네트워크 웜 전파 시뮬레이터의 설계 및 구현

구본현°, 이종성, 문종섭, 김동수*, 서정택*, 박응기*
고려대학교 정보보호대학원
국가보안기술연구소*
{koo191°, airforcy, jsmoon}@korea.ac.kr {iskim,seojt,ekpark}*@etri.re.kr

Network Worm Propagation Simulator Design and Implementation

Bonhyun Koo°, Jongsung Lee, Jongsub Moon, Dongsoo Kim*, Jungtaek Seo* and Eungki Park*
Graduate School of Information Security, Korea University
National Security Research Institute*

요 약

2003년 1.25 대란을 통해 우리나라와 같이 초고속 인터넷망의 인프라를 갖춘 국가는 웜에 의한 DDoS 공격 등에 취약하다는 것이 입증되었다. 이러한 취약성을 극복하기 위해서는 웜의 공격에 대해 웜 코드 자체에 대한 세부적인 분석과 전파 특성을 관찰하는 것이 중요하다. 하지만 웜의 전파 특성이나 취약점을 확인할 수 있는 방법으로는 소스코드 디어셈블러, 웜이 전파된 후 감염된 호스트들을 분석하는 방법이외에는 타당한 기법들이 제시되지 않고 있다. 웜 코드를 실제 네트워크 환경에서 테스트하기 위한 환경을 구축하기 위해서는 많은 시간과 비용이 소요되며, 제도나 법률에 반하는 비현실적인 방법이라 할 수 있다. 이에 본 논문에서는 심각한 피해를 유발할 수 있는 치명적인 웜들의 시뮬레이션을 통해 웜의 전파 과정에서 발생하는 트래픽을 분석, 확인할 수 있는 시뮬레이터를 제시하고자 한다.

1. 서 론

시뮬레이션은 실제 환경을 실제로 수행할 수 없을 때 실제 환경과 거의 동일한 환경을 프로그래밍 등을 통해 수행하는 과정을 말한다[1]. 이러한 시뮬레이션이 가능한 시뮬레이터의 구현을 통해 실제 웜의 전파 과정과 웜에 의한 트래픽 발생결과를 확인할 수 있는 기능을 제공할 수 있으며, 웜의 취약점 및 전파 과정을 방해하거나 억제시킬 수 있는 요소들의 확인을 통해 잠재적인 웜의 차단기법을 설계할 수 있다. 나아가 새로운 웜의 출현으로 인한 피해를 예방할 수 있다.

2. 기존 웜 시뮬레이션 기법들

웜의 동작을 시뮬레이션 할 수 있는 기존의 웜 시뮬레이터들은 크게 수치 보수를 이용한 시뮬레이션 기법과 네트워크 기반 시뮬레이션 기법으로 나눌 수 있다.

수치 보수를 이용한 시뮬레이션 기법들로는 SIR, SIS Model을 이용한 기법, RCS, AAWP Model 그리고 Kill Signal Model 등이 소개되었다.

네트워크 기반 시뮬레이션 기법은 크게 네트워크 이벤트 기반의 시뮬레이터 상에 웜 코드 모듈을 삽입하는 기법과 독립적인 웜 코드의 모델을 시뮬레이션하는 기법으로 나눌 수 있다. 전자를 대표하는 시뮬레이터는 SSFNet 및 NS-2가 있으며, Weaver, NWS, DDosVax와 같은 시뮬레이터들은 후자를 대표하는 모델로 제시되었다[2].

3. 웜 트래픽 테스트 베드 환경

실험환경을 위해 라우터로는 Cisco 2524, 2502 각 1대와 Windows를 사용하는 Pentium-IV PC 2대를 이용하였으며, 각 PC에는 가상 호스트를 2개씩 설정하여 총 6대의 호스트를 연결하여 네트워크를 구축했다.

그림 1은 실제 구축한 네트워크의 구성도이다. 외부 네트워크로부터 물리적인 경로 차단하여 실험에서 발생하는 패킷들은 라우터와 각 호스트들에 의해서만 생성됨에 따라 웜 트래픽에 대한 신뢰성을 확보하였다.

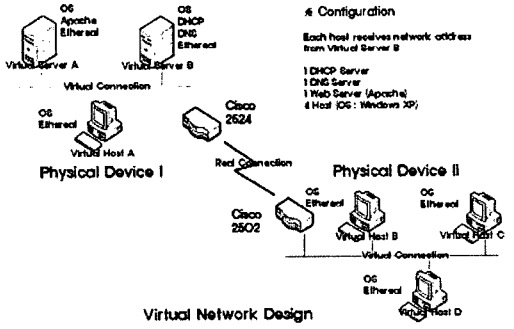

그림 1. 테스트 베드 구성 환경

라우터의 라우팅 알고리즘을 RIP(Routing Information

Protocol)로 설정하고 A, B class address를 사용할 경우 디폴트 서브넷 마스크가 설정(RIP는 CIDR을 지원하지 않음[3])되는 것을 방지하기 위해 C class 주소를 사용하였으며 세부내용은 표 1과 같다.

표 1. 가상 실험 네트워크 주소 구성도

장비	세부 내용	
Cisco 2502	Ethernet0	200.200.100.1/24
	Serial0	200.200.200.1/24
	Routing Algorithm	Routing Information Protocol
	RIP Network	200.200.100.0 200.200.150.0 200.200.200.0
	Serial clock rate	56000
Host A	VMware 1	IP : 200.200.100.2/24
	VMWare 2	IP : 200.200.100.3/24
Host B	VMWare 3	IP : 200.200.150.2/24
	VMWare 4	IP : 200.200.150.3/24

웜 트래픽은 라우터의 Cisco IOS(IGS-I-L Ver. 1.0)에서 지원하는 Debug 기능을 사용하였으며, 호스트에서는 Ethereal(Ver. 0.10.30)을 이용하여 각각 수집하였다. 수집된 트래픽 데이터는 Protocol Type, Source Address, Destination Address, Response Type 등 이다

4. 수집 Raw Packet의 XML 인코딩

본 논문에서 제시된 Worm Traffic Analysis Simulator (이하 WTAS)는 Microsoft .Net 환경에서 C# 언어를 이용하여 개발하였다. 시뮬레이션을 구현하기 위해 router에서 수집한 raw packet들을 XML로 Parsing하는 과정을 수행하였고, 그림 2는 Packet에 대한 XML 변환 과정이 수행되는 Layer의 구성 화면이다.

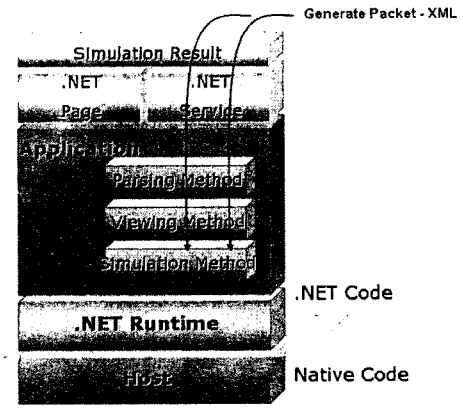

그림 2. XML Parsing 및 적용 Layer

5. 시뮬레이터의 설계 환경

WTAS의 시뮬레이션은 테스트 베드 환경에서 웜을 발생시켜 웜 트래픽을 생성하였고, 생성된 웜 트래픽의 raw packet들은 XML 인코딩을 과정을 통해 WTAS 엔진에 적용되는 과정을 거치게 된다. 웜의 발생 시간에 따른 각 Protocol 별 발생 비율과 랜덤 스캐닝에 의한 IP address의 각 옥텟 별 발생 분포 등 생성된 웜의 전체적인 트래픽을 시뮬레이터의 분석기를 통해 확인할 수 있도록 설계되었다.

6. 시뮬레이터 구성

WTAS에는 크게 3개의 analyzer interface를 제공한다. 먼저 시뮬레이션 환경에서 발생한 전체 트래픽에 대한 분석기와 감염시킬 호스트를 찾는 웜의 랜덤 스캐닝으로 생성된 IP address의 각 옥텟별 분포에 대한 분석기, 마지막으로 웜에 발생된 트래픽의 프로토콜에 대한 분석기로 구성되어 있다. WTAS를 이용해 시뮬레이션이 가능한 웜으로는 W32.HLLW.Lovgate, W32.Sasser.Worm, W32.Beagle.A@mm 3종류이다.

그림 3은 Sasser에 의해 발생한 인터넷 프로토콜에 대해 각 옥텟별로 분석이 가능한 분석윈도우 이다. 이를 통해 웜에서 사용되는 랜덤 스캐닝 기법을 확인할 수 있으며, 또한 이를 분석함으로써 웜의 패턴을 구축하고, 초기 탐지기법등을 확립할 수 있다.

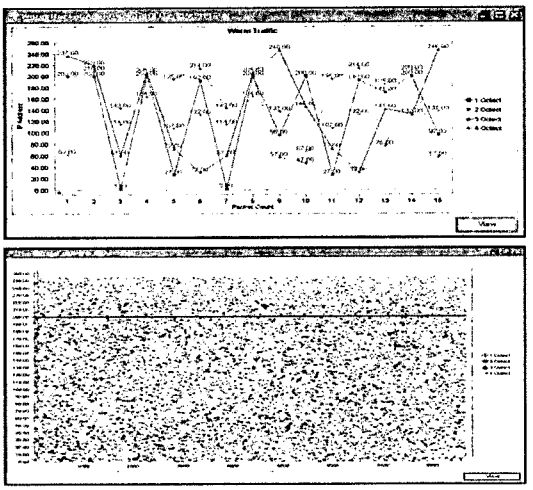

그림 3. Sasser에 의해 발생한 랜덤 스캐닝에 대한 IP address analyzer

시만텍의 웜 분석보고서[4]에 따르면 Sasser의 경우 Island Hopping 방식의 랜덤 스캔 기법을 사용하여, 웜의 스캐닝 트래픽 발생시 마지막 두 개의 옥텟만 랜덤하게 생성(A.B.x.x)하는 비율이 25%, 마지막 세

개의 옥텟을 랜덤하게 생성하는(A.x.x.x) 비율이 23%, 전체 옥텟을 랜덤하게 생성되어지는 비율이 52%의 전체 비율을 나타내며,127.0.0.1, 10.x.x.x, 172.16.x.x, 172.31.x.x, 192.168.x.x, 169.254.x.x등의 예약된 주소공간은 사용되지 않는다. 이러한 웜의 랜덤생성 트래픽의 비율 분포 및 사용되는 IP 주소공간은 실제로 그림 3에 소개된 Analyzer를 통해 시각적으로 확인이 가능하다.

그림4 는 웜에 의해 발생한 트래픽에 대해 프로토콜별로 분석 가능한 분석윈도우 이다. 이 Analyzer를 이용하여 웜에 의해 발생한 ARP,TCP,UDP,ICMP 등과 같은 프로토콜에 대해 분석을 할 수 있으며, 이를 통해 웜에서 발생하는 프로토콜이 어떠한 비율을 가지는지에 대해 시각적으로도 쉽게 확인이 가능하다.

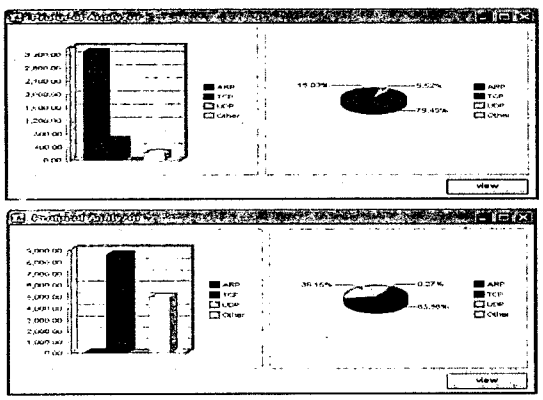

그림 4. 프로토콜 분석 윈도우 (Sasser 와 Lovgate)

7. 시뮬레이션 결과

WTAS 시뮬레이터의 시뮬레이션 결과는 6절에서 제시한 Analyzer들을 통해 웜의 발생 트래픽에 대한 흐름과 프로토콜별 분석과 IP의 옥텟별 분포 등을 확인할 수 있었다.

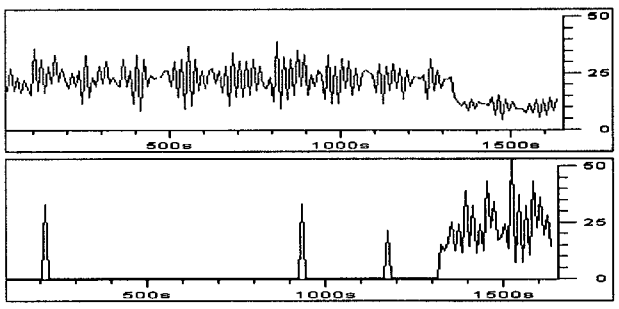

그림 5. Lovgate 웜의 발생 초기 ARP 트래픽량(상단)과 TCP 트래픽량(하단) 분석

그림 5는 Lovgate 웜의 초기 전파 시 발생하는 ARP 트래픽과 그 후 Random Scanning으로 인한 트래픽 발생시 생성되는 TCP 트래픽의 그래프이다. 그림5 에서 보여 지는 초기 ARP 트래픽의 증가량 역시 그림 4(상단) 에서 소개한 WATS의 프로토콜 Analyzer를 통해 시뮬레이션으로 직접 확인이 가능하다.

8. 결론

본 논문에서 제시한 웜 전파 시뮬레이터를 통해서, 실제 환경에서 발생하는 다양한 웜들의 전파가 진행되는 과정과 전파를 통해 발생되는 트래픽상의 프로토콜과 랜덤 스캐닝 IP의 옥텟별 분포 등을 분석할 수 있다. 이러한 분석기능을 통해 웜의 Early Detection 기능이나 Anomaly Detection 방식을 사용하는 기존의 IDS 혹은 IPS 등에 적용이 가능한 Signature 혹은 Pattern의 확장 구현이 가능할 것이라 본다. 웜의 전파 과정을 패치의 적용 유무와 Firewall, IPS 등의 영향력 등을 적용한 다양한 환경에서의 호스트의 감염률을 시뮬레이션 하는 기능에 대해서는 추후 연구를 통해 보완해야 할 것이다.

참 고 문 헌

[1] Wagner, D., et al "Experiences with Worm Propagation Simulations" ACM Workshop on Rapid Mal-code (WORM) 2003

[2] Harsha Talkad, "Survey of Worm Traffic Simulaors ", Course project for Security and Privacy in Computing Csci 8980-002 Fall 2003

[3] Cisco Guide site : http://www.cisco.com/en/US/products/hw/routers/ps233/products_installation_and_configuration_guide_chapter09186a008007e409.html

[4] Symantec security response site : http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html