USB 보안 모듈과 Active Directory를 활용한 인프라 구축에 관한 연구

남기철*, 이덕규*
*서원대학교 정보보안학과
rornfl1492@naver.com, deokgyulee@seowon.ac.kr

A Study on Making of Infrastructure through Utilizing USB Security Module and Active Directory

Gi Cheol Nam *, Deok Gyu Lee*
*Dept. of Information Security, SeoWon University

요 약

자체 제작한 프로그램인 USB 보안 모듈과 Active Directory를 활용하여 서버에서 다수의 클라이언트를 관리할 수 있는 인프라를 구축한다. USB 보안 모듈과 기존 소극적인 보안 정책으로 인해 개인 또는 내부망으로 사용하고 있는 Active Directory의 보안 정책을 결합하여 극단적이고 폐쇄적인 강력한 보안 기능을 가능케 하며 그 효용성을 제안 한다.

1. 서론

IT산업이 도래하고 기술이 발전함에 따라 IT 자산을 보호하기 위해 백신, 방화벽, 침입 탐지 시스템 등 보안 시스템 또는 솔루션을 구축하고 운영한다. 그렇다고 해서 해당 조직의 보안 수준이 완벽하다고 볼 수 없지만, 위험을 상당수 방지할 수 있어서 조직의 형태에 따라 시스템을 이해하고 어떤 솔루션을 사용하는지에 따라 보안 수준이 판가름 난다.

취약점은 언제 어디서나 생겨나고 해킹 기술 또한 나날이 발전함에 따라 보안은 항상 뒤따라가며 완벽한 보안은 없다. 상황을 고려하지 않고 무작정 많은 보안 시스템을 도입하게 된다면 오히려 보호하려고 하는 IT자산이 외부로 더 노출될 수 있고 많은 위협이 생겨나는 모호한 상황에 처할 수 있다.

[그림1] Active Directory와 USB의 결합

본 논문은 [그림1]과 같이 Active Directory의 도메인과 그룹 정책을 사용하여 인프라를 구축하고 자체 개발한 USB 보안 모듈과 결합하여 극단적이고 폐쇄적인 보안 시스템을 적용해 살펴보고자 한다.

현재 많은 전산실에서 컴퓨터 환경은 점차 커지고 복잡해지고 있다. 네트워크/시스템 관리자는 해당 자원을 효율적으로 관리하는데 많은 어려움을 겪게 되었고 일반 사용자는 자신이 원하는 네트워크/시스템 자원을 쉽게 찾지 못하는 결과를 낳게 되었다. 이러한 문제로 자산관리나 패치 관리의 어려움 등이 나타나고 있으며 안정적인 PC관리 방안의 부재로 인해 관리 비용이 증가되고있다.

이러한 문제를 해결하기 위해 네트워크상의 개체에 대한 정보를 계층적으로 관리하는 Active Directory (AD)라는 디렉터리 서비스가 널리 사용되고 있다. [1]

기존 Active Directory의 그룹 정책은 상세하고 행위별 세분화된 정책을 제공한다. 화면 잠금이나 컴퓨터 사용을 아예 불가능할 정도의 정책을 원하는 사용자는 다른 보안 솔루션과 결합하여 사용할 수도 있다. Active Directory는 개인 또는 내부 망에서 데이터베이스와 연결하여 인사 관리로 사용하거나

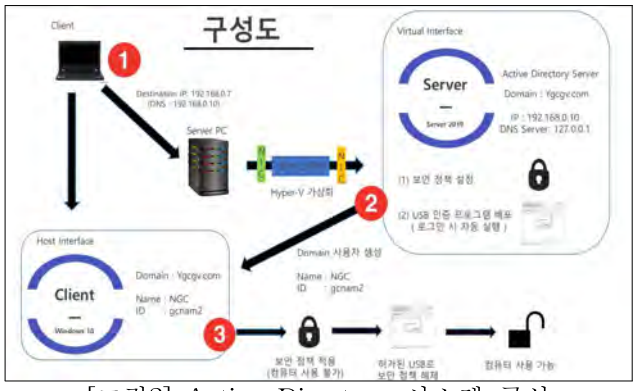
LOB와 결합하는 등 다양한 방면으로 사용될 수 있다.

기본으로 제공되는 서비스일뿐더러 많은 기능과 다른 LOB자원과 유연하게 연동할 수 있기 때문에 외부적인 극단적인 기능을 추가하여 Active Directory와 결합한다면 시스템과 물리적인 보안 등 다양한 측면의 보안을 실현할 수 있다는 것이 본 논문의 목표이자 제안 방식이다.

2. 제안 방식

2-1 Active Directory

Windows 2000 이상의 제품군에서 지원하는 계층적 디렉터리 서비스이며 네트워크, 사용자 또는 그룹을 통합적으로 관리하는 기능을 지원한다. LDAP 프로토콜 기준을 만족하고 클라이언트는 DNS상에 구현된 Active Directory로 액세스할 수 있다. 또한, 다른 Active Directory와도 결합을 허용하며, 각 서버의 역할을 지정하여 체계적인 관리가 가능한 인프라를 구축할 수 있다.



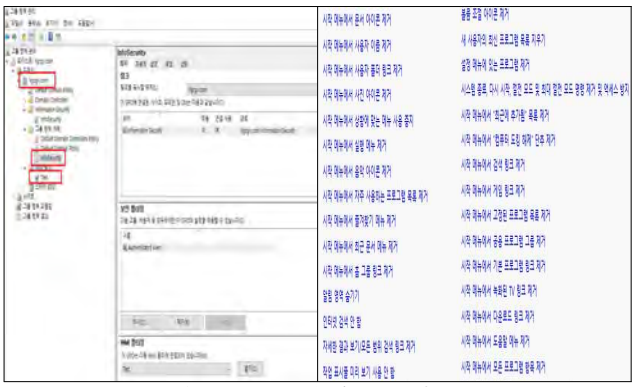
[그림2] Active Directory 시스템 구성

2-2 구성

서버의 하드웨어 자원을 효율적으로 사용하기 위해 Hyper-V 가상화를 활용하여 Windows Server 2019 Active Directory를 구축하였다.

Active Directory에는 기본적으로 DNS 서버가 탑재되어 있어서 도메인 인증서 역할을 설치 후 DNS가 Loopback이 되도록 네트워크 설정을 해준다. Forest 내 처음 설치한 컴퓨터는 자동으로 Forest의 Root Domain Controller로 지정된다.

Active Directory가 설치되면 [그림2]와 같이 해당 Forest의 도메인명 'Ygcgv.com'으로, 클라이언트를 이행하여 Active Directory에 액세스한다.



[그림3] 그룹 정책 UI 및 종류

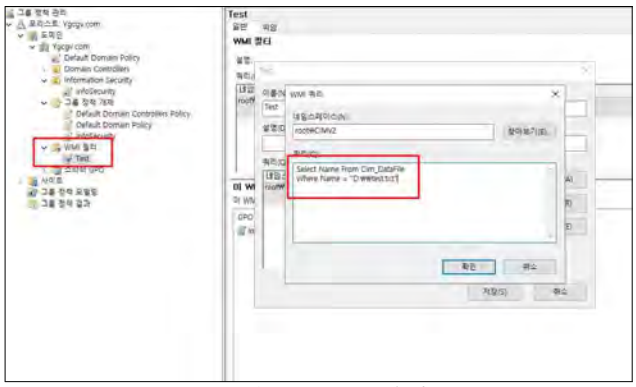
Active Directory에서 미리 설정된 그룹 정책에 따라서 액세스 된 클라이언트는 상시 그룹 정책을 적용받고 관리된다. 그룹 정책의 종류와 구분은 다양하지만 대개 시스템에 해를 가하지 못하도록 특정 기능을 제거하는 등 소심한 정책들로만 구성되어 있다.

[그림3]과 같이 구성된 Active Directory의 그룹 정책뿐만 아니라 극단적인 차단 기능(화면 잠금 등)을 추가한 USB 보안 모듈 프로그램과 함께 사용한다. 서로 필요한 부분을 보완하며 강력하고 관리하기 편한 보안 시스템을 구현해내는 것을 실현한다.

2-3 보안정책

Active Directory의 그룹 정책에는 수많은 종류가 있다. 서비스를 강제적으로 종료하지 못하거나 권한이 없는 파일에 액세스할 수 없는 등 서버 관리자가 지정한 비정상적인 행동을 할 수 없도록 클라이언트에 정책을 적용할 수 있다. 사용자 또는 컴퓨터별 목적과 상황에 따라 정책을 일부 적용하거나 제외할 수 있어 매우 유연하게 구성할 수 있다.

아무리 적절하고 다양한 그룹 정책을 적용해도 보안사고가 일어나지 않을 것이라고는 할 수 없다. 컴퓨터의 모든 기능을 막지 못할뿐더러 로그온 패스워드를 알고 있는 사람이라면 컴퓨터 자체는 사용할 수 있기 때문이다. Active Directory의 기본 기능으로 정책을 동적으로 적용할 수 있는 WMI 필터가 제공되어 어느 정도 보안 수준을 올릴 수 있다.

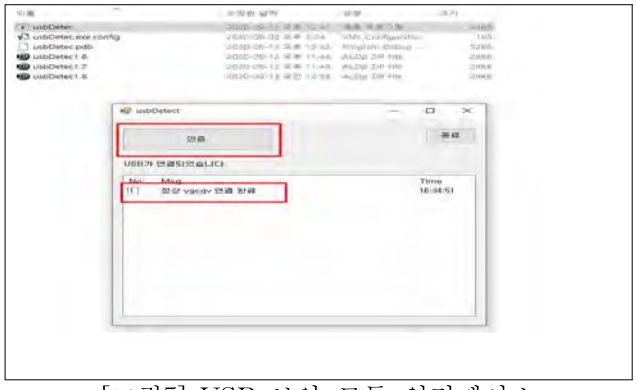


[그림4] WMI 필터

WMI 필터링은 SQL과 비슷한 WQL 언어로 클라이언트가 특정 조건이나 시기에 정책을 적용받을 수 있게 할 수 있는 동적 동작을 가능케 한다. Query 값이 출력되면 True, NULL이면 False를 반환하여 True일 때 정책이 적용된다.

특정 시간에만 정책을 적용하거나 클라이언트의 운영체제 버전 또는 Drive 이름 등을 Query 하여 True일 때 정책을 적용할 수 있다. 본 논문에서는 USB가 인식되었을 때 즉, True일 때 정책을 적용받지 않아야 하므로 파일의 존재 여부에 따라 [그림4]와 같이 WMI 필터를 적용했다.

2-4 USB 보안 모듈



[그림5] USB 보안 모듈 인터페이스

Active Directory에 액세스 되어 있는 클라이언트는 프로그램 배포 정책을 통해 컴퓨터가 켜지면 자동으로 자체 개발한 USB 보안 모듈이 실행되게 설정했다. [그림5]는 USB 보안 모듈이 실행된 직후 모습이다. 인증된 USB를 연결하라는 Message Box 하나뿐인 것 같지만, 저 상태의 화면 그대로 정지시켜 버린다. 마우스 클릭은 물론 키보드조차 동작하지 않는다. USB 보안 모듈의 핵심 기능인 화면 잠금이다. 인증된 USB가 없거나 허가되지 않은 사람이 컴퓨터에 접근하면 과부하가 걸렸다고 생각할 수 있기 마련이다. 하지만 사실은 USB 보안 모듈이 실행되는 즉시 Print Screen을 통해 현재 화면을 저장한 후 종료할 수 없는 사진을 화면에 뿌려주는 역할만 한다. 따라서 사진 위에 마우스 클릭을 하면 아무런 작동이 안 되는 것이다.

외부 사용자로부터 PC를 보호하기 위해 본 보안 시스템이 실행되어지고 있을 때 작업관리자가 1순위로 실행된다면 본 시스템을 강제종료할 수 있기 때문에 작업관리자를 배제하도록 프로그램을 설계해야 한다. 또한 작업표시줄의 실행 권한이 관리자 권한보다 높으므로 작업표시줄에서 작업관리자를 호출했을 때 1순위로 호출되기 때문에 작업표시줄 또한 배제하여야 한다.[2]

때문에 키보드 잠금 및 시스템 키(Alt+F4, Alt+Tap) 잠금은 따로 구현되어 있다. 컴퓨터 종료나 작업관리자 실행은 Active Directory의 그룹 정책으로 제거해 놓는다.

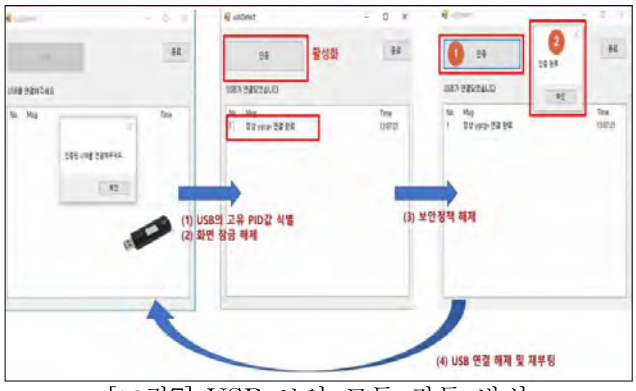
USB 보안 모듈이 연결된 USB의 PID값을 식별하고 나면 USB 보안 모듈의 인터페이스가 출력된다. 더불어 잠겨 있던 마우스 클릭과 키보드 잠금이 정상 작동하게 된다. 이후 인증 버튼을 클릭하면 Active Directory 그룹 정책이 적용되지 않아 온전히 컴퓨터를 사용할 수 있다. 사용 후 USB가 해제되는 순간 화면이 다시 잠긴다. 아래 [그림6] 사진은 USB 보안 프로그램 내 PID값을 저장해 놓은 코드의 일부분이다.

```
// usb 정보가 담긴 enum
// 여기에 USB 시리얼 번호를 등록하면 된다.
public enum UsbSerial
{
    //USB 1  sjh1
    [StringValue(@"USBSTOR#DISK&VEN_GENERIC&PROD_STORAGE_DEVICE&REV_0220#6&2869A60E&1")]
    USB1 = 1,

    //USB 2  sjh2
    [StringValue(@"USBSTOR#DISK&VEN_MASS&PROD_STORAGE_DEVICE&REV_1.00#121220180204&0")]
    USB2 = 2,

    //USB 3  ngc
    [StringValue(@"USBSTOR#DISK&VEN_ADATA&PROD_USB_FLASH_DRIVE&REV_1100#29917213102200E3E&0")]
    USB3 = 3,

    //USB 4
    [StringValue(@"추가할거 넣으셈")]
    USB4 = 4,
}
```

[그림6] USB PID값 저장 코드

WMI 필터는 True일 때 정책을 적용받는다. 즉, 그림[4]에서 설정한 것과 같이 특정 파일이 존재해야 한다. 본 논문에서는 True일 때 정책을 적용받지 않아야 하므로 인증 버튼을 누르면 특정 파일을 삭제하는 내부 명령어를 구현해 놓았다. 따라서 특정 파일이 없으므로 WMI 필터는 False를 반환하고 정책이 적용받지 않게 된다. 이 특정 파일은 로그오

프 및 컴퓨터 종료 시 Power Shell Script를 통해 다시 생성된다.



[그림7] USB 보안 모듈 작동 방식

(1) 정해진 PID값을 가진 USB가 인식됐는지 식별
(2) USB 인증 문구가 출력됨과 동시에 화면 잠금 해제 및 인증 버튼 활성화
(3) 인증버튼을 누르면 Active Directory의 보안 정책 해제
(4) USB 인식을 해제하면 (1)번으로 돌아감

3. 결론

Active Directory의 그룹정책과 자체 제작한 USB 보안 모듈의 극단적인 보안 기능으로 소유인증 기반의 보안 인프라를 구축하였다. 인증된 USB가 연결되었을 때 WMI 필터를 위한 특정 파일은 삭제된다. 이후 해제되었을 때 Active Directory가 적용한 정책은 특정 파일이 생겨야 하므로 컴퓨터를 재부팅 하거나 로그오프 해주어야 한다. 이는 한 번 인증되면 비 인가된 다른 사용자도 컴퓨터를 사용할 수 있는 말이 된다. USB 보안 모듈은 단지 USB의 연결 여부로 화면 잠금을 실행하기 때문에 위 같은 상황이 발생하더라도 USB 보안 모듈이 그 역할을 다하게 된다.

USB 보안 모듈이 Active Directory 그룹정책과의 결합뿐만이 아니라 자체적으로도 극단적인 보안 기능이 있지만, 추가 기능 개발을 목표로 둠으로써 보안 위협을 내포하고 있는 소스코드를 지양하고 보안 코드 작성 및 추가 기능 개발하는 것을 향후 목표로 하고 있다. 또 다른 목표는 USB의 분실이다.

USB메모리는 USB플래시 드라이브 혹은 USB디스크 등으로 불리며 크기가 매우 작아 높은 휴대성을 제공하며, 용량대비 가격이 저렴해 이미 많은 사용자를 확보하고 있다.

반면, USB 메모리의 휴대성으로 인하여 USB메모리의 분실 및 도난이 잦아졌고 그로 인한 개인정보 및 기업의 주요정보 유출 사고가 발생하는 문제점이 발생하였다.[3]

이처럼, USB를 도난당하거나 잃어버리는 것에 대한 방안 또한 해결해야할 과제이다. 뿐만 아니라, 향후 발생 가능한 보안 위협에 대한 추가와 위험한 함수들에 대한 분류를 통해 더욱 많은 취약성 검사가 가능하도록 노력해야 한다. 많은 보안 위협은 외부로부터의 공격만이 아니라 소스코드 자체에 내포하고 있다. 기능적으로는 정상적이지만 함수의 특성상 외부의 침입을 유발하거나 위험한 동작을 보일 가능성이 있으므로 더욱 안전한 함수의 사용이 필수적이다.

Active Directory와 USB 보안 모듈의 결합으로 서로의 적절한 기능을 이용해 강력한 보안 인프라를 구축할 수 있었다.

(1) Active Directory의 네트워크 인증 중앙화 관리
(2) 자체 개발한 USB 보안 모듈의 보안 기능
(3) Active Directory 그룹 정책으로 USB 보안 프로그램 물리적 원격 관리

Active Directory의 많은 기능을 사용해보면서 어떻게 활용하느냐에 따라 다양한 용도로 사용될 수 있었음을 알았으며, USB 보안 모듈 프로그램을 개발하면서 적은 기능으로 많은 위협을 방지할 수 있다는 것을 깨달았다. 보안 시스템이나 솔루션을 상황에 맞는 적절한 기능을 활용하지 못한다면 불필요하거나 효율적이지 못한 인프라를 구축할 수 있다는 것을 알 수 있었으며 보안의 대상과 목적을 파악하고 상황에 맞는 적절한 보안 기능과 인프라를 구축해야 함을 느낄 수 있었다.

참고문헌

[1] 김승현, Windows Active Directory Service 권한명칭을 이용한 네트워크 프린팅 설정을 위한 알고리즘pp 366-366, 학술 논문, 한국정보과학회(2010)
[2] 이세훈, USB 저장 장치와 스마트폰을 이용한 윈도우 OS PC보안 시스템 구현pp 318-318, 학술 논문, 한국컴퓨터정보학회(2016)
[3] 이선호, 이임영, USB메모리를 위한 보안 솔루션에 관한 연구pp94-94, 멀티미디어학회 논문지(2010)