윈도우즈 시스템에서 집중방해요소 차단 기술

네트워크 패킷(packet) 차단과 프로세스 제어

2019-13674 양현서

©yhs0602@snu.ac.kr

서론

연구 주제

윈도우 환경에서 온라인 학습 집중 보조를 위해 필요한 네트워크 패킷(packet) 차단과 프로세스 제어 기술을 연구한다.

연구 동기 및 목적

1. 온라인 수업이 증가하면서 집중을 도와주는 솔루션의 개발이 절실하나, 소수의 솔루션만이 제공되어 소비자의 선택의 폭이 좁다.
2. 집중방해요소 차단 솔루션을 구현하려면 특수 권한 접근을 위해 NT 레거시 드라이버 개발이 필수적이지만 이를 구현하기 위한 기술인 DDK(Driver Development Kit)는 진입 장벽이 높다.

이에 따라 집중방해요소 차단 솔루션을 제작할 때 필요한 부분을 집중적으로 연구하는 것이 이 연구의 목적이다.

이론적 배경

API(Application Programming Inverface)

API란 응용프로그램이 특별한 기능을 사용할 수 있도록 운영체제가 제공하는 기능의 집합이다.

보호 링과 윈도우 드라이버 모델

높은 특권을 가진 링 0에서 동작하는 프로그램을 개발하기 위해서는 DDK라는 특별한 API를 사용하여야 하며, 윈도우 드라이버 모델이 이러한 API를 제공한다.

WFP(Windows Filtering Platform)

WFP는 네트워크 필터링 기능을 제공하는 응용 프로그램을 만들기 쉽도록 윈도우가 제공하는 API의 모음이다.

콜백함수

콜백함수란 특정 사건이 발생했을 때 실행하게 설정하는 개발자가 정의한 코드이다.

연구 방법

1. 윈도우 디바이스 드라이버를 개발하는 방법 연구 : 윈도우 디바이스 드라이버를 개발하기 위한 지식이 담긴 도서(윈도우 디바이스 드라이버)를 조사하여 정리한다. 기본적인 기능을 가진 윈도우 디바이스 드라이버를 생성하여 제어하는 방법을 실험하고 정리한다.
2. 방화벽 개발 관련 정보를 참고하여 네트워크 필터링 방법 연구: 네트워크 패킷(packet) 필터링을 구현한 라이브러리를 조사하여 구현을 분석하거나 해당 라이브러리를 이용하는 방법을 연구하고 테스트한다.
3. 백신 개발 관련 정보를 참고하여 프로세스 필터링 방법 연구: 오픈 소스 백신 소프트웨어의 소소크도나 Windows API 문서를 참조하여 프로세스 필터링 프로그램을 개발하여 테스트한다.

연구 결과

연구 결과, 다음과 같이 구성하여 개발하면 네트워크 패킷 차단 및 프로세스 제어 기능을 구현할 수 있다는 결론을 내려 예시 응용 프로그램을 개발하였다.

구조도

1. DeviceIoControl (마셜링 이용) 프로세스 차단 목록 관리
2. PsSetCreateProcessNotifyRoutine으로 콜백 함수 등록
3. 프로세스 실행 시 운영체제가 콜백 함수 호출
4. 드라이버가 차단 목록에 의해 프로세스 실행 허용/차단
5. 네트워크 감시 기능 실행/중지, 차단 사이트 관리
6. WinDivert 라이브러리 이용
7. WinDivert 드라이버 로드 및 제어
8. Windows 필터링 플랫폼에 WinDivert.sys 드라이버 등록
9. 네이티브 네트워크 API 호출

   다음은 프로그램 실행 결과이다. 예시의 의도대로 메모장 실행이 차단되는 것을 볼 수 있다.

연구 결과 소스 코드 저장소

Github에서 본 포스터의 소스 코드를 탐색할 수 있다. 해당 저장소의 주소는 다음과 같다. https://github.com/KYHSGeekCode/Self-Protecting-Driver

한계점 및 논의

HTTPS

HTTPS 환경에서는 패킷이 암호화되기 때문에 패킷을 감시하는 것만으로는 사용자가 접근하는 URL 정보를 얻어오기 어렵다. 이 문제를 해결한다면 한 단계 더 나아갈 수 있을 것이다.

시사점

이 연구는 타 분야에 비해 자료를 이해하기 어려운 DDK를 이용한 NT 레거시 윈도우 디바이스 개발이라는 분야에 유용한 예시를 제공하며, 이 연구를 통해 작성한 구현을 이용하여 비대면 강의 시 학생들의 집중을 도와주는 솔루션을 만드는 데 큰 도움을 준다는 데서 의의가 있다.

References

[1] 이봉석, 『윈도우 디바이스 드라이버』, *한빛미디어*, 2009.