제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

인터넷 웜 트래픽 분석을 위한 웜 생성도구 설계 및 구현

최 병 철*, 최 양 서*, 서 동 일*
* 한국전자통신연구원 정보보호연구단 네트워크보안그룹

요 약

인터넷 웜은 하루에도 수많은 변종을 만들어내고 있어서, 바이러스 백신에 의존한 치료만으로는 한계가 있다. 인터넷 웜의 전염 자체를 막고, 이를 분석하기 위해서는 인터넷 웜이 자신의 복제를 위해 사용하는 방법과 같은 환경이 필요하다. 인터넷 웜 트래픽 생성 시스템은 수많은 인터넷 웜이 자신을 스스로 복제하기 위한 유사한 방법으로 네트워크상에 트래픽을 생성한다. 본 연구는 인터넷 웜의 자기 복제 과정을 분석할 수 있도록 하여, 인터넷 웜의 전파 과정을 원천적으로 막을 수 있도록 설계 및 구현하는 것이 본 연구의 목표이다.

Design and Implementation of Internet Worm Traffic Generation System

Byeong Cheol Choi, Yang Seo Choi, Dong Il Seo*

ABSTRACT

The Internet worm is changed rapidly and virus vaccine can not defense the whole Internet worm. To prevent them form spreading into network and analysis specifications, we design and implement the Internet Worm Traffic Generator. In this research, we offer the real worm propagation environment through protocol and scenario specification.

1. 서 론

인터넷 사용자의 급증으로, 이제는 인터넷 없이는 단 하루도 생활이 힘든 시대로 접어들게 되었다. 2003년 1월 25일, 국내 인터넷 망이 일시 정지되었던 단 하루 동안, 기업들의 엄청난 금전적 손실은 물론이고, 수많은 네티즌들이 인터넷이 되지 않는 환경에서 많은 불편을 겪었다.

인터넷 웜이 인터넷 전체를 위협할 수 있는 존재임은 이미 증명된바 있다. CodeRed 웜의 경우 국내 행정망을 마비시키는 결과를 초래했으며 Slammer 웜은 국내 인터넷 망을 정지시키는 초유의 사태를 유발했었다. 이러한 인터넷 웜은 자신 스스로를 복제하는 과정에서 상당수의 네

트워크 트래픽을 유발하며 전체 시스템에 영향을 미친다. 인터넷 웜은 공격 당한 시스템뿐 아니라, 주변의 시스템까지 함께 감염시켜, 네트워크 전체에 영향을 미친다는 것을 알 수 있으며, 이 자가복제 과정에서 네트워크 트래픽이 엄청나게 증가한다.[1-3]

인터넷 웜은 하루에도 수많은 변종을 만들어 내고 있어서, 바이러스 백신에 의존한 치료만으로는 한계가 있다. 인터넷 웜의 전염 자체를 막을 수 있어야 하므로, 이를 분석하기 위해서는 인터넷 웜이 자신의 복제를 위해 사용하는 방법과 같은 환경이 필요하다. 인터넷 웜 트래픽 생성 시스템은 수많은 인터넷 웜들이 자신을 스스로 복제하기 위한 방법으로 사용하는 것과 같은 방법으로 네트워크상에 트래픽을 생성한다. 이들 인터넷 웜들의 자기 복제 과정을 분석할 수 있도록 하여, 인터넷 웜의 전파 과정을 원천적으로 막을 수 있도록 돕는 것이 이 연구의 목표이다.

2. 설계 및 구현

인터넷 웜 트래픽 생성 시스템은 크게 정책 서버 프로그램과 Agent 프로그램으로 구성된다. 정책 서버 프로그램은 각 Agent 프로그램의 활동 상황 모니터링 과 기본 적인 활동 정책 등 배포 하는 기능을 한다.

Agent 프로그램은 실제 PC에서 인터넷 웜처럼 동작하는 프로그램으로 정책에 따라 활동한다. 이 프로그램은 취약성을 가진 취약점 모듈과 실제 공격과 감염을 위한 패킷을 생성하는 트래픽 패킷 생성 모듈로 구성된다.

취약점 모듈은 인터넷 웜에 감염이 가능한 취약성을 가지는 취약점 프로그램으로 실험용 네트워크에서 취약성을 가지는 것으로 간주되는 호스트에 설치하여 실험용 인터넷 웜의 확산을 방치하는 기능을 수행한다. 트래픽 패킷 생성 모듈은 인터넷 웜 클라이언트 모듈은 취약서버의 보안결함을 이용하여 실제 감염 가능한 인터넷 웜과 임의 조작된 패킷의 생성 및 트래픽을 유발하는 클라이언트로 구성되며 인터넷 웜은 단순히 자가 증식을 수행하며 트래픽을 유발하는 클라이언트는 웜 감염 시 발생할 수 있는 네트워크 트래픽을 생성한다.

인터넷 웜 트래픽 생성 시스템은 사용자 혹은 관리자가 미리 정해 놓은 정책을 기본으로 하여 인터넷 웜의 확산을 재연한다. 이 때 사용 되는 정책은 각 클라이언트 Agent 와 정책 관리 서버에서 설정 및 변경이 가능하다. 정책 관리 서버는 정책을 설정 하는 기능 외에도 각 클라이언트 Agent 프로그램들의 상태 즉, 실행 여부 및 동작 여부 등을 모니터링 할 수 있고 클라이언트 Agent 프로그램의 종료, 실행 중지 및 재시작 등의 명령을 수행 할 수 있다. 정책 정보는 클라이언트 Agent 프로그램이 인터넷 웜과 비슷한 동작을 할 수 있도록 패킷을 조작하는 기본적인 설정을 가지고 있는 정보로서 IP 데이터, TCP 데이터, UDP 데이터, ICMP데이터 그리고 동작 시나리오로 이루어져 있다.

주요설계/구현화면구성

IP 데이터 설정하는 화면은 아래와 같다.

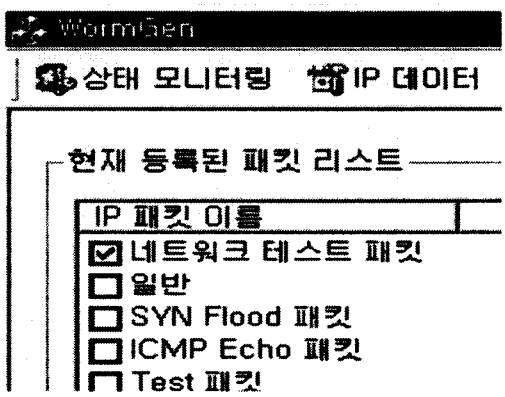

그림 1 IP 데이터 설정

IP 헤더 정보를 입력하여 특정한 IP 헤더 정

보를 등록 할 수 있고, 등록된 IP 헤더 정보에 대한 내용을 볼 수 있다. 데이터 내용 항목은 실제 만들어지는 IP 헤더 정보의 실제 데이터 값을 16진수로 표현한다.

TCP 데이터 설정 화면은 아래와 같다.

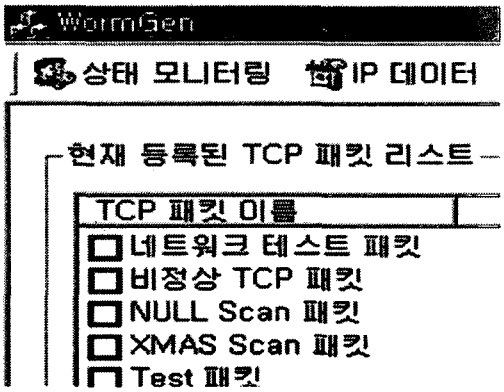

그림 2 TCP 데이터 설정

TCP헤더 정보를 직접 입력하여 TCP 헤더를 만들어 저장할 수 있다. 저장된 TCP 헤더 패킷들 중에서 특정 패킷을 선택하여 사용할 수 있다.

UDP 데이터 설정 화면은 아래와 같다.

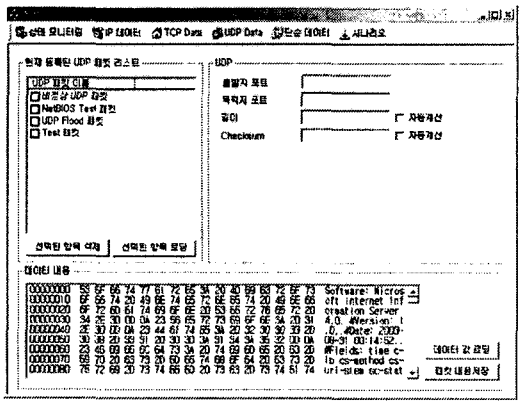

그림 3 UDP 데이터 설정

UDP 헤더 정보를 직접 입력하여 UDP 패킷을 만들 수 있다. 만들어진 UDP 패킷은 저장할 수 있도록 되어 있다. 저장된 UDP 헤더 정보를 선택하여 특정 패킷을 만드는데 사용 할 수 있다.

단순 데이터 설정하는 화면은 아래와 같다.

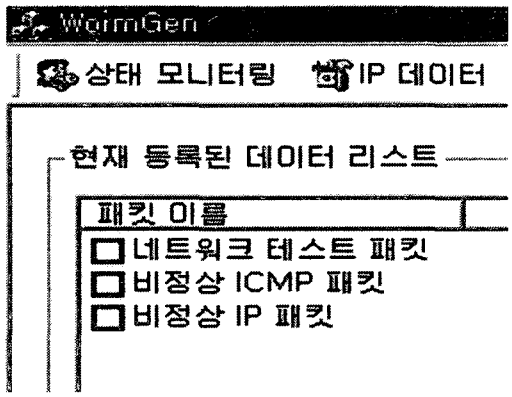

그림 4 단순 데이터 설정

패킷 내용을 외부에서 가져와서 저장 할 수 있도록 되어 있다. 비정상적인 ICMP 패킷이나 비정상 IP 패킷 등을 저장해 놓을 수 있다.

동작 시나리오를 설정하는 화면 아래와 같다.

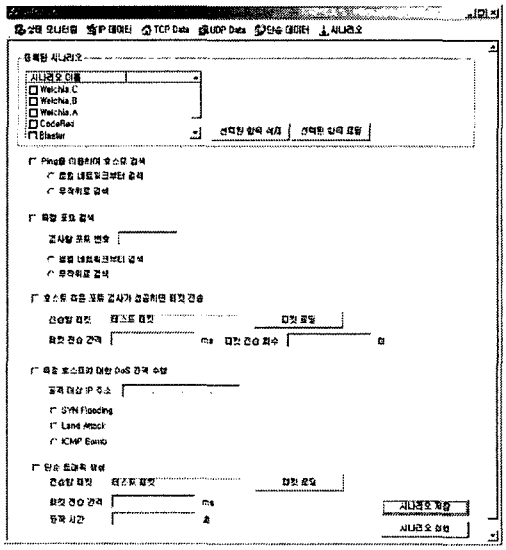

그림 5 웜 동작 시나리오 설정

특정 동작을 정의 한 시나리오를 등록하여 관리 할 수 있게 되어 있다. 실제 인터넷 웜 동작 할 수 있도록 특정 공격들을 정의 할 수 있다. 호스트 검색 방법을 같은 네트워크로 한정할 것이지 아니면 무작위로 만들어진 네트워크 주소로 할 것 인지를 선택 할 수 있다. 확산을 위해 사용할 포트 번호를 선택할 수 있고 이 포트를 검사하는 방식으로 같은 네트워크를 할 것 인지 아니면 무작위로 선택된 네트워크로 할 것인지를 선택 할 수 있다. 포트 검색에 성공한 경우 전송할 패킷 데이터를 선택할 수 있고 이 패킷을 어떤 간격으로 몇 번 전송 할 것인지 선택할 수 있다. DoS 공격 대상을 선택 할 수 있다. 그리고 DoS 공격에 사용되는 공격 방식을 선택할 수 있다. 제공되는DoS공격 방식 SYN Flooding, Land Attack, ICMP Bomb 등이 있다. 단순 트래픽 생성 목적의 웜을 재현하는 경우에는 단순 패킷 생성을 선택하여 발생 시킬 패킷을 선택 하고 패킷 전송하는 시간 간격과 패킷을 생성 시키는 시간을 설정 할 수 있다. 모든 설정 완성 되면 실제 인터넷 웜을 재현 할 수 있다.

3. 결론

인터넷 보급률은 계속해서 늘어나고 있지만, 인터넷 이용자들의 보안의식은 상대적으로 부족해진 것이 현실이다. 날이 갈수록 수많은 해킹 프로그램과 인터넷 웜이 만들어지고 있는데, 이들은 확산력이 매우 뛰어나고 변종들도 함께 만들어지면서 해킹 혹은 인터넷 웜으로부터 피해를 입는 사용자들이 늘고 있다.

인터넷 웜은 자신 스스로를 복제하는 과정에서 상당수의 네트워크 트래픽을 유발하며 전체 시스템에 영향을 미친다. 그러므로, 이러한 인터넷 웜의 동작 특성 및 전파 속도와 그에 따른 영향을 분석하여야 할 필요성이 있다. 그러기 위해서 동작 특성이 다른 각각의 인터넷 웜 Agent를 실험용 네트워크에 설치하여 변화를 관찰하고 네트워크의 변화를 모니터링 해볼 수 있는 시스템이 필요하다. 이를 위해 인터넷 웜 트래픽 생성 시스템이 설계되었다.

인터넷 웜 트래픽 생성 시스템의 특징은 아래와 같다.

- 정책에 따른 유해 패킷 생성
- 관리가 가능한 DoS 공격 및 인터넷 웜 Agent 동작
- 인터넷 웜 Agent의 동작을 관리하는 중앙 서버

본 연구의 결과로 만들어진 인터넷 웜 전파과정 등은 현재 나타나고 있는 인터넷 웜들을 모델로 개발되었으나, 인터넷 웜들은 보안 취약점과 해킹 방법들의 발전과 다양화에 편승하여 점점 다양해지고 발전하고 있기 때문에 현재와 다른 모습의 인터넷 웜은 나타날 것이다. 따라서 이러한 발전한 인터넷 웜 이동 경로를 추적하고 사용하는 보안 취약점을 분석하여 새로운 인터넷 웜 확산 경로를 추가하는 지속적인 시스템의 지속적으로 업그레이드가 필요하다.

참고문헌

[1] Zesheng Chen, Lixin Gao and Kevin Kwiat, "Modeling the spread of Active Worms," Proc. of IEEE INFOCOM, 2003 .

[2] Nicholas Weaver, "A Brief History of The worm," Nov. 1997,

[3] Jose Nazario, with Jeremy Anderson, Rick wash and Chris Connelly, "The Future of Internet Worms " . Crimelabs research, July 20, 2001.

최 병 철

1998년 : 서울시립대학교 제어계측공학과 공학사

2001년 : 서울시립대학교 전자전기공학부 공학석사

2001. 1.~현재 한국전자통신연구원 정보보호연구단 연구원

최 양 서

1996년 : 강원대학교 전자계산학과 이학사

2000년 : 서강대학교 컴퓨터공학과 공학석사

2000. 6.~현재 한국전자통신연구원 정보보호연구단 연구원

서 동 일

1989년 : 경북대학교 전자공학과 공학사

1994년 : 포항공과대학교 정보통신학과 공학석사

2002년 : 충북대학교 전자계산학과 (박사과정 수료)

1989. 1.~1992. 2. : 삼성전자종합연구소

1994. 3.~현재 한국전자통신연구원 정보보호연구단 네트워크보안구조연구팀장