USB 보안 모듈과 Active Directory를 활용한 최적의 보안정책에 관한 연구

안수용* 이덕규*
*서원대학교 정보보안학과
tysj712@naver.com, deokgyulee@seowon.ac.kr

A study on optimal security policy using USB security module and Active.

Su Yong An *, Deok Gyu Lee*
*Dept. of Information Security, SeoWon University

요 약

자체 제작한 프로그램인 USB security module과 Active Directory를 활용하여 서버에서 다수의 클라이언트를 관리할 수 있는 시스템을 구축한다. USB 보안 모듈과 Active Directory의 보안정책을 결합하여 극단적이고 폐쇄적인 강력한 보안을 가능케 하며 보안정책별 효용성을 살펴보고자 한다.

1. 서론

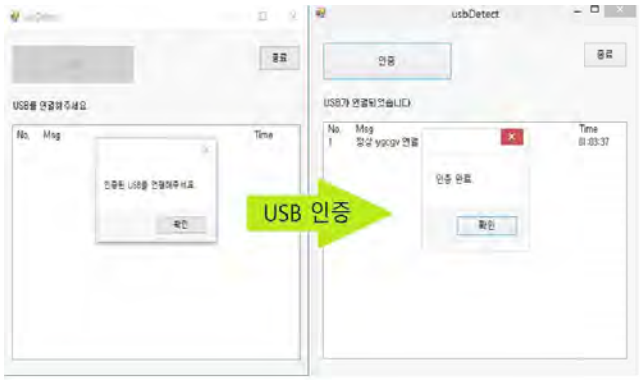
IT가 나날이 발전함에 따라 Security는 항상 뒤따라간다. Security는 매우 중요한 부분이기 때문에 상황에 맞는 적절한 Security system과 policy가 도입되어야 하고, 그렇기 때문에 Active Directory를 이용한다. Active Directory는 서버에서 도메인을 활용한 중앙 집중형 관리를 가능케 하기 때문에 대다수의 기업이 사용하고 있다. 사용자의 필요성에 의해서 어떤 Infra와 Security policy를 적용하느냐에 따라 Security function이 달라지기 때문에, 자체 제작한 USB와 Active Directory를 활용하여 강력한 Security system을 만들기 위해 보안정책별 효용성을 연구해보고자 한다.

2. 에이전트 개발도구의 요구사항

사용자의 필요성에 따라 강력한 보안 시스템을 제공하기 위해서는 USB security module과 다양한 Security policy가 제공되어야 한다.

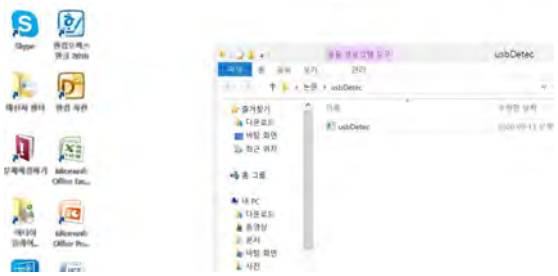
2-1. USB security module의 기능

2-1-1. USB security module의 실행과 USB 인식



USB security module 실행 후 인증된 USB를 인식 하면 정상적으로 보안 해제 가능.

2-1-3. 화면 잠금과 키보드 잠금



인증되지 않은 USB를 사용하거나, USB를 제거하면 USB security module이 실행되어 사용하던 화면 그대로 Rock이 걸리며, System Key도 사용불가.

3. Active Directory 대표적 보안정책 종류

3-1. 응용 프로그램제어 정책

3-1-1. AppLocker

-실행파일규칙

-Windows Installer

- 스크립트 규칙

3-2. 네트워크

3-2-1. Windows Connect Now 마법사의 액세스 금지

3-2-2. 네트워크 연결

-LAN 또는 원격 액세스 연결의 구성 요소 추가 및 제거금지

-고급 메뉴의 고급 설정 항목 액세스 금지

-TCP/IP 고급 구성 금지

-LAN 연결의 구성 요소 사용/ 사용 안 함 설정 금지

-모든 사용자 원격 액세스 연결 삭제 허용 등

3-2-3. 오프라인 파일

-관리적으로 지정된 오프라인 파일

-서버 연결이 끊기면 수행할 비기본 동작

-이벤트 로깅 수준

-서버 연결이 끊기면 수행할 동작

-오프라인 파일 폴더 사용금지

-오프라인 파일의 사용자 구성금지 등

3-3. 시스템

-Ctrl+Alt+Del 옵션

-그룹 정책

-드라이버 설치

-로그온

-로캘 서비스

-이동식 저장소 액세스

-인터넷 통신 관리 등

3-4. 바탕화면

-사용자가 수동으로 프로필 폴더를 리디렉션 하는 것을 금지

-바탕 화면에 잇는 모든 항목 숨기기 및 사용 안 함

-바탕 화면 정리 마법사 제거

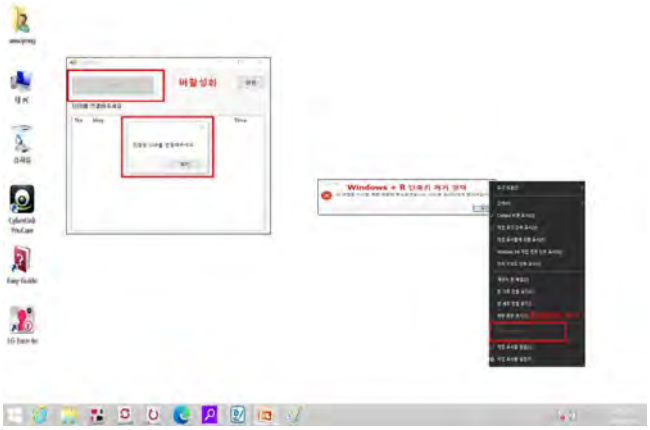
-바탕 화면에서 내 문서 아이콘 제거

-바탕 화면의 네트워크 위치 아이콘 숨기기

-종료할 때 설정 저장 안 함 등

4. USB security module과 security policy의 결합

4-1. Windows + R 단축키 제거 정책과 작업 관리자 제거 정책 적용



Windows + R 단축키제거 정책과 작업관리자 제거정책을 적용 했을 때 USB security module의 기능과 결합하여 Windows + R 단축키 사용과 작업관리자 동작을 차단하고 폐쇄적인 security system이 구축되었다.

4-1-2. 인증 된 USB 인식 후 Security policy 해제

인증된 USB 인식 후 Windows + R 단축기 사용과 작업관리자 동작이 활성화 된 것을 확인함으로써 Security policy가 해제 된 것을 확인 가능.