시도 시 나오는 화면이다. NAC 에이전트 미설치 사용자는 네트워크가 차단되어 있으며, 네트워크 접속을 위해서는 NAC 에이전트 설치 유도 아이콘을 실행하여야 한다.



<그림 5> 사용자 등록/인증 화면

그림5은 NAC 에이전트 설치 완료 후 사용자 등록/인증하는 단계를 나타내었다. 사용자는 네트워크 접속을 위해 보안담당자(또는 관리자)로부터 사전에 네트워크 사용을 위한 사용자 등록을 수행해야하며, 아이디와 인증번호를 부여받아야 한다. 아이디는 회사 내부직원, 용역직원, 임시방문객 등으로 세분화하여 관리된다. 사용자 등록/인증 단계를 수행하지 않으면, 네트워크가 차단된다.

<그림 6> 필수 SW 설치 화면

그림6은 필수 SW 설치 유도 화면을 나타낸다. NAC 에이전트 설치 및 사용자 등록/인증 완료 후 필수적으로 설치해야하는 SW의 설치 유무를 확인한다. 필수 SW가 설치되지 않으면 네트워크를 차단하게 된다. 필수 SW의 종류는 보안담당자가 결정할 수 있으며, 본 논문에서는 저장매체제어 SW(통합PC보안)를 필수 설치 SW로 선정하였다.

3.4 고찰

본 논문에서 제안된 모델은 네트워크 접속을 위해서는 반드시 NAC 에이전트와 필수 SW(저장매체제어 등)를 설치해야만 한다. 네크워크 접속을 위해 부여된 사내 IP 발급 수량과 네트워크 사용자의 필수 SW 설치 수량을 비교한 결과 그 수가 일치하였다. 즉, NAC 시스템을 통하여 비인가자의 네트워크 접근을 차단할 수 있었으며, 동시에 저장매체제어 시스템을 통하여 내부자료 유출을 방지하게 되어 보안강화가 되었음을 살펴볼 수가 있다.(표2)

<표 2> 특정부서(연구소) 네트워크 접속 현황자료

구분	수량(개)	비고
네트워크 등록 IP(인증완료)	50	연구소
NAC 에이전트 설치 PC	50	〃
저장매체제어 SW 설치 PC	50	〃
네트워크 접근허가 IP	50	〃

Ⅳ. 결론

본 논문에서는 네트워크 통제 및 저장매체 통제를 효율적으로 관리할 수 있는 방법에 대하여 살펴보았다. 본 논문에서 제한한 모델은 기본적으로 NAC 시스템을 통하여 네트워크 접근 전에 반드시 필수 SW(저장매체제어)를 설치하도록 유도하였다. 만일 필수 SW를 설치하지 않을 경우 네트워크를 차단함으로써 비인가자의 네트워크 차단 및 동시에 중요자료 유출을 미연에 방지할 수 할 수 있도록 개선하였다.

향후, 보안관리 강화를 위해 추가로 반영되어야 하는 필수 설치 SW를 체계적으로 조사하고, 제안된 모델에 적용하여 현업에 활용될 수 있도록 지속적인 연구가 필요하다.

참고문헌

[1] 이대효, “NAC(Network Access Control) 기술동향 분석 및 개선에 관한 연구”, 성균관대학교 대학원 석사학위논문, 2008.12
[2] 박두희, “NAC구축 환경에서 비인가 사용자 단말의 내부 네트워크 격리를 위한 보안 시스템”, 숭실대학교 대학원 석사학위논문, 2012.06
[3] 전한수, “NAC시스템 구축에 따른 사용자 보안강화에 대한 연구”, 고려대학교 대학원 석사학위논문, 2008.07
[4] 한수진, “NAC 네트워크 보안의 새지평을 연다”, 보안뉴스(2006.10.17)
[5] 박홍재, “망분리 환경에서의 효율적인 정보기술아키텍처 관리시스템(EAMS) 보안대책에 관한 연구”, 고려대학교 대학원 석사학위논문, 2012.06.
[6] 박희섭, “안전한 개인 휴대형 저장장치 보안관리 설계 및 구현”, 공주대학교 대학원 석사학위논문, 2008.02