情 報 保 護 學 會 誌
第 16 卷 第 2 號, 2006. 4

IPv6 환경에서 침입탐지 및 웜의 전파 특성

전 용 희*

요 약

인터넷 주소 고갈 문제를 해결하고 QoS를 효과적으로 제공하기 위하여 IPv6가 개발되었다. IPv6는 IPSec이라는 자체의 보안 요소를 탑재하고 있기 때문에 보안의 중요성이 강조되는 유비쿼터스 사회에서 기존의 IPv4가 가지고 있던 문제점을 해결할 수 있을 것으로 기대한다. 그러나 IPv6의 도입에 따른 IPv4/IPv6 전환 시 보안 문제와 IPv6 자체의 보안 특성 등에 대하여 분석할 필요가 있다. 본고에서는 IPv6 환경에서 침입탐지 및 웜의 전파 특성에 대하여 기술하고자 한다.

Ⅰ. 서 론

IPv4에서의 제한된 주소 공간과 다른 기본적인 결점을 극복하기 위하여, 새로운 인터넷 프로토콜 버전인 IPv6가 개발되었다. 128 비트의 주소길이를 가진 IPv6는 미래에 기대할 수 있는 모든 연결된 기계에 거의 무한대의 주소 풀을 쉽게 제공할 수 있으며, 유비쿼터스, BcN(Broadband convergence Network), 홈 네트워크 서비스 등을 효율적으로 구축하기 위한 인프라 기술로서 도입되고 있다.

일반적으로 IPv6에서는 매우 흩어진 주소 공간으로 인하여 랜덤-스캐닝 웜에 대하여 더 큰 보호를 제공할 것이라고 알려져 있다. 이와 같은 낙관적인 측면에서 보면, 모든 빠르게 전파하는 웜은 어떤 형태의 스캐닝을 사용하기 때문에, IPv6를 기반으로 하는 BcN에서 이런 웜이 사라질 것이라는 생각이다. 그러나 수행된 연구에 의하면, IPv6에서도 IPv4와 마찬가지로 특정한 스캐닝 전략을 사용하는 지능적인 웜은 빠른 속도로 전파될 수 있음을 보여준다.[10,12]

[3]에서는 안전한 IPv6 네트워크 환경 구축 및 운영을 위하여 필요한 보안 취약성 및 대응방안에 대하여 기술하고 있다. 그러나 IPv6 환경에서의 스위치에 대한 공격, 바이러스, 웜 등 데이터 링크 계층 및 응용 계층에 대한 보안 취약성과 대응방안들은 다루지 않고 있다. 정보통신부가 2003년 9월에 발표한 'IPv6 보급 촉진 계획'에 따르면, 국내 IPv6 도입 계획은 3단계로 진행되며, 마지막 단계인 2007년부터 2010년 사이에 백본망, 액세스망, 단말기에 모두 IPv6로 교체하도록 되어있다.

본고에서는 IPv6의 도입에 따른 보안 취약성을 알아보고, IPv6 환경에서 침입탐지 및 웜의 전파 특성에 대한 영향을 분석 기술한다.

Ⅱ. IPv6의 보안 취약성과 위협

2.1 IPv6의 취약성

IPv6의 도입으로 일반적인 보안 특성이 좋아질 것으로 기대되나, 또한 예상치 못한 취약성도 있을 수 있다. IPv6 환경에서 다음과 같은 보안 취약성이 있다.[3]

- IPv6의 확장된 주소 범위로 취약한 호스트를 찾기 위한 포트 스캐닝 공격이 어려운 반면, 동시에 공격자를 추적하기도 어렵다.
- 침입탐지시스템과 침입방지시스템은 IPv6의 새로운 기능 및 보안 기능 처리를 위한 CPU 오버헤드로 인하여 서비스거부 공격 가능성이 높다.
- 라우팅 헤더 등의 확장 헤더를 악용하여 침입차단시스템을 우회할 수 있다.
- 공격자는 IPv6 주소 자동 설정 기능을 악용하여 정상적인 주소 할당을 방해하거나 정상적인 세션

* 대구가톨릭대학교 공과대학 컴퓨터정보통신공학부(yhjeon@cu.ac.kr)

을 종료할 수 있다.

멀티캐스트를 주소를 이용한 공격에서, IPv4 환경에서는 공격자가 취약한 시스템을 찾기 위해 8 비트 크기의 서브넷 주소를 일반적으로 사용하여 2^8개 호스트들에 대해 무작위적인 스캔을 수행한다. 반면에, IPv6 환경에서는 IPv6의 서브넷 주소 크기인 64 비트의 주소에 대하여 최대 2^{64} 개의 호스트들을 스캔해야 하므로, 공격자가 이 범위를 줄이기 위하여 보안 취약성을 이용할 수 있다.

IPv6에 새로이 도입된 주소 체계인 애니캐스트(anycast)를 이용한 공격이 발생할 수 있다. 애니캐스트 서비스에서 송신자의 요청은 애니캐스트 라우터를 통하여 짧은 홉거리, 낮은 비용, RTT(Round Trip Time) 등을 고려하여 적합한 그룹의 멤버에게 전달되며, 이때 그룹 멤버는 응답 메시지의 소스 주소를 글로벌 유니캐스트 주소로 변경하여 송신자에게 응답한다. 이 경우 인증되지 않은 애니캐스트 그룹 멤버가 거짓 정보를 광고하거나 해당 멤버에 의해 송신자의 주소를 변경할 수 있는 보안 취약성으로 인하여, 위장공격(Masquerading) 및 DoS 공격이 가능하다.

IPSec 터널링을 이용하는 경우 IPv6 메시지가 암호화되어 전송되기 때문에 침입차단시스템에서는 패킷의 접근제어를 할 수 없어 공격자가 침입차단시스템을 우회할 수 있다.

2.2 IPv4와의 위협 비교

IPv6 보안은 여러 가지 면에서 IPv4 보안과 같다. 그러나 IPsec의 사용을 넘어 IPv4와 IPv6 사이에는 몇 가지의 중요한 차이가 존재한다.[5] 이런 차이가 IPv6 네트워크가 경험하게 될 공격의 유형을 변화시킨다.

아래와 같은 9 가지의 공격이 IPv6에 적용할 경우에 상당한 차이를 가진다. 어떤 경우에는 공격이 더 쉬울 수도, 더 어려울 수도, 혹은 공격 방법의 차이만 있을 수 있다.

- reconnaissance(정찰): IPv4에서는 공격 정보를 수집하기 위하여 Ping sweep, 포트 스캔, 응용 및 취약성 스캔 등의 잘 알려진 방법을 이용한다. 그러나 IPv6에서는 ping sweep이나 포트 스캔을 완수하기가 더 어렵다. IPv6에서의 새로운 멀티캐스트 주소가 라우터나 NTP(Network Time Protocol) 서버 등과 같은 핵심 시스템을 더 쉽게 찾을 수 있도록 한다. 아울러 IPv6의 서브넷 크기가 정찰에 영향을 미친다.
- 비인가된 접근: IPv6에서는 IPsec에 대한 요구사항으로 호스트 접근 제어를 더 쉽게 할 수 있지만, 접근 제어 기술의 필요성은 같다.
- 헤더 조작 및 단편화: 단편화는 네트워크 보안 장치를 피하거나, 네트워크 인프라를 직접 공격하기 위하여 주로 사용된다. 중간 장치에서의 IPv6 단편화는 금지되어 있지만, 보안 장치를 우회하는 위협 측면에서는 동일하다.
- Layer3과 Layer 4 스푸핑: IPv6의 전역적인 집합된 주소 성질로 인하여 Layer 3 스푸핑 방지를 위하여 필터링을 쉽게 설정 할 수 있다. Layer 4 스푸핑 측면에서는 다르지 않다.
- ARP(Address Resolution Protocol)과 DHCP (Dynamic Host Configuration Protocol): IPv6에서 아직까지 DHCPv6, 자동설정, 이웃-발견 남용을 탐지하거나 막을 보안 도구가 없다.
- Broadcast amplification 공격(smurf): IPv6 멀티캐스트 소스 주소를 가진 패킷들에 대하여 입구 필터링(ingress filtering)을 구현하여 대응할 수 있다.
- 라우팅 공격: IPv6에서도 BGP 인증을 위하여 MD5에 의존하며, IS-IS 인증을 위하여 IPv4와 같은 인증 메커니즘을 이용한다. OSPFv3와 RIPng와 같은 프로토콜을 위하여 IPsec을 이용한다.
- 바이러스 및 웜: 다음 절에서 기술한다.
- 전환(transition), 변환(translation) 및 터널링 기법: 듀얼 스택, 터널링, 변환의 각 방법에 대하여 보안 취약성이 존재한다.

위의 항목에 대한 보다 자세한 내용은 [5]를 참조할 수 있다.

Ⅲ. 침입탐지에 대한 영향

현재 많은 침입탐지시스템들이 개발되어 있지만, 아직 IPv6 프로토콜을 지원하기 위하여 현재의 IDS를 확장하기 위한 노력은 적은 편이다. 본 장에서는 웜의 탐지를 위하여 사용되는 IDS가 IPv6에 대하여 어떤 영향을 받을 것인가에 대하여 기술한다.[1,2,10] IPv6와 IPv4사이의 주요 차이와 그 영향은 아래와 같이 요약될 수 있다.

- 단순화된 헤더: IPv6에서 헤더와 확장 헤더의 여러 필드의 해체(decomposition)가 효율적으로 일어날 수 있다. 이것은 패킷-당 처리 속도에서의 이득을 의미하며 기가급의 인터페이스에서 중요한 척도이다. 성능은 헤더 내에 단편화 정보가 없음(확장 헤더에 의하여 취급)으로 인하여 더욱 증진된다. 그러나 IPv4를 위하여 개발된 단편화 공격은 부정확한 데이터그램 재결합이 여전히 발생할 수 있기 때문에 쓸모없게 되지는 않는다.
- 대규모 주소 공간: 대규모 주소의 활용으로 모든 장치가 인터넷에 연결되는 유비쿼터스 네트워킹 시대가 열릴 것이다. 특히 홈네트워크의 구현으로 여러 가전기기들이 인터넷에 연결된다. 이런 어플라이언스들은 통신을 위하여 TCP/IP를 가진 임베디드 운영체제를 실행하는데, 만일 이런 장치들의 소프트웨어에 보안 결점이 존재한다면, 원격 사용자로 하여금 통제를 허용하게 되고 분산 서비스 거부(DDOS) 호스트로 사용할 수 있다. 이런 홈네트워크 환경이 널리 사용됨에 따라 헤아릴 수 없을 만큼의 단순 시스템에 의한 공격의 가능성에 직면할 수도 있다.

더구나 IPv6는 설계에 의하여 어떤 장치가 네트워크 세그먼트 상의 이웃(neighbour)을 찾을 수 있는 방법을 단순화 하였다. ICMPv6를 이용하여 IPv6 주소를 할당하기 위한 미리-정의된 링크-로컬 "이웃 발견" 절차가 만들어 졌으며, 이것은 호스트 사이의 차별자로 48 비트 이더넷 주소를 사용한다. NIDS (Network-based Intrusion Detection System)는 주소 할당이 더 이상 공개적이지 않기 때문에 동적으로 제공된 주소를 가지는 장치를 발견하기는 더욱 힘들게 된다. 이더넷 카드를 단순히 변경함으로써 주소-기반 룰을 쉽게 차단할 수 있다.

이상에서 IPv6의 매우 유용한 여러 가지의 특징들이 IDS에게는 심각한 장애가 될 수 있음을 알 수 있다. 특히 IPv6 인터넷 연결성을 가지는 임베디드 장치는 더욱 그렇다.

- 내재된 인증 및 암호 패킷-레벨 지원: 이런 IPv6의 내장된 기능으로 인하여 "암호화된 공격 문제"를 아주 급격하게 악화시킬 가능성이 있다는 분석이 있다.[6] 인증된 암호화된 링크에 의하여 운반되는 트래픽이 합법적이라는 보장이 없고 게다가 NIDS에 관한한 불법적이라는 것이다. 이것이 NIDS에 IPv6를 도입하기 위하여 가장 중요한 어려움으로 지적하고 있다. 왜냐하면, 정교한 NIDS는 ESP의 내용을 조사하지 않더라도 각 패킷 내의 AH의 유효성을 적어도 검정하기를 원한다. 그런데 SSL과 SSH 키 생성을 위한 그리고 메가비트/초 율에서 on the fly로 패킷을 복호화하기 위하여 지원되는 고속 암호화 사이에 분명한 차이가 있기 때문이다.[10]
- 단순화된 경로배정
- 헤더 내의 체크섬 없음
- 헤더 내에 단편화 정보 없음

정교한 NIDS 설치를 가진 환경으로 IPv6의 도입은 큰 문제가 발생될 것 같지는 않다. 가장 중요한 장애는 아마도 인증 및 암호화이다. 정교한 NIDS는 ESP의 내용은 조사를 하지 않더라도 모든 패킷 내의 AH의 유효성을 적어도 검정하기를 원한다. 이것이 가장 추적하기 어려운 문제일 것으로 보고 있다.

Ⅳ. 관련 연구

4.1 개요

본 절에서는 현재 웜이 IPv6 네트워크에서 얼마나 효율적으로 전파될 수 있는지 살펴본다. 이를 위하여 RCS(Random Constant Spread) 모델을 기반으로 한 전파 특성을 분석한다.[12]

가장 빠른 웜의 하나로 Sapphire 웜이 있다. 이 웜은 마이크로소프트 SQL 서버를 수행하는 컴퓨터에서의 버퍼 오버플로 취약성을 이용하기 위하여 404 바이트 UDP 패킷을 사용한다. Sapphire의 확산 전략은 linear congruent 의사난수 생성 알고리즘 사용에 의한 랜덤 스캐닝을 기반으로 한다. UDP기반 공격이기 때문에 Sapphire의 확산 속도는 TCP 연결 지연이 아닌 각 침해된 기계의 인터넷 대역폭에 의하여 제한된다.

4.2 RCS 모델

RCS 모델은 [9]에 상세히 기술되어 있으며, 스캔-기반 고속-전파 웜의 확산 과정을 설명하기 위하여 사용되었다. 이 모델은 [7]과 [11]에서 전통적인 취약-감염(SI: susceptible-infected) 모델로 또한 불려지며 취약 및 감염 개체 사이에 동질적인 임의의 접촉

을 통한 감염 확산의 성장을 기술한다. 이 연구 결과에서 RCS 모델이 웜의 고속 전파 과정을 정확히 반영할 수 있다는 것을 보여주었다.

RCS 모델의 유용성이 비록 제한적이지만, 적절히 확장함으로써 웜의 전파 효율성을 개선하기 위한 여러 가지 새로운 기법의 영향을 나타낼 수 있다. RCS 모델에서 머신은 단지 두 상태(취약 및 감염)를 가진다. 머신은 웜 공격에 대하여 원래 취약한 반면, 감염된 후 즉시 감염성으로 되고 그 상태에 영원히 머무른다. RCS 모델은 감염 호스트의 어떤 취급이나 제거를 고려하지 않기 때문에 고속-전파 웜의 연구에 아주 적합하다. 이것은 고속-전파 웜이 우리가 알기도 전에 확산을 완료한다는 사실과 부합된다.

[7]에서 상세히 기술된 바와 같이, RCS 모델은 병원균에 의하여 생기는 새로운 감염(혹은 사고)의 수는 감염된 개체의 수, 감염되지 않은 개체의 율과 평균 접촉율의 곱에 의하여 결정된다고 지시한다. 아래와 같은 표기가 사용된다.

- N: 전체 취약 인구의 크기
- S(t): 시간 t에서 감염에 걸릴 수 있는 수
- I(t): 시간 t에서 감염의 수
- β: 접촉 율(contact rate)
- s(t): 시간 t에서 취약율(S(t)/N)
- i(t): 시간 t에서 감염율(I(t)/N)

위의 표기를 사용하면, RCS 모델은 (1)과 같이 정의된다.

$$\frac{dI}{dt} = I\frac{S}{N}\beta \tag{1}$$

(1)은 (2)와 같이 표현될 수 있다.

$$\frac{di}{dt} = \beta i(1-i) \tag{2}$$

이 방정식을 풀면, 시간 t에서 감염된 개체의 비율을 (3)과 같이 구할 수 있다.

$$i(t) = \frac{e^{\beta(t-T)}}{1+e^{\beta(t-T)}} \tag{3}$$

이 식에서 β나 T 모두가 실제 웜의 확산동안 탐지하거나 웜과 네트워크 가정으로부터 계산할 수 있는 "직접적인" 파라미터가 아니다. 따라서 아래와 같은 파라미터를 정의한다.

- r: 스캔 율(scan rate)
- P: 실제 주소 공간
- I_0: 시간 t=0에서 감염수

웜의 전파를 위한 탐색(probe)은 전체 취약 인구의 크기와 다른 IP 주소의 크기에 비례하는 확률로 취약 호스트에 도달할 것이기 때문에, 위의 표기를 이용하면, (4)와 같은 방정식을 얻을 수 있다.

$$\beta = r\frac{N}{2^P} \tag{4}$$

T(적분 상수)는 어떤 시간에서 알려진 감염 수에 의하여 계산될 수 있으며, I_0에 의하여 결정될 수 있다. 따라서 RCS 모델에서 웜의 전파 속도에 영향을 미치는 직접적인 파라미터는 r, N, P, I_0이다. 표 1은 RCS 모델에서 관심 있는 네 가지 파라미터의 실제 데이터를 보여준다.

[표 1] IPv4와 IPv6에서 RCS 모델 파라미터 값

	IPv4	IPv6
N	75,000	75,000
r	4,000	4,000
P	32	64
I_0	1	1
β	2.1	0.513
T	5.35(30 초)	21.88(수천 년)

IPv4와 IPv6 네트워크에서 시나리오 사이의 차이점은 실제 주소 공간의 크기뿐이다. IPv4는 32 비트 주소 길이를 가지는 반면, IPv6은 128 비트로 증가되었다. 그러나 IPv4에서는 전체 인터넷을 고려하지만, IPv6에서는 전체 네트워크 대신에 /64 서브네트워크에 먼저 초점을 맞춘다. /64 서브네트워크는 IPv6 인터넷에서 가장 작고 기본적인 서브네트워크이며, 지역 엔터프라이즈 네트워크의 대부분의 요구사항을 만족할 수 있다. 표 1은 또한 처음 네 가지 파라미터로부터 계산된 해당 접촉율 β와 적분 상수 T를 보여준다. 스캔율 4,000은 인터넷 레벨의 평균이며, IPv6의 실제 주소 공간 크기 64는 기본 IPv6의 서

브네트워크 크기이다.

V. 웜의 전파 특성

128비트의 주소 길이로 IPv6는 우리가 미래에 예측할 수 있는 모든 연결된 장치에 대한 "무한한" 주소풀을 쉽게 제공할 수 있다. IPv6의 거대한 주소 공간이 스캔-기반 웜에 대하여 본질적인 장벽을 제공할 것으로 생각된다. 거의 모든 고속-전파 웜이 어떤 형태로든 인터넷 스캐닝을 사용하기 때문에, IPv6 기반의 차세대 인터넷에서는 고속-전파 웜이 사라질지 모른다는 매우 낙관적인 전망이 있을 수 있다. 그러나 이러한 결론을 내리기 전에 적어도 세 가지 요인이 고려되어야 한다.[12]

- IPv6의 거대한 주소 공간을 자동적으로 감소시키는 설계 선택
- 웜의 전파 효율성을 증가시키기 위하여 채택될 수 있는 다양한 기법
- 웜 고속 전파의 현재 병목을 제거할 수 있는 미래 인터넷의 진보

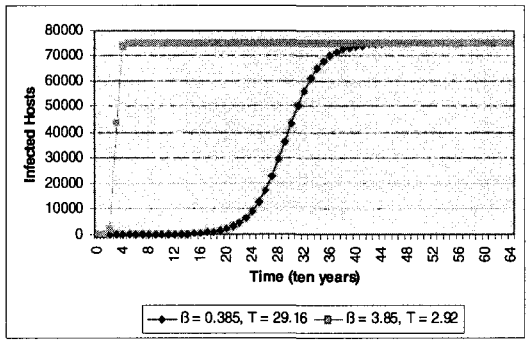
본 절에서는 RCS 모델을 사용하여 적절히 확장함으로써 IPv6 네트워크에서 고속 전파 웜이 발생될 수 있는지의 여부를 조사하기 위하여 위의 세 가지 요인 분석에 대하여 기술한다.

IPv6 네트워크에서 웜의 전파 속도를 가속화하기 위하여 적어도 위와 같은 세 가지 방법이 존재한다. 위의 세 가지 범주의 인자들이 얼마나 빨리 웜의 전파를 가속화시킬 수 있는지 보기 위하여, 앞에서 기술한 RCS 모델에서의 네 가지 직접적인 파라미터에 대한 영향을 알아본다. 그러나 RCS 모델의 제한으로 인하여, 어떤 효과는 적절히 알아 낼 수 없다. 이때에는 약간의 확장이 필요하다. 이런 개선을 점차적으로 적용하여, IPv6 네트워크에서 고속-전파 웜이 가능하게 만들 수 있다.

5.1 스캔 율 r의 증가

Sapphire와 같은 현재의 고속-전파 웜들은 타겟 취약성에 대하여 TCP 연결보다는 UDP 패킷을 사용한다. 결과적으로 이런 웜들은 연결 지연 제한이 아닌 네트워크 대역폭 제한적이다. 따라서 현재 인터넷의 대역폭을 증가시키는 것이 웜이 전파할 수 있는 보다 나은 환경을 만드는 것이 된다.

이론적으로, 인터넷에 대하여 100 Mb/s 연결을 가진 감염머신은 초 당 30,000 스캔 이상을 생성할 수 있다. 실제로는 대역폭 제한과 패킷 당 오버헤드로 인하여, Sapphire의 확산에서 직접 관측된 가장 큰 탐사 율(probe rate)은 초 당 26,000 스캔이었다. 웜 성장의 초기 단계에서는 웜별 초당 인터넷 평균은 대략 4,000 스캔이다. 그림 1은 스캔율을 증가시켰을 때의 감염 호스트 수를 보여준다.[12]



〔그림 1〕 스캔율을 증가시켰을 때의 감염 호스트의 수

〔그림 1〕에서 볼 수 있듯이, β=3.85일 때, 감염 호스트가 포화가 되기 위하여 40년 정도 걸린다. IPv6가 본격적으로 도입되는 고성능 차세대 네트워크에서는 웜의 전파 속도도 그 만큼 빨라질 것이다. Sapphire 웜의 경우 초당 300,000 혹은 3,000,000 스캔 정도까지 증가될 수 있다.

5.2 전체 취약 집단의 크기 증가: N

Blaster같은 웜들은 코어 윈도우 컴포넌트 내의 취약성을 목표로 하며, 이전의 네트워크-기반 웜들이 목표로 하는 서버 소프트웨어보다 광범위한 위협을 생성하며 훨씬 높은 밀도의 취약 시스템을 초래한다. 컴퓨터의 사용이 보편화됨에 따라, 사용상 편리함의 이유로 마이크로소프트웨어와 같은 단일 제품의 경향이 증가되는 추세이다. 미래에 이런 경향이 지속된다면, IPv6가 결과적으로 보급될 때 현재보다 훨씬 높은 정도의 취약성이 예상된다.

하이브리드 웜은 여러 가지 취약성을 이용함으로써 전체 취약 집단의 크기를 또한 증가시킬 수 있다. Nimda가 이러한 웜으로 가장 대표적이다.

5.3 실제 주소 공간 감소: P

이 방법이 IPv6 네트워크의 대규모 주소 공간을

극복하는 가장 효과적인 방법이다. 서브넷 스캐닝은 웜이 전체 인터넷이 아닌 지역 네트워크에 집중하도록 만든다. 라우팅 웜(Routing worm)은 경로배정이 가능하지 않은 주소 공간 부분을 자동적으로 제거할 수 있기 때문에 전체 인터넷 상에 확산할 때 특별히 효과적이다. IPv4 네트워크의 재번호부여(renumbering)의 어려움을 극복하기 위하여 IPv6는 동적인 재번호부여를 허용하는 몇 가지의 설계 선택을 포함하고 있다. 이것중의 하나는 48 비트 MAC 주소로부터 (IPv6 주소의 마지막 64 비트) EUI(Extended Unique Identifier) 필드를 유도하는 것이다. MAC 주소로부터 EUI 필드를 유도하는 방법은 표준이기 때문에, 이것은 /64 IPv6 서브넷의 실제 주소 공간을 48 비트로 더욱 감소시킨다. 표준 유도 방법을 이용하여 초당 300,000 스캔의 스캔율을 가진 Sapphire의 성능은 취약 호스트의 대부분을 침해하는데 단지 6일이 걸리는 것으로 나타났다.

IPv6의 다른 좋지 않은 설계 측면은 밀접한 주소 할당이다. 가장 큰 엔터프라이즈 네트워크도 단지 수만 개의 머신만을 가질 것이기 때문에, 만약 주소가 밀접하게 할당된다면, /64 서브넷의 실제 주소 공간은 32 비트 혹은 16 비트 정도까지 더욱 감소될 것이다. 이런 경우, 웜이 IPv4 네트워크와 IPv6 네트워크를 침해하는데 차이가 없게 된다.

5.4 초기 감염 호스트의 증가: I_0

미리-생성된 히트 목록(hit list)은 전체 감염 시간의 대부분을 차지하는 초기 단계에서 웜의 전파를 극적으로 가속화할 수 있다. 플래시 웜(flash worm)으로 불리는 이론적인 웜은 침해를 이행하기 위하여 잠재적인 취약 호스트의 전체 주소를 사용하기 까지 한다.

미리 생성된 히트 목록은 IPv6 네트워크에서 특별히 효과적이다. IPv6 네트워크에서 모든 호스트들이 DNS 이름을 가질 것이다. 이 경우 성공적인 DNS 공격으로 더욱 많은 호스트 주소가 공개될 수 있다. 미리 생성된 히트 목록으로 인한 1,000 개의 초기 감염 호스트 수를 가정하여, 하루 안에 취약 호스트의 90%가 침해될 수 있음이 나타났다.

이상에서 보았듯이, RCS 모델의 각 파라미터를 점차적으로 증가시킴으로써 IPv6 네트워크에서도 웜이 충분히 빠르게 전파될 수 있다는 것을 볼 수 있다. [12]에서는 IPv4 네트워크에서 웜의 전파와 비교를 잘 하기 위하여, 이전의 예제에서 Sapphire의 파라미터들을 사용하였다. /64 IPv6 네트워크에서 75,000 취약 호스트를 가지는 것이 실제적이지 못하다. 그래서 [표 2]에서와 같은 더욱 실제적인 데이터를 기반으로, 얼마나 빨리 웜이 전파될 수 있는지를 분석한다.

[표 2] /64 IPv6 네트워크에서의 실제적인 파라미터

파라미터	값	비 고
스캔 율 r	300,000 스캔/초	기가비트 이더넷 가정
전체 집단 M	20,000	/64 IPv6 엔터프라이즈 네트워크에서 합당한 값
전체취약 집단 N	10,000	단일 제품으로 인함
실제 주소 공간 P	48	자동-구성 요구사항으로 인함
초기 감염 호스트 수 I_0	501	1000 호스트 사전생성 목록 가정. 그 중 500개가 취약으로 가정

[표 2]의 파라미터를 기반으로 시간에 따른 감염 호스트수의 변화로 취약 호스트의 단지 20% 만이 하루 안에 침해될 수 있음을 보여준다. 하루는 웜 전파의 통상적인 경계치(threshold)이다. 왜냐하면 하루 뒤에는 다양한 조치사항들이 추가적인 확산을 방지하기 위하여 취해질 수 있기 때문이다. 그러므로 RCS 모델에 부합되지 않는 추가적인 개선이 이루어져야 한다.

5.5 스캐닝 외에 확산동안 호스트 주소 발견

수동/은닉(stealthy) 웜은 몇 개의 서버를 침해하고 클라이언트가 악성 페이로드를 다운로드하기를 기다린다. Nimda와 같은 몇 하이브리드 웜들은 이런 방법을 그들 확산 접근의 하나로 채택하고 있다.

위상적 스캐닝(topological scanning)은 새로운 타겟을 선택하기 위하여 희생(victim) 머신 상에 포함된 정보를 사용한다. 이 기법이 IPv6 네트워크에서 매우 유효하게 되는 두 가지 요인은 다음과 같다.

- 모든 호스트가 DNS 이름을 가진다.
- 거의 모든 현대의 운영체제는 응용으로부터 DNS 요구를 쉽게 하기 위하여 어떤 종류의 DNS 캐시를 가진다.

위상적 스캐닝을 고려하기 위하여 새로이 침해된 호스트에서 발견될 수 있는 IP 주소의 수를 반영하는 파라미터 F를 RCS 모델에 추가한다. 간단히 하기 위

하여 전체 웜 확산 과정동안 각 호스트의 DNS 캐시가 동일하게 유지된다고 가정한다.

다른 파라미터 값들은 [표 2]와 같이 두고 F값을 50으로 하였을 때, 하루 안에 대부분의 취약 호스트가 침해될 수 있다는 것을 보여준다.

웜의 추가적인 속도 증진을 위하여 위의 모델을 더 확장한다. 첫 번째 확장에서 하이브리드 웜을 가정하였다. 이 웜은 자신이 공격하는 모든 머신으로부터 호스트 주소를 알아낼 수 있지만 그들의 일부만 다른 취약성을 통하여 통제한다. 이런 경우 웜은 해당 네트워크 내의 모든 호스트에서 IP 주소를 알아낼 수 있지만, 추가적인 전파를 위하여 그들 중에서 일부분만 좀비(zombie)로 선택한다. 이 모델에서 대부분의 취약 호스트를 침해하기 위하여 단지 13 시간만 필요한 것으로 나타났다.

두 번째 확장에서, 변하지 않는 DNS 캐시 가정을 좋게 만든다. 호스트가 처음으로 감염될 때 F 개의 IP 주소가 발견될 수 있다. 그 후 같은 머신이 침해될 때마다 F'개의 새로운 IP 주소가 DNS 캐시 갱신으로 밝혀질 수 있다. 이 새로운 모델에서, F 값이 50이고 F'값이 10일 때, 웜은 약간의 성능 개선을 보여주는 것으로 나타났다.

마지막으로, 위의 두 가지 확장을 결합하여 새로운 모델을 얻을 수 있으며, 이 모델에서는 모든 취약 호스트의 90%를 침해하기 위하여 이제 단지 6 시간만이 필요한 것으로 나타났다. 이런 짧은 시간동안 웜의 확산을 방지하기 위하여 우리가 취할 수 있는 행동은 거의 없기 때문에, IPv6 네트워크에서 웜의 고속 전파를 실제로 가능하게 만들 것으로 예측된다.

5.6 스캐닝 노력의 중복 최소화

순열 스캐닝(permutation scanning)이 스캐닝 노력의 중복을 극적으로 감소시킬 수 있으며, 이것은 한 머신이 웜에 의하여 단지 한 번만 침해된다는 것을 의미한다. 그러나 이전의 확장된 RCS 모델을 기반으로 순열 스캐닝을 적용하면, 약간의 모순이 발생한다. 즉, 중복 스캐닝이 DNS 캐시 갱신으로 인하여 여분의 IP 주소를 알아낼 수 있게 된다.

그러므로 순열 스캐닝과 위상적 스캐닝 둘 다 이용하기를 원한다면 더욱 정교한 기법이 적용되어야 한다. 만약 웜이 캐시 갱신을 기다리기 위하여 감염 머신 상에 쓰레드를 유지할 수 있다면, 모든 머신은 단지 한 번만 침해될 수 있다.

Ⅵ. 분 석

V에서 기술하였듯이, 적어도 세 가지의 IPv6 설계 선택이나 타협점(tradeoff)을 사용하여 IPv6 네트워크에서 웜의 전파를 가속화시킬 수 있음이 분석되었다.[12]

- 밀접하게 할당된 IPv6 주소
  이것은 IPv6 설계자보다는 네트워크 관리자에 의하여 행해진 선택이다. 밀집주소 할당은 IPv6의 실제 주소 공간을 극적으로 감소시킬 수 있으며, 이것이 웜의 스캔 효율성을 증가시킨다. 그렇다고 해서 주소를 희박하게 할당하는 것도 쉬운 것이 아니다. 네트워크 관리자는 각 주소가 고르게 떨어지도록 충분한 주의를 기울여야 한다.
- 48 비트 MAC 주소로부터 IPv6 주소의 EUI 필드를 유도하는 표준 방법
  이것은 실제로 IPv6의 설계 타협점이다. 동적 네트워크 재번호부여와 같은 특징을 허용하기 위하여, 자동 구성 요구사항은 EUI 필드 내의 16 비트 주소 공간을 희생하며, 이것이 웜의 전파를 65,536 배 가속화 시킬 수 있다. 이것에 대하여 두 가지 수정을 할 수 있다.
  - 전체 주소 공간을 유지하면서 자동 구성을 허용하는 새로운 설계
  - 가장 작은 서브넷에 대하여 더 많은 주소 비트 부여
- 모든 호스트는 DNS 이름을 가진다.
  이 선택은 확산 동안 IP 주소를 알아낼 뿐만 아니라 미리 생성된 히트 목록을 만들기 위하여 사용될 수 있다. 이 설계를 이용하여 서버뿐만 아니라 정규 호스트들도 DNS 서버 공격이나 호스트 DNS 캐시 공격에 의하여 또한 발견될 수 있다. 그러므로 IPv6에서 이 설계 선택의 유지를 원한다면 DNS 서버와 호스트 DNS 캐시의 안정성이 보장되어야 한다.

Ⅶ. 맺음말

기존의 인터넷 망이 BcN으로 진화함에 따라 네트워크 대역폭 증가에 따른 웜의 전파 속도 가속화, 서비스 통합으로 인한 네트워크 위협의 증대가 우려되고 있다. 본고에서는 웜의 확산에 대한 IPv6의 영향을 분석하기 위하여 관련 연구에 대한 고찰을 수행하였다. RCS 모델과 확장 모델을 사용하여, IPv6 설계 선택/타협점, 스캐닝 기법 개선과 네트워크 품질 증가 등을

이용함으로써 IPv6 네트워크, 적어도 /64 서브넷에서 고속 전파 웜이 확실히 가능하다는 것을 보았다. 세 가지의 가속화 요인 중에서 가장 큰 요인은 IPv6 네트워크의 설계 선택 및 타협점으로부터 생겨난 것이다.

향후 추진될 연구 과제로는 다음과 같은 내용이 제시되었다.[12]

- 순열 스캐닝과 위상 스캐닝의 혼합 효과는 아직 알려지지 않았다. 순열 스캐닝은 RCS 모델의 확장에 맞출 수 없기 때문에, 시뮬레이션이 수행되어야 한다.
- 분석은 /64 서브넷에 대하여 초점을 맞추었다. 전체 IPv6 인터넷에서의 웜의 전파를 보기 위하여, 매우 복잡한 인터넷 시뮬레이터가 개발되어야 한다.
- 현재 웜의 확산을 방지하는 방법으로 봉쇄(containment)가 가장 인기 있는 방법이다. 그러나 현재 웜의 매우 빠른 속도로 인하여 별로 효과적이지 못하다. IPv6가 고속 전파 웜을 막을 수 없을지라도, 속도는 어느 정도 감소시킬 수 있다. 그러므로 현재의 봉쇄 기법이 IPv6 네트워크에서 효과적인지 알기 위하여 추가적인 연구가 수행되어야 한다.[4,8]

참 고 문 헌

[1] 전용희, "인터넷 웜의 탐지 및 대응기술", 한국통신학회지 제22권 제8호, pp. 1088-1103, 2005년 8월.

[2] 신승원, 오진태, 김기영, 장종수, "인터넷 웜 공격 탐지 방법 동향", 전자통신동향분석, 제 20권 제1호, pp.9-16, 2005년 2월.

[3] 한국정보보호진흥원, IPv6 보안 기술 해설서, 2005년 10월.

[4] Min Cai et al., "Collaborative Internet Worm Containment", IEEE Security and Privacy, pp.24-33, May/June 2005.

[5] Sean Convey & Darrin Miller, IPv6 and IPv4 Threat Comparison and Best Practice Evaluation(v1.0).

[6] J. O. Kephart and S. R. White, "Directed-graph Epidemiological Models of Computer Viruses", Proc. of the IEEE Symposium on Security and Privacy, pp343-359, 1991.

[7] David Moore et al., "Inside the Slammer Worm", IEEE Security and Privacy, pp33-39, 2003.

[8] Jose Nazario, *Defense and Detection Strategies against Internet Worms*, Artech House, 2004.

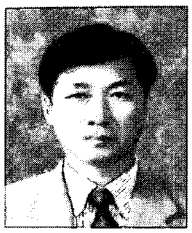
[9] S. Staniford, V. Paxon and N. Weaver, "How to Own the Internet in Your Spare Time", 11th Usenix Security Symposium, San Francisco, August 2002.

[10] Arrigo Triulzi, "Intrusion Detection Systems and IPv6", SPI2003.

[11] N. Weaver, S. Staniford, and V. Paxson, "Very Fast Containment of Scanning Worms", Proc. of 13th USENIX Security Symposium, pp.29-44, August 2004, California.

[12] Jing Yang, "Fast Worm Propagation in IPv6 Networks", Malware Seminar Spring, November 2004.

〈著 者 紹 介〉



전 용 희(Yong-Hee Jeon)
종신회원

1971.3~1978.2 고려대학교 전기공학과
1985.8~1987.8 미국 플로리다공대 대학원 컴퓨터공학과
1987.8~1992.12 미국 노스캐롤라이나주립대 대학원 Elec. and Comp. Eng. 석사, 박사
1978. 1~1978.11 삼성중공업(주)
1978.11~1985.7 한국전력기술(주)
1979.6~1980.6 벨기에 벨가톰사 연수
1989.1~1989.6 미국 노스캐롤라이나주립대 Dept of Elec. and Comp. Eng. TA
1989.7~1992.9 미국 노스캐롤라이나주립대 부설 CCSP (Center For Comm. & Signal Processing) RA
1992.10~1994.2 한국전자통신연구원 광대역통신망연구부 선임연구원
1994.3~현재 대구가톨릭대학교 컴퓨터·정보통신공학부 교수
2001.3~2003.2 대구가톨릭대학교 공과대학장 역임
2004.2~2005.2 한국전자통신연구원 정보보호연구단 초빙연구원
관심분야: 네트워크 보안, BcN QoS & Security, 웜 모델링 및 대응 기술, 통신망 성능분석