SharpPcap 기반의 대화형 패킷 분석기의 설계

유재헌 · 최성룡 · 김민철 · 김진모 · 황소영

부산가톨릭대학교

Design of Packet Analyzer Using SharpPcap

Jaeheon Yoo · Seongryong Choi · Minchul Kim · Jinmo Kim · Soyoung Hwang

Catholic University of Pusan

E-mail : momoscaptin@naver.com

요 약

네트워킹의 기술이 발전하면서 네트워크 환경에서의 해킹 기법이 나날이 진화되고 있어 심각한 문제로 번지고 있다. 본 논문에서는 패킷 스니핑을 통해 송/수신되는 패킷들을 모니터링 및 분석함으로써 사용자 보안에 대한 취약점을 최소화하고, 사용자가 정의한 규칙에 의해 네트워크 프로토콜 분석 및 트래픽 통계 수집, 필터링의 기능을 제공하는 패킷 분석기의 설계를 제시한다. 그리고 C# .NET 개발 환경에서 SharpPcap을 활용하여 사용자가 직관적인 구조로 필요한 정보를 보다 쉽고 효율적으로 관리할 수 있는 대화형 패킷 분석 도구를 개발하였다.

ABSTRACT

As network technology advances hacking techniques are also evolving. This paper proposes design of a packet analyzer to monitor and analyze data packets in networks. The proposed packet analyzer offers functions such as packet sniffing, filtering and statistics. We implemented a prototype packet analyzer in C# .NET development environment using SharPcap.

키워드

packet analyzer, packet sniffer, WinPcap, SharpPcap

Ⅰ. 서 론

최근 네트워크의 발전으로 대부분의 정보시스템들은 인터넷을 통해 다양한 서비스를 이용하고 있다. 이처럼 네트워크를 이용한 시스템이 대중화된 반면, 네트워크 발전에 따라 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래의 의도된 용도로 사용하지 못하게 하는 DoS공격, 여기에 좀비 PC를 이용하여 공격성이 진화된 형태의 DDoS공격 그리고 기존에 알려지지 않았던 취약점들을 대상으로 하는 APT공격 등 해킹 기법이 점점 진화되고 있다. 이러한 문제들을 해결하기 위한 한 방법으로 네트워크 환경에서 송/수신되는 패킷들을 모니터링 하는 패킷 분석 도구를 개발하는 연구들이 진행되고 있다.

패킷을 분석하는 대표적인 프로그램들로 와이어샤크(Wireshark), 옴니피크(Omnipeek) 등이 있으며, 이는 실제 상용화되거나 오픈 소스로 제공되어 네트워크의 문제, 분석, 통신 프로토콜 개발 등 다양한 용도로 활용되고 있다.

하지만 대부분의 패킷 분석 도구들은 모니터링을 통해 패킷 정보를 분석하는 기능들로 사용자가 대화형 구조에서 원하는 정보를 검색, 편집할 수 있는 기능들은 제한적이다. 패킷 분석도구와 관련된 기존 연구들로는 최소화된 보안 취약점을 통해 효율적으로 패킷 정보를 모니터링할 수 있는 시스템 구조를 설계한 연구[1], 패킷 정보를 임의 시간마다 누적하여 IP별 데이터의 크기를 측정 및 제어하는 방법을 제안한 연구[2] 등이 진행되었다. 이러한 연구들 역시 네트워크 상태를 모니터링하고 전달되는 패킷 정보를 단방향으로 분석하는데 초점이 맞추어져 있다. 최근 WinPcap을 활용하여 사용자가 시스템을 제어할 수 있는 GUI기반 패킷 분석기를 제안한 연구[3]가 진행되었지만 사용자 인터페이스에 초점이 맞추어져 있어 대화형 구조에 대한 구체적인 방향

이 제시되고 있지 않다.

따라서 본 논문에서는 SharpPcap기반의 패킷 스니핑 방법을 활용하여 네트워크 상에서 송/수신되는 패킷들을 대화형 구조를 통해 모니터링 뿐 아니라 사용자의 보안에 대한 취약점을 최소화할 수 있는 분석 시스템을 설계하도록 한다.

II. SharpPcap을 활용한 패킷 분석기 구성

제안하는 대화형 패킷 분석기는 패킷 스니핑을 활용하여 네트워크 환경에서 전달되는 패킷들을 모니터링 및 분석하는 구조이다. 그리고 패킷 캡쳐 라이브러리인 SharpPcap을 이용하여 C# .NET 환경에서 사용자가 대화식 제어를 할 수 있는 패킷 분석기를 구현한다.

(1) 네트워크 어댑터

일반적으로 네트워크 어댑터에는 2계층의 MAC Address정보와 3계층의 IP Address 정보를 가지고 있다. 패킷을 전송 받을 때 자신에게 전달될 것인지 확인하기 위해 패킷 내용의MAC 주소와 자신의 MAC 주소가 일치하는지 비교한다. 주소 정보가 일치하면 분석 후 운영체제로 넘겨주고, 아니면 폐기하는 구조이다.

(2) 무차별 모드(Promiscuous Mode)

무차별 모드(Promiscuous Mode)란, 수신된 프레임이 자신의 주소와 상관없는 목적지 주소를 갖는데도 이를 수용하는 모드이다. 일반적으로 네트워크 어댑터는 받은 이더넷 프레임의 MAC 주소를 확인한 후 자신의 MAC 주소가 아니면 이더넷 프레임을 폐기한다. 그러나 무차별 모드 기능을 이용하여 자신의 MAC 주소가 아님에도 모든 이더넷 프레임을 수용한다[4].

(3) WinPcap 라이브러리

Pcap(Portable Packet Capturing Library)은 간단하게 패킷을 캡쳐하기 위한 함수들의 모음을 의미한다. 유닉스 계열 운영체제들은 LibPcap 라이브러리에 Pcap을 포함하고 있으며, 윈도우 환경에서는 WinPcap이라는 LibPcap 포팅을 이용한다[5].

(4) SharpPcap 라이브러리

SharpPcap은 .NET 환경의 패킷 캡쳐 프레임워크이며, 이미 알려진 Pcap과 WinPcap 라이브러리를 기반으로 하고 있다. 또한 패킷 캡쳐, 인젝션 분석 및 생성 관련한 API를 제공하고 있다. 본 연구는 C# .NET환경에서 패킷 분석기를 구현하기 위하여 WinPcap기반의 SharpPcap 라이브러리를 활용한다[6].

III. 대화형 패킷 분석기 설계

본 연구는 전송계층으로부터 송/수신되는 패킷 정보들을 대화식 구조에서 캡쳐하고 분석하는 패킷 분석기를 설계한다. 그림 1은 이를 나타낸 것으로 사용자가 보다 쉽고 직관적인 구조로 패킷을 분석 및 활용할 수 있도록 설계한다.

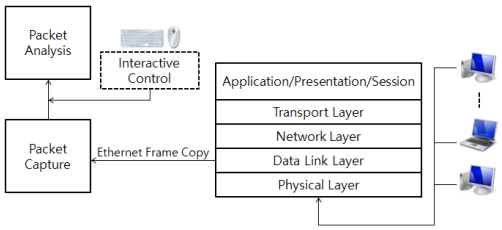

그림 1. 제안한 대화형 패킷 분석기 구조

네트워크 상에서 송/수신하는 사용자 시스템과 여러 시스템간의 패킷 정보는 물리계층(Physical Layer)을 통해 들어오며, 링크계층(Data Link Layer)은 송/수신지 MAC주소 정보, 네트워크계층(Network Layer)에서는 송수신지 IP 주소 및 발신지 IP 주소를 담고 있다. 또한 전송계층(Transport Layer)에서의 송/수신지 포트번호 정보를 통해 응용계층(Application Layer)에서 규정된 프로토콜 통신이 이루어진다. 이를 기반으로 본 연구는 C# .NET 환경에서 SharpPcap을 활용하여 실시간으로 패킷 캡쳐 및 계층별 헤더정보를 분석하고, 대화식으로 제어할 수 있도록 한다.

우선 사용자가 정의한 네트워크 환경에서 송/수신되는 패킷 정보가 정상적으로 캡쳐되는지 여부를 SharpPcap 라이브러리를 활용하여 확인한다. 그림 2는 이를 나타낸 것으로 대화형 구조를 제외한 패킷 캡쳐만을 콘솔 프로젝트를 통해 확인한 것이다. 하지만 콘솔 기반으로 구현한 프로젝트 결과는 기존의 연구들과 마찬가지로 사용자가 단방향으로 정보를 모니터링하는데 국한되어 직접적으로 컨트롤을 할 수 없어 패킷들을 분석하는데 어려운 구조를 갖고 있다. 따라서 본 연구는 사용자가 대화식 제어를 함으로써 효과적으로 결과를 확인할 수 있도록 한다.

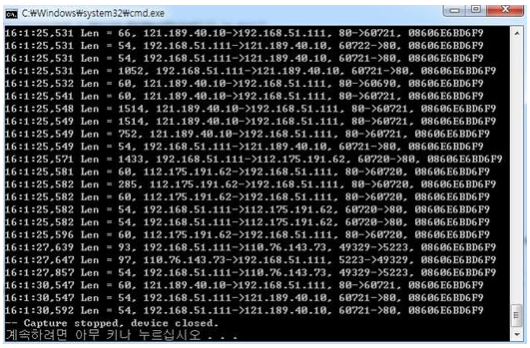

그림 2. 콘솔 기반의 캡쳐된 패킷 정보 결과

본 연구에서 SharpPcap을 이용하여 사용자가 직관적인 구조에서 시스템을 제어 할 수 있도록 C# .NET환경에서 송/수신되는 패킷 정보들을 캡쳐, 분석하는 기능으로 구성된 패킷 분석기를 구현한다. 대화식 구조의 핵심 기능은 다음과 같다.

(1) 네트워크 어댑터의 목록 검색

일반적으로 SharpPcap 기반 응용 프로그램이 수행하는 첫 단계로 연결된 네트워크 어댑터의 목록을 검색해야 한다. SharpPcap에서 제공하는 CaptureDeviceList함수를 통해 컴퓨터에 연결된 모든 디바이스 목록을 자동 검색한다. 그림 3은 이를 나타낸 것으로 네트워크 어댑터의 목록을 검색한 결과다.

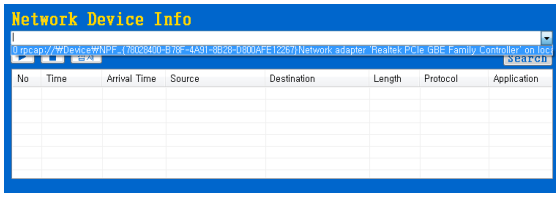

그림 3. 네트워크 어댑터의 목록을 검색한 결과 화면

(2) 실시간 패킷 캡쳐

컴퓨터의 네트워크 어댑터의 목록을 획득하면, 검색된 내용 중 연결하고자 하는 네트워크 디바이스 정보를 선택하여 해당 PC와 상대방 PC간의 오고가는 패킷을 실시간으로 캡쳐한다. 패킷의 정보로는 디바이스 시간, 패킷 도달시간, 송/수신지의 IP주소, 패킷크기, 전송계층에서의 포토번호에 따라 규정된 응용계층 프로토콜 타입이 출력된다. 그림 4는 실시간으로 패킷을 캡쳐한 결과다. 이는 모니터링 뿐 아니라 악성 스크립트가 삽입되거나 불명확한 IP를 갖는 등의 의심 패킷만을 사용자가 대화식 제어를 통해 분류 및 관리할 수 있으며, 이를 통해 유사 패킷이 접근할 경우 이에 대한 대처를 할 수 있는 기능을 제공한다.

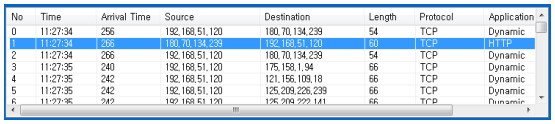

그림 4. 실시간 패킷 캡쳐 결과 화면

(3) 패킷의 계층별 헤더 정보 출력

실시간으로 캡쳐된 패킷 중 한 프레임을 선택하면 이더넷 계층(Ethernet)의 Source MAC Address, Destination MAC Address, IP계층의 Version, Source Address와 Destination Address, TTL(Time to Live), Header length, Total length 등의 헤더 정보, TCP계층의 Source port, Destination port, Acknowledgment number, Checksum, Sequence number, Window size, Urgent pointer 등의 계층별 자세한 헤더 정보와 Hex 정보로 출력한다. 그림 5는 실시간으로 패킷을 캡쳐한 정보 중 한 프레임 선택해서 계층별의 헤더정보와 HEX 정보로 출력한 결과다. 사용자가 패킷 정보를 Source, Destination 주소 또는 프로토콜 순으로 선택 정렬하여 볼 수 있도록 하여 패킷의 패턴 및 분석을 용이하도록 한다.

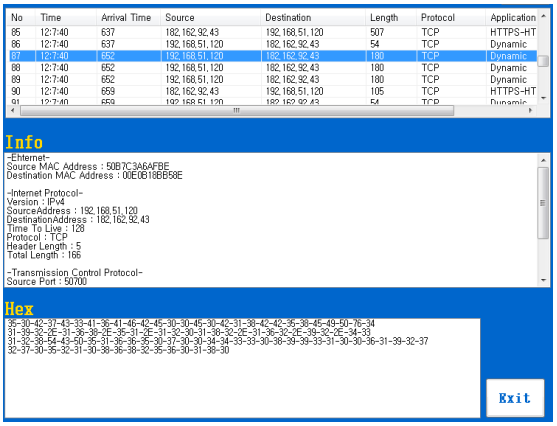

그림 5. 계층별 헤더 정보와 Hex정보 결과 화면

(4) 패킷 정보 저장

(2)의 실시간 패킷 캡쳐 과정에서 사용자가 선택한 패킷 정보를 별도의 텍스트 파일로 보관할 수 있도록 한다. 이는 선택한 패킷의 세부 정보를 캡쳐된 날짜 및 시간별로 관리할 수 있도록 할 뿐만 아니라 유사 패킷들만을 모아 해당 패킷이 캡쳐된 시간 기록을 확인할 수 있는 기능도 제공한다. 그림 6은 원하는 패킷 정보를 텍스트 파일로 저장한 결과이다.

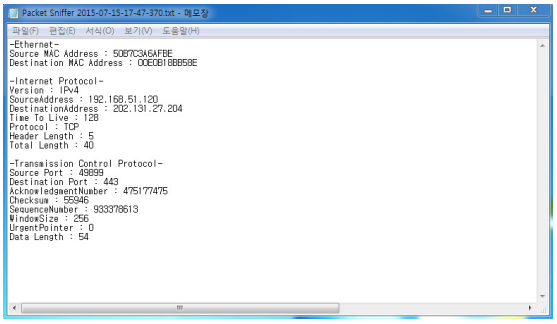

그림 6. 패킷 정보를 텍스트 파일로 저장한 결과 화면

Ⅳ. 결 론

본 논문에서는 C# .NET 환경에서 SharpPcap 라이브러리를 이용하여 네트워크 어댑터의 정보를 받아 실시간으로 패킷 캡쳐 및 상세한 계층별 헤더정보와 HEX 정보를 분석하고 별도의 이미지화하여 보관할 수 있도록 기능을 구현하였다. 또

한 사용자가 직관적인 구조에서 네트워크 오류 등에 대한 조기 탐지를 효율적으로 관리있는 대화형 패킷 분석을 구현하였다. 그러나 패킷 분석기가 TCP 기반으로만 구현 단계에 있으므로 아직 개선의 여지가 많다.

향후 연구 계획으로 비연결형 전송 서비스를 제공하고 상위 어플이케이션에서의 DHCP, BOOTP, RTP, SIP, DNS, TFTP 등이 포함한 UDP 기반의 분석 기능을 추가할 것이다. 또한 네트워크에서 각 프로토콜 계층의 트래픽 용량, 처리량 등 통계적으로 나타낼 수 있는 시각화된 그래프 기능과 네트워크 라인을 통해서 흐르는 패킷을 사용자가 이해하기 쉽게 변환해주는 프로토콜 정밀 분석 기능 등 다양한 기능들을 메뉴로 추가하여 완성된 시스템을 구현할 계획이다.

참고문헌

[1] 정성모, 송재구, 김석수, 박길철, “패킷 스니핑을 활용한 효율적인 모니터링 시스템에 관한 연구,” 2009 한국정보기술학회하계학술대회논문집, pp.587-590, 2009.

[2] 이정훈, 김희철, 고정국, “네트워크 상태 모니터링용 패킷 분석기의 구현,” 2004년 한국멀티미디어학회추계학술발표대회논문집, pp. 757-760, 2004.

[3] 유재헌, 이근형, 김진모, “WinPcap을 활용한 GUI기반 패킷 분석기의 설계”, 2015 한국컴퓨터종합학술대회논문집, pp.2042-2044, 2015.

[4] 전준상, 정연서, 소우영, “패킷 스니핑과 IP 스푸핑을 이용한 TCP/UDP 패킷 생성기의 설계,” 제32회 한국정보과학회 추계학술발표회 논문집, 제32권, 2호, pp.649-651, 2005.

[5] 이성옥, 주강, 정회경, “LibPcap를 이용한 Cacti기반 네트워크 트래픽 모니터링 시스템,” 한국정보통신학회논문지, 제16권, 8호, pp. 1613 -1618, 2012.

[6] http://www.codeproject.com/Articles/12458/SharpPcap-A-Packet-Capture-Framework-for-NET