인터넷 환경에 따른 인터넷 웜 확산 방식 연구

신 원*

A Study on the Spread of Internet Worms by Internet Environments

Shin, Weon*

요 약

최근 빠른 속도로 확산되는 Code Red Worm, Slammer Worm과 같은 인터넷 웜은 인터넷에서 주요한 위협이 되고 있다. 이러한 인터넷 웜을 막기 위해서는 웜의 확산 방식과 웜 확산에 영향을 끼치는 인터넷 환경을 이해하는 것이 필수적이다. 본 논문은 인터넷 환경에 따른 웜 확산의 정확한 모델링을 그 목표로 한다. 이를 위하여 다양한 실험을 통하여 주소 체계와 인터넷 속도에 따른 웜 확산의 양상을 분석한다.

ABSTRACT

Fast spreading Internet worms, such as Code Red and Slammer, have become one of the new major threats of the Internet recently. In order to defend against theses worms, it is essential to understand how Internet worms propagate and how different Internet factors affect worm spreading. In this paper, we intend to describe the spread of worms on Internet environments accurately. Therefore we model and analyze the spreading effects by various simulations considering Internet addressing and speed. The results lead to a better prediction of the worm spreading on current and future Internet environments.

키워드

Internet Worm, Worm Spreading

Ⅰ. 서 론

다양한 국가에서 널리 보급된 인터넷 기술은 수많은 사용자들이 일상생활에서 사용하고 있으며, 다양한 서비스들이 시간적, 공간적 제약을 극복하여 인터넷 상에서 제공되고 있다. 또한 유비쿼터스 환경이 도래함에 따라 누구나 언제 어디에서나 인터넷을 접속할 수 있는 휴대 인터넷과 방송, 인터넷, 통신을 융합하여 언제 어디서나 양질의 멀티미디어 서비스를 받을 수 있는 광대역 통합망인 BcN(Broadband convergence Network)도 새롭게 등장하고 있다. 그러나, 다양한 인터넷 기술과 어플리케이션이 등장함에 따른 역기능들도 함께 증가하고 있는데, 그 중 가장 많이 이루어지는 것이 서버 및 네트워크 구조 또는 서비스의 가용성에 엄청난 피해를 가져오는 인터넷 웜 공격이다.

일반적으로 인터넷 웜은 소프트웨어의 구현 버그, 설계 결함 등의 취약성을 이용하여 시스템의 권한을 획득하고 자기 자신을 복제하여 허가되지 않은 동작을 수행하는 악성 코드(Malicious Code)이다. 이 과정 중에 수행되는 코드와 발생되는 패킷은 시스템 및 네트워크 환경에 오버헤드를 초래할 뿐만 아니라 서비스 거부 공격을 수행한 것과 같이 정상적인 서비스가 불가능하도록 만

* 동명대학교 정보보호학과

접수일자 : 2007. 7. 30

든다. 따라서, 고성능 네트워크 환경에서 인터넷 웜의 확산은 단순한 악성 코드의 확산을 의미할 뿐만 아니라 네트워크 기반구조를 사용불능으로 만드는 분산 서비스 거부 공격의 의미를 가진다.

본 논문에서는 인터넷 웜 확산 모델링을 통하여 현재 인터넷 환경에서 각 요인에 따른 웜 확산과 그 영향을 분석하고자 한다. 먼저 2장에서는 적용가능한 관련 웜 확산 모델에 대하여 살펴보고, 3장에서는 인터넷 환경에서 웜 확산을 분석하여 실제 환경을 고려한 시뮬레이션을 수행한다. 4장에서는 실험 결과에 의한 웜 대응 방안을 살펴본 후 마지막 5장에서 결론을 맺는다.

Ⅱ. 인터넷 웜 확산 모델

2.1 웜 확산 모델과 개선

컴퓨터 바이러스가 특정 파일에 기생한 후 그 숙주 파일이 실행되는 순간 바이러스가 동작하는 기생형 악성 코드인데 반하여, 인터넷 웜은 독립적인 악성 코드로 일반 프로그램처럼 자신만으로도 실행이 가능하며 다양한 시스템 자원을 활용하여 정의된 동작을 수행한 후 네트워크를 통하여 자기 자신을 복제하여 전파한다. 최근 등장하는 인터넷 웜의 특징을 살펴보면 다음과 같다.

- 크기의 감소 : Nimda Worm이 60KB, Code Red Worm이 4KB, Slammer Worm이 404B로 그 크기도 작아지고 있음
- 스캐닝 속도의 증가 : 감염 대상을 신속하게 찾아 확산하는 속도를 증가시키기 위해 랜덤 스캐닝을 사용하고 있으며 갈수록 고속화되고 있음
- 비연결 방식을 이용한 무작위 배포 : TCP (Transmission Control Protocol) 패킷을 이용한 연결 전송 방식에서 UDP(User Datagram Protocol) 패킷을 통한 비연결 전송 방식을 사용
- 네트워크 자원의 고갈 : 시스템을 직접 공격하는 것은 물론 다량의 패킷을 발생하여 네트워크 대역폭을 고갈, 결국 DoS(Denial of Service) 또는 DDoS(Distributed DoS)의 효과를 유발

Cliff C. Zou 등[1]은 인터넷 웜의 스캐닝에 따른 성능을 분석하였는데, 일반적인 웜의 스캐닝 형태인 균등 스캐닝을 수행하는 RCS(Random Constant Spread) Worm의 동작에서 다음 식을 유도하여 인터넷 환경의 웜 확산을 설명하였다.

$$\frac{dI(t)}{dt}=\beta I(t)[N-I(t)],\ \ \beta=\frac{\eta}{\Omega} \qquad ①$$

여기서, β는 웜 확산율, η는 웜의 단위 시간 당 평균 스캐닝 수, Ω는 웜이 스캐닝할 수 있는 전체 호스트 주소 공간, N은 감염가능한 전체 호스트 수, $I(t)$는 시각 t에 감염된 호스트 수를 나타낸다. 특히, RCS Worm은 호스트 주소 공간을 균등하게 스캐닝하므로 웜 확산율 β는 고정값이다.

수식 ①에서 확산율 β가 고정된 상수값인데 반해 Two-factor Worm Model[2]에서는 네트워크 오버헤드와 인간의 대응을 함께 고려하여 웜 확산 속도 감소 정도를 반영하여 확산율 β를 시간에 따라 변화하는 함수 $\beta(t)$로 나타낸다.

$$\beta(t)=\beta_0(1-\frac{I(t)}{N})^{\phi} \qquad ②$$

여기서, β_0는 초기 확산율이고 ϕ는 감염 호스트 비율에 의해 변화하는 확산율을 반영하는 값이다. 수식 ①에서 β를 시간에 따라 변화하는 함수 $\beta(t)$로 두고, 수식 ②를 대입하면 다음과 같은 수식을 구성할 수 있다.

$$\frac{dI(t)}{dt}=\beta_0(1-\frac{I(t)}{N})^{\phi}I(t)[N-I(t)],\ \ \beta_0=\frac{\eta}{\Omega} \qquad ③$$

여기서, β_0는 수식 ②에서와 같이 초기 확산율이고 초기값은 수식 ①의 β와 같다. 즉, ϕ가 0이라면 확산율 $\beta=\beta_0$로 RCS Worm에 해당하며 수식 ①과 수식 ③은 동일한 수식이고, ϕ가 0이 아닌 경우에는 웜 확산 감소율을 적용한 개선된 확산 모델에 해당한다.

그림 1은 위 식들을 이용하여 2001년 7월 전세계 컴퓨터 359,000대를 감염시켰던 Code Red 웜의 확산을 그래프로 그린 것이다. 여기서, 감염 가능한 전체 수 $N=359{,}000$, 확산율 $\beta=358/2^{32}=8.34\times10^{-8}$이다. 그림 2는 CAIDA[3]에서 제공하는 Code Red 웜의 실제 측정치이다. 살펴본 바와 같이 상당히 유사하다는 것을 확인할 수 있다.

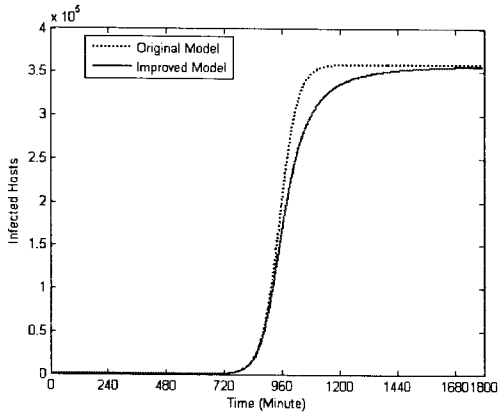

그림 1. 모델링에 의한 Code Red 웜 확산
Fig. 1 Code Red Worm spreading by modeling

위 결과를 살펴보면 모델링에 의한 웜 확산과 실제 측정값이 거의 비슷한 형태를 그리고 있으며, 특히 수식 ①을 적용한 Original Model보다 수식 ③을 적용한 Improved Model이 실제 측정값에 더 근접함을 확인할 수 있다.

2.2 인터넷 웜 확산율

만약 인터넷 웜이 특정 대역폭을 가진 네트워크 환경에서 확산되고 주소 공간 Ω가 고정되어 있다고 가정하면, 수식 ①에서 웜 확산율 β는 스캐닝 수 η에 전적으로 의존하게 된다. 또한, 웜이 스캐닝할 때 발생하는 단위 시간 당 패킷의 크기는 이론적으로 해당 네트워크의 대역폭을 초과할 수 없으므로 다음이 성립한다.

$$\eta \times s \leq B \qquad ④$$

여기서, s는 웜의 크기, B는 최대 대역폭을 나타낸다.

예를 들어, Slammer 웜이 10Mbps IPv4 환경에서 확산된다면, Slammer 웜의 크기는 404B로 알려져 있으므로 수식 ④를 이용한 다음의 계산에서 최대 스캐닝 수는 $\eta = 3244$임을 알 수 있다. 단, 감염 호스트의 성능, 패킷 오버헤드 등은 무시한다고 가정한다.

$$\eta \leq \frac{B}{s} = \frac{10 \times 1024 \times 1024\ (bps)}{404 \times 8\ (byte)} = 3244.356\cdots$$

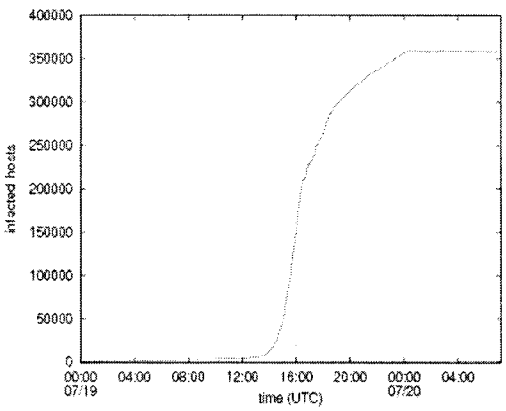

그림 2. Code Red 웜 확산 실제 측정값
Fig. 2 The spread of Code Red Worm

Slammer 웜은 RCS 웜으로 IPv4 주소 전체를 스캐닝한다는 사실이 알려져 있으므로 이를 통하여 초기 웜 확산율을 계산하면 $\beta = 7.55 \times 10^{-7}$이다.

$$\beta = \frac{\eta}{\Omega} = \frac{3244}{2^{32}} = 0.0000007553\cdots$$

즉, Slammer 웜은 10Mbps 속도의 IPv4 인터넷 환경에서는 초당 3244회 스캐닝을 수행하고 7.55×10^{-7}의 확산율로 확산된다는 사실을 알 수 있다.

실제 웜에 대한 관찰 결과로써 TCP를 이용하여 전파되는 Code Red 웜은 4KB 크기로 2001년 당시 분당 평균 358개의 IP 주소를 스캔한 것으로 관찰되었고[4], UDP를 이용하여 전파되는 Slammer 웜은 404B 크기로 2003년 당시 초당 평균 4,000개의 IP 주소를 스캔한 것으로 관찰되었다[5]. 특히, Slammer 웜은 100Mbps 대역폭에서 대역폭 제한과 패킷 오버헤드 등으로 인하여 최고 26,000개를 스캐닝할 수 있는 것으로 관찰되었다[5]. 여기서 실제 Slammer 웜의 관찰 결과에 의하면 호스트 성능, 패킷 오버헤드 등 여러 요인으로 인하여 관찰된 스캐닝 수는 이론적인 스캐닝 수의 약 80%임을 알 수 있다.

Ⅲ. 인터넷 웜 확산 실험

3.1 웜 확산율 산정과 실험 조건

2007년 4월 ITIF(Information Technology and Innovation Foundation)에서 조사한 OECD 국가의 인터넷 평균 속도 측정 결과에 따르면 일본이 61.0Mbps, 한국이 45.6Mbps, 미국이 4.8Mbps이었고, OECD 30개국의 평균 인터넷 속도는 9.0Mbps로 조사되었다[6].

인터넷 웜에 대한 확산율 β는 앞에서 설명한 바와 같이 전체 호스트 수, 네트워크 대역폭에 따라 좌우되는데, Slammer 웜이 균일하게 전체 IP 주소를 스캔하면서 네트워크 대역폭을 최대한으로 사용하고 패킷 오버헤드는 따로 고려하지 않는다고 가정한다면 수식 ④에 의해 Slammer 웜의 주요 국가별 평균 웜 확산율은 표 1과 같다. 단, 1.25 대란 당시의 평균 인터넷 속도는 웜 평균 스캐닝 수를 이용하여 거꾸로 산정한 값이다.

표 1. 국가별 평균 인터넷 웜 확산율
Table 1. Infection rate

국가	평균 웜 확산율(β)	평균 인터넷 속도(Mbps)
한국	3.44×10^{-6}	45.6
일본	4.61×10^{-6}	61.0
미국	3.63×10^{-7}	4.8
OECD 30개국 평균	6.80×10^{-7}	9.0
1.25 대란 평균	9.31×10^{-7}	*12.3*

실험을 수행하기 위하여 다음과 같이 가정한다. 첫째, Slammer 웜이 현재 인터넷 주소 체계인 IPv4 환경에서 확산하고, 해당 네트워크의 대역폭을 최대한 사용한다고 가정한다. 둘째, 각 국가는 평균 인터넷 속도를 최대 대역폭으로 하는 단일 네트워크로 구성되었다고 가정한다.

3.2 감염 호스트 수에 따른 웜 확산 실험

그림 3은 감염가능한 전체 호스트 수를 $N = 100{,}000$으로 두고, 최초 웜 감염 호스트 수를 1대, 10대인 경우에 대해 1.25 대란 당시와 현재 우리나라의 환경에 맞추어 실험한 결과이다.

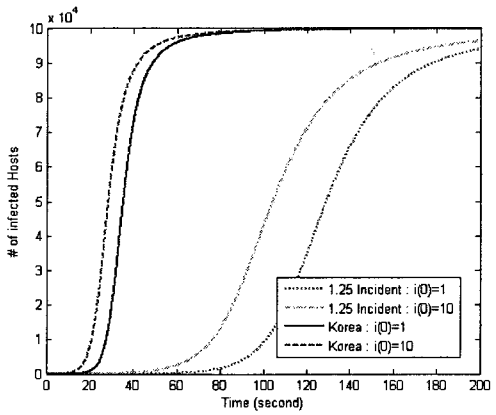

그림 3. 감염 호스트 수에 따른 웜 확산
Fig. 3 Worm spreading by infected hosts

초기 감염 호스트 수가 1대인 경우보다 10대인 경우 더 빠른 속도로 인터넷 웜이 확산한다는 사실을 확인할 수 있다. 즉, 인터넷 웜은 최초 확산을 시작할 경우 감염 호스트 수가 많으면 많을수록 상호 작용에 의해 훨씬 더 빠른 속도로 확산할 수 있다는 사실을 보여준다.

3.3 인터넷 속도에 따른 웜 확산 실험

그림 4는 각 국가별 감염가능한 전체 호스트 수를 $N = 100{,}000$으로 동일하게 두고 표 1의 웜 확산율을 국가별로 적용하여 수행한 실험 결과이다.

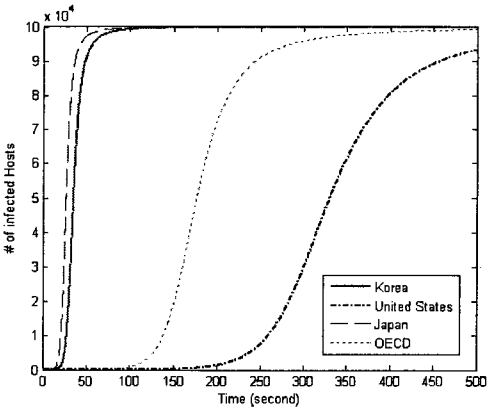

그림 4. 인터넷 속도에 따른 웜 확산
Fig. 4 Worm spreading by Internet speed

평균 인터넷 속도가 높은 한국과 일본은 급속도로 인터넷 웜이 확산하였으며, 상대적으로 평균 인터넷 속도가 낮은 미국과 OECD 30개국은 낮은 속도로 인터넷 웜이 확산한다는 사실을 확인할 수 있다.

3.4 인터넷 주소 체계에 따른 웜 확산 실험

그림 5는 감염가능한 전체 호스트 수를 $N=100,000$으로 두고, 인터넷 웜 제작자가 인터넷 주소 체계에 대한 정보를 이용하여 전체 호스트 주소 공간을 줄여 스캐닝하도록 웜을 구현한 경우 웜 확산을 비교한 실험 결과이다.

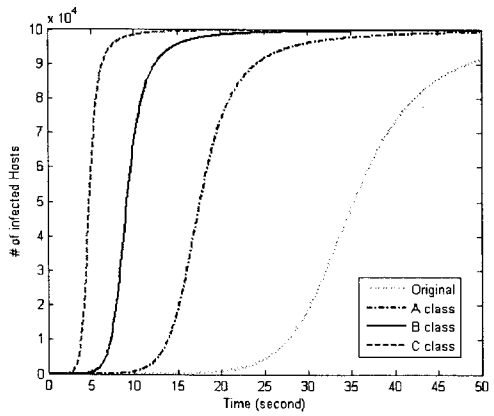

그림 5. 인터넷 주소 체계에 따른 웜 확산
Fig. 5 Worm spreading by Internet addressing

인터넷 웜이 IPv4 주소 공간 모두를 무작위로 스캐닝하는 것이 아니라 인터넷 주소 체계 중 A, B, C 각 클래스만을 스캐닝하도록 구현한 경우, 실험 결과와 같이 전체 호스트 주소 공간을 효율적으로 줄일 수 있으며 웜 확산 속도에 있어서도 매우 큰 영향을 끼칠 수 있다는 사실을 확인할 수 있다.

Ⅳ. 인터넷 웜 대응 방안

앞의 수식 및 실험 결과를 이용하여 인터넷 웜에 대응하기 위한 효과적인 방안을 살펴보면 다음과 같다. 웜 확산에 있어서 가장 큰 영향을 끼치는 요인은 감염가능한 전체 호스트 수 N, 최초 감염 호스트 수인 $I(0)$, 웜 확산율 β를 포함한 3가지로 이들 요인을 가능한 한 얼마나 작게 할 수 있느냐가 인터넷 웜을 대응하는 핵심 사항이다. 이러한 특성을 잘 활용하여 고속으로 확산되는 인터넷 웜을 막기 위해서는 다음과 같이 기술적 대응과 관리적 대응이 함께 이루어져야 한다.

기술적 대응

1. 감염가능한 전체 호스트 수 N의 감소 : 지속적인 보안 패치를 통하여 운영체제 및 어플리케이션의 보안 취약성과 버그를 줄여 이를 이용한 인터넷 웜이 확산하기 어렵도록 하기 위하여 수식 ①과 ③에서 감염가능한 전체 호스트 수 N을 감소시킨다. 패치 적용은 최근 운영체제 및 어플리케이션에서 기본 기능을 제공하고 있으므로, 개인의 경우 이를 활성화하여 사용하고 대규모 조직의 경우 PMS(Patch Management System)를 적극 활용한다.
2. 최초 감염 호스트 수 $I(0)$의 감소 : 개인 PC 또는 각종 서버에 백신, 침입차단시스템(Firewall) 및 침입탐지시스템(IDS, Intrusion Detection System)을 설치하고 항상 최신 버전으로 운영함으로써 인터넷 웜에 감염되지 않도록 한다. 이러한 대응을 통하여 최초 감염 호스트 수인 $I(0)$를 감소시켜 인터넷 웜의 확산을 늦추는 효과를 볼 수 있다.

관리적 대응

1. 웜 확산율 β의 감소 : 수식 ①과 ③에 의해 웜 확산율 β에 직접적으로 영향을 끼치는 것은 웜의 단위 시간 당 평균 스캐닝 수 η, 웜이 스캐닝할 수 있는 전체 호스트 주소 공간 Ω이다. 즉, 웜 확산율 β를 감소시키기 위해서는 η를 작게, 주소 공간 Ω를 크게 하면 된다.
   - 일반적으로 η는 최대 대역폭 B에 의존하므로 대역폭을 가능한 한 감소시키면 웜 확산을 억제할 수 있다. 그러나 현실적으로 타당하지 않은 방법이다.
   - 주소 공간 Ω를 크게 하기 위한 방법으로 32비트 크기의 현재 IPv4에서는 어려운 일이지만 128비트 크기의 IPv6로의 이전이 그 대안이 될 수 있다. 인터넷 주소의 크기가 4배 늘어남으로써 웜이 스캔해야 할 주소 공간의 크기는 이론적으로 296으로 늘어나 확

산율에 큰 영향을 끼칠 수 있다.

2. 개인 PC의 95% 이상을 특정 운영체제를 사용하고 있는 우리나라에서는 인터넷 웜이 쉽게 확산할 수 있는 천혜의 조건을 가지고 있다. 일반적으로 인터넷 웜은 단일 플랫폼을 대상으로 제작되어 확산되므로 개인 PC 또는 각종 서버의 플랫폼을 다양화하여 감염가능한 전체 호스트 수 N을 줄이는 것도 하나의 방법이 될 수 있다.

V. 결 론

인터넷은 전세계를 하나의 네트워크로 연결하여 누구나 원하는 정보를 얻을 수 있도록 한 네트워크의 네트워크(Network of Network)로, 수천만 대의 컴퓨터가 인터넷을 통하여 다양한 정보들이 전송되고 있다. 이러한 환경에서 발생하는 해킹, 바이러스, 컴퓨터 범죄 및 사기 등은 새로운 위협으로 인식되고 있다. 그 중 운영체제 및 네트워크의 취약점을 이용하여 급속도로 확산되는 인터넷 웜은 무차별적으로 네트워크 기반 구조를 공격하는 가장 큰 위협 으로, 인터넷 웜의 확산은 직접적으로는 해당 네트워크에서 시스템의 정상적인 동작을 못하도록 할 뿐만 아니라 간접적으로는 인터넷 기반 구조 및 제공 서비스의 신뢰성에 대한 심각한 타격을 주는 특징을 가진다. 특히, Slammer Worm에 의해 발생한 1.25 대란은 초고속 인터넷을 통한 정보화 사회를 지향하는 한국에 있어 네트워크 기반 구조 보호에 대한 새로운 시사점을 제시하였다.

본 논문에서는 현재 문제가 되고 있는 인터넷 웜 확산에 대한 모델을 제시함으로써 실제 인터넷 환경에서 그 영향을 분석하였다. 이를 위하여 네트워크 대역폭에 따른 웜 확산율을 산정하여 이미 발생한 인터넷 웜이 웜 확산 모델에 따라 동작함을 보였으며, 네트워크 대역폭, 주소체계 등을 고려하여 현재 인터넷 환경에서 발생할 수 있는 인터넷 웜 확산을 실험하였다. 본 논문의 결과는 네트워크의 고성능화에 따른 인터넷 웜 확산을 예측하고 그에 대한 대응 방안을 마련하는데 직접 활용할 수 있을 것이다. 이를 기반으로 향후 국내 광대역 통합망에서 웜 확산 모델링에 대한 연구와 융합망과 같은 서로 이질적인 네트워크 환경에서 인터넷 웜 확산과 대응에 대한 연구도 함께 진행되어야 할 것으로 사료된다.

참고문헌

[1] Cliff C. Zou, Don Towsley, Weibo Gong, "On the Performance of Internet Worm Scanning Strategies", Elsevier Journal of Performance Evaluation, vol. 63, no. 7, pp. 700-723, 2006

[2] Cliff C. Zou, Weibo Gong, Don Towsley. "Code Red Worm Propagation Modeling and Analysis", 9th ACM Conference on Computer and Communication Security (CCS'02), pp. 138-147, 2002

[3] "The Spread of the Sapphire/Slammer Worm", http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html

[4] Cliff C. Zou, Lixin Gao, Weibo Gong, Don Towsley, "Monitoring and Early Warning for Internet Worms", 10th ACM Conference on Computer and Communication Security (CCS'03), pp. 190-199, 2003

[5] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, N. Weaver. "Inside the Slammer Worm". IEEE Magazine on Security and Privacy, vol. 1, no. 4, pp. 33-39, 2003

[6] Daniel K. Correa, "Assessing Broadband in America: OECD and ITIF Broadband Rankings", http://www.itif.org/, 2007

저자소개

신 원(Shin, Weon)

2005.3 ~ 현재 동명정보대학교 정보보호학과 조교수

2002.3 ~ 2005.1 (주)안철수연구소 선임연구원

※관심분야 : 소프트웨어 보안, 악성코드 확산, 이동 에이전트 시스템, 암호 프로토콜 응용