인터넷 웜 전파 특성 파악을 위한 시뮬레이션 환경 연구

이민수,조재익,구본현,문종섭
고려 대학교 정보보호 대학원
{leesle,chojaeik,koo191,jsmoon}@korea.ac.kr

A study on the Simulation environment for analyzing internet worm propagation

MinSooLee, Jaeik Cho, Bonhyun Koo, Jongsub Moon
GSIS/CIST, Korea University

요 약

현재 인터넷 웜에 관한 관심과 연구가 활발해 지면서 인터넷 웜 전파 특성 시뮬레이션 방법에 관한 연구가 많이 진행 되고 있다. 하지만, 연구 되어온 기법들은 대부분 웜의 스캔기법과 같은 웜 자체에 전파 되는 알고리즘에 대해서만 고려한 시뮬레이션 환경을 제시 하였다. 웜의 특성 상 좀더 실제 네트워크 환경과 비슷한 환경을 제공 하려면, 웜의 전파 알고리즘 외에, 각 호스트들에 취약점 패치 유무, 타깃 호스트들의 Computing Power, 각 네트워크의 밴드위스 & 지연시간, 네트워크 별 보안 장비(방화벽, IPS)의 유무 등 여러 가지 웜 전파에 영향을 미치는 요소들이 존재한다. 따라서 본 연구에서는 먼저 웜의 전파에 영향을 미치는 요소를 특성에 따라 크게 4가지로 분류 해보고, 이를 효율적으로 시뮬레이션 환경에 적용 할 수 있는 방안을 제안한다.

1. 서 론

인터넷이라는 용어가 생활의 일부가 되어 버린 지금 많은 부분들이 빠르고 편리 해졌다는 것에 대해 반론을 제시 할 사람은 아무도 없을 것이다. 인터넷 많은 장점을 가지고 있으며, 또한 여러 가지 위협 요소를 가지고 있다.

웜은 위에서 언급 했던 위협 요소 중 가장 대표적인 사례라 볼 수 있다. 유비쿼터스 용어가 많이 사용 되고 홈 네트워크가 형성되어 사용 되고 있는 지금 웜에 대한 위협은 어느 때 보다 더 위험한 요소가 되었다. 또한, 최근 국가간의 분쟁이 있을 때마다 각 국의 해커들이 웜을 통하여 서로 사이버 전을 진행 하는 것도 확인 할 수가 있다. 이에 따라 웜 자체에 대한 연구는 물론 웜의 발생 시 대처 할 수 있는 여러 가지 기술들에 대해서도 관심을 가지고 연구를 해야 할 필요성이 대두 되고 있다. 이에 본 논문에서는 웜에 대한 연구의 기반 기술이 될 수 있는 시뮬레이션 환경에 대해 알아 보고자 한다. 이를 위해 현재 제시된 웜 시뮬레이션 환경의 한계점에 대해 알아보고, 이를 보완하기 위해서 필요한 방법에 대해서 논의 해보고자 한다.

기존의 시뮬레이션 환경에 대해서 2장에서 확인 해보고, 웜 시뮬레이션 환경 구축을 위한 웜의 분류 방법과 실제 환경과 유사한 환경을 위하여 현재 시뮬레이터에서 고려하지 않았던 시뮬레이션 환경에 대해서 3장에서 논의 하고, 이러한 환경을 시뮬레이션 환경에 적용 할 수 있는 방법에 대해서 4장에서 제시한다.

2. 관련 연구

웜 시뮬레이션 환경은 여러 가지 위험성에 의해서 실제 네트워크 환경에서 쉽게 제공 해 주지 못한다. 이에 많은 연구들이 제시한 웜에 대한 모델의 검증을 위해 많은 시뮬레이션 환경을 제시하고 이를 이용하여 검증 하고 있다.

기존의 네트워크 시뮬레이션을 위해 사용하였던 환경을 기반으로 웜 관련 모듈을 추가하여 검증 하는 방법과, 웜 자체를 위한 시뮬레이션 환경을 구성 하는 방법으로 크게 나눌 수 있다. 첫 번째 경우의 NS-2 시뮬레이터[1]를 대표적인 예로 들 수 있으며, 두 번째의 경우 Computer Engineering and Networks Laboratory(TIK)의 DDOS-VAX 프로젝트[2], Bruce Edigar 의 NWS 그리고,SSF-Net (Scalable Simulation Frameworks)를 예로 들 수 있다.

이처럼 웜의 실험을 위하여 여러 가지 다양한 방식의 시뮬레이션 환경에 대한 연구도 진행 중에 있다. 하지만 이러한 시뮬레이션 환경들은 대부분 웜의 전파 특성(scan 기법,전파 특성 등) 과 같은 각 실험에서 제시한 웜의 요소에 대해서만 지원을 해주기 때문에, 좀 더 실제 네트워크와 비슷한 환경을 제공하는 방향으로의 연구가 필요하다.

3.인터넷 웜 시뮬레이션 환경

웜의 가장 큰 특징은 스스로 네트워크를 이용하여 전파된다는 점이다. 따라서 웜의 전파 특성을 분석 한다는 것은 웜에 대한 연구에서 가장 중요한 부분이라 할 수 있다.

하지만 웜의 특성 상 실험을 위하여 실제 네트워크를 이용한다는 것은 거의 불가능 하며, 가능하더라도 극히 제한적인 분리된 작은 네트워크 환경 안에서만 가능 하겠다. 따라서 웜의 전파 특성을 연구를 위해서 시뮬레이션 환경은 필수적인 요소라 할 수 있다.

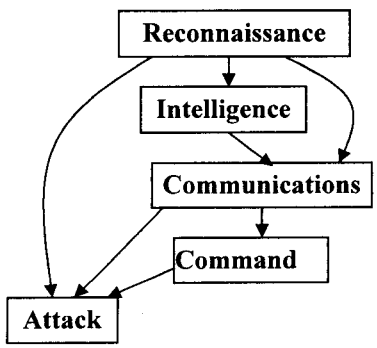
웜 시뮬레이션 환경 하에 웜의 전파 특성 분석 방법은 다음과 같은 장점을 얻을 수 있다..

- 전파 속도를 예측 가능
- 웜에 의한 피해 상황을 예측 가능.
- 웜 분석을 위한 reverse-engineer기법 보완.
- 네트워크 상에서 웜의 영향력 파악 가능.
- 웜의 진화방향 예상 가능.
- 웜 전파에 영향을 주는 요소 파악.

3.1 웜 구성 요소 분류

Nazario et al.은 웜을 다섯 가지 요소로 구분을 하였다.[3] 웜은 이 다섯 가지의 요소들 중 일부를 포함하거나 전체를 다 포함 할 수 있다.

- Reconnaissance
  웜이 전파 하기 위해 적합한 호스트를 찾는 요소
- Attack-Components
  실제 타켓 시스템을 공격 하기 위한 요소
- Communication-Components
  같은 종류의 웜에 감염된 호스트끼리 통신 할 수 있는 요소
- Command-Components
  감염 된 호스트 들에게 2차적인 행동을 수행 할 수 있도록 제공 해주는 요소
- Intelligence-Components
  웜의 전파 효율성을 위해 각 웜 노드에게 여러 가지 정보를 제공해 주는 요소



<그림 1. 웜 구성 요소 구성도>

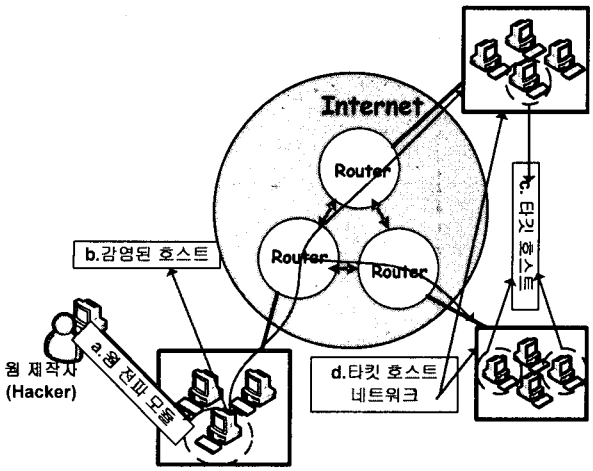
<그림 1>은 각 요소 별 실행 가능 한 순서의 연관성을 보여 주고 있다. 이처럼 각 요소들은 역할들이 유기적인 연관성을 기준으로 구분 할 수 있으며, 또한 시뮬레이션 환경을 구성 하는데 명확한 기준을 제공 할 수 있다는 점에서 매우 중요하다.

3.2 시뮬레이션 환경을 위한 웜 네트워크 요소 분류

3.1에서 제시한 웜 내부 구성 요소의 분류를 기반으로 웜 네트워크의 구성 요소를 시뮬레이션 환경에 적합한 요소로 분류하였다. 다음의 <표1> 은 웜 네트워크 구성 요소들을 시뮬레이션 환경을 기준으로 분류 하였고, 이에 따른 세부 요소 들에 대해 나열 하였다.

<표 1. 시뮬레이션 환경을 위한 웜 네트워크 요소 분류>

분류 이름	세부 내용 분류에 따른 요소
a. 웜 전파 모듈(자체)	자신을 네트워크를 통하여 전파 시키기 위한 모듈을 의미하며, 이 모듈의 여러 가지 특성에 따라 웜 전파 특성이 영향을 받는다
	* 웜 Reconnaissance 요소가 사용하는 프로토콜(TCP, UDP) * 웜 Attack 요소가 사용하는 취약점을 갖는 OS 종류 및 버전
b. 감염 된 호스트	전파 모듈과는 다른 개념으로 웜은 감염된 호스트의 리소스들을 기반으로 계속해서 전파 된다는 관점에서 감염 된 호스트의 자원을 의미하며 이는 웜의 전파특성에 영향을 미칠 수 있다.
	* 호스트의 성능(Computing Power) *사용중인 프로토콜 (PPP, ADSL, E-thernet)
c.취약점 가진 타깃 호스트	웜의 요소 중 Reconnaissance 요소 가 작동 시 타깃 호스트의 상태에 따라 다르게 반응이 일어 날 수 있다.
	* 취약점의 패치 유무(취약점에 대한 패치가 된 호스트 인지의 유무)
d.취약점 가진 타깃 호스트 소속 네트워크	타깃 호스트가 속한 네트워크의 자원 및 장비들의 상태에 따라 전파에 영향을 미친다
	* Network Bandwidth (타깃 호스트가 속한 네트워크의 성능 *네트워크 보안 장비의 유무(Firewall, IPS)



<그림 2. 시뮬레이션 환경 구성 요소 분류>

시뮬레이션 환경에 영향을 미치는 요소를 기준으로 분류한 모습을 그림 2에서는 보여 주고 있다.
각 요소들을 조금 더 세부적으로 하나씩 예를 들어 살펴보자

첫 번째로 웜 전파 모듈에서는 웜이 전파 되기 전에 타깃 호스트들에 대한 정보를 얻어 오는 과정에서 사용 되는 프로토콜이 무엇 인지에 따라 여러 가지 응답 시간이 달라진다. 가령 TCP는 UDP에 비해 연결 설정,flow control, congestion control을 한다. 또한 각 OS별로 UDP 패킷 사이즈의 제한이 각기 다르다.

두 번째로 감염된 호스트의 관점에서 새로운 타깃에 전파 시킬 때 호스트의 성능은 웜 전파에 영향을 줄 수 있으며, 또한 감염된 호스트의 프로토콜이 ADSL을 사용 한다면, uplink와 downlink의 속도의 차이 또한 웜 전파의 영향을 줄 수 있는 요소 중에 하나라고 볼 수 있다.

세 번째로 취약점을 가지는 호스트의 관점에서는 취약점에 대한 패치 상태의 유무가 영향을 미칠 수 있는 요소라고 볼 수 있다.

마지막으로 취약점을 가지는 호스트의 네트워크의 관점에서는 bandwidth가 웜 전파에 영향을 미칠 수 있으며, 네트워크 보안 장비의 유무, 설정의 유무 또한 큰 영향을 미칠 수 있다.

3.3 환경 요소의 적용 방법

앞서 언급 했던 것처럼 현재까지 연구 되었던 시뮬레이션 기법은 <표1>에 제시된 것 중 웜 전파 모듈만을 고려하였다. 이에 따라 실제 네트워크 상황을 정확히 표현 하지 못한다. 좀 더 실제 네트워크 환경과 유사한 환경을 제공하기 위하여 본 논문에서는 <표1>에서 시뮬레이션 결과에 영향을 줄 수 잇는 요소들을 기준으로 웜 네트워크 구성을 분류 하였다.

이러한 각 요소들을 시뮬레이션 환경에 적용 시키기 위해서 본 논문에서는 크게 두 가지 방법을 제시한다.

<표 2. 환경 요소 적용 방법>

제시 방법	세부 설명
구성 요소 별 value matrix작성	<표1>에 제시된 세부 요소들의 값을 각 특성을 기준으로 value matrix를 작성 하고 각 시뮬레이터 구성 시 각 네트워크에 특성에 따라 matrix를 활용 하여 시뮬레이션을 실행 한다.
통합 latency 값 정의	value matrix 복잡성을 보완하기 위하여 <표1>에서 제시된 특성들을 고려 하되 하나의 latency 가중치를 10단계로 생성을 하고, 이를 시뮬레이션 환경에 적용을 한다.

4. 결론 및 향후 연구 과제

본 논문에서는 실제 네트워크와 가까운 시뮬레이션 환경을 제공 하기 위해서 고려해야 할 사항 들에 대해서 웜 네트워크의 분류 방법을 통해 살펴 보고, 시뮬레이션의 정확성을 높이기 위하여 value matrix와 latency 가중치 방법을 제안 하였다. 본 논문에서 제안한 방법을 시뮬레이션 환경에 적절히 적용을 시키기 위한 이론적 연구가 추가로 필요하며, 많은 실험을 통하여 최적의 value matrix와 latency의 기준이 제시 되어야 한다. 또한 인터넷 웜의 구조 및 전파 특성에 대한 시뮬레이션 환경에 대한 연구도 계속해서 진행 되어야 한다.

참 고 문 헌

[1] ICSI, " The Network Simulator - ns-2" 2005 http://www.isi.edu/nsnam/ns/index.html

[2] Wagner, D., et al " Experiences with Worm Propagation Simulations" ACM Workshop on Rapid Malcode (WORM) 2003

[3] Nazario,J., et al., " The Future of Internet Worms," 2001 Blackhat Briefings, LasVegas, NV, July 2001.