특

서비스 거부공격과 스캐닝을 통한 공격에 따른 대응기술

김 병 승[1], 손 희 정[2], 박 세 웅[3]

목 차

1. 서 론

지난 수년 동안 빠른 속도로 보급된 인터넷은 사회 전반적인 영역에서 많은 변화를 가져왔다. 인터넷을 이용하여 업무의 효율성 증대가 이루어 졌고, 전자메일이나 전자 상거래 등 각종 편리한 서비스들이 자리를 잡아가고 있다. 이렇듯 인터넷의 급속한 성장으로 긍정적인 효과를 많이 누리게 되었지만, 부정적인 측면 역시 많아져 직접적인 대단위 피해를 입기도 한다. 그중 최근에 가장 주목을 받고 있는 것이 바로 네트워크 보안의 문제인데, 이는 개인 정보나 기업정보의 유출, 네트워크 마비 등의 사회적인 문제를 야기 시키고 있다. 특히 고속 네트워크 인프라가 전 세계적으로 발전되고 보급되면서 네트워크를 마비시키는 악의적인 공격들은 그 피해 범위가 점차 확대되고 있으며, 이로 인해 입게 되는 손실은 경제적 시간적으로 전과는 비교할 수 없을 정도로 커져버렸다. 금년 1월에 Slammer 웜[4]이 원인이 되었던 인터넷 대란 사태로 인한 국내의 피해규모는 유무형적으로 수십억에서 수천억까지 달하는 것으로 전문가들은 산출하고 있다[1]. 이러한 피해가 단 몇 분만의 공격으로 일어난 사실을 보면 최근 네트워크 보안 문제가 얼마나 심각한지를 알 수가 있다.

네트워크의 이러한 보안상의 허점은 예전부터 많이 공개되어졌고 보완이 요구되어졌다. 인터넷 대란은 보안에 대한 무관심이 한 원인으로 작용하였지만 전체 네트워크가 마비되었다는 점은 단지 보안에 대한 무관심 때문이라고 설명하기는 어렵다. 최근의 공격들은 파괴력이 크기 때문에 개인 사용자뿐만 아니라 네트워크 전반에 걸친 대응이 필요하게 되었고 이에 대한 연구들이 활발하게 진행되고 있다.

본 고에서는 서비스 거부 공격과 스캐닝을 중심으로 최근 네트워크 공격 기법들의 현황을 살펴보고, 아울러 이에 대한 대응방법으로 현재 많은 연구가 진행되고 있는 침입탐지 시스템을 알아보도록 한다.

1) 서울대학교 전기공학부 석사과정
2) 서울대학교 전기공학부 네트워크 보안 전공 석사
3) 서울대학교 전기공학부 부교수
4) Slammer 웜은 SQL_ Overflow 웜, Sapphire, Wom.SQL.Slammer, W32.SQLEXP.Worm, SQLSlapper,Worm_SQLP1434.A 등으로 불리도 한다.

2. 서비스 거부 공격 기법과 현황

서비스 거부 공격(Denial of Service Attack)은 간단히 말해 여러 기법을 이용하여 목표 대상 호스트의 마비 및 네트워크 성능 저하를 일으켜 서비스를 하지 못하도록 하는 기법이다.
이러한 서비스 거부 공격은 크게 다음의 유형으로 분류할 수 있다[2].

〈표1〉 공격의 유형과 특징공격의 유형

대역폭 공격	ICMP, TCP SYN, UDP flood를 이용하여, 많은 양의 패킷을 보냄으로써 피해자의 네트워크를 마비시킴
자원 고갈 공격	시스템을 침투한 후에 공격하거나, TCP SYN flood등을 이용하여 시스템의 CPU사용율, 메모리, 파일시스템 등의 자원을 고갈시킴
프로그램 오류 공격	Ping패킷 처리의 오류를 이용한 'Ping of Death' 또는 IP 패킷의 단편화를 이용한 공격 등이 있으며, 시스템의 소프트웨어를 패치 함으로써 해결가능 함
라우터와 DNS 공격	라우터 패킷에 대한 적법한 인증절차가 없는 점을 이용하여 라우팅 엔트리를 조작하거나 또는 DNS 엔트리를 조작하여 피해자의 서비스를 마비시킴
혼합된 공격	Email 폭탄이나 웜, 바이러스 등으로써 대역폭 공격과 자원 고갈 공격의 효과를 동시에 일으키는 공격

이 중 대표적인 것으로 SYN flooding attack과 스머프 공격(Smurf attack), UDP flooding 공격을 들 수 있다. SYN flooding 공격은 TCP의 3-way handshaking 기법에 의한 연결과정의 취약성을 이용한다. 공격자는 소스 주소를 변조(IP spoofing)하여 SYN패킷을 공격대상에 보내고 수신자는 SYN/ACK 패킷을 송신한 후 연결 확인을 위해 일정시간 ACK 패킷을 기다리게 된다. 보내진 SYN/ACK은 목적지를 찾지 못하므로 ACK 패킷은 돌아오지 않게 되어 공격 받은 시스템은 대기하게 되거나 패킷 재전송을 하게 된다. 이때 시스템은 자원을 소모하게 되는데 이러한 SYN 패킷을 많이 받게 되면 결국 자원소모가 심하게 되어 서비스가 불가능해진다. 최근에는 급속히 전파된 웜에 의해 소스 주소를 변조하지 않고 직접 공격패킷을 발생하기도 하는데, CodeRed 웜이 그 대표적인 예다[3].

스머프 공격은 브로드캐스트 허용의 취약성을 직접적으로 이용한다. 공격자가 브로드캐스트 주소로 ICMP 핑 메시지를 보내게 되면 그 메시지를 수신한 네트워크에 있는 모든 시스템들은 응답 메시지를 보내게 된다. 이때 핑 메시지의 소스주소가 공격 대상의 주소로 변조되어 있기 때문에 공격 대상의 네트워크는 많은 양의 ICMP 핑 응답 메세지로 넘쳐나게 되고 결국 대역폭이 전부 소모되어 서비스가 불가능해진다.

UDP flooding 공격은 UDP 프로토콜의 특성을 이용한다. 공격자는 공격대상을 향해 계속적인 UDP패킷을 보냄으로써 공격 대상 네트워크의 대역폭을 소모시켜 서비스를 불가능하게 만든다. 보통 UDP 패킷공격은 자동화된 웜에 의해 발생하는 경우가 많다. 지난 1월에 발생한 Slammer 웜의 경우 감염을 위한 스캐닝으로 인해 다량의 UDP 패킷이 네트워크에 유입되면서 UDP flooding 공격 특성을 나타내었다.

최근에는 위와 같은 일반적인 서비스 거부 공격보다는 좀더 진화한 형태인 분산 서비스 거부공격이 주를 이루고 있으며 더 나아가 분산 리플렉션 서비스 거부 공격도 이루어지고 있다. 분산 서비스 거부 공격이란 공격자에 의해 조정되는 여러개의 좀비(Zombie)들이 동시에 협력하여 공격하는 형태를 말한다. 이러한 자동화된 툴은 주로 CodeRed, Nimda등의 웜에 의해 자동으로 전파되는데, 특히 금년 1월에 발생한 Slammer 웜으로 인한 인터넷 대란 역시 웜에 의한 분산 서비스 거부 공격의 특성을 가지고 있다.

자동화된 툴인 웜들은 발전을 거듭하고 있다. 최근 웜의 특징은 감염 가능한 호스트를 직접 스캐닝하여 알아냄으로써 전파속도가 빠르고 동시에 대역폭을 소모시키는 분산 서비스 거부 공격을 한다는 점이다. CodeRed나 Nimda 등의 웜 역시 랜덤 IP를 목적지로 하여 TCP 스캐닝을 함으로써 전파속도를 빠르게 하였다. 특히 인터넷 대란의 원인인 Slammer 웜은 슈도 랜덤 제네래이터 알고리즘을 사용하여 스캐닝을 보다 효율적으로 하였고, TCP가 아닌 UDP를 사용함으로써 네트워크 대기시간(network latency)을 짧게 하여 보다 빠르고 강력한 스캐닝과 공격을 하였다[4].

2002년 1월 11일 미국 네트워크 회사인 깁슨 리서치는 새로운 형태의 분산 서비스 거부 공격형태인 분산 리플렉션 서비스 거부 공격(Distributed Reflection Denial of Service Attack)을 발견하였다[5]. 분산 리플렉션 서비스 거부 공격은 TCP 프로토콜과 라우팅 테이블 운영상의 취약성을 이용한다. 공격자는 공격대상의 IP주소로 출발지 주소를 변조한 SYN 패킷을 정상적인 TCP 서버(리플렉션 서버)들에게 보내고, 변조된 SYN 패킷을 받은 TCP 서버들은 SYN/ACK 패킷으로 공격대상에게 응답한다. 이로써 공격대상이 되는 네트워크는 자신과 상관없는 SYN/ACK 패킷들에 의해 대역폭을 소모하게 된다. 분산 리플렉터 서비스 거부 공격은 대역폭이 큰 정상적인 TCP 서버를 리플렉터로서 쉽게 이용할 수가 있고, 리플렉터가 많을수록 경유 라우터에 의해 경로가 분산되어 백트랙킹이 어렵기 때문에 일반적인 분산 서비스 거부 공격보다는 대응하기 어렵다[6].

3. 스캐닝 기법의 현황 및 탐지

네트워크 스캐닝이란 해킹을 시도하기 위한 사전단계로 해킹을 위한 준비단계라고 할 수 있다. 네트워크 스캐닝은 크게 호스트 스캐닝과 포트 스캐닝으로 나눌 수 있다. 호스트 스캐닝은 특정 서비스(목적지 포트)에 대해서 취약성을 갖고 있는 호스트를 찾기 위해 공격자가 다양한 임의의 호스트의 특정 포트에 대해 수행하는 방식이다. 포트 스캐닝은 특정 호스트에 대해 수행하며 해당 호스트에서 제공하는 열려진 서비스(목적지 포트)를 찾기 위해 포트번호를 바꾸어 가는 방식이다. 최근에는 어떤 시스템이나 응용 프로그램 등의 취약성 논의가 있은 후 그 취약성을 가지고 있는 호스트를 찾기 위한 호스트 스캐닝이 대부분이다. 이렇게 찾아낸 호스트의 포트를 이용하여 웜의 전파 및 백도어 등의 해킹툴을 감염시키는데 사용한다. 〈표 2〉는 해킹에 사용된 포트의 특징을 나타내고 있다[7].

〈표 2〉 해킹에 이용되는 포트별 특징

번호	주요서비스	참고사항
80	web 서비스	CodeRed, Nimda 등의 공격에 사용
[illegible]	NETBIOS	인터넷 웜인 OPASOFT의 공격방법에 사용
1433	MS-SQL	Spida 웜의 공격에 사용
1434	MS-SQL	Slammer 웜의 공격에 사용
2222	Apache 웜 백도어	
[illegible]	Squid	릴레이를 허용하는 서버를 찾는 스캔
[illegible]	mIRC	mIRC 프로그램을 이용한 트로이 목마 공격에 사용
12345	netbus	Window98용 백도어 netbus에서 사용
27374	SubSeven	Window용 백도어 subseven에서 사용

〈표 3〉 CERCC-KR에 보고된 것과 RTSD에 탐지된 포트별 스캐닝의 합계

포트번호	2002년 12월	2003년 1월	2003년 2월	포트번호	2002년 12월	2003년 1월	2003년 2월
21	99	114	97	443	15	15	43
22	15	18	17	445	77	127	180
23	4	9	6	515	5	1	4
25	377	200	136	1433	204	150	100
53	8	5	7	1434	0	429	7
80	173	262	151	8080	2	1	0
110	3	0	0	12345	124	121	7
111	6	12	10	17300	0	0	61
137	-	254	386	27374	105	116	27
139	12	309	47	기타	724	53	148

〈표 3〉은 스팸릴레이 서버를 찾기 위한 메일 포트(25번)와 NETBIOS 포트(137번), 웹포트, FTP에서 사용되는 TCP포트(21)들의 스캔이 지속적으로 많은 비중을 차지하고 있으며 웜 전파를 위한 스캔도 적지 않음을 나타낸다. 특이한 점은 Slammer 웜에 사용되는 1434포트 스캔이 2002년에는 전혀 발견되지 않았지만 2003년 1월에 급격히 증가한 후 2월에 감소하는 것이다.

4. 대응방안 및 연구동향

서비스 거부 공격 및 스캐닝 등의 공격에 대한 대응방법으로는 얼마 전까지만 해도 알려진 취약성에 대한 지속적인 버그 패치작업과 트래픽 모니터링을 들 수가 있다. 즉, 시스템 관리자의 관심과 보안정책으로 어느 정도 해결이 가능했다. 공격 사례들을 보면 관리자나 사용자의 부주의에 의해서 비롯된 것들이 많았다. 하지만 아무리 주의를 기울여도 지능화된 해커들의 공격수법을 사전에 완벽히 대응하기란 쉽지 않다. 특히 최근에는 네트워크 자체를 공격 하는 수법이 증가하는 추세이기 때문에 취약성 보완만으로는 대응하기가 어렵다. 이에 따른 네트워크 보안 기술 연구가 진행되어 왔고 대표적인 시스템으로 방화벽과 침입탐지 시스템을 들 수 있다.

본 절에서는 대표적인 네트워크 보안 시스템인 방화벽과 침입탐지 시스템의 제품에 대한 현황을 살펴보고 침입탐지 시스템 연구에 대해서 소개를 하겠다.

4.1 대응 시스템 제품 현황

서비스 거부 공격과 스캐닝을 방어하기 위해 기존의 침입차단, 침입탐지, 라우터 등의 네트워크 장비 업체에서 다양한 방법의 연구가 되어 왔다. SYN flooding attack과 같은 경우에는 3-Way handshaking으로 인한 호스트의 ACK 수신을 위한 지연 부담을 덜기 위해 Checkpoint사의 Firewall-1에 적용된 SYN Defender 방식이 있으며, Netscreen사와 TopLayer사의 제품에서 사용하는 SYN Proxy 방식 등이 있다. SYN Defender 방식은 침입차단시스템에서 호스트가 기다리는 SYN+ACK 패킷을 대신 보내 주는 방식의 개념을 적용한 것이며, SYN Proxy 방식은 정상적인 ACK이 올 때까지 침입차단 제품에서 연결을 관리하는 방식이다. 또한 SYN 패킷을 수신하였을 때 지연을 발생하지 않고 많은 연결의

〈표 4〉 2002년 12월 Information Security Magazine 침입탐지 시스템 업체

회 사 명	제 품 명	특 징
Cisco Systems	IDS 4230	하드웨어 타입, 자동 서명 업데이트 방식, T3라인까지 사용가능
Enterasys Networks	Dragon Sensor	하드웨어 타입, 자동 서명 업데이트 방식, 프로토콜 분석 유니코드 탐지기능, 패턴 분석
Guardent	Guardent Managed Detection	서비스 타입, 자동 서명 업데이트 방식, 프로토콜 분석 유니코드 탐지기능, 패턴 분석, 스텔스 모니터링
Nokia	IP 650	하드 웨어 타입, 자동 서명 업데이트 방식, 프로토콜 분석 유니코드 탐지기능, 패턴 분석, 스텔스 모니터링, TCP 연결 리셋

〈표 5〉 침입 탐지 시스템의 평가요소

평 가 요 소	설 명
정 확 성	false positive 와 false negative를 얼마나 줄일 수 있는가
침입 방어	탐지된 공격에 대해서 실시간 방어와 방화벽과의 연동성
공격 탐지 능력	얼마나 많은 종류의 공격을 탐지할 수 있으며 알려지지 않은 공격을 탐지 할 수 있는지의 여부
적 용 성	다양한 네트워크 토폴로지에 적용 가능하며 고속망에서 사용 가능한가
반 응 성	공격이 감지되었을 때 조치사항이 적절한가
유연한 정책 관리	보안 정책을 다양하게 적용할 수 있는지
확 장 성	실시간 감지와 실시간 업데이트 가능, 원격 조정가능여부

관리에 용이한 SYN-Cookies를 이용하는 방법도 제안되었다[8]. 최근에는 방화벽 및 라우터와 연동을 할 수 있도록 하는 침입 탐지 시스템과 침입 방지 시스템이 출시되고 있다. 각 제조사들은 고유의 탐지 알고리즘을 특허화 하여 타사와의 차별화를 두고 있다. 〈표 4〉는 최근 활발한 움직임을 보여주는 국외의 침입탐지 시스템 업체와 제품 몇 가지를 나타내고 있다[9].

〈표 5〉는 이러한 제품들을 비교하기 위해 서비스 거부 공격을 검출하고 방어하는데 어떤 평가요소가 있는지 나열하였다.

4.2 침입 탐지 시스템

침입 탐지 시스템은 크게 호스트 기반(HIDS)과 네트워크 기반(NIDS)으로 나눌 수 있다. 호스트 기반 침입탐지 시스템은 로그파일 생성에서부터 호스트의 실시간 인터넷 감시, 설정 변화 상태 확인 등 호스트자체에서 개별적으로 가능한 침입 탐지를 하는 시스템이다. 반면에 네트워크 기반 침입탐지 시스템은 실제 네트워크 상에서의 패킷을 분석하여 서비스 거부공격이나 스캐닝을 감지하는 시스템이다. 최근에는 분산 서비스 거부 공격이나 웜 등에 의한 스캐닝이 많이 발생하기 때문에 네트워크 기반 침입탐지 시스템의 중요성이 날로 커지고 있다. 또한 호스트 기반에서 침입탐지를 할 수 있더라도 공격자를 찾아내기 위해서는 네트워크 기반의 침입탐지 시스템이 필요하다.

네트워크 기반 침입탐지 시스템은 크게 서명기반(Signature based)과 비정상성 기반(Anomaly based)으로 나뉜다. 서명기반 방식이란 이미 알려진 공격이나 스캐닝의 특성을 이용하여 패킷을 분석하여 그것과 일치하는 패턴이 나타날 때 공격으로 판단하는 것이다. 따라서 많은 서명을 보유하여 효과적으로 패턴을 찾을 수 있어야 성능이

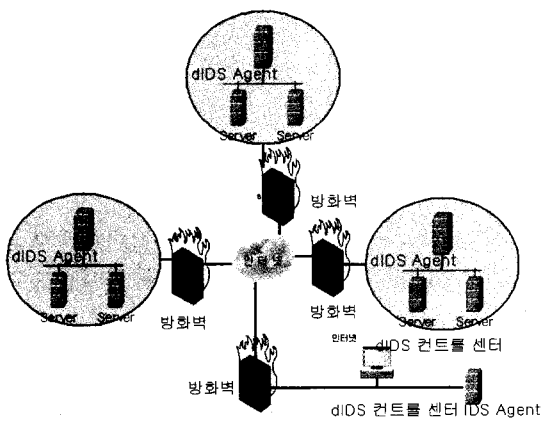
뛰어난 시스템이 된다. 지금의 침입 탐지시스템의 대부분은 서명기반으로 되어있다. 그러나 알려지지 않은 공격에 대해서는 검출할 수 없는 단점이 있다. 이러한 단점을 해결하고자 최근에는 서명 이외에 회사마다 자체적으로 고안한 비정상성 트래픽 및 프로토콜 분석을 기반으로 한 SNA (Suspicious Network Activity)를 정의하여 공격을 판단하는 기능을 추가하고 있다. 또는 중앙 관제센터를 통하여 새롭게 발견된 공격패턴에 대한 서명을 사용자 레벨의 침입탐지 시스템에 빠르게 전달함으로써 단점을 해결할 수 있도록 한다. 현재까지 상용화된 침입탐지시스템에서는 대부분 서명기반 방식에 추가적으로 자사의 고유한 SNA를 이용하는 것으로 알려져 있다.

4.3 침입 탐지 시스템의 발전

침입 탐지 시스템은 아직 불완전한 요소들이 많다. 잘못된 긍정(false positive), 잘못된 부정(false negative)이 항상 존재하기 때문에 정확한 판단으로 방화벽과 연동하기가 힘들다. false alarm 방지는 매우 중요한 일이며 기업들은 자신들이 공격을 당할지언정 정상적인 고객을 불편하게 할 수 없다고 말한다. 또한 침입탐지를 해도 다른 도메인들과의 연동이 없으면 해결할 수 없는 일들이 많아졌다. 이러한 문제들을 개선하는 연구가 이루어지고 있으며 대표적인 예로 침입 방지 시스템과 분산 침입 탐지 시스템을 들 수 있다.

침입방지 시스템(Intrusion Prevention System)은 기존의 IDS가 행하는 네트워크상의 트래픽을 수동적으로 분석하는 것이 아니라 방화벽처럼 능동적으로 트래픽을 분석하고 막는 역할을 한다. 기존 침입탐지 시스템이나 방화벽과 다른 점은 공격자로 하여금 공격 성공여부를 알 수 없게 하거나, 공격자로 하여금 계속 공격하게끔 해서 피해를 입지 않은 채 공격자의 정보를 모을 수 있다는 것이다.

분산 침입탐지 시스템(distributed Intrusion Detection System)은 여러 도메인 상에 자동화된 에이전트를 두고 각자 정보를 중앙 분석 서버로 전달한다. 분산 침입탐지 시스템의 중앙 서버는 이러한 정보들을 이용해 공격자의 경로와 기법을 빠르고 효과적으로 분석함으로써 공격자를 고립시키고 공격에 대한 대응을 할 수 있다.



(그림 1) 분산 침입 탐지 시스템 개요

이러한 네트워크 토폴로지 상에서의 연구 이외에 비정상성 탐지에 대한 연구도 활발히 되고 있다. 하지만 false alarm의 위험성 때문에 비정상성 기반의 침입탐지시스템에 대해서는 아직까지는 학문적으로만 연구되고 있다. 비정상성을 판단하기 위해 샘플 데이터를 이용하여 훈련(Training)을 거치는 경우와 훈련 없이 자동으로 전체 특징에서 소수의 이상성을 보이는 특이점(Outlier)을 추출하는 경우가 있다. 비정상성을 판단하기 위하여 기존의 통계분야에서 연구된 특이점 제거(Outlier detection)에 관한 연구나 인공지능과 데이터 마이닝 분야에서 연구되어 온 패턴 분류(Pattern classification)의 연구가 활발히 적용되고 있다[10].

비정상성 기반의 침입탐지시스템은 공격을 판단하는데 많은 모호성이 있기 때문에 알려지지 않은

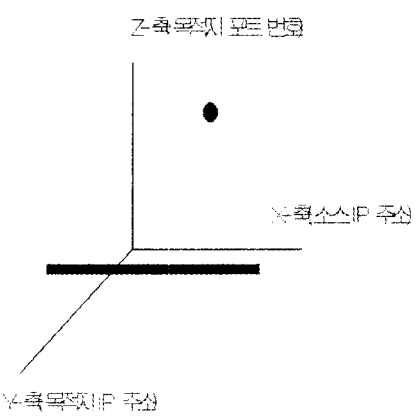
데이터에 대한 적응력은 가질 수 있지만 부정확할 확률도 높게 된다. 따라서 검출결과에 대해 사용자의 판단이 입력되어 실제 공격 여부가 확인되어야 할 필요가 생기게 된다. 또한 비정상성기반의 침입탐지 시스템은 서명기반의 검출 방식보다 계산량이 많은 경향이 있어 고속망에 대한 적용이 어려울 수가 있다. 현재 Mazu Networks의 침입탐지 시스템인 Mazu Enforcer는 이상이 발견되면 자동화된 툴을 이용하여 방화벽에 필터를 적용할 수 있도록 되어있다. 하지만 잘못된 긍정(false positive)의 문제 때문에 관리자의 판단하에 동작시키도록 구성되어 있다[11].

잘못된 긍정을 판단하고 정책을 제시하는 관리자의 역할은 매우 중요하다. 이러한 관리자들에게 빠르고 정확한 판단을 할 수 있도록 실시간으로 트래픽 모니터링과 그 데이터를 시각화 하는 방법은 침입탐지 시스템을 더욱 효율적으로 발전시킬 수 있다[12,13].

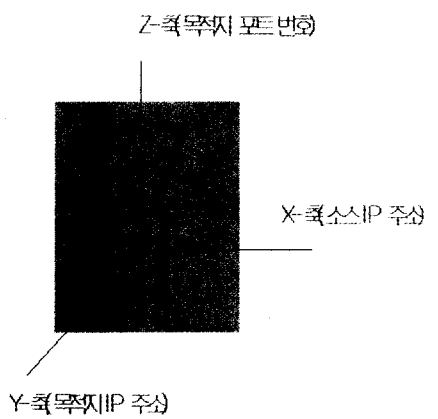
5. 결 론

해킹 기술은 점점 더 악의적이며 지능화되어 가고 있다. 특히 광범위한 인터넷 보급으로 인해 시스템의 취약성과 그를 이용한 다양한 툴이 공유됨에 따라 별다른 지식 없이도 해킹이 가능한 시대가 왔다. 또한 개별 호스트가 아닌 네트워크 전반에 걸친 공격으로 그 수법이 발전되고, 웜에 의한 자동화 된 툴로써 그러한 공격이 이루어진다는 점이 방어를 더욱 어렵게 한다.

네트워크 보안을 가장 어렵게 하는 것 중에 하나로 빠른 공격속도를 들 수 있다. 올 2003년 1월 인터넷 대란 사태에 원인이 되었던 Slammer 웜은 첫 번째 나타난 워홀 웜(Warhol worm)이라고까지 불리울 정도로 그 전파속도가 엄청났다[14]. 워홀 웜은 이론상 15분 내에 전세계의 취약한 호스트에 전파될 수 있는 이상적인 웜의 형태를 말한다. CAIDA의 보고서[15]에 따르면 10분만에 전세계 90%의 취약한 호스트가 이번 Slammer 웜에 감염되었으므로 워홀 웜은 실제로 증명된 셈이다. 전파시간과 공격속도는 공격을 초기에 발견했다고 하더라도 사람으로서는 대응하기 힘든 시간이다. 따라서 앞으로는 자동화된 공격 툴인 웜의 발전에 맞추어 대응기법도 자동화가 되어야 할 것이다. 하지만 여기서 선행되어야



(그림 2) 단순한 서비스 거부 공격과 소스 주소변조(Spoofing)를 사용한 특정 포트로의 서비스 거부 공격



(그림 3) 소스주소변조(Spoofing)를 사용한 랜덤 포트로의 서비스 거부 공격

할 문제는 잘못된 긍정(false positive)을 해결해야 한다는 것이다.

또한 네트워크 보안을 어렵게 하는 또 다른 이유는 각 도메인의 보안 시스템이 내부 보안에만 집중되어 있다는 점이다. 이로 인해 전체 네트워크에 공격이 발생할 경우 자신의 도메인은 방어가 가능하지만 다른 네트워크와의 연결은 끊어져 결국 고립되는 형태가 될 수 있다. 지금의 네트워크는 인터넷(또는 외부망)에 연결되지 않으면 죽은 네트워크라 할 수 있다. 이를 해결하기 위해서는 각 도메인에 존재하는 대응 시스템 간 정보의 상호 결합과 그에 따른 상호 협력기능이 필수적이다. 이를 위해 각 도메인은 ISP(Internet Service Provider)와의 공조가 이루어져야한다. 현재 국내 ISP 업체들은 네트워크 보안 서비스를 제공하고 있다[16].

완벽한 보안은 불가능하다. 하지만 거의 완벽하게 만들 수는 있다. 이를 위해 사용자는 보안의식을 가지고 지속적인 대응을 해야 하며, 관리자는 보안 시스템을 철저히 운영하고 문제가 발생하면 신속히 대처, 분석할 수 있어야 한다. 또한 각 도메인은 ISP와의 공조에 의해 적절한 보안 인프라를 구성해야 하며, 정부는 보안 산업 활성화와 관계법령 정비를 통해 국가 전체에 걸친 체계적인 네트워크 보안이 자리 잡을 수 있도록 노력해야 할 것이다.

참고문헌

[1] "사상초유 '인터넷 대란' 발생", 중앙일보 조인스 뉴스, 2003.01.25.

[2] Scambray,McClure,Kurtz, HACKING EXPOSED 4th edition, McGraw Hill, 2001.

[3] David Moore, Colleen Shannon, k claffy, "Code-Red: a case study on the spread and victims of an Internet worm", Internet Measurement Workshop November 2002.

[4] Stuart Staniford, Vern Paxon, Nicholas Weaver, "How to Own the Internet in Your Spare Time", the Proceedings of the 11th USENIX Security Symposium 2002.

[5] Vern Paxson, "An Analysis of using Reflectors for Distributed Denial-of-Service Attacks", Computer Communication Review, July 2002.

[6] Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, "Practical Network Support for IP Traceback", ACM SIGCOMM 2000.

[7] "2003년 2월 해킹바이러스 통계 및 분석 월보",pp. 1,한국정보보호진흥원, 2003.2.

[8] D. J. Bernstein, "SYN cookies", http://cr.yp.to/syncookies.html, 1996.

[9] "Prerimeter/Network Security/ Availability", Information Security Magazine Dcember 2002, pp. 106, 2002.

[10] Wenke Lee, Phlip K. Chan, Eleazar Eskin, Wei Fan, Mattew Miller, Shlomo Hershkop, Junxin Zhang, "Real Time Data Mining-based Intrusion Detection",2001.

[11] Mazu Networks, "http://www.mazu-networks.com/products/enforcer.html", 2002.

[12] 손희정, "서비스 거부 공격/분산서비스 거부 공격과 네트워크 스캐닝의 자동 검출과 시각화 방법", 서울대학교 전기공학부 석사 논문, 2003.2.

[13] 손희정, 박세웅, 김효곤, 이희조, "네트워크 상태 표시 장치 및 그 방법.", 특허 출원번호 제10-2003-0008826, 2003.2.12.
[14] Nicholas C Weaver,"Warhol Worms: The Potential for Very Fast Internet Plagues", 2002.
[15] David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, Nicholas Weaver, "The Spread of the Sapphire/Slammer Worm", http://www.caida.org/ outreach/papers/2003/sapphire/, 2003.
[16] 이승민, 김명은, 남책용, 손승원, "ISP 보안 서비스 기술 동향", ETRI IT정보센터 2002.11.20.

저자약력

김 병 승

2002년 고려대학교 전기전자전파 공학부(학사)
2003년-현재 서울대학교 전기공학부(석사과정)
관심분야: 네트워크 보안
이 메 일: kbs@netlab.snu.ac.kr

박 세 웅

1984년 서울 대학교 전기공학부(학사)
1986년 서울 대학교 전기공학부(석사)
1991년 University of Pennsylvania(박사)
1991년-1994년 AT&T Bell 연구소 연구원
1994년-현재 서울대학교 전기공학부 부교수
관심분야 : 유,무선 네트워크 성능분석, 네트워크 보안
이 메 일 : sbahk@netlab.snu.ac.kr

손 희 정

1996년 한국과학 기술원 전산학과(학사)
1996년-2001년 LG전자 연구원
2003년 서울대학교 전기공학부 네트워크 보안 전공(석사)
관심분야: 네트워크 보안
이 메 일: hjsohn@netlab.snu.ac.kr