NAC솔루션을 활용한 효과적인 망혼용 탐지 기법

박종현*, 김창훈*

*대구대학교 컴퓨터공학

johpark74@naver.com

Effective Multi-homed host Detection Method Using Nac Solution

Jong-hyun Park*, Chang Hoon Kim*

*Department of Computer Engineering, Daegu University.

요 약

업무 전산망분리는 금융·공공기관을 시작으로 내부에서 운영 중인 중요 정보자산을 외부의 사이버 위협으로부터 보다 완벽하게 보호하기 위하여 도입·운영 중인 네트워크 보안의 한 분야이다. 하지만 물리적 또는 논리적 방법에 의해 전산망을 분리하여 운영하는 기관에서도 PC 사용자의 부주의 또는 의도적인 망혼용 시도 등으로 전산망 분리의 근본적인 취지를 저해하는 사례가 빈번히 발생하고 있다. 그리고 대부분의 기관·학교에서는 비인가 단말기에 대한 네트워크 접근 통제를 위해 업무망과 인터넷망에 독립적으로 정보보호 솔루션을 설치하여 IP와 MAC Address 기반의 통제를 실시하고 있다. 하지만 이런 Stand Alone환경에서는 내부의 인가된 단말기의 업무망과 인터넷망을 혼용 사용에 대한 통제가 불가능하다. 본 고에서는 현재 도입·운영 중인 NAC(네트워크 접근 제어)솔루션을 사례로 전산망 분리환경에서 발생할 수 있는 망혼용 단말기에 대해서 보다 효과적인 탐지 및 대응 방안에 대해서 제안하고자 한다

I. 서론

우리나라 전산망 분리는 2006년 “해외발 국가기관 해킹 실태 및 대처방안” 일환으로 국가기관 업무전산망과 인터넷 분리 방침이라는 대통령 보고 자료에서 처음 언급되기 시작했으며 2007년 국가/공공기관 업무전산망 분리 실무매뉴얼을 제작하여 방통위, 기재부 등에서 시범적으로 망 분리 사업을 추진하였다. 2008년부터 1, 2차 국가기관 망 분리 사업을 진행하였고, 2010년에는 지자체 및 산하기관으로 확대되어 2020년 기점으로 대부분의 공공기관에서 구축 완료하였다.[1]

또한 개인정보의 기술적·관리적 보호조치를 위하여 관련 법령에서는 매출액 등 일정 조건이상의 기업에 전산망 분리를 의무화하고 있다.

전산망 분리 초기에는 대규모 예산 투입 또는 사용자 불편 등의 여러 가지 어려움으로 전산망 분리 사업이 난항을 겪기도 하였으나 10년이 지난 현재는 법 준수 및 사용자 인식 개선 등으로 안정화 되었다.

하지만 이후 분리된 전산망을 운영함에 있어 정보시스템 서비스 연속성 및 PC사용자 불편 해소를 위한 다양한 불법적인 행위가 계속되고 있다. 본 고에서는 분리된 전산망을 운영하고 있는 기관에서 공통적으로 발생하는 유형별 망혼용 사례를 살펴보고 효과적인 해결방안을 제시한다.

II. 망혼용 유형 및 대응 방안

1.1 MAC Clone(Spoofing) 사례 및 대응

윈도우 환경에서는 랜카드의 속성정보 변경을 통하여 MAC주소를 변경할 수 있도록 허용한다.

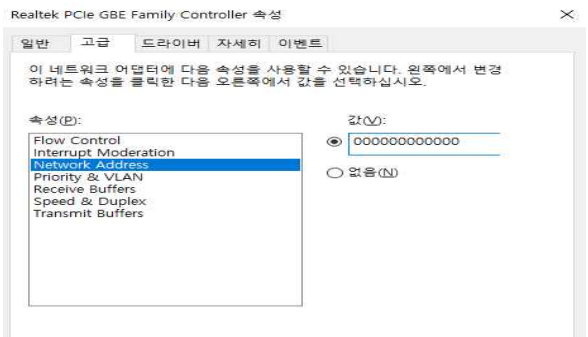

그림 1 MAC 주소 변경

PC사용자는 임의로 MAC주소를 변경함으로써 중요정보를 처리하는 정보시스템 관리자 계정에 대한 권한을 획득할 수 있다.

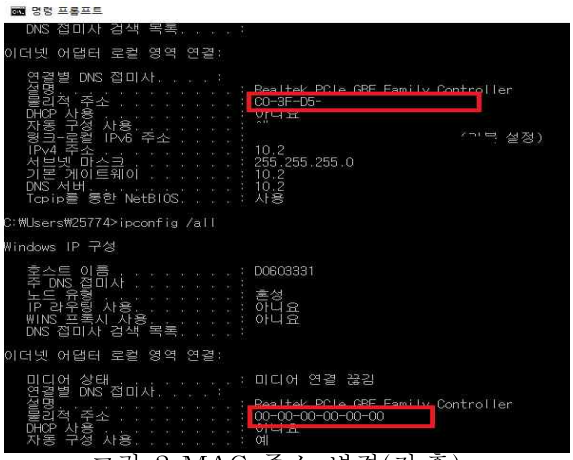

그림 2 MAC 주소 변경(전,후)

이 사례에 대한 해결책은 사전에 관리자를 포함한 PC단말기의 IP 및 MAC주소를 사전에 수집하고 데이터베이스화하여 관리함으로써 새로운 PC추가 또는 변경으로 인한 기존 네트워크 자원(IP,MAC등)에 대한 중복 사용을 차단할 수 있다. 이를 위하여 네트워크 접근제어 솔루션에서는 MAC주소에 대한 Clone을 방지하기 위한 기능을 제공하고 있다.

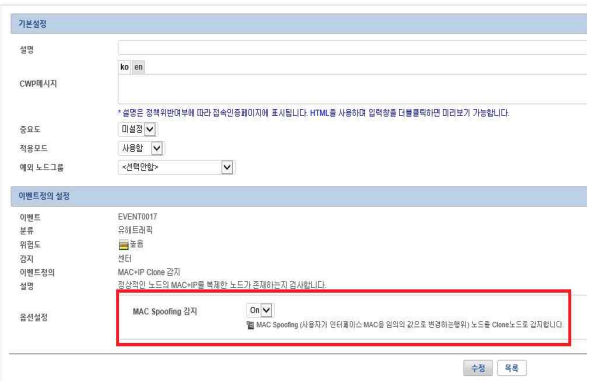

그림 3 MAC Spoofing 설정 화면

이와 함께 고려해봐야 할 문제점으로는 관리자의 랜카드를 탈취하여 공격자의 PC에 설치한 후 정보시스템에 접근을 시도하는 경우이다. 이 경우에는 앞에서 살펴본 해결안으로는 보안사고를 방지할 수 없다.

랜카드 변경에 대한 권한 우회공격을 사전에 방지하기 위해서는 PC단말기의 플랫폼 정보 즉, CPU나 메인보드 등 사전에 PC 단말기에 설치된 다양한 정보를 수집 관리함으로써 새로운 하드웨어 추가로 인한 정보 변경이 발생할 경우(ex, 메인보드 교체, HDD의 용량 증가 등)에도 보다 효과적인 대응이 가능하다. 즉 권한 우회에 대한 네트워크 서비스의 차단을 수행하게 함으로써 관리자 랜카드 획득의 경우에도 충분히 권한 획득을 제어할 수 있다.

그림 4 단말기 HW 구성 변경 감지 및 차단

1.2 외장 랜카드 망우회 사례 및 대응

전산망 분리 환경에서 가장 손쉽게 전산 망우회(업무망PC에서 인터넷망 연결)를 시도할 수 있고 가장 빈번하게 발생하는 망우회 방법은 외장형태(USB, 블루투스, 테더링 등)의 무선 랜카드를 연결하는 방법이다.

이 문제에 대한 가장 효과적인 대응 방법은 PC로 연결되는 모든 경로의 외장형태의 기기를 사전에 차단하는 것이다. 이를 위해 네트워크 접근제어 솔루션에서 매체 제어 기능을 활성화하여 외부 매체(USB, SD카드, CD-ROM 등) 제어를 통해 외부망 연결을 차단한다.

그림 5 매체 제어 기능 설정 화면

1.3 정상 행위를 통한 망혼용 사례

앞에서 살펴본 사례들은 비정상적인 행위를 수행하는 패턴 분석을 통해 사전에 감지 또는 차단하는 경우를 살펴보았다. 다음은 정상적으로 네트워크 접근에 대한 승인을 획득함으로써 전산망을 우회할 수 있는 사례를 설명하고자 한다. 업무망에 접근하기 위하여 사전에 정상적인 관리적 절차를 통해 접근을 시도한 후 동일한 PC단말기를 이용하여 인터넷망 접속 신청 및 승인을 획득한 경우 업무망 및 인터넷망 연결을 동시 사용 가능하게 된다.

이는 전산망 분리에 따라 업무망과 인터넷망에서 별도 네트워크 접근제어 솔루션을 독립적으로 운영함에 따른 부작용(Side Effect)이다.

이런 망혼용을 효과적으로 방지하기 위한 방안은 업무망 PC를 인터넷망에 연결할 경우 자동으로 차단하는 것이다. 업무망에서 운용 중인 네트워크 접근제어 솔루션의 PC단말기에 대한 정보(IP, MAC주소 등)를 인터넷망의 네트워크 접근제어 솔루션과 상호 연동·교환함으로써 해결할 수 있다.

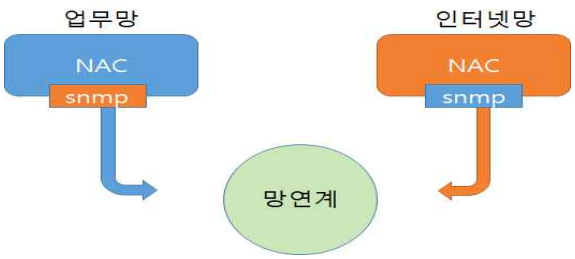

그림 6 업무망·인터넷망 SNMP 교환

위에 그림을 통해 알 수 있듯이 업무망과 인터넷망에 운용 중인 네트워크 접근제어 솔루션은 SNMP프로토콜을 이용하여 PC단말기의 정보(IP, MAC주소)를 상호 송수신함으로써 업무망·인터넷망용 네트워크 접근제어 솔루션에서 운용 중인 PC단말기 정보를 상호 비교함으로써 동일 PC단말기 망혼용 여부를 감지 및 차단한다.

1.4 실시간 모니터링 체계 구축

위에서 제안한 네트워크 접근제어 솔루션을 활용한 다양한 망혼용에 대한 대응 방안들은 실제 적용을 통하여 효과성이 검증되었으며, 실제 전산망 혼용에 대한 시도를 현저히 감소시켜 주었다. 하지만 이런 대응 방안에 대한 적용과 함께 고려해야 할 중요한 사항은 전산망 혼용에 대한 위반 사항을 실시간으로 모니터링하고 주기적으로 점검할 수 있는 업무절차 마련이 필요하다. 그리고 보안담당자는 정기적인 점검 절차를 통해 비정상적인 망혼용에 대한 접근 시도를 탐지·차단하고 망혼용에 대한 위규자 교육 및 처벌 등 관리적인 요소와 앞에서 제안한 다양한 기술적인 요소들을 병행하여 구현함으로써 전산망 혼용을 방지할 수 있다.

III. 결론

전산망 분리는 외부의 모든 사이버위협으로부터 원천적으로 기업의 중요자산을 보호할 수 있는 대안으로 대두되어 막대한 비용을 투자하여 금융 또는 공공분야를 필두로 일반 기업까지 확대 해나가고 있다. 하지만 전산망 분리 사업이 완료된 이후에도 안정된 전산망 분리 운용을 저해하는 여러 가지 취약요인이 생겨나고 있으며, 그 대표적인 예로써 사용자 PC단말기에서 업무망과 인터넷망을 혼용해서 사용하려는 시도가 자주 발생하고 있다. 기관이나 기업에서는 제한된 예산과 인력으로 인하여 새로운 보안 취약요소에 대해서 능동적으로 대처하기 쉽지 않은 환경에 놓여 있다. 본 고에서는 예산·인력·가용자원의 제한적인 기업 환경에서 가장 효과적으로 전산망 혼용을 대응하기 위해 별도의 예산 투입 없이 현재 운영 중인 정보보호시스템 자원을 활용하여 각 기업에서 발생할 수 있는 망혼용 사례를 제시하고 적용 가능한 다양한 보안 대응 방안을 제안하였다.

[참고문헌]

[1] 안랩연구소, 이용진, 망 분리의 필요성 및 방식