윈도우 소켓 응용프로그램 인터페이스 후킹을 이용한 네트워크 퍼징 방법

■ 보유기관 한국전자통신연구원

■ 주요 발명자

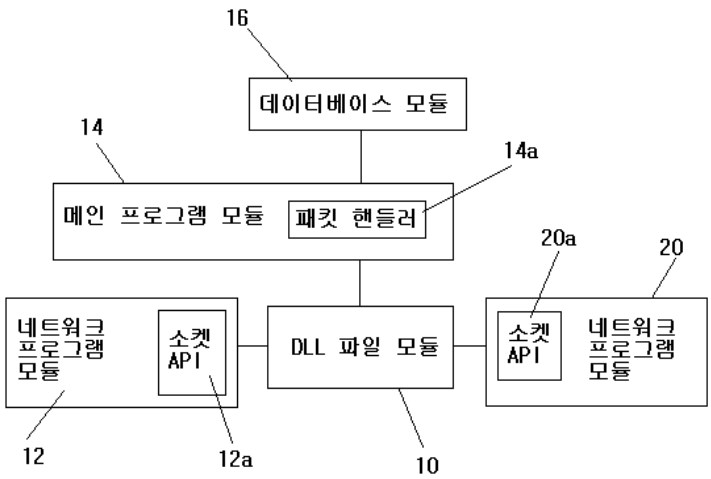
■ 권리사항	
· 출원번호	10-2007-0062325
· 출원일	2007년 6월 25일
· 현재상태	■ 등록 □ 공개(심사중) □ 미공개
■ 기술완성도	□ 기초연구단계 ■ 실험단계 □시작품단계 □ 제품화단계

■ 적용가능분야 및 목표시장 스마트폰 등 네트워크 보안 프로그램 시장

■ 기술 개요

본 기술은 윈도우 소켓 API(Application Programming Interface) 후킹을 이용한 네트워크 퍼징 시스템 및 그 방법에 관한 것임

■ 기술 개념도

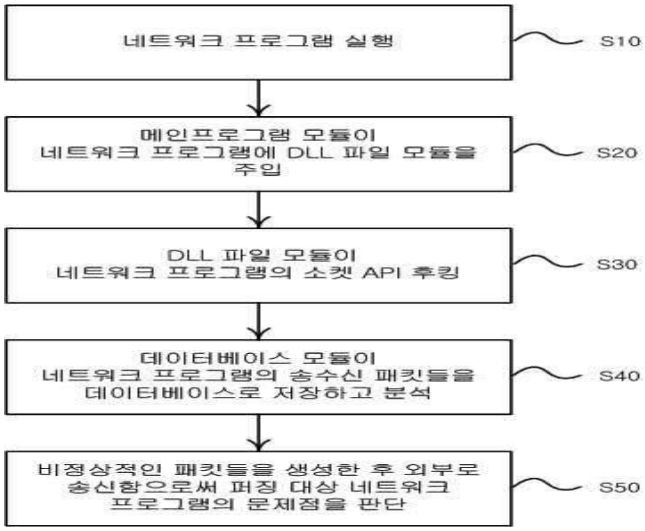


[그림] 본 기술에 따른 윈도우 소켓 응용프로그램 인터페이스 후킹을 이용한 네트워크 퍼징 시스템을 나타낸 블록도

■ 기술 내용 및 동향

[상세 기술 내용]

- 본 기술은 MS 윈도우 운영체제에서 동작하는 네트워크 프로그램을 대상으로 동적 링크 라이브러리 주입(Dynamic Linked Library injection; 이하, DLL 주입이라 함)을 통하여 네트워크 프로그램에 소켓 API 후킹 기능을 삽입함으로써, 네트워크 프로그램이 소켓 API 함수를 사용하여 상대편 네트워크 프로그램과의 송수신하는 패킷을 가로챈 다음, 그 패킷 내의 데이터에 다양한 퍼징 데이터 셋을 추가하여 해당 패킷을 조작하거나 비정상적인 패킷으로 만들어 송신함으로써 범용적인 프로토콜뿐만 아니라, 알려지지 않은 프로토콜에 대해서 네트워크 퍼징을 수행하는 기술임



[그림] 발명에 따른 윈도우 소켓 응용프로그램 인터페이스 후킹을 이용한 네트워크 퍼징 방법을 나타낸 플로차트

[기술의 특 · 장점]

- 기준의 프로토콜 분석과 퍼저 제작을 거치지 않고, 임의의 프로토콜을 사용하는 네트워크 프로그램을 이용하여, DLL 주입을 통한 소켓 API 후킹으로 네트워크 퍼징을 자유롭게 할 수 있음
- 네트워크 퍼징을 수행하기 위해 프로토콜 분석부터 퍼저의 제작까지 많은 인력과 시간이 소모되는 않는 장점이 있음

[기술동향]

- 네트워크 퍼징을 수행하는 퍼저들은 퍼징 작업을 위해, 먼저 목표가 되는 프로토콜을 사용하는 프로그램에 대해서, 프로토콜 분석을 선행하는데, 프로토콜의 개략적인 통신 순서와 패킷구성 등에 대해 조사하여 그에 알맞은 네트워크 퍼징 순서 또는 패킷을 생성하는 과정을 거침
- 이 과정을 바탕으로 프로토콜에 적절한 퍼저를 생성하게 되는데, 프로토콜 분석에서부터 퍼저 제작까지의 과정이 실제 네트워크 퍼징을 하는 것보다 많은 노력과 시간을 소비하게 된됨
- 또한, 네트워크 퍼저 프레임 워크 형태의 퍼저 제작 도구들은 새로운 프로토콜에 대한 퍼징을 위해, 정형화된 패킷 송수신 기법을 제공하고 있지만, 전적으로 프로토콜 분석은 사용자의 몫이고, 패킷 구조의 생성 또한 사용자에게 전부 의존함.
- 결국 현재 출시되어 있는 네트워크 퍼저들은 잘 알려진 프로토콜에 대해서만 퍼징 작업을 수행할 수 있으므로 알려지지 않은 프로토콜에 대한 퍼징 작업은 반드시 새로운 형태의 퍼저가 제작되어 져야만 가능함

■ 관련 기술		
1	출원번호	10-2007-0115337
	발명의 명칭	이동통신 시스템의 네트워크 운용 방법 및 장치
2	출원번호	10-2006-0111028
	발명의 명칭	무선 IPv6 기반의 경로 최적화 방법

■ 시장 동향

[시장 동향]

- 퍼징 기술은 웹 퍼징, 네트워크 퍼징, 메모리 퍼징, 파일 퍼징등의 기술이 있으며, 그중 네트워크 퍼징은 서버의 데몬을 대상으로 하여 조작된 패킷을 전송하는 것으로, 서버의 데몬은 소켓을 통하여 클라이언트와 통신을 하는 어플리케이션임
- 클라이언트에서 서버로 보낸 메시지는 데몬에서 받아서 파싱을 한 후, 연산 처리가 된며, 필요에 따라서 데몬은 다시 라이언트에 게 메시지를 보내기도 하고, 데몬 역시 사람이 만든 어플리케이션인데다, 클라이언트로부터 받은 메시지를 파싱하는 과정, 즉 사용자의 입력이라는 과정을 거치므로 취약점이 존재할 수 있음
- 그렇기 때문에 네트워크 프로토콜 퍼저는 클라이언트의 입장에서 메시지를 조작하여 소켓을 통해 서버로 전송하는 기술이 개발되어 있음

[시장 경쟁력 분석]

- IT 제품의 지능화, 그린화, 무선화에 힘입어 소프트웨어의 중요성이 한층 증가함에 따라 소프트웨어의 보안 취약점을 이용한 공격 위협 또한 커지고 있고, 네트워크 인프라가 전국적으로 구축되면서 발달한 온라인 환경은 웹 소프트웨어의 활성화를 가져왔지만, 본질적으로 개방된 웹상에서는 소프트웨어의 취약점을 이용한 보안 사고의 위험성이 매우 높으므로 상술한 네트워크 퍼징 기술은 그 활용 범위성이 높다고 판단됨

■ 문의처	
· 소속	기술사업화실
· 담당자	유준상
· 연락처	042-870-4827, yjs39@ensec.re.kr