情 報 保 護 學 會 誌
第17卷 第2號, 2007. 4

비정상 트래픽 공격 유형 분석

전 용 희*, 장 종 수**

요 약

네트워크 트래픽에서 비정상(anomaly)을 탐지하는 것은 아주 중요하지만 아직 완전히 해결되지 않은 문제이다. 비정상 유형을 관찰하기 위하여 일반적으로 트래픽 플로(traffic flow)를 감시한다. 트래픽 플로는 여러 가지 네트워크 트래픽의 형태를 제시한다. 이런 트래픽 플로의 집합에 대한 분석은 매우 복잡한 문제이고, 또한 트래픽 플로 수집을 위해서는 많은 자원이 소요된다. 본 논문에서는 비정상 트래픽 유형을 공격 형태 및 트래픽 플로 두 가지의 다른 측면에서 제시하고 그 특성을 기술한다. 그리고 앞으로 나타날 새로운 웜 공격 유형에 대하여도 제시한다.

Ⅰ. 서 론

비정상 트래픽은 네트워크 트래픽이 보통 때와는 다르게 아주 갑자기 변화하는 것이며, 다수의 링크에 걸쳐서 흔히 나타난다. 비정상을 진단하는 것은 네트워크 운영자뿐만 아니라 사용자에게도 매우 중요하다. 문제되는 트래픽의 비정상 특성은, 그것이 악성이든 비고의성 트래픽이든지에 관계없이 분석되어야 한다. 그 이유는 다음과 같다[1].

- 비정상은 네트워크에서 혼잡을 생성하고, 라우터에서 자원 사용을 제한함으로써 네트워크 운용 관점에서 탐지되어야 한다.
- 어떤 비정상 트래픽은 네트워크에 그다지 충격을 주지는 않지만, 종단 사용자에게는 엄청난 영향을 미칠 수 있다.

IP 네트워크에서의 비정상 트래픽에 대한 탐지와 이해는 아직 잘 정의되지 않은 문제이다. 트래픽 특성화에 대한 논문은 많이 존재하지만, 트래픽 비정상에 대하여는 더 많은 연구가 필요하다.

원칙적으로 트래픽 플로를 감시함으로써 대부분의 비정상 유형을 관측할 수 있어야 한다. 그러나 트래픽 플로의 전체 집합 안에 존재하는 정보의 범주를 추출하는데 진보가 별로 없는 상태이다. 그 이유는 다음과 같다[2].

- 트래픽 플로는 여러 가지 가능한 형태의 네트워크 트래픽을 제시 한다.
- 모든 플로의 집합은 매우 높은 차원의(high-dimensional) 공간을 차지한다.
- 따라서 모든 트래픽 플로를 수집하는 것은 매우 많은 자원이 소모된다.

본 논문에서는 비정상 트래픽 공격 유형을 컴퓨터 및 네트워크 공격 유형 측면과 트래픽 플로 측면에서 기술한다. 그리고 앞으로 예측되는 웜의 새로운 공격 유형에 대하여도 제시하고자 한다.

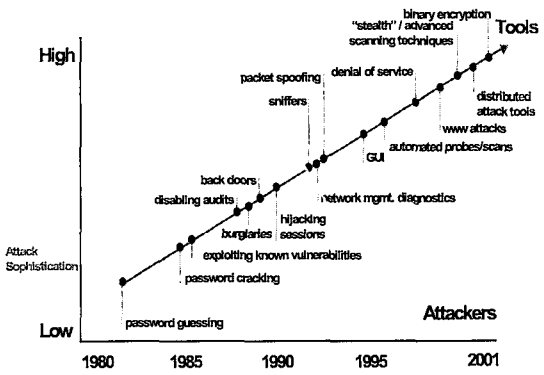
Ⅱ. 관련 연구

2.1 공격 유형

공격 유형에 대하여 기술하기 전에 먼저 컴퓨터와 네트워크 공격에 대하여 분류할 필요가 있다. 컴퓨터 공격(Computer Attack)은 어떤 방법으로든 컴퓨터 시스템 공격을 목표로 하는 공격이다. 이 공격은 데이터의 파괴 혹은 접근, 컴퓨터를 망가뜨리거나 성능을 저하시키는 것을 포함한다. 전통적으로 컴퓨터에 대한 공격은 바이러스, 웜, 버퍼-오버플로 공격 및 DoS(Denial of Service) 공격을 포함하였다.

네트워크 공격(Network Attack)은 대부분 어떤 방법으로든 네트워크를 사용하는 컴퓨터에 대한 공격이다.

* 대구가톨릭대학교 컴퓨터정보통신공학부(yhjeon@cu.ac.kr)
** 한국전자통신연구원 정보보호연구단 보안응용그룹 그룹장(jsjang@etri.re.kr)



〔그림 1〕 공격의 정교화 대 침입자 기술 지식[3]

네트워크는 웜과 같은 공격을 전송하기 위하여 사용될 수 있고, 혹은 분산 DoS 공격 같은 공격의 수단이 될 수 있다. 네트워크를 필요로 하는 컴퓨터에 대한 공격은 네트워크 공격이다. 일반적으로, 네트워크 공격은 컴퓨터 공격의 부분집합으로 분류된다. 그러나 컴퓨터를 공격하지 않고, 부착된 네트워크를 공격하는 여러 가지 형태의 네트워크 공격이 있다.

1978년 웜의 개념이 만들어진 후, 모리스 웜이 출현하게 된다. 1981년에는 첫 번째 바이러스가 나왔으며, 그 이후로 바이러스가 가장 보편적인 공격 형태가 되었으며 안티-바이러스 도구의 개발을 촉진시켰다. 좀 더 최근에는 DoS와 DDoS 같은 새로운 공격이 개발되었다. 그림 1은 1980년대 초반부터 2000년대 초반까지의 연도별 공격 경향을 보여 준다.

컴퓨터와 네트워크 공격에서 최근의 주요한 두 가지 경향은 혼합 공격(Blended Attacks)과 정보전(Information Warfare)이다[4]. 이 두 가지가 새로운 공격이 생성되는 방법에 영향을 끼쳤으며, 또한 공격의 미래를 형성할 것으로 판단된다. 2001년 6월에 출현한 코드 레드도 혼합 공격의 한 형태이다. 혼합 공격은 더욱 강력한 공격을 생성하기 위하여 두 개 이상의 공격이 함께 일어나는 것이다. 1988년에 출현한 원래의 모리스 웜도 혼합 공격 형태이다. 새로운 형태의 혼합 공격은 이전의 혼합 공격보다 훨씬 더 손해를 끼치고 더욱 효과적이다. 2003년 2월에 발간된 Symantec의 인터넷 보안 위협 보고서(Internet Security Threat Report) 3권은 혼합 공격이 인터넷 공동체에 가장 큰 위협이며 더욱 더 파괴적인 혼합 위협에 대한 가능성이 존재한다는 것을 밝히고 있다. 4권에서는 2002년 후반부터 혼합공격이 20% 증가하였다는 것을 보여준다. 더욱 많은 취약성이 발견됨에 따라, 혼합 공격이 더욱 더 빈번하게 발생하고 더욱 파괴적으로 될 것으로 판단된다. 정보전 개념도 새로운 연구 개발 분야이다.

2.2 기존 연구

네트워크 어노멀리(반드시 트래픽 어노멀리는 아닌)를 분류한 일반 영역은 근래에 많은 관심을 받아왔으나, 주로 아래 분야에 대한 연구가 수행되었다.

- 인터넷 침입 행위 특성화[5]
- IP 네트워크에서의 실패 이벤트 특성화[6]
- 인터넷 웜 분류[7]
- DoS 공격 분류[8]
- DoS 방어 분류[9]

이전의 비정상 트래픽 분류에 관련된 연구들은 단일 라우터 혹은 링크에서 행해진 플로 측정으로부터 비정상(어노멀리)을 탐지하고 분류하는데 초점을 맞추어 왔다. 대표적으로 수행된 연구들은 아래와 같다.

- Barford 등은 단일-링크 바이트 어노멀리를 특성화하기 위하여 플로 트래픽의 웨이브렛(Wavelet)-기반 신호 분석 방법을 채택하였다[10].
- Duffield 등은 표본된 트래픽 측정으로부터 웜 감염 집단을 추정하기 위한 기법을 제안하였다[11].
- Jung 등은 Flash Crowd 행위로부터 DoS 공격을 구분하기 위하여 웹 서버에 대한 위상적 클러스터링(topological clustering) 휴리스틱을 제안하였다[12].

Ⅲ. 공격 형태 분류

공격의 형태는 아래와 같이 분류될 수 있다[4].

3.1 바이러스

바이러스는 파일을 통하여 감염되고 전파되는 자기-복제 프로그램으로 정의된다. 그러나 종종 웜과의 구분이 분명하지 못하고 혼동될 때도 있다. 바이러스의 주요 형태는 아래와 같다.

3.1.1 파일 감염자

파일 감염자(File Infector) 바이러스는 파일속에 자신을 삽입하여 희생 컴퓨터상의 파일을 감염시킨다. 보

통 이러한 파일은 윈도우의 .EXE 혹은 .COM과 같은 실행 파일이다. 감염 파일이 수행될 때, 바이러스도 실행된다.

3.1.2 시스템 및 부트 레코드 감염자

1990년대 중반까지 가장 통상적인 바이러스 유형이었으나, 현대적인 운영 체제의 도입으로 거의 생성되지 않는다.

3.1.3 매크로 바이러스

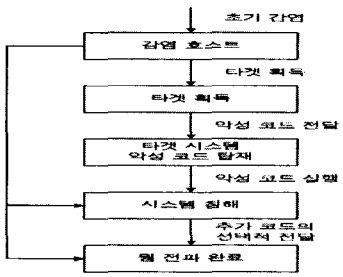
마이크로소프트 워드와 같은 프로그램을 실행할 때 감염되는 악성 매크로이다. 문서에서 정보를 삭제하거나 구문을 삽입한다. 전파는 주로 감염 파일을 통하여 이루어진다. 만일 사용자가 감염된 문서를 열면 바이러스가 설치되고 후속 문서도 또한 감염된다. Melissa와 같은 어떤 매크로 바이러스는 전자메일을 통하여 전파된다. 이와 같이 전파되는 Melissa는 대량-메일링 웜으로도 볼 수 있다.

3.2 웜

웜은 어떤 방법으로든 네트워크상으로 전파되는 자기-복제 프로그램이다. 바이러스와 다르게 웜은 전파하기 위하여 감염 파일을 필요로 하지 않는다. 두 가지 형태의 주요한 웜이 있다: 대량-메일링 웜과 네트워크-인식 웜

3.2.1 대량-메일링 웜

대량-메일링 웜(Mass-mailing worm)은 바이러스로도 분류되는 공격이다. [4]에서는 전자메일로 확산되는 웜으로 분류하고 있다. 공격 벡터로 네트워크를 이용하는 전자메일을 사용하기 때문에 웜으로 분류하고 있다. 예를 들어 Melissa같은 공격이 대량-메일링 웜이다.



〔그림 2〕 웜의 대표적인 전파 단계

3.2.2 네트워크-인식 웜

이 웜이 인터넷에서 주요한 문제가 된다. SQL 슬래머와 같은 웜은 인터넷이 잘 작성된 웜에 의하여 얼마나 피해를 입을 수 있는가를 보여주었다. 네트워크-인식 웜은 〔그림 2〕와 같은 대표적인 전파 단계를 가진다. 단계별로 발생하는 대표적인 활동은 아래와 같다[13]:

(1) 초기 감염 단계 : 웜에 의하여 이미 감염된 시스템이 존재하고 그 웜이 시스템 상에서 활동적이라는 가정에서 시작한다.

(2) 타겟 획득 : 이 단계에서 IP 주소, 전자 메일, 파일 시스템 전달 등을 통하여 목적지 시스템에 도달을 시도한다. 웜은 또한 타겟 시스템에 수동적으로 전달될 수 있다. 예를 들어, 웜에 감염된 웹 콘텐츠가 웹 서버에 의하여 타겟으로 전달 될 수 있다.

(3) 악성 코드 전달 : 일단 시스템이 목적지로 정해지면, 감염을 준비하기 위하여 목적지 시스템으로 웜을 전달 할 필요가 있다. 코드 전달은 네트워크 파일 시스템, 전자 메일, 웹 클라이언트, 원격 명령 셸, 혹은 버퍼 오버플로 등과 관련된 패킷 페이로드의 일부로써 전달됨이 관측되었다.

(4) 악성 코드 실행 : 웜 전파를 위하여 악성 코드가 다음과 같은 방법으로 실행된다.
- 명령 라인으로부터 직접 호출
- 버퍼 오버 플로 혹은 다른 프로그램적 공격
- 전자 메일 클라이언트
- 웹 클라이언트
- 사용자 간섭
- 타깃 시스템에 의한 자동 실행

(5) 추가 코드의 선택적 전달 : 타깃 시스템이 침해된 후, 추가적인 코드가 FTP/TFTP, 네트워크 파일 시스템을 통하여 전달될 수 있다.

3.2.3 트로이 목마

트로이 목마(Trojan Horse)는 겉으로는 사용자에게 유용한 프로그램으로 보이지만, 악의적인 목적을 가진

프로그램을 말한다. 트로이 목마의 특별한 형태로 논리 폭탄(Logic Bomb)이 있다. 이것은 일정한 조건이 만족되면 행동을 개시한다.

3.3 버퍼 오버플로

버퍼 오버플로(Buffer Overflow)는 컴퓨터 및 네트워크 공격 수단으로 아마도 가장 많이 사용되는 방법이다. 이 공격은 단독으로는 시행되지 않으며 보통 혼합 공격 형태로 이루어진다. 버퍼 오버 플로는 버퍼가 넘치는 것을 허용하는 프로그래밍 오류를 이용한다. 만약 버퍼가 용량이상으로 차게 되면, 버퍼를 채우는 데이터가 인접 메모리로 오버플로가 생길 수 있다. 이렇게 되면 데이터를 오손시킬 수 있고 프로그램의 실행을 변경하기 위하여 사용될 수 있다. 두 가지 형태의 주요한 버퍼 오버 플로가 있다.

3.3.1 스택 버퍼(Stack Buffer) 오버 플로

가장 통상적인 버퍼 오버 플로 형태이다. 버퍼 오버 플로를 발생시켜 버퍼 속에 악성 코드를 삽입시키거나, 실행할 코드의 순서를 지시하는 포인터에 중복 쓰기(overwrite)하여 악성 코드를 가리키도록 하여, 공격자가 프로세스의 제어권을 장악하는 공격이다.

3.3.2 힙 오버 플로(Heap Overflow)

힙 오버플로는 스택 오버 플로와 비슷하나 생성하기가 더욱 어려운 공격이다. 힙은 동적으로 할당된 데이터를 저장한다. 스택에 할당된 데이터와 힙 할당된 데이터의 차이를 아래에서 보여 준다[4].

```
#include <stdlib.h>
int main(){
    char stack_buffer[256];
    char *heap_buffer = (char *) malloc(256 * sizeof(char));
    return 0;
}
```

힙은 스택처럼 반환 주소를 보통 포함하지 않는다. 그래서 스택이 사용되는 것보다 프로세스 상에서 통제권을 획득하는 것이 더욱 어렵다. 그러나 힙은 데이터나 함수에 대한 포인터(pointer)를 포함한다. 버퍼 오버 플로를 발생시켜 공격자로 하여금 프로세스의 실행을 조작할 수 있도록 허용하는 공격이다. 예를 들어, 중요한 시스템인 파일명을 가진 스트링 버퍼를 오버 플로시켜, 공격자는 그 시스템 파일에 중복쓰기를 위하여 프로세스를 이용할 수 있다.

3.4 DoS 공격

DoS(Denial of Service) 공격은 컴퓨터나 네트워크의 서비스를 사용할 수 없도록 불통시키거나 심각하게 성능을 저하시키는 공격이다. 다음과 같은 세 가지 주요 공격 형태가 있다.

3.4.1 호스트 기반

호스트 기반 DoS 공격은 컴퓨터 공격을 목표로 하며, 운영 체제, 응용 소프트웨어, 혹은 타깃 호스트 구성의 취약성을 이용한다.

1) 자원 호그

자원 호그(Resource Hog)는 컴퓨터상의 자원을 고갈시키기 위한 공격이다. CPU 타임이나 메모리 사용 같은 자원들이 보통 타깃이 된다. 예를 들어, fork bomb은 흔한 자원 호그이다. Fork bomb은 child process를 연속적으로 spawn하여 시간이 지남에 따라 더 많은 자원이 사용되게 된다. 이 공격은 쉽게 탐지된다. 운영체제의 취약성을 이용하는 다른 자원 호그로 CPU 자원을 소비하는 Snork이 있다[14].

2) Crasher

Crasher는 호스트 운영 체제의 취약점을 목표로 하며, 호스트 시스템을 충돌시켜 다시 시작(restart)하도록 설계된 호스트-기반 DoS 형태이다.

3.4.2 네트워크-기반

정상적인 사용자를 위한 대역폭이 감소되도록 패킷들로 네트워크를 범람(flooding) 시키는 것이다. 플러딩 공격의 세 가지 주요 방법은 아래와 같다.

- TCP Flood : TCP 패킷이 타깃으로 범람한다.
- ICMP Echo Request/Reply: ICMP 패킷들이 타깃으로 범람한다.

• UDP Flood : UDP 패킷들이 타깃으로 범람한다.

3.4.3 분산

DDoS 공격은 많은 수의 공격 호스트를 이용하여 하나의 타깃이나 타깃들로 동시 다발적으로 공격하는 형태이다. 마스터 노드가 타깃에 대한 공격을 개시하도록 데몬(daemon) 노드들을 제어하기 위하여 사용된다.

3.5 네트워크-기반 공격

여기서는 운영되고 있는 네트워크와 프로토콜에 대한 공격 유형을 기술한다.

3.5.1 스푸핑

공격자가 다른 합법적인 사용자로 위장하거나 희생 호스트로부터 기존 통신을 조작한다. MAC 주소 스푸핑과 IP 스푸핑 등 표준 TCP/IP 네트워크 프로토콜 스택에서 여러 가지의 스푸핑 방법이 있다.

3.5.2 세션 하이재킹

세션 하이재킹(Session Hijacking)은 공격자가 희생 호스트 사이에 일어나고 있는 세션을 장악하는 프로세스이다. 보통 TCP 계층에서 발생하며 Telnet과 FTP 같은 응용 세션을 장악하기 위하여 사용된다.

3.5.3 무선 네트워크 공격

WEP(Wired Equivalent Protocol)은 802.11x 네트워크에서 무선 네트워크상으로 전송되는 데이터를 암호화하기 위하여 사용되는 표준이다. 이 프로토콜은 스트림 암호(Stream Cipher)를 사용하는데, 24-비트 초기화 벡터가 재사용됨으로 인하여 공격자가 네트워크상의 트래픽을 복호화하기 위한 정보 수집을 위하여 사용될 수 있다. WEP가 가진 문제점을 해결하기 위하여 WEP 버전 2가 제안되었다.

3.5.4 웹 응용 공격

웹 응용 공격의 형태로는 아래와 같은 것이 있다[4].

(1) Cross Site Scripting: 웹 응용 내에 악성 목적을 위하여 사용되는 스크립트를 내장시킨다.
(2) Parameter Tampering: 공격자가 웹 응용을 구동하기 위하여 사용되는 파라미터를 식별하여 그 파라미터를 조작하기 위하여 URL 헤더를 수정하는 단순한 공격이다.
(3) Cookie Poisoning: 쿠키를 수정하여 웹 응용이 민감한 데이터를 주도록 속이는 것이다. 이 공격은 보통 쿠키가 암호화되기 때문에 큰 위협은 되지 않는다.
(4) 데이터베이스 공격: 웹 응용을 구동하는 하부 데이터베이스 접근을 목적으로 하는 웹 응용 공격이다.
(5) Hidden Field 조작: 공격자가 HTML 페이지를 다운로드하여 페이지 안에 포함된 숨은 필드를 변경하여 해당 페이지를 서버에 다시 올린다.

3.6 물리적 공격

물리적 공격은 컴퓨터와 네트워크에 대하여 물리적으로 행해지는 공격으로 본고에서는 기술하지 않는다.

3.7 기타 공격

• 패스워드 공격: 패스워드 추측/사전 공격, 전수(Brute Force) 공격, 구현 이용 공격 등이 있다.
• 정보 획득 공격: 스니핑(Sniffing), 매핑(Mapping), 보안 스캐닝 공격 등이 있다.

Ⅳ. 트래픽 플로관점 분류

트래픽 플로(Traffic Flow) 관점에서 비정상 트래픽 유형을 아래와 같이 분류할 수 있고 각각에 대하여 간단한 정의, 특징 및 예제를 제시한다[2].

4.1 ALPHA

• 정의 : 비정상적으로 높은 율로 점대점(pointto- point) 바이트 전달
• 특징 : 하나의 지배적인 쌍(소스 및 목적지)에 기인하는 B(Byte), P(Packet) 및 BP 트래픽 급상승(혹은 스파이크(spike))

• 예제 : 대역폭 측정 실험

4.2 DoS/DDoS(Denial of Service/Distributed DoS)

• 정의 : 한 희생자에 대한 (분산) 서비스 거부 공격
• 특징 : P, F(IP 플로), FP 트래픽의 급상승. 하나 이상의 소스 IP에서 한 목적지로 트래픽 집중. 다수의 OD(Origin-Destination) 플로를 포함 가능하며 보통 20분 이하 지속.
• 예제 : 대량의 패킷이 빈번한 DoS 공격 타깃인 포트(예, 포트 0)에 있는 하나의 IP 목적지 주소로 전송된다.

4.3 Flash Crowd

• 정의 : 자원/서비스에 대한 비정상적인 대규모 요구
• 특징 : 주요 목적지 IP 및 주요 목적지 포트로 F 혹은 FP 트래픽 급상승. 보통 잠시 동안만 유지되며 하나의 OD 플로로 제한됨.
• 예제 : 하나의 IP(포트 80)로 대규모의 웹 요구를 발생시키는 다수의 인스턴스

4.4 Scan

• 정의 : 취약 포트를 위하여 호스트 스캐닝(포트 스캔) 혹은 타깃 포트를 위하여 네트워크 스캐닝(네트워크 스캔)
• 특징 : 주요 소스로부터의 플로로써 유사한 수의 패킷을 가진, F 트래픽 급상승; 목적지 IP와 포트의 지배적인 결합이 없음. 다수의 OD 플로를 포함할 수 있고 보통 10분미만 지속.
• 예제 : 포트 139에 대한 네트워크 스캔(NetBIOS)

4.5 웜

• 정의 : 보안 결함을 이용한 네트워크를 통하여 확산되는 자기-전파(self-propagating) 코드
• 특징 : 주요 목적지 없이, 단지 주요 포트만 가지고 IP 플로 트래픽 급상승
• 예제 : 주요 포트 1433을 가진 플로 발견(MS SQL-Snake 웜에 사용된 것으로 알려짐)

4.6 점-대-다중점

• 정의 : 한 서버에서 많은 사용자로 콘텐츠 분배
• 특징 : 주요 소스로부터 많은 목적지로, 모두 같은 (잘 알려진) 포트로 P, B 혹은 BP 트래픽 급상승
• 포트 119에서 대규모 목적지 집합으로 단일 서버 브로드캐스트(뉴스 nntp 서비스)

4.7 outage

• 정의 : OD 쌍 사이에서 교환되는 트래픽을 감소시키는 이벤트
• 특징 : BFP 트래픽이 보통 0까지 감소됨. 장기간 (수시간) 지속될 수 있으며 모든 인스턴스에서 다수의 OD 쌍에 영향을 미침.
• 예제 : 계획된 유지보수 다운 시간의 인스턴스, CHIN PoP로 부터의 측정 실패

4.8 입구-시프트(Ingress Shift)

• 정의 : 고객이 한 입구점으로부터 다른 입구점으로 트래픽을 이동한다.
• 특징 : 한 OD 플로에서의 F 트래픽 감소 및 다른 플로에서 F 트래픽 급상승. 지배적인 속성 없음. 다수의 OD 플로 포함.
• 예제 : 멀티홈 Abilene 고객 CALREN이 LOSA outage 동안 LOSA로부터 SNVA로 트래픽을 이동시킴.

위에서 보여주는 것은 탐지된 비정상 트래픽 유형이 아주 광범위하다는 것이다. 이들을 분류하여 보면 아래와 같다.

• 비정상 종단-사용자 행위 : Alpha, Flash Crowds, 점-대-다중점
• 악성 종단-사용자 행위 : 사실상의 DoS, DDoS, 웜 혹은 잠재적인 악성 스캔
• 운용 이벤트 : 장비 outage(outage), 다운스트림 트래픽 엔지니어링(입구점 이동)

위의 분류는 IP 네트워크에서 표본 된 플로 측정으로부터 탐지될 수 있는 네트워크에 걸친 트래픽 비정상의 범위를 특성화한 첫 번째 연구이다[2].

V. 새로운 공격유형

5.1 개요

혼합 공격(Blended Attack)이 예전부터 있어 왔지만, 코드 레드(Code Red)와 님다(Nimda)와 같은 공격으로 최근 부상하고 있다. 혼합 공격은 다수의 위협을 포함하는 공격이다. 예를 들어 다수의 전파 수단이나 다수의 공격 페이로드를 가질 수 있다.

혼합 공격의 첫 번째 발생은 1988년 일어난 모리스 웜으로 볼 수 있다. 모리스 웜은 유닉스 기반 시스템에서 다수의 취약성을 공격하고 그것을 통하여 전파되었다. 코드 레드와 님다 같은 공격도 다수의 취약성을 이용하고 다수의 공격을 개시하는 혼합 공격 유형으로 볼 수 있다.

혼합 공격이 주요한 보안 위협의 한 가지가 되었으며 앞으로도 지속적으로 중요한 문제가 될 것으로 예상된다. 본 장에서는 일반적으로 잘 알려진 코드 레드와 님다에 대한 기술은 생략하고 앞으로 예측되는 웜의 새로운 공격 유형에 대하여 살펴본다.

5.2 웜의 새로운 공격 유형

최근 웜에 관한 백서, 학회에서의 발표내용과 개인적인 토의 등을 통하여 [15]에서는 다양한 파괴적인 특성을 가진 웜들의 출현에 대비하여야 한다고 기술하고 있다. 본 절에서는 이런 새로운 웜 유형의 특징에 대하여 분석한다.

5.2.1 복수 플랫폼 웜(Multi-platform Worms)

대부분의 웜들은 보통 웜 당 한 형태의 운영체제를 공격하기 때문에, 관리자는 적절한 방어를 위하여 한 형태의 시스템에 패치를 설치하면 된다. 그러나 가까운 미래에 슈퍼 웜(Superworm)은 윈도우, 리눅스, 솔라리스, BSD 및 다른 복수 운영체제 형태를 이용할 것이다. 이 모든 것이 하나의 웜 탄두 안에 포함된다.

복수 플랫폼 웜에 대한 방어를 위하여 운영체제의 형태에 관계없이 모든 시스템에 패치를 할 필요가 있다. 이미 인터넷에서는 작은 수이나마 복수 플랫폼 웜이 출현하였다. 2001년 5월 Sadmind/IIS 웜이 선 솔라리스와 마이크로소프트 윈도우를 목표로 인터넷을 통하여 전파된 바 있다. 이 웜은 솔라리스 머신의 원격 관리를 협조하기 위하여 사용되는 sadmind 서비스를 이용하여, 희생 머신으로부터 마이크로소프트 IIS 웹 서버로 확산되고, 다시 솔라리스 머신으로 전파되는 주기를 계속한다.

5.2.2 복수 익스플로잇 웜(Multi-exploit Worms)

지금까지의 웜은 대부분 한 시스템의 하나의 취약성을 이용하고, 새로운 희생 머신으로 확산하는 형태였다. 어떤 새로운 웜들은 많은 수의 네트워크-기반 응용의 허점을 이용하여 여러 가지 방법으로 시스템에 침투한다. 하나의 웜이 한 웜 탄두에 모든 것을 갖추고 5, 20 혹은 더 많은 취약성을 이용할 수 있을 것으로 예측하였다. 이용할 수 있는 취약성이 많을수록 더욱 성공적으로 빠르게 웜이 확산될 것이다. 한 시스템이 어떤 취약점에 대하여 패치가 되었더라도 복수 익스플로잇 웜은 여전히 다른 취약성을 이용하여 시스템을 장악할 수 있을 것이다. 지금까지의 가장 성공적인 복수 익스플로잇 웜의 예로는 Nimda를 들 수 있으며, 어떻게 대응하는지에 따라서 12 가지의 다른 방법으로 시스템으로 확산될 수 있다.

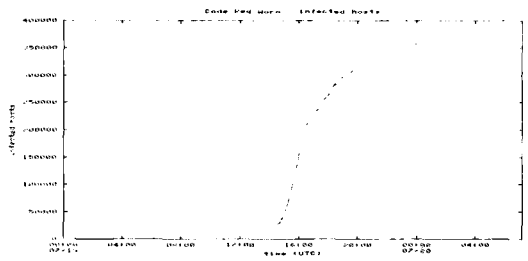
5.2.3 제로-데이 익스플로잇 웜

현재까지의 대부분의 웜들은 시스템 공격을 위하여 이미 알려진 취약성을 사용하였다. 코드 레드와 님다 같은 웜들도 수개월 전에 발견된 버퍼 오버 플로와 다른 익스플로잇을 사용하여 확산되었다. 이렇게 이미 알려진 취약성에 대하여는 미리 패치를 제작하여 배포할 수 있다.

그러나 미래에는 소위 "제로-데이(zero-day)" 익스플로잇을 사용하여 시스템을 파괴할지도 모른다. 이 경우 패치가 이용 가능하지 않기 때문에 어떻게 웜이 확산되는지 알기 위하여 더 많은 시간이 소요될 것이다.

5.2.4 고속 확산 웜

웜은 원래 빠른 확산을 시도한다. 웜의 한 인스턴스(instance)는 새로운 희생자를 스캔하기 위하여 사용되고, 정복되면 더 많은 타깃을 스캔한다. 그러므로 웜은 지수적(exponential) 기반으로 확산한다. [그림 3]은 코



(출처: http://www.caida.org/)

〔그림 3〕 관측된 코드 레드 전파-감염 호스트의 수

드 레드 웜에 대한 감염 호스트의 수를 보여준다.

[그림 3]에서 보면, 웜의 전파를 세 가지의 단계로 대략 구분할 수 있다: 늦은 시작 단계(slow start phase), 빠른 확산 단계(fast spread phase), 늦은 종료 단계(slow finish phase). 많은 호스트들이 감염되고 다른 호스트를 감염시키는데 참여하고 난 후, 웜은 취약 호스트들이 빠르게 거의 선형적인 속도로 감염되는 빠른 확산 단계에 들어간다. 전파 율은 모든 취약적 호스트의 약 80%가 감염될 때 감소되기 시작하며, 대부분의 취약 호스트들이 감염된 때에, 웜은 늦은 종료 단계에 들어간다.

광대역통합망(BcN : Broadband convergence Networks)과 같은 초고속 통신망에서는 웜의 확산을 가속화 시킬 수 있다. 네트워크 대역폭이 증가함에 따라, 웜의 전파에 대응할 수 있는 시간도 단축된다. 따라서 웜의 전파 특성에 대한 이해와 웜을 조기에 탐지하고 격리할 수 있는 메커니즘에 대한 연구가 시급하다[16].

코드 레드나 슬래머와 유사한 웜은 고속망에서 훨씬 높은 감염률을 가질 수 있고 타겟 집단을 더욱 빠르게 포화시킬 수 있다. 고속망에서는 감염된 호스트가 잠재적인 타겟과 통신하는 것을 용이하게 만들어 단순역학 모델에서 $\beta(1-a(t))$를 증가시킬 수 있다. 단순 역학 모델은 다음과 같이 재배열 될 수 있다:

$$T_p = \frac{\ln P(N-J(0)) - \ln (1-P)J(0)}{\beta N}$$

여기서 T_p는 모집단의 P 부분, 즉 PN 호스트를 감염시키기 위하여 걸리는 시간을 나타낸다. 이 결과는 만약 웜이 조사 율(probe rate)을 두 배로 하기위한 대역폭을 발견한다면, 즉 감염 파라미터 β를 실제적으로 두 배로 한다면, 반 정도의 시간으로 목표 집단을 포화시킬 수 있다는 것을 의미한다. 따라서 고속 망에서 웜은 더 높은 감염률을 얻을 수 있고 목표 집단을 더욱 빠르게 포화시킬 수 있다.

[17]에서는 적어도 세 가지의 IPv6 설계 선택이나 타협점(tradeoff)을 사용하여 IPv6 네트워크에서 웜의 전파를 가속화시킬 수 있다고 기술하고 있다.

• 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.

RCS 모델과 그것의 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 보여준다. 세 가지의 가속화 요인 중에서 가장 큰 요인은 IPv6 네트워크의 설계 선택 및 타협점으로부터 생겨난 것으로 지적하고 있다.

5.2.5 폴리모픽 웜(Polymorphic Worms)

폴리모픽 웜(PW)은 침입탐지를 회피하고, 역공학 분석을 따돌리고, 필터를 통과하기 위하여 외양을 변경하는 웜을 의미한다. 다른 웜 인스턴스의 바이트 시퀀스를 완전하게 다르게 보이게 하는 웜이다. 폴리모픽 프로그램은 소프트웨어 코드를 스크램블링하여 외양을 동적으로 변경할 수 있으며, 새로운 소프트웨어가 완전히 다른 명령어로 구성되어 있을지라도 그 코드는 여전히 정확히 같은 기능을 가진다. 폴리모피즘은 단지 외양만 변경되고 코드의 기능은 변경되지 않으며, 웜의 페이로드가 탐지 시그너처와 일치하지 않도록 전체 웜을 다른 변화된 버전으로 자동적으로 변형시킨다. 웜이 폴리모픽으로 되면 각 세그먼트는 on the fly로 새로운 코드가 생성되며, 다른 외양을 가져 탐지를 어렵게 만든다. 그러므로 같은 기능을 가지면서 수백만 개의 유일한 웜 세그먼트가 네트워크에 산재 할 것이다. 통상적인 방법으로는 원래의 웜 코드를 난수 키를 가지고 암호화하고, 키를 위해 매번 인스턴스와 함께 변경되는 복호기를 생성한다. 폴리모픽 엔진에 의해 수행되는 웜 코드는 변경되지 않는다.

5.2.6 메타모픽 웜(Metamorphic Worms)

폴리모피즘(Polymorphism)을 이용하여 외양을 변경할 뿐 아니라, 새로운 웜은 metamorphosis(변형 작용)를 이용하여 또한 그들의 행위를 동적으로 변경시킬 것으로 예측된다[15]. 이 기법을 사용하면 추가적인 공격 능력이 웜 속에 숨겨질 수 있다. 폴리모픽 기술은 웜의 기능성은 같이 유지하면서 웜 코드를 변경하는 반면에, 메타모픽 코드는 웜의 기능성도 실제로 변경한다. 메타모픽 웜은 역공학이 더욱 어렵게 때문에 공격자에게 유리하고 그러므로 방어가 힘이 든다. 이 메타모픽 기법이 폴리모피즘과 결합되어 사용되면 이러한 웜들은 훨씬 더 방어하기가 어려울 것이다.

Ⅶ. 맺음말

정보통신망에서 비정상 행위를 탐지하고 이해하는 것은 아직까지 완전히 해결되지 않고 있는 어려운 문제 중의 하나이다. 각종 웜에 의하여 발생되는 비정상 트래픽에 의한 위협도 증가되고 있다. 따라서 본 논문에서는 비정상 트래픽에 의한 새로운 네트워크 공격 유형에 대하여 제시하였다. 먼저 비정상 트래픽 유형 분석을 위하여 공격 형태 관점과 트래픽 플로 관점에서 기술하였다. 새로운 공격 유형 분석에서는 다양한 파괴적인 특성을 가진 앞으로 출현이 예상되는 웜의 유형에 대하여 기술하였다. 악성 웜은 확산 능력과 손상 규모를 증가시키면서 지속적으로 진화되고 있다. 앞으로의 웜은 다양한 파괴적인 특성을 가질 것이며, 이들의 형태는 멀티 플랫폼, 멀티 익스플로잇, zero-day, 폴리모픽, 메타모픽 등의 형태가 될 것이다. 국내에서도 광대역통합망 환경에서 새로운 공격 유형에 효과적으로 대처하기 위한 대응방법과, 웜의 발생 시 웜의 확산을 방지하기 위한 웜 봉쇄 기술에 대하여 체계적인 연구가 필요하다고 사료된다.

참고문헌

[1] Anukool Lakhina, Mark Crovella, and Christophe Diot, "Diagnosing Network-Wide Traffic Anomalies", SIGCOMM'04, Aug. 30-Sep.3, 2004. Portland, Oregon, USA.

[2] A. Lakhina, M. Crovella, and C. Diot, "Characterization of Network-Wide Anomalies in Traffic Flows", IMC '04, Taormina, Sicily, Italy, Oct. 2004.

[3] Howard F. Lipson, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. Technical report, CERT Coordination Center, Nov. 2002.

[4] Simon Hansman, A Taxonomy of Network and Computer Attack Methodologies, University of Canterbury, New Zealand, Nov. 2003.

[5] V. Yegneswaran, P. Barford, and J. Ullrich, "Internet Intrusions: Global Characteristics and Prevalence", In ACM SIGMETRICS, San Diego, June 2003.

[6] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, and C. Diot, "Characterization of Failures in an IP Backbone", In IEEE INFOCOM, Hong Kong, April 2004.

[7] N. Weaver. Warhol Worms: The Potential for Very Fast Internet Plagues, http://www.cs.ber-

keley.edu/~nweaver/warhol.html.

[8] A. Hussain, J. Heidemann, and C. Papadopoulos, "A Framework for Classifying Denial of Service Attacks", In ACM SIGCOMM, Karlsruhe, Aug. 2003.

[9] J. Mirkovie and P. Reiher, "A Taxonomy of DDoS Attacks and Defense Mechanisms", ACM CCR, April 2004.

[10] P. Barford, J. Kline, D. Plonka, and A. Ron, "A Signal Analysis of Network Traffic Anomalies", In Internet Measurement Workshop, Marseille, Nov. 2002.

[11] N. Duffield, C. Lund, and M. Thorup, "Estimating Flow Distributions from Sampled Flow Statistics", In ACM SIGCOMM, Karlsruhe, Aug. 2003.

[12] J. Jung, B. Krishnamurthy and M. Rabinovich, Flash Crowds and Denial of Service Attacks: Characterization and Implications for CDNs and Web Sites. In *World Wide Web Conference*, Hawaii, May 2002.

[13] Glenn Gebhart, Worm Propagation and Countermeasures, SANS Institute, 2004.

[14] Internet Security Systems, ISS Security Advisory: "Snork" Denial of Service Attack Against Windows NT RPC Service. 1998. http://xforce.iss. net/xforce/alerts/id/advise9.

[15] Ed Skoudis and Lenny Zeltser, Malware: Fighting Malicious Code, Prentice-Hall, 2004, (Chapter 2: Virus, 3: Worm).

[16] Xuan Chen and John Heidemann, Detecting Early Worm Propagation through Packet Matching, Technical Report ISI-TR-2004-585, 2004.

[17] Jing Yang, "Fast Worm Propagation in IPv6 Networks".

<著者 紹介>

전 용 희 (Yong-Hee Jeon)

1971.3~1978.2 고려대학교 전기전자전파공학부

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

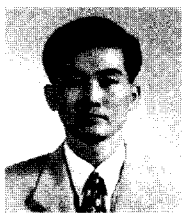
1992.10~1994.2 한국전자통신연구원 광대역통신망연구부 선임연구원

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



장 종 수(Jong-Soo Jang)

1984년 경북대학교 전자공학과 학사,

1986년 경북대학교 대학원 전자공학과 석사,

2000년 충북대학교 대학원 컴퓨터공학과 박사,

1989년 7월~현재 한국전자통신연구원 정보보호연구단 보안응용그룹 그룹장/책임연구원,

관심분야 : Network Security, 정책기반보안관리, 비정상트래픽탐지, 유해정보차단