패킷 스니핑과 IP 스푸핑을 이용한 TCP/UDP 패킷 생성기의 설계

전준상0* 정연서** 소우영*
*한남대학교 컴퓨터공학과
**한국전자통신연구원
*{yeerock0, wsoh}@neuro.hannam.ac.kr
**jys847@etri.re.kr

Design of Packet Generator for TCP/UDP Protocols Using Packet Sniffing and IP Spoofing

Junsang Jeon0*, Younseo Jeong**, Wooyoung Soh*
*Dept of Computer Engineering, Hannam University
**Electronics and Telecommunications Research Institute

요 약

네트워크 제품을 개발 하거나 제품의 성능을 시험할 경우 다양한 패킷 생성기나 장비를 이용하여 패킷을 생성한다. 그러나 이러한 패킷 생성기들은 TCP 세션연결 없이 패킷을 생성 전송하여 수신측에서 잘못된 패킷으로 인식하는 문제나 TCP 덤프 데이터를 구하기 힘든 문제, 그리고 하드웨어 장비의 경우 가격이 상당히 고가인 문제가 있다. 이러한 문제점을 해결하고자 본 논문에서는 Ip Spoofing기술과 Sniffing기술을 이용하여 TCP와 UDP 프로토콜 패킷을 생성할 수 있는 패킷 생성기를 제안한다.

1. 서 론

최근 네트워크 인프라의 발달로 대부분의 정보시스템들이 네트워크를 이용하여 사용되어지고 있다. 네트워크를 이용한 정보시스템은 언제 어디서나 정보시스템에 접근 할 수 있다는 장점이 있으나, 네트워크에 노출되어 있다는 단점이 존재한다. 또한 정보시스템들을 개발할 때 여러 가지 경우에 대한 테스트를 진행하지 않으면, 제품이 출시된 후 사용자에게 막대한 손실을 줄 수도 있다. 이러한 문제점들을 해결하기 위해 네트워크를 이용하는 제품들은 가상의 패킷을 생성하여 해당 시스템에 전송해 봄으로써, 추후에 발생할 문제점들을 줄이려 노력하고 있다. 그러나 이러한 테스트를 진행하기 위해서 필요한 패킷 생성기나 장비들은 TCP패킷을 인식하지 못하거나, TCP 덤프데이터를 구하기 힘든 경우, 그리고 가격이 비싸기 때문에 사용하기 어려운 문제점들이 있다.

본 논문에서는 이러한 문제점을 해결하기 위해 패킷 스니핑과 IP 스푸핑 기술을 이용하여 다중으로 TCP 세션연결을 할 수 있고, 다양한 패킷을 생성할 수 있는 패킷 생성기를 설계하여 제안한다.

본 논문의 2장에서는 설계된 패킷 생성기에 사용되어지는 기술들을 조사하고, 3장에서는 패킷 생성기의 설계를 제안하고, 4장에서 결론 및 향후연구과제로 끝을 맺는다.

2. 관련연구

2.1 TCP 프로토콜

TCP 프로토콜은 연결 지향(connection oriented) 프로토콜(호스트끼리 통신을 하기 위해서는 우선 서로 연결해 놓아야 통신이 가능한 프로토콜)이며, 3웨이 핸드쉐이크를 통해 연결이 이루어진다. 먼저 클라이언트는 서버의 응답을 받은 경우 연결이 이루어진 것으로, 서버는 자신의 응답신호에 대한 클라이언트의 응답을 받은 경우 연결이 이루어진 것으로 간주한다. 간혹 서버의 응답신호에 대한 클라이언트의 응답신호가 서버에 전달되지 않은 경우가 있는데 이런 경우 서버는 잠시 동안 불안정한 상태로 남게 되며 정상적인 작동을 하지 못할 수도 있게 된다.

그림 1.은 3웨이 핸드쉐이크 방식을 도식화 한 것이다.

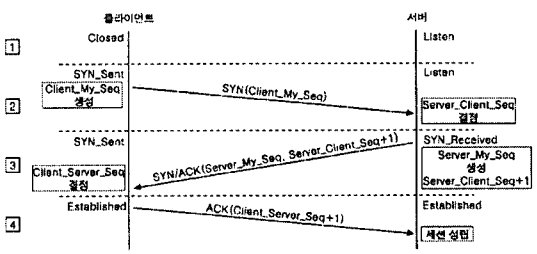

그림 1. 3웨이 핸드쉐이크

이와 같은 과정을 통해 TCP프로토콜은 연결이 이루어지게 된다.

2.2 패킷 스니핑

스니퍼는 컴퓨터 네트워크상에 흘러 다니는 트래픽을 엿듣는 도청장치라고 말할 수 있다. 그리고 스니핑(Sniffing)이란 이러한 스니퍼를 이용하여 네트워크상의 데이터를 도청하는 행위를 말한다.

스니핑은 LAN 상에서 개별 호스트를 구별하기 위한 방법으로 이더넷 인터페이스는 MAC(Media Access Control) 주소를 갖게 되며, 모든 이더넷 인터페이스의 MAC 주소는 서로 다른 값을 갖는다. 따라서 로컬 네트워크상에서 각 각의 호스트는 유일하게 구별될 수 있다. 그림 2.는 이더넷(ethernet) 프레임의 포맷을 나타낸다.

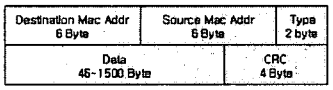

그림 2. 이더넷 프레임 포맷

이더넷 포맷은 type에 따라 그림 3.과 같은 3가지로 구성된다.

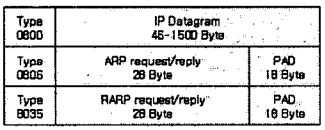

그림 3. 이더넷 포맷의 3가지 타입

이더넷은 로컬 네트워크내의 모든 호스트가 같은 선(wire)을 공유하도록 되어 있다. 따라서 같은 네트워크내의 컴퓨터는 다른 컴퓨터가 통신하는 모든 트래픽을 볼 수 있다. 하지만 이더넷을 지나는 모든 트래픽을 받아들이면 관계없는 트래픽까지 처리해야 하므로 효율적이지 못하고 네트워크의 성능도 저하될 수 있다. 그래서 이더넷 인터페이스(LAN 카드)는 자신의 MAC address를 갖지 않는 트래픽을 무시하는 필터링 기능을 가지고 있다. 이 필터링 기능은 자신의 MAC address를 가진 트래픽만을 보도록 한다. 또한 이더넷 인터페이스에서 모든 트래픽을 볼 수 있도록 하는 기능인 프로미시우스 모드(promiscuous mode)로 설정하여 로컬 네트워크를 지나는 모든 트래픽을 도청할 수 있게 된다[2][3][4].

2.3 IP 스푸핑

IP 스푸핑(Spoofing)이란 IP속이기란 의미이다. 즉, 타겟호스트와 신뢰관계를 맺고 있는 다른 호스트로 IP를 속여서 들어가는 걸 의미한다. 미 국방성의 TCP/IP 프로토콜 표준은 1979년 인터넷을 구현하기 위해서 디자인 되었다. 가장 많이 쓰이는 TCP/IP는 4.2BSD 시스템에서 구현된 것으로 Bell Lab과 미국방성 네트웍에서 사용되었다. 4.2BSD 유닉스 TCP/IP 프로그램은 매우 유동적이며 사용하기 편리하지만 보안측면에서는 많은 약점을 가지고 있다. 이 약점의 하나를 공격하는 IP 스푸핑 Attack은 1985년 Morris에 의하여 아이디어가 처음 지적되었고 실제로 1995년도에 사용되었다.

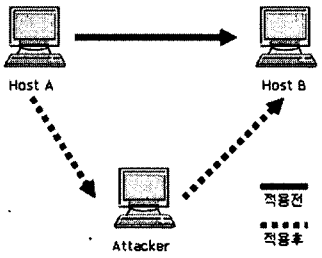

그림 4. 스푸핑 적용 효과

그림 4.처럼 스푸핑은 LAN 상에서 송신부의 패킷을 송신과 관련 없는 다른 호스트에게 가지 않도록 하는 스위칭 기능을 마비시키거나 속여서 자기 컴퓨터에게 그 패킷이 오도록 처리하는 것을 말한다. 이 경우 송신부에서 내 컴퓨터로 오는 패킷을 다시 수신부로 전송해야 하는데 이를 릴레이(Relay)라 한다. 릴레이를 하지 않으면 송신부와 수신부 사이에 네트워크가 마비된 것처럼 되어 버리기 때문에 반드시 릴레이를 해 주어야 한다. 그리고 릴레이를 할 경우 내 컴퓨터에서 그 패킷을 변조할 수도 있는데, 이는 TCP나 UDP 계층에서 자체적인 프로토콜의 인증 과정의 절차로 인해 수신부에서 패킷을 포기(drop)한다[5][6][7].

3. 패킷 생성기 설계

3.1 전체 시스템 구성

본 논문에서 제시하는 패킷 생성기는 스노트 룰을 기본으로 하여 패킷에 대한 정보를 수집하고, 이를 이용하여 패킷을 생성하여 해당 시스템에 전송하게 된다. 그리고 전송된 결과를 수집하여 사용자에게 전송결과를 보여준다.

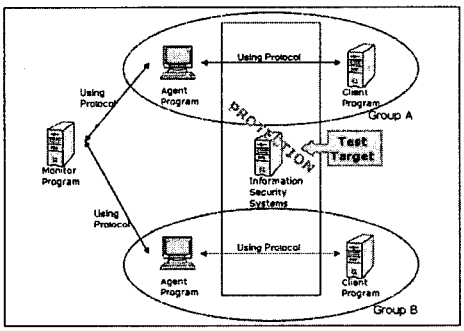

그림 5. 패킷 생성기의 전체 구성도

본 패킷생성기의 구성을 살펴보면, 모니터 프로그램에서 패킷에 대한 정보를 선택하여 에이전트 프로그램으로 명령을 하달한다. 명령을 받은 에이전트 프로그램은 UDP인 경우 패킷을 생성하여 바로 전송하게 되고, TCP인 경우 3웨이 핸드쉐이킹을 통해 TCP연결을 수행한 후 패킷을 전송하게 된다. 클라이언트 프로그램은 로그기록을 살펴보다가, 패킷에 대한 정보를 로그에 남기고 이를 에이전트 프로그램을 통해 모니터 프로그램으로 전송한다. 모니터 프로그램은 전송된 결과를 수집하여 해당 결

과를 출력한다.

3.2 모니터 프로그램

모니터 프로그램은 사용자가 명령을 내리고, 결과를 볼 수 있는 콘솔로 사용된다. 모니터 프로그램은 크게 전송할 패킷의 시나리오를 작성하여 에이전트에 전송하는 시나리오 모듈과 클라이언트로부터 오는 전송결과를 수집하여 분석, 결과를 출력하는 전송결과 출력 모듈로 나눌 수 있다.

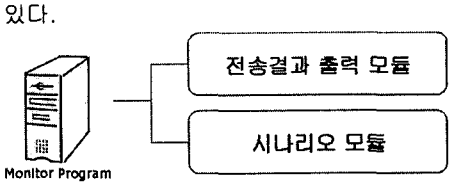

그림 6. 모니터 프로그램

3.3 에이전트 프로그램

에이전트 프로그램은 작성된 시나리오를 바탕으로 공격에 대한 패킷을 생성하여 해당하는 클라이언트 프로그램으로 전송하는 역할을 담당하는 부분이다.

최근의 네트워크에는 다양한 소스에서 전송되어 지는 패킷들이 있으므로, 이를 위해 하나의 에이전트 프로그램이 여러 개의 IP주소를 가지고 있는 것처럼 보이기 위해 패킷을 스니핑하는 모듈이 추가되어 있고, TCP프로토콜을 이용하는 공격을 위해 스니핑 된 정보를 이용한 IP 스푸핑 기술로 3웨이 핸드쉐이킹을 하는 모듈도 추가되어 있다.

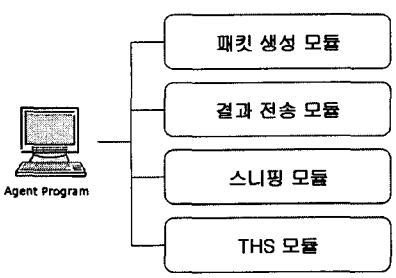

그림 7. 에이전트 프로그램

3.4 클라이언트 프로그램

클라이언트 프로그램은 타겟 시스템에 설치하는 프로그램이다. 이를 이용하여 에이전트 프로그램에서 전송하는 패킷에 대한 수신여부를 파악할 수 있다.

먼저 클라이언트 프로그램은 자신에게 전송되어지는 패킷에 대한 전송결과를 수집한다. 또한 로그를 남겨 전송 여부를 수집한다. 이렇게 수집된 결과들은 에이전트 프로그램에게 전송되어 지며, 전송되어진 결과는 에이전트 프로그램이 수집하여 모니터 프로그램에게 전송하여 출력되어진다.

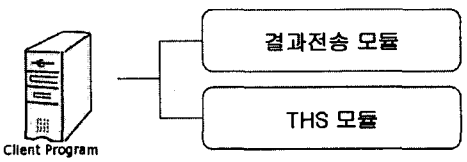

그림 8. 클라이언트 프로그램

4. 결론 및 향후연구과제

네트워크를 사용하는 프로그램들은 일정한 프로토콜에 따라 통신을 수행한다. 일반적으로 TCP/IP 프로토콜이 사용되며, TCP/IP 통신은 UDP와 TCP로 나뉠수 있다. UDP의 경우 비연결지향 방식이기 때문에 별도의 연결과정이 없어 패킷을 생성하여 전송하는데 문제가 없지만, TCP의 경우 연결지향 방식이기 때문에 3웨이 핸드웨이킹이란 연결기법이 필요하다.

본 논문에서는 UDP와 TCP 통신의 두 경우 모두 만족시키기 위하여, 패킷스니핑과 IP 스푸핑 기술을 사용하여 TCP 연결을 맺을 수 있는 패킷 생성기의 설계를 제안하였다. 이를 이용하면, 좀 더 정확한 패킷을 생성하여 타겟 시스템에 전송할 수 있으며, 추후 설계를 바탕으로 개발과정을 거치면서 좀 더 완성도 높은 패킷 생성기의 개발이 필요하다.

참고문헌

[1] 최용락, 소우영, 이재광, 이임영, "컴퓨터 통신보안 3판", 그린, 2005.

[2] Ryan Spangler, "Packet Sniffing on Layer 2 Switched Local Area Networks", Packetwatch Research, 2003.

[3] Mikro Tik, "Packet Sniffer", Mikro Tikls SIA, 2004.

[4] Michael J Jipping, Andrew Kalafut, "Investigating Wired and Wireless Networks Using a Java-based Programmable Sniffer", ITiCSE'04, 2004.

[5] Anat Bremler-Barr, Hanoch Levy, "Spoofing Prevention Method", IEEE, 2005.

[6] Josha Bronson, "Protecting Your Network From ARP Spoofing-Based Attacks", Foundstone, 2004.

[7] Sean Whalen, "An Introduction to ARP Spoofing", 2001.