API 후킹 모듈을 이용한 개인 방화벽 운용 시스템

한종길* · 김종찬* · 반경진* · 김치용** · 김응곤*

*순천대학교 컴퓨터과학과

**동의대학교 영상정보공학과

Personal Firewall Operating System Using API Hooking Modules

Jong-Gil Han* · Jong-Chan Kim* · Kyeong-Jin Ban* · Kim Cheeyong** · Eung-Kon Kim*

*Sunchon National University

**Dong-Eui University

E-mail : seaghost@sunchon.ac.kr

요 약

네트워크 구축 시 방화벽 설치에 대한 어려움이 있으며, 이를 운용하기에 막대한 비용이 요구된다. 개인용 컴퓨터에 홈 네트워크 방화벽을 구축하기에는 경제적으로 많은 부담이 된다. 이러한 경제적 부담에 의해 각 가정에 대해 방화벽을 구축하지 않고 개인용 PC들은 기업용 방화벽을 적용해서 방화벽 내부 해킹에 대해서 많은 문제점이 나타난다. 본 논문에서는 API 후킹 모듈을 이용한 개인 방화벽 운용에 관한 것으로 휴대용 저장장치에 쓰기 및 삭제가 불가한 영역을 형성하였다. 그리고 해당 영역으로 API 후킹을 위한 알고리즘을 제안하였다. 제안한 알고리즘은 개인용 컴퓨터에 방화벽 설치 및 활용이 손쉽게 이루어져 사용 편의성을 증대시킬 수 있을 것으로 사료된다.

ABSTRACT

The popularization and development of 3D display makes common users easy to experience a solid 3D virtual reality, the demand for virtual reality contents are increasing. This paper proposes VR panorama system using vanishing point location-based depth map generation method. VR panorama using depth map gives an effect that makes users feel staying at real place and looking around nearby circumstances.

키워드

방화벽, USB 메모리, API 후킹 알고리즘

Ⅰ. 서 론

오늘날 방화벽은 네트워크의 구성에 필수적인 요소가 되었으며 인터넷의 발달과 맞물려 처리용량이 증가되었다[1,2]. 처리용량의 증가는 현재의 생활 및 업무 환경에 엄청난 변화를 가져왔다. 일상생활에서는 인터넷을 이용할 수 없고 컴퓨터가 없다는 것은 상상할 수도 없을 정도로 그에 대한 의존도가 높아지고 반드시 없어서는 안 될 환경이 되었다[3].

종래의 방화벽 시스템은 대규모 네트워크가 필요한 기업을 대상으로 기술개발이 이루어졌고, 방화벽 설치의 어려움이 있다. 그리고 이를 운용하기에 막대한 비용이 요구된다. 개인이 자신의 홈 네트워크에 방화벽을 구축하기에는 경제적으로 많은 부담이 된다. 이러한 경제적 부담에 의해 각 가정에 대해 방화벽을 구축하지 않고 가정들의 그룹에 대해 기업의 방화벽을 적용한 경우 방화벽 내부의 해킹에 대해 취약하게 된다. 사용자는 개인 PC, 학교, 게임방, 공공장소의 컴퓨터를 사용하거나, 임의의 컴퓨터를 사용하기에 안정성을 보장받지 못한다는 문제점이 야기되고 있다.

본 논문에서는 API 후킹 모듈을 이용한 개인 방화벽 운용에 관한 것으로 휴대용 저장장치에 쓰기 및 삭제가 불가한 영역을 형성하고, 해당 영역으로 API 후킹을 위한 알고리즘을 제안하였다.

Ⅱ. 관련연구

2.1 방화벽의 정의 및 시스템 구성

방화벽은 정책(policy)를 구현함에 있어서 네트워크를 통한 데이터 교환을 제어하는 능력을 추가하고 있다. 방화벽은 네트워크 패킷을 검사하고, 이 패킷들이 네트워크를 통과하는 것이 허가되어야 한다. 이를 통화하지 않으면 상기 검사에 기초하여 판정하지 못하는 결과가 나오게 된다. 방화벽을 통해 구현되는 정책은 하나 이상의 필터에 의해 정의된다. 각각의 필터는 필터 파라미터 및 이에 연관된 액션(action)을 포함한다.

방화벽 시스템 구성은 스크리닝 라우터가 가장 간단한 방화벽 시스템이다. 이 방법은 일반적으로 IP 필터링 기능이 추가된 하드웨어 라우터를 이용해서 IP 패킷들의 접근제어를 행하는 방법이다. 이 방법은 간단히 구현이 가능하다는 장점이 있을 수 있으나, 많은 단점이 존재한다. 로그 정보를 남길 수 없고, 만일 하드웨어 라우터의 펌웨어에 버그가 존재한다면 망 전체가 공격당할 위험이 있다.

스크리닝 라우터 없이 내부 망과 외부 망사이에 시스템을 놓고 시스템의 TCP/IP 포워딩 기능을 막음으로써 구현되는 방화벽 시스템이다. 그러므로 두 망사이에는 직접적인 트래픽이 불가능하다. 여기서 시스템은 두 개의 망 인터페이스를 가지고 있어야 한다. 예를 들자면 두 개의 랜카드 또는 한 개의 Slip 인터페이스, 한 개의 랜카드로 구성되어 질 수 있다.

응용 프로그램 게이트웨이는 프록시 게이트웨이라고도 한다. 인터넷상의 많은 소프트웨어는 자료를 저장하고 전송하는 방식을 택하고 있다. 예를 들면 메일 프로그램이나, USENET 뉴스 등을 들 수 있다. 응용 프로그램 게이트웨이는 각각의 망 서비스별로 정보를 전송하는 방법이다. 이 방법은 IP 단계가 아닌 응용 프로그램 단계에서 수행되어 진다. 즉, 방화벽을 사이에 두고 서비스를 양쪽으로 전송하는 방식이다.

Ⅲ. API 후킹 모듈 운영 및 효과

API 후킹 모듈은 임의의 공간에 설치된 컴퓨터에 방화벽 설치가 용이하고, 임의의 컴퓨터를 안정적으로 사용 할 수 있도록 휴대용 저장장치를 이용하여 개인 방화벽을 설정한다. USB 메모리 형태를 갖는 휴대용 저장장치를 이용함으로써, 휴대의 간편성과 플러그 앤 플레이 기능으로 인한 사용의 편의성을 기반으로, 개인 컴퓨터 이외에 학교, 공공시설, PC방에서 설치된 임의의 컴퓨터 사용시, 각종 바이러스, 악성코드, 해킹과 같은 위험요소를 사전에 방지하고, 휴대용 저장장치에 저장된 개인정보를 보호할 수 있는 API후킹모듈을 포함하는 휴대용 저장장치 및 이를 이용한 개인 방화벽을 운용한다. 그리고 휴대용 저장장치의 비가용 영역을 설정하고, 해당 영역으로 API 후킹 알고리즘을 기반으로 한 개인 방화벽을 실행토록 함으로써, 외부 침입에 대한 대응을 용이하게 처리할 수 있다. USB 메모리를 이용한 개인방화벽을 실현함에 있어 플러그앤 플레이 기능을 제공함으로써, 개인 컴퓨터에 대한 방화벽 설치 및 활용이 손쉽게 이루어져 사용 편의성을 증대시킬 수 있다.

API후킹 모듈을 포함하는 휴대용 저장장치는 상기 하우징 내로 인입 설치되는 메모리 소자 및 통신 프로토콜에 따라 데이터의 입출력을 관리 제어하는 제어소자를 포함하되, 상기 메모리 소자는 플래시 메모리로 구현되어 네트워크 정책정보를 등록 관리하는 정책관리 영역 및 ROM 셀을 이용한 데이터 쓰기 불가 영역으로 형성되거나, 기 등록된 네트워크 정책이 등록 관리되고, 네트워크 API후킹 알고리즘에 기반으로 네트워크 정책에 따른 네트워크 접속 여부를 결정하는 방화벽 운용영역으로 분할된다.

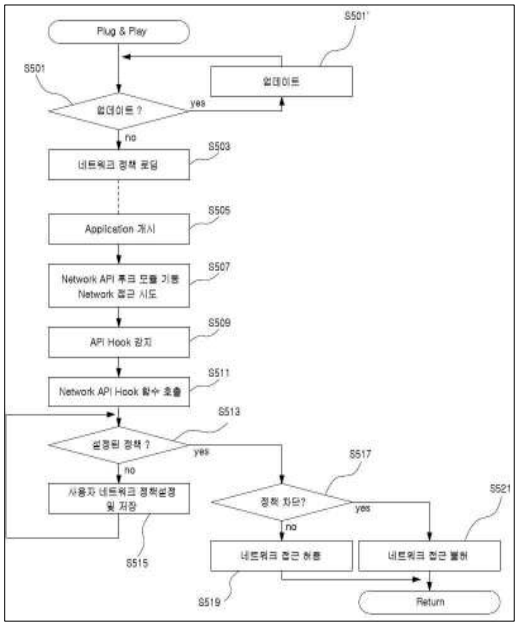

그림 1. API 후킹 모듈 USB메모리 방화벽 운용 흐름도

Ⅳ. 결 론

본 논문에서 제시하는 API 후킹모듈을 이용한 USB메모리 개인방화벽은 현재 무분별하게 이루어지는 해킹, 보안 분야에서 활용 할 수 있다. 개인용 USB 메모리에 API 후킹을 이용한 네트워크 차단 기능을 수행할 수 있는 방화벽 알고리즘을 특정 영역에 탑재함으로써, 컴퓨터 사용시 USB를 이용한 플러그 앤 플레이 기능의 방화벽 실행이 가능하다. 따라서, 방화벽 사용의 편의성을 증대시키고, 계속적으로 높아지는 방화벽 운용의 비용 절감효과를 유도하여, USB메모리의 후대성에 기인하여 네트워크 접속의 안정성을 확보할 수 있다. 방화벽 알고리즘의 개발로 누구나 쉽게 방화

벽 알고리즘 구축으로 USB메모리에 쉽게 개인 방화벽을 구축 할 수 있게 심층적으로 연구할 것이다.

참고문헌

[1] 천준호, “DDos 공격에 대한 방화벽 로그 기록 취약점 분석”, 2007.
[2] 행정자치부, 전자정부전문위원회, “정보 시스템 구축 운영 기술 가이드라인 2.0”, 2005
[3] 박정진, “네트워크 패킷제어와 에이전트를 통한 소프트웨어 설치 방법에 관한 연구”, 2008
[4] Marcus J. Ranum “Thinking About FireWall” TIS Inc., 1994
[5] http://blog.paran.com/nayasan/2601693
[6] http://ntfaq.co.kr/4049