제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

망 분리 솔루션에 대한 보안 취약성 분석

이성록, 고웅, 곽진
순천향대학교 정보보호학과
e-mail : slping@naver.com, wgo@sch.ac.kr, jkwak@sch.ac.kr

Analysis of Security Vulnerability in Separate Network Solution

Seongrok Lee, Woong Go, Jin Kwak
Dept of Information Security Engineering, Soonchunhyang Univ.

요 약

기업 내 주요 정보를 보호하기 위한 방안으로 다양한 솔루션이 제시되었으나 내부 자료의 유출을 막는데 한계가 존재하였다. 기업들은 이런 문제점을 해결하기 위한 대안으로 업무망과 인터넷망을 분리하여 사용하는 망 분리 솔루션을 도입하고 있다. 망 분리 솔루션은 PC 기반의 방식과 전환 장치기반, SBC 기반, PC 가상화 기반 방식으로 구분할 수 있다. 이러한 망 분리 솔루션은 망을 분리하는 방식에 따라 취약성이 존재할 수 있다. 따라서 본 논문에서는 망 분리 솔루션의 각 방식에 대하여 분석하고 망 분리 솔루션에 존재할 수 있는 취약성을 도출하고자 한다.

1. 서론

기업 내 주요 정보를 보호하기 위한 방안으로 보안 USB, 자료유출방지시스템, PC 보안 제품 등 다양한 솔루션이 제시되고 있으나 기업 내 자료 유출을 막는데 한계가 존재하였다. 이런 문제점을 해결하기 위하여 업무영역인 내부망과 인터넷영역인 외부망을 별도로 구축하여 업무에 사용하는 PC와 외부 인터넷을 사용하기 위한 PC를 분리하는 PC 기반 네트워크 분리 방식의 망 분리 솔루션이 등장하였다. PC 기반 네트워크 분리 방식의 망 분리 솔루션의 경우 내부 자료 유출을 방지하는 효과는 뛰어나지만 고비용으로 효율성이 많이 떨어지며 업무망 PC의 자료 유출을 감시하기 위한 자료유출방지시스템, 보안 USB 시스템 등 별도의 부가적인 보안 솔루션이 요구되었다.

PC 기반 네트워크 분리 방식의 망 분리 솔루션이 가지고 있는 고비용 문제점을 해결하기 위해 대안으로 전환 장치를 통한 네트워크 분리 방식의 망 분리 솔루션, PC 가상화를 통한 네트워크 분리 방식의 망 분리 솔루션 등이 등장하였다. 이러한 방식의 망 분리 솔루션은 1대의 PC를 네트워크 인터페이스 전환 기술, 가상화 기술을 통해 내부영역과 외부영역으로 구분지어 내부영역은 업무망에만 접근할 수 있으며, 외부영역에서는 외부인터넷을 사용하도록 하여 PC 기반 네트워크 분리 방식의 망 분리 솔루션과 같은 효과를 나타낸다. 또한 부가적으로 디바이스 통제를 통해 외부저장매체, 프린터 드라이버 등 PC 디바이스를 통제하여 자료유출방지 기능도 일부 지원하고 있다. [1][2]

본 논문에서는 망 분리 솔루션에 대하여 조사하고 이러한 망 분리 솔루션에 존재할 수 있는 취약성을 분석한다.

2. 관련연구

망 분리의 목적은 내부 네트워크망과 외부 네트워크망을 분리 하여 외부로 연결되는 인터넷 망으로부터의 악성코드, 바이러스, 해킹과 같은 공격을 차단하고 내부 정보의 유출을 막는 것에 있다. 망 분리 솔루션의 유형은 <표 1>과 같다.

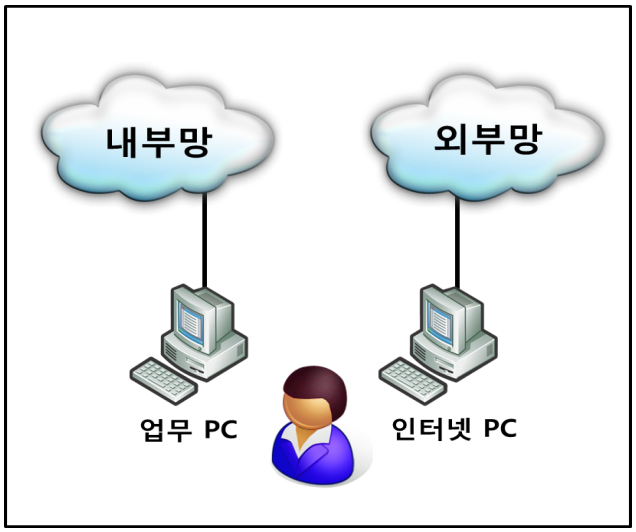
<표 1> 망 분리 솔루션의 유형과 구성요소

유형	구성 요소
PC 기반 네트워크 분리	- 내부(업무)망 PC - 외부(인터넷)망 PC
전환 장치를 통한 네트워크 분리	- 내부(업무)망 하드디스크 - 외부(인터넷)망 하드디스크 - 망 분리 전환 장치
SBC 기반의 네트워크 분리	- SBC 접속 프로그램 - SBC 서버군
PC 가상화를 통한 네트워크 분리	- 사용자 PC - 가상화 구동 프로그램 - 내·외부망 네트워크 통제를 위한 GW

2.1 PC 기반 네트워크 분리

PC 기반 네트워크 분리 방식의 망 분리는 말 그대로 물리적으로 네트워크를 분리하여 외부망과 내부망을 따로

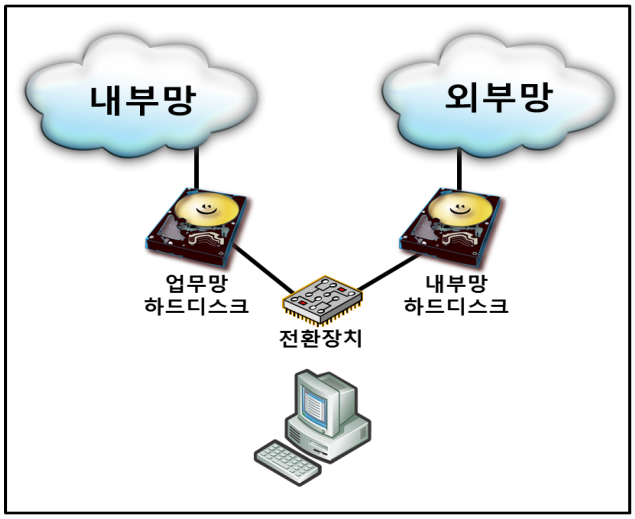
구축하는 것이다. PC 기반 네트워크 분리는 업무용 환경에 내부망과 외부망 두 대의 PC를 이용하여 물리적으로 네트워크를 분리하는 방식이다. 내부망 PC는 인터넷 사용이 불가능한 환경인 업무망 영역에만 연결하여 업무처리용으로만 사용하고, 외부망 PC는 외부네트워크에 연결하여 인터넷을 사용하는 목적으로만 사용하여 업무망에는 접근을 하지 못하게 한다. 이러한 방법을 통해 PC기반 네트워크 분리는 인터넷을 통한 외부의 공격으로부터 내부 시스템을 원천적으로 보호하므로 망 분리 방식 중 보안상 가장 안전한 방식이다. 하지만, PC기반 네트워크 분리방식은 사용자 한명 당 2대의 PC를 확보해야 하므로 많은 예산이 소요된다. 또한 보안 USB, 자료유출방지 등 외부 자료 반출입에 대한 통제를 위해 부가적인 보안 솔루션 도입이 요구된다. PC 기반 네트워크 분리의 운영환경은 (그림 1)과 같다,



(그림 1) PC 기반 네트워크 분리의 운영환경

2.2 전환 장치를 통한 네트워크 분리

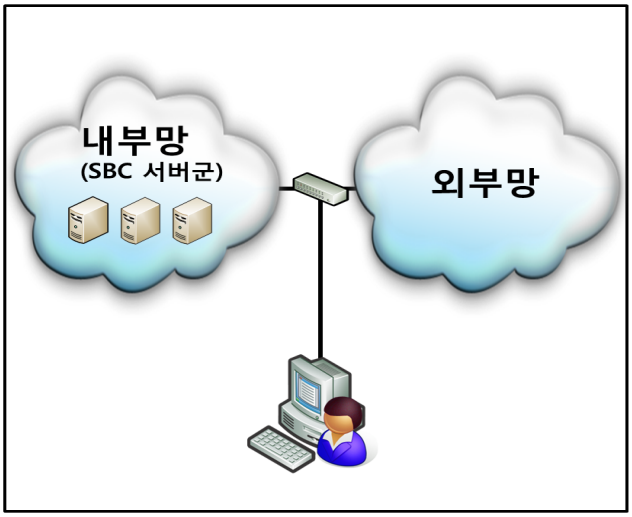
전환 장치를 통한 네트워크 분리는 하드디스크, IP 주소, 라우팅 정보 등 정보처리 및 네트워크 연결에 필요한 자원을 업무용과 인터넷용으로 나누고 망 분리 전환 장치를 통해 사용자가 PC 운용환경을 선택하도록 하여 업무망과 인터넷을 물리적으로 분리하는 방식이다. 사용자는 PCI 카드 형태로 사용자 PC에 내장되어 전환 장치를 통해 필요에 따라 업무망과 인터넷을 선택하여 사용하여 업무자료 작성 및 보관은 내부망 하드디스크에 저장하고, 인터넷 검색자료 등 외부자료는 외부망 하드디스크에 저장한다. 전환 장치를 통한 네트워크 분리방식은 하나의 PC를 전환 장치를 통해 2대의 PC를 사용하는 것과 같은 보안 방안을 제공하여 PC기반 네트워크 분리방식보다 예산소요는 적지만, 전환 장치를 통해 망을 전환에 따른 시간 지연이 발생하여 업무효율성이 떨어진다. 전환 장치를 통한 네트워크 분리의 운영환경은 (그림 2)와 같다.



(그림 2) 전환 장치를 통한 네트워크 분리의 운영환경

2.3 SBC 기반의 네트워크 분리

SBC 기반의 네트워크 분리는 서버기반 컴퓨팅(SBC) 기술을 이용한 망 분리 방식이다. 사용자 PC는 기본적으로 외부망에 연결되어 있어 인터넷 사용 시 기존 PC를 사용하고, 업무 시에는 중앙의 SBC 환경을 위한 에뮬레이터를 사용해 업무자료 작성 및 저장하여 내부 자료의 유출을 차단한다. 모든 사용자는 업무자료 작성 및 저장행위는 서버에서 하기 때문에 서버의 과부하가 생길 수 있다. SBC 기반의 네트워크 분리의 운영환경은 (그림 3)과 같다.[3]

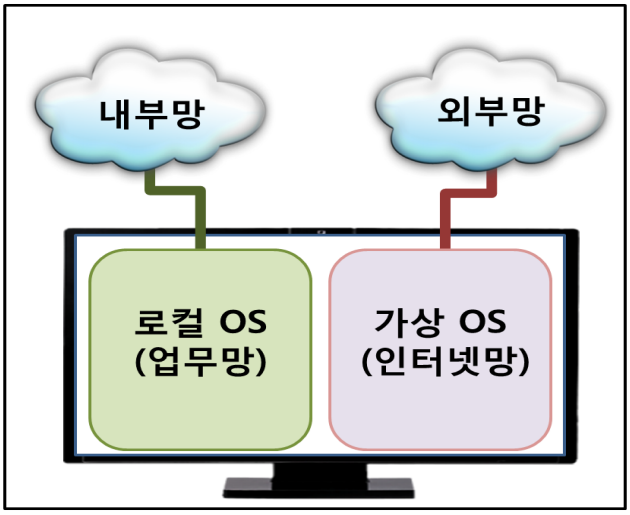


(그림 3) SBC 기반의 네트워크 분리의 운영환경

2.4 PC 가상화를 통한 네트워크 분리

PC 가상화를 통한 네트워크분리는 가상화 기술을 통해 사용자 PC의 운영체제를 내부용 OS와 외부용 OS로 나누어 각각의 영역에서 서로 다른 네트워크로 접속하도록 해주는 방식이다. 사용자는 1대의 PC에서 업무망 접속 시에는 실제 OS를 사용하고, 외부망 접속시에는 가상화

OS를 사용한다. 이를 통해 내부망 PC, 외부망 PC 2대의 PC를 사용하는 것과 같은 효과를 낼 수 있으며, SBC 기반의 네트워크 분리방식에 비해 추가적으로 도입해야 하는 시스템이 적어 예산 절감 효과가 있다. 하지만, 가상화 OS에 대한 안정성이 확보 되지 않을 경우 외부 공격에 취약할 수 있다. PC 가상화를 통한 네트워크분리의 운영환경은 (그림 4)와 같다.[4]



(그림 4) PC 가상화를 통한 네트워크분리의 운영환경

3. 망 분리 솔루션의 보안 취약성 분석

전환 장치, PC 가상화를 통한 망 분리 솔루션들은 2대의 사용자 PC를 사용하는 PC 기반 네트워크 망 분리 솔루션이 가지고 있는 문제점인 고비용, 비효율성 문제를 해결하고 있는 것과 같이 보이지만 1대의 PC가 OS 커널을 공유하여 사용하기 때문에 커널 단에서 각 영역에 대한 분리가 제대로 이루어지지 않을 경우 메모리 공유, 프로세스 공유 등의 문제점으로 인해 악의적인 사용자가 내부망에 접근하여 내부 자료를 유출 할 수 있다. 망 분리 솔루션이 가질 수 있는 보안 취약성 목록은 <표 2>와 같다.

<표 2> 망 분리 솔루션의 보안 취약성

침해 대상	취약성 분류
메모리	- 메모리 해킹을 이용한 작업 중인 문서 접근 취약점 - 사용자 메모리 공유 취약점 - 입출력 장치 공유 취약점 - 메모리 자원 고갈 취약점
파일시스템 (디스크)	- 파일공유 취약점 - 파일시스템 자원 고갈 취약점
프로세스	- 프로세스 접근 취약점 - 프로세스 강제 종료 취약점
네트워크	- Packet Capturing을 통한 내부망 트래픽 유출 취약점
저장매체	- 저장매체 공유로 인한 취약점

3.1 메모리 침해 취약성

메모리 자원에 대한 확실한 통제가 이루어지지 않는다는 것은 각 영역에서 메모리를 공유한다는 말이 된다. 그렇다면 외부영역으로 침투한 공격자에 의해 로컬역역에서 열람 중인 문서가 외부 영역으로 저장될 수 있을 것이다. 또한 공격자는 외부영역에서 스파이 프로그램, DLL 인젝션 공격 등을 통해 내부 영역의 OS 메시지(키보드 입력값 등) 모니터링이 가능할 수 있고 외부 영역에서 메모리 자원을 고의로 고갈시켜 내부 영역의 업무를 방해할 수 있으며, 내부 영역에서 실행 종료한 프로그램에 대한 메모리 잔여 정보에 접근하여 내부 영역의 데이터를 유출 할 수 있다.

3.2 파일시스템 침해 취약성

내부 영역과 외부영역의 파일시스템에 대한 확실한 통제가 이루어지지 않게 되면 서로 다른 영역의 파일시스템에 저장되어 있는 데이터에 접근하거나 확인할 수 있고 일반적인 OS 파일시스템 공유를 통해 내부 영역과 외부 영역 간 데이터 유출 경로가 생성 될 수 있으며 비인가 파일 필터 드라이버를 삽입하여 내부 영역에 저장되어야 할 데이터가 외부 영역에 저장될 수 있다. 그렇게 되면 외부 영역으로 침투한 공격자는 내부 영역에서 설정한 공유 폴더에 접근하는 등의 행위를 통해 업무망의 자료에 접근이 가능할 수 있으며, 외부 영역에서 내부 영역으로 악성코드, 해킹프로그램 등을 유입하여 사용자 PC를 무력화 시킬 수 있다. 또한, 공격자는 외부 영역의 파일시스템 자원을 고갈시켜 사용자가 PC를 정상적으로 운영하는 것을 방해할 수 있다.

3.3 프로세스 침해 취약성

각 영역간의 확실한 프로세스 통제가 되지 않게 되면 서로 다른 영역에서 실행중인 프로세스를 확인할 수 있을 것이다. 공격자가 외부 영역으로 침투하여 이를 알게 되면 공격자는 내부 영역에서 실행되고 있는 프로세스에 접근하여 내부정보를 침해하거나 외부로 유출할 수 있으며, 실행중인 프로세스를 강제 종료하여 사용의 업무에 피해를 가할 수 있다. 또한 공격자가 외부 영역에서 실행하고 있는 프로세스에 DLL 인젝션 공격을 통해 내부 영역의 동일한 프로세스에도 DLL 인젝션 공격을 받을 수 있다. 이 경우 외부 영역을 통해 내부 영역의 운영체제 메시지에 대하여 모니터링이 가능할 수 있다.

3.4 네트워크 침해 취약성

NIC 카드에 대한 확실한 통제가 되지 않게 되면 패킷 스니핑 도구를 이용하여 외부 영역과 내부 영역에서 서로의 패킷정보를 확인할 수 있을 것이다. 공격자는 이러한 취약성을 이용해 간단한 네트워크 정보 변경을 통해 외부

영역에서 내부 영역의 네트워크에 대한 패킷을 모니터링 하여 내부망의 전송되는 데이터의 정보를 얻을 수 있다. 또한 외부 영역에서 내부 영역의 네트워크 정보(IP주소, MAC 주소)를 조회할 수 있으면 공격자는 해당 정보를 이용하여 외부 영역의 네트워크 정보를 내부 영역의 네트워크 정보로 변경하여 내부 영역에 접근하여 내부정보를 외부로 유출시킬 수 있을 것이다.

3.5 외부저장매체 침해 취약성

CD, USB 등 외부 저장매체에 대한 통제가 안 될 경우 내부 영역에서 사용하기위해 연결한 저장매체가 외부 영역에서도 접근할 수 있으며 외부 영역을 통해 저장매체의 연결을 확인한 공격자는 저장매체에 저장되어 있는 내부 자료들을 외부로 유출 할 수 있다. 또한, 저장매체의 통제가 이루지지 않게 되면, 인터넷상의 악성 프로그램들이 외부 영역, 저장매체, 내부 영역 순의 경로를 통해 내부 영역으로 유입될 위험이 있다.

4. 결론

본 논문에서는 망 분리 솔루션에 존재할 수 있는 취약성들에 대하여 분석하였다. 전환 장치, PC 가상화 등의 기술을 이용하여 1대의 PC를 사용한 망 분리 방식의 솔루션은 PC 기반 네트워크 분리 방식의 망 분리 솔루션과 같은 효과를 보이며 비용절감 효과도 가지고 있다. 그러나 OS 커널을 공유하여 프로세스, 메모리, 파일시스템, 디바이스(외부저장매체, NIC) 등에 대한 통제가 적절히 이루어지지 않을 경우 외부 인터넷을 사용할 수 있는 외부 영역을 통해 내부 영역의 데이터가 유출 될 수 있다. 이런 문제를 해결하기 위해서는 내부 영역과 외부 영역 간 실행되는 프로세스가 별도로 동작하도록 제한해야 한다.

메모리와 파일시스템의 경우 내부 영역이 접근할 수 있는 메모리 영역과 외부 영역이 접근할 수 있는 영역을 제한하여 각 영역 간 침해가 발생하지 않도록 제한해야 하며, 메모리 버퍼오버플로우로 인한 영역 간 침해가 발생되지 않도록 해야 한다. 네트워크 분리의 경우 각 영역 간 네트워크 정보를 조회할 수 없도록 OS의 해당 인터페이스를 제한해야 하며, 각 영역이 다른 영역의 네트워크 정보를 변조할 수 없도록 제한해야 한다. 디바이스 통제 또한 외부저장매체, CD-ROM 등 자료를 유출할 수 있는 디바이스에 대하여 내부 영역, 외부 영역이 동시에 접근할 수 없도록 제한하여 디바이스를 통한 데이터 공유가 되지 않도록 해야 한다.

마지막으로 전환 장치, PC 가상화 등의 망 분리 솔루션을 도입하여 운영 할 경우 외부 영역을 통해 내부 영역이 침해될 수 있는 취약성이 존재하는지 충분한 검증을 통해 결정하여야 한다.

참고문헌

[1] 김재우, 김정수, 한영섭, “분리망에서 EAI 기반의 개발 아키텍쳐 설계 및 구현”, 한국인터넷정보학회 2010학술발표대회, pp.257-267, 2010.06

[2] 김인혁, 김태형, 김정한, 임병홍, 엄영익, “시스템 보안을 위한 가상화 기술 활용 동향”, 정보보호학회지, 제19권 제2호, pp.26-34, 2009.04

[3] 이은배, 김기영, “망 분리기반의 정보보호에 대한 고찰”, 정보보호학회지, 제20권 제1호, pp.39-46, 2010.02

[4] 김진미, 배승조, 정영우, 심규호, 고광원, 우영춘, “유틸리티 컴퓨팅 시대를 여는 가상화 기술 동향”, [IITA] 정보통신연구진흥원 학술정보 주간기술동향 1208호

[5] 김지연, 김형종, 박춘식, 김명주, “클라우드 컴퓨팅 환경의 가상화 기술 취약점 분석연구”, 정보보호학회지, 제19권 제4호, pp.72-77, 2009.08