情 報 保 護 學 會 誌
第 15 卷 第 2 號, 2005. 4

인터넷 웜(Worm) 탐지기법에 대한 연구

신 승 원*, 오 진 태*, 김 기 영*, 장 종 수*

요 약

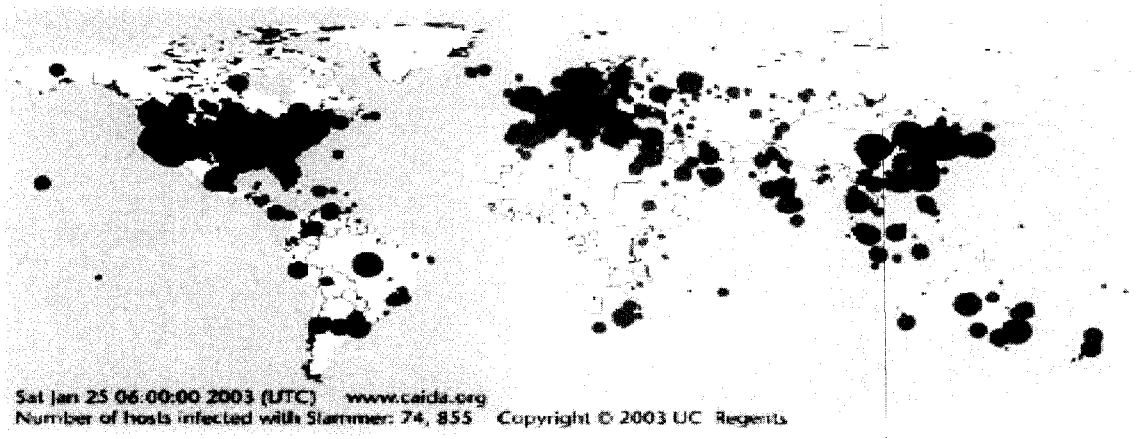
오늘날 네트워크 보안 기술은 해커의 침입 탐지 및 제어, 분산 서비스 거부 공격의 방지 등 많은 분야에서 발전하여 왔다. 그러나, 최근 많은 문제를 발생시키면서 등장한 인터넷 웜은 기존의 네트워크 보안 장비들을 무력화 시키며 인터넷 상에 연결된 많은 호스트들을 감염시키고 동시에 네트워크 자원을 소모시켜 버렸다. 실상 초기의 웜은 작은 규모의 네트워크에서 퍼지는 정도 일뿐 심각한 피해를 주는 경우는 거의 없었고 따라서 이에 대해서 심각한 대비책 등을 생각하지는 않았다. 그러나 2001년 발생한 CodeRed 웜은 인터넷에 연결된 많은 컴퓨터들을 순식간에 감염시켜 많은 경제적, 물질적 피해를 발생시켰고, 그 이후 2003년 1월에 발생한 Slammer 웜은 10분이라는 짧은 순간 안에 75000 여대 이상의 호스트를 감염시키고 네트워크 자체를 마비시켰다. 특히 Slammer 웜은 국내에서 많은 피해를 유발시켰기에 더더욱 유명하다. 명절 구정과 맞물려 호황을 누리던 인터넷 쇼핑 몰과, 인터넷 금융 거래를 수행하던 은행 전산소 등을 일시에 마비시켜 버리면서 경제적으로도 실질적인 막대한 피해를 우리에게 주었다. 이런 웜을 막기 위해서 많은 보안 업체 및 연구소들이 나서고 있으나, 아직은 사전에 웜의 피해를 막을만한 확실한 대답을 얻지 못하고 있다. 본 논문에서는, 현재 수행하고 있는 여러 웜의 탐지기법에 대해서 조사한 결과를 설명하고, 이어서 본 연구소에서 수행하고 있는 웜의 탐지 기법에 대해서 설명하고 간단한 탐지 결과를 보일 것이다.

Ⅰ. 서 론

네트워크의 양적 그리고 질적인 진화는 우리가 가진 많은 것을 변화 시켰다. 수 Kbps에 이르던 전송 속도는 Mbps를 넘어서 이제는 Gbps를 넘어서고 있으며, 처음 두 대학간을 연결하는 것으로 시작된 인터넷은 전 세계를 연결하고 있다. 가히 전 세계의 거의 모든 사람이 인터넷이라는 매체로 서로 연결되어 있으며, 동시에 누구나 이런 기회를 가질 수 있는 환경이 된 것이다. 그리고 이런 진화와 발전은 인터넷을 이용하는 사람들에게 많은 기회를 안겨 주고 있다. 서로 마주보며 사고팔던 물건들을 인터넷 상에서 직원이나 실제 물건 창고 없이, 사고 팔 수 있게 됐으며, 돈을 찾고 예금하기 위해 은행으로 향하던 사람들은 간단하게 웹 브라우저를 통해서 돈을 넣고 옮기고 확인할 수 있게 되었다. 그러나, 이런 기회의 세계, 인터넷에도 역시 수많은 위험이 도사리고 있는 현 세상처럼 그 자체로도 여러 가지 위험성을 지니고 있다. 안전하리라 믿었던 인터넷이었지만 사람들은 자신의 개인 정보를 타인이 훔쳐보는 것을 겪어야 했고, 상업적 이익을 위해 구축한 많은 인터넷 서버들이 분산 서비스 거부 공격 (DDOS) 이나 해커들의 침입에 맥없이 무너져 멈춰 버리는 것을 경험하게 되었다. 가상의 세계에서 가상의 경제가 아닌 실제 돈이 오가고 개인의 실제 정보가 오가는 상황에서 이러한 피해는 현실의 피해와 별반 차이가 없을 것이다. 따라서 이러한 피해를 막기 위하여 네트워크 보안 업체들이 등장하고, 바이러스 백신, 방화벽, 침입 탐지/방지 시스템, 통합 보안관리 시스템 등등이 등장하게 되었다.

이러한 시스템들은 여러 해커들의 침입 시도나 무분별한 분산 서비스 거부 공격 (DDOS)들로부터 우리의 시스템들을 잘 보호해 왔고, 앞으로도 그럴 것이다. 그러나 이런 보안 시스템들도 최근 (처음 등장은 1988년부터, 그러나 실제 사람들에게 많은 영향

* 한국전자통신 연구원 책임연구원 (sigcomm@naver.com, {showme, kykim, jsjang}@etri.re.kr)



〔그림 1〕 Slammer Worm의 감염도 (출처: CAIDA www.caida.org)

력을 끼친 것은 1999년 이후) 네트워크상에 급속하게 퍼지고 있는 인터넷 웜 (Worm) (혹은 웜)에 대해서는 1차적인 차단도 쉽게 하지 못하고 있는 실정이다. 인터넷 웜 (Worm)은 인터넷 상의 다른 네트워크 공격과는 달리 스스로 자신을 복제하여 네트워크상에 연결된 다른 컴퓨터들로 스스로 자신을 전송하는 프로그램이다.

맨 처음 Morris 웜이 등장하였을 때는 그 속도나 파급력이 크지 않았으나, 2001년의 CodeRed나 2003년의 Slammer 웜 같은 경우 대다수의 보안 장비들을 무력화 시키고, 급속도로 네트워크로 퍼져 나가서 엄청난 사회적 피해를 주었다. Slammer 웜의 경우, 전 세계에 미친 여파는 엄청났다. 그림 1에서 볼 수 있는 바와 같이 10분 동안, 전 세계에 있는 75000개 이상의 호스트를 감염시켰으며, 스캐닝을 위한 엄청난 양의 UDP 패킷은 무방비 상태로 있던 수많은 호스트들을 감염시켰을 뿐만 아니라 네트워크 자체를 마비시켜 버렸다. 특히 국내의 경우 2003년 1월 25일 구정과 맞물려 1.25대란이라 불리게 될 정도로 많은 경제적 사회적 피해를 안겨 주었다.

그렇다면 이렇게 많은 피해를 주고 있는 웜은 어떤 것이고 도대체 어떤 방법으로 탐지를 해야 하는 것일까? 현재까지 완벽한 답은 아직 없지만, 웜에 대한 탐지 및 대응을 위해서 많은 보안 회사들이 팔을 걷어 붙여 나섰고, 많은 연구 기관이나 대학에서 이들에 대한 조사 및 연구가 이루어지고 있다. 본 논문에서는 이런 현재의 연구와 실제 사례를 들어 보이려고 한다. 먼저, Ⅱ장에서는 인터넷 웜에 대한 정의와 소개, 그리고 현재 알려진 웜의 종류 등에 대해서 언급할 것이다. 그리고 Ⅲ장에서, 웜의 탐지 방법에 대한 다양한 연구들을 언급할 것이며, 이어서 Ⅳ장에서 현재 ETRI의 정보보호 연구단에서 수행하고 있는 웜 탐지 기법에 대해서 설명할 것이다. 그리고 마지막으로 Ⅴ장에서 결론을 내릴 것이다.

Ⅱ. 인터넷 웜 (Worm)에 대한 소개

본 장에서는 인터넷 웜에 대한 간략한 정의와 그리고 이들의 종류 등에 대해서 언급할 것이다.

2.1 인터넷 웜 (Worm)이란 무엇인가?

인터넷 웜(Worm) 이란 무엇일까? 다양한 정의들이 있지만, 가장 보편적으로 쓰이는 정의는 다음과 같다.

"인터넷 웜 (Worm)은 스스로 자신을 복제하여 네트워크상에 연결된 다른 컴퓨터들로 자신의 복제 본을 전송하여 다른 컴퓨터를 감염시키는 프로그램이다."

이런 정의 때문에 바이러스와 혼동하게 되는데, 바이러스와 인터넷 웜은 다르다. 인터넷 웜은 바이러스처럼 스스로 자신을 복제하긴 하지만, 바이러스는 보통 사람의 행동에 의해서 (파일 복사 및 실행 등) 퍼지게 되지만, 웜의 경우, 자신을 스스로 복사해서 네트워크상에 연결된 다른 호스트에 스스로를 전파 시킨다는 점에서 차이를 보인다. 보통 웜의 경우 스캐닝 단계와, 전파 단계를 통해서 감염된다. 스캐닝 단계는 웜이 자신이 감염시킬 수 있는 네트워크에 연결된 호스트를 찾는 단계로, TCP 프로토콜을 사용하는 웜의 경우 TCP SYN 패킷을 보내서 응답을 받아서 스캐닝 정보를 받곤 한다. UDP의 경우엔 UDP Req-

uest 메시지를 보내고 이에 대한 응답 메시지를 통해서 그 정보를 확인할 수 있다. 그리고 좀 더 진화한 웜의 경우 스캐닝과 감염을 동시에 시키는 경우도 있다. 특히 UDP 프로토콜을 이용하는 웜이 이런 경우가 많은데, 스캐닝 패킷에 자신의 복제 본을 담아서 스캐닝을 하면서 응답을 하는 호스트에 바로 자신의 복제 이미지를 전송하게 되는 것이다.

2.2 인터넷 웜 (Worm)의 분류

많은 웜이 나타났지만, 1999년 이후로 급작스럽게 나타난 관계로 체계적으로 웜을 분류한 자료가 많지 않았다. 2003년에 발표된 몇 편의 논문들을 통해서 웜을 분류하는 몇 가지 방법들을 알 수 있다. 웜을 분류하는 시도는 크게 웜의 외부적인 특성 (전파되는 방식)을 바탕으로 분류한 것과[1], 웜 외부적인 특성과 내부의 동작을 모두 고려하여 분류한 방법이 있다.[2] 웜 내부의 동작을 바탕으로 분류하는 것은 그 분석과 내용이 복잡하기에 우선 분류하기 쉬운 외부적인 특성을 바탕으로 분류한 예를 들어 보자. Symantec 사의 Darrell M. Kienzie와 Network Associates 사의 Matthew C. Elder는 웜을 크게 E-Mail 웜, Windows File Sharing 관련 웜, 그 밖의 웜들의 세 가지로 나누었다. 먼저 E-Mail 웜은 말 그대로 E-Mail을 통해서 전파되는 웜에 대한 것이다. E-Mail에 첨부된 파일 형태로 전파되는 것으로, 사용자가 E-Mail을 보고 실행파일을 실행해야만 전파되는 것부터, E-Mail을 여는 순간 감염되는 것 까지 다양한 종류가 있다 이런 웜들로는 Christmas Tree 웜이나 Sircam등의 웜이 있다. 그리고 Windows File Sharing 관련 웜의 경우 운영체제가 Windows 계열인 경우 발생하는 것으로서, Windows 운영체제에서 File Sharing (파일 공유) 관련 네트워크 서비스를 실행 시켰을 때 이들을 통해서 감염되는 웜에 대한 것이다. 이런 웜들로는 NetLog 웜이나, Shorm 웜 등이 있다. 그리고 마지막으로 일반적인 웜들은 위의 두 가지 경우가 아닌 다른 방식으로 전파되는 웜들을 말하는 것으로, 우리에게 많이 익숙한 CodeRed나 Slammer 등과 같은 웜들이 있다.

그리고 좀 더 복잡하게 분류한 방식은 UC. Berkeley 대학의 Nicholas Weaver와, ICSI의 Vern Paxson, Silicon Defense사의 Stuart Staniford, 그리고 MIT Lincoln Lab의 Rebert Cunningham이 제안한 것이다. 이들은 웜을 분류할 때 5가지 분류를 이용하였는데, 그 내용을 보면, 먼저 웜이 자신이 감염시키고자 하는 호스트를 찾는 방법에 의한 분류, 그리고 웜이 전파되는 네트워크 매개체에 의한 분류, 그리고 웜이 활동하는 방식에 의한 분류, 그리고 웜의 내부에 있는 데이터에 대한 분류, 그리고 마지막으로 웜 프로그램의 의도와 같은 사회학적 분류 체계를 작성하였다. 그러나, 이들은 실제로 웜을 분류하여 보인 것이 아니라 웜을 분류할 수 있는 체계적인 분류 방법을 제시한 것으로 차후 발생하는 웜이나 기존의 웜을 분류하고자 할 때 하나의 기준으로 활용할 수 있을 것이다. 이에 대한 좀 더 자세한 설명은 [2]에 서술되어 있다.

Ⅲ. 인터넷 웜 (Worm) 탐지 기법들

앞장에서 서술한 웜의 정의와 웜의 종류에 대한 것을 바탕으로 이번 장에서는 웜을 탐지하는 기법들에 대해서 알아볼 것이다.

3.1 알려진 웜에 대한 탐지 기법

말 그대로 이미 널리 알려진 웜에 대한 탐지를 위한 것이다. 이것은 기존의 패턴 매칭 반식으로 네트워크 공격을 탐지하던 것으로 대부분의 침입 탐지/방지 시스템에서 적용이 가능하다. 이는 먼저 웜이 퍼지고 난 후 이들에 대한 정보를 수집해서 이런 정보를 바탕으로 웜에 대한 Signature를 생성한 후 이것을 가지고 탐지하는 방식이다. 예를 들어, 이미 널리 알려진 CodeRed 웜이나 Slammer 웜의 경우, 많은 사람들이 그에 대한 분석을 수행하여서, 그 내부에 특정한 ASCII 값으로 이루어진 패턴을 찾아 낼 수 있었다. 그리고 이러한 패턴은 Signature가 되어, 차후에 다른 패킷들 내에서 이러한 패턴이 발견되면 이를 CodeRed 웜 혹은 Slammer 웜으로 간주하게 되는 것이다. 이러한 방식은 웜을 False-Positive가 적게 (정확하게) 탐지할 수 있는 확률이 높다는 장점이 있으나, 반대로 이미 알려진 웜에 대해서만 탐지가 가능하다는 단점이 있다. 따라서, 새로 발생하는 웜에 대해서는 탐지할 수 없고, 만약 Slammer 웜처럼 엄청난 속도로 네트워크에 연결된 호스트를 감염시키면서 네트워크를 동시에 마비시키는 웜들에 대해서는 그 대처가 한계가 있다고 할 수 있다.

이 탐지 방법은 Open Source 네트워크 침입 탐지 시스템인 Snort[3]를 비롯하여, 대부분의 Signature 기반의 상용 침입 탐지 혹은 방지 시스템들에서 적용이 가능하다.

3.2 비정상 트래픽 분석을 이용한 탐지

이 방법은 알려진 웜보다는 알려지지 않은 새로운 웜의 가능성을 차단하기 위한 것으로, 네트워크 상을 오가는 트래픽의 특성을 분석하고 이들 중 웜으로 생각되는 트래픽 패턴을 찾아서 이를 웜 공격으로 간주하는 것이다. 이러한 방식은 이전에 발생하지 않은 웜 공격이라 할지라도 미리 발견하여 차단할 수 있다는 장점이 있다. 따라서, Slammer 웜과 같은 웜 역시 조기에 발견하여 사전에 차단할 수 있게 된다. 그러나, 이러한 방법은 아직 정확한 탐지가 어렵고 (오탐율이 상대적으로 높음) 그 구현이 쉽지가 않다는 단점이 있다. 그러나, 현재 알려진 웜을 탐지하는 것 만으로는 네트워크를 보호할 수 없기 때문에 비정상 트래픽 특성 분석을 이용한 탐지 방법은 현재 많은 연구가 되고 있으며 앞으로도 계속 발전하리라 본다. 본 장에서는 현재 각 연구소 및 대학 등지에서 연구되고 있는 비정상 트래픽 특성 분석을 이용한 탐지 방법에 대해서 좀 더 알아보려 한다.

3.2.1 Real Time Anomaly Detection 프로젝트 (MIT)[4,9]

MIT에서 이루어지고 있는 연구로 수학적인 알고리즘 (대표적으로 TRW 알고리즘[4])을 이용해서 트래픽 패턴을 분석해서 웜을 찾아내는 방법을 제시하고 있다. 이 프로젝트에서 가장 대표적인 TRW 알고리즘은 세션관련 정보를 이용하여 웜을 탐지하는 방식이다. 예를 들어, TCP 프로토콜의 경우, 처음 연결을 위하여 SYN 패킷을 보내게 되는데, 웜 역시 이와 같은 동작을 수행하여야 한다. TRW 방식은 이러한 TCP SYN 과 같은 패킷들을 우선적으로 스캐닝 동작으로 간주하고 이 정보를 바탕으로 Sequential Hypothesis Testing 방식을 이용해서 비정상 트래픽 패턴을 찾아내게 된다.

간단하게 TRW 알고리즘에 대해서 설명하면 다음과 같다. 먼저, Y라는 값을 어떤 특정 호스트의 TCP 연결의 성공과 실패를 나타내는 연속적인 값이라고 하자. 그러면, Y는 다음과 같이 나타내어 질 수 있다.

$Y_i = S(0)$, 연결이 성공한 경우

$Y_i = F(1)$, 연결이 실패한 경우

그러면, 우리는 위의 수식을 바탕으로 어떤 호스트 H에 대해서 스캐닝이 발생한 경우와 아닌 경우를 다음과 같은 확률로 나타낼 수 있다.

$$\Pr[S \mid H_{\text{scanning}}] < \Pr[S \mid H_{\text{benign}}]$$

$$\Pr[F \mid H_{\text{scanning}}] > \Pr[F \mid H_{\text{benign}}]$$

그리고 이에 대한 Likelihood Function을 작성하여 본다면 다음과 같이 정의할 수 있다.

$$\phi(S) = \frac{\Pr[S \mid H_{\text{scanning}}]}{\Pr[S \mid H_{\text{benign}}]} < 1$$

$$\phi(F) = \frac{\Pr[F \mid H_{\text{scanning}}]}{\Pr[F \mid H_{\text{benign}}]} > 1$$

그리고, 위의 두 식을 Y에 대한 식으로 변환 하면 다음과 같이 정리할 수 있다.

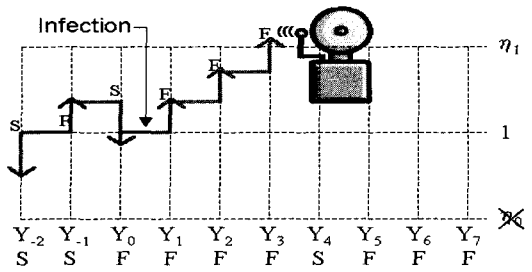
$$\phi(Y_i) = \frac{\Pr[Y_i \mid H_{\text{scanning}}]}{\Pr[Y_i \mid H_{\text{benign}}]}$$

$$\Lambda(\boldsymbol{Y}) = \prod_{i=1}^{n} \frac{\Pr[Y_i \mid H_{\text{scanning}}]}{\Pr[Y_i \mid H_{\text{benign}}]} = \prod_{i=1}^{n} \phi(Y_i)$$

이렇게 정리된 수식을 바탕으로 실제 호스트 H에서 TCP 연결이 발생하는 경우, 만약 연결이 성공하게 되면 위의 $\Lambda(Y)$는 TCP 연결이 성공하는 경우 양의 값(+)를 나타내게 되고, 반대로 연결이 실패하는 경우 음의 값(-)을 나타내게 된다. 따라서, 어떤 호스트 H에서 TCP 연결에 대한 SYN 패킷을 내보낼 때 마다 위의 값이 변하게 되고, 호스트 H에서 계속 TCP 연결을 실패하는 경우 이 값이 계속 커지게 된다 (양의 값이 계속 증가하기 때문에). 이 때 이 커지는 값이 Threshold 값보다 크게 되면 아래의 그림 2처럼 웜 공격으로 간주하게 된다. TRW 방식은 수식은 복잡하지만, 실제 구현 복잡도는 높지 않으며, 빠르게 TCP 웜을 잡아 낼 수 있다는 장점이 있다. 그러나, UDP 웜에 대한 탐지 방법이 없다는 단점이 있다.

3.2.2 DEWP (Detecting Early Worm Propagation through Packet Matching) 방식 (ISI)[5]

DEWP (Detecting Early Worm Propagtion



〔그림 2〕 TRW 방식을 이용한 탐지 예제

through Packet Matching) 방식은 ISI (Informa-tion Sciences Institute)에서 제안한 방식으로, 네트워크 상에 유입되는 트래픽 들을 특정 패턴들로 분류하여 웜을 탐지하는 방식이다. 보통 정상적인 트래픽에 비해서 웜과 같은 경우 특정 네트워크 서비스 포트로 유입되는 트래픽의 양이 많게 된다. 이 방식은 이러한 성질을 이용해서 특정 포트가 다른 포트에 비해서 혹은 이전에 비해서 갑자기 많은 트래픽 들을 받게 되면 이를 웜으로 의심하고 이를 탐지하는 것이다. DEWP 방식에서는 네트워크 패킷의 데이터를 볼 필요는 없다. 단지 특정 네트워크 포트로 전달된 패킷들과 그 포트에서 다시 외부로 전송된 패킷들에 대한 정보만 있으면 된다. 즉, DEWP 방식에서는 매 T 시간 동안 특정 포트로 전달된 패킷의 양과, 그 포트에서 나간 양을 비교하여 EWMA (Exponential Weighted Moving Av-erage) 알고리즘을 이용하여 변화량을 추적하게 되고 변화가 발생하면 이를 웜 공격으로 간주하게 되는 것이다. 먼저, 트래픽 양의 변화를 찾기 위하여 다음과 같은 수식을 정의한다.

$$N^i = \alpha \times N^i + (1-\alpha) \times N$$

이 때, N은 특정 포트로 유입되는 트래픽의 근원지 주소들의 수를 말하고 N'은 이들의 평균적인 수치를 말한다. 위의 수식에서 만약 N 〉 N' * (1 + s)인 조건을 만족하게 되면 이를 웜으로 간주하게 되는 것이다. 이 때 s는 표준 편차를 의미한다. 즉, 전체적인 알고리즘을 정리하면, 특정 네트워크 포트로 유입되는 패킷의 근원지 주소들의 수가 갑자기 많아지는 경우 이를 웜으로 간주하는 것이라 할 수 있다.

이 방식의 경우 쉽고 간편하게 웜을 찾아 낼 수 있다는 장점이 있으나, Hot Spot과 같이 갑자기 외부 접속자가 많아지는 사이트의 경우 웜과 일반 사용자의 빈도가 비슷해지는 경우가 발생하기 때문에 이에 대한 탐지를 잘못할 경우가 많이 일어날 수 있다는 단점이 있다.

3.2.3 Statistical Intrusion Detection 방식 (University of Massachusetts, Amherst)[6]

Statistical Intrusion Detection 방식은 말 그대로 통계학 적인 방식을 이용하여 웜을 탐지하는 방식이다. 이 기법에서 주로 사용한 모델은 실제 전염병 같은 것의 전파를 설명할 때 쓰이는 Epidemic Model이다. 이 연구에서는 이 Epidemic Model을 바탕으로 웜의 전파를 설명하고 실제 네트워크 트래픽을 가지고 Model을 만들어서 웜의 Model과 일치하는 경우 이를 웜으로 판단하게 된다. 먼저 Epi-demic Model을 만들기 위해서 이들은 CodeRed와 Slammer 웜에 대한 자료를 수집해서 실제 웜의 Model을 만들어 냈다. 먼저 이 연구에서 정리한 웜의 Model에 대해서 살펴보자.

Simple Epidemic Model

$$dI(t)/dt = bI(t)S(t) = bI(t)[N(t) - I(t)]$$

여기에서 I(t)는 시간 t에서 감염된 호스트의 수이고, N은 모집단의 크기, b는 감염율을 나타낸다. 위의 모델은 기본적인 Epidemic Model로서 실제 전염병이 퍼지는 경우 만약 어떤 호스트가 전염병에 감염이 되면 계속 감염이 되어 있다고 가정하게 된다. 따라서 한 번 감염된 호스트가 다시 치료될 수 도 있다는 것을 고려하지 않는 등의 문제로 실제 환경에서 적용하기에 어려움 이 있다. 따라서 이 연구에서는 이 Model을 개선한 Kermack-Mckendrick Epidemic Model을 이용하였다.

Kermack-Mckendrick Epidemic Model

$$dI(t)/dt = bI(t)S(t) - gI(t)]$$
$$dU(t)/dt = gI(t)]$$
$$N = I(t) + U(t) + S(t)$$

여기에서 b는 감염율을 나타내고, g는 제거된 감염된 호스트의 제거율, S(t)는 시간 t에서 취약한 호스트의 수, N은 모집단의 크기를 나타낸다.

이 연구에서는 이러한 Model들을 이용해서 실제 웜 데이터를 바탕으로 이 Model들의 일치성을 확인한 후 패러미터들을 조정하여 실제 값과 유사하게 만들어 냈다. 그리고, 이러한 Model은 차후에 실제 네

트워크 트래픽을 대상으로 만들어진 Model과 비교 기준이 되고, 만약 실제 네트워크 트래픽으로부터 만들어진 Model이 웜으로부터 만들어진 Model과 유사하다면 이를 웜으로 판별하게 된다.

이러한 방식은 웜을 보다 정확하게 (수학적인 근거를 바탕으로) 탐지하는 것이 가능하지만, 실제 구현하기에 복잡도가 높은 단점이 있다.

3.2.4 Autograph 프로젝트 (CMU)[7]

Autograph Project는 Carnegie Mellon University에서 현재 수행되고 있는 프로젝트로 비정상 트래픽 탐지 방식으로 웜을 탐지하기 위한 방법이라고 하기 보다는 웜으로 추측되는 패킷들을 잡아서 자동으로 웜에 대한 Signature를 생성하고자 하는 것이다. 이 프로젝트의 주 관심사가 비정상 트래픽에의한 탐지는 아니지만, 웜에 대한 탐지 결과를 바탕으로 자동으로 Signature를 생성해서 빠른 시간안에 웜을 차단하고자 하는 근본 목표는 다른 프로젝트와 같다고 할 수 있다. 그리고 생성된 signature는 여타 다른 침입 탐지 혹은 방지 시스템에 그대로 적용될 수 있다. Autograph에서는 웜이라고 의심되는 패킷들의 데이터를 따로 모아서 별도의 콘텐츠 블록을 작성하게 된다. 이는 의심스러운 패킷에 대한 것을 모은 것으로, 유사성을 찾는 알고리즘을 이용해서 공통 패턴을 찾아낼 때 이용되게 되는데 이때 Rabin's Fingerprint [8]알고리즘을 이용하게 된다. 이 알고리즘은 간단한 Modular 연산을 이용해서 콘텐츠 블록 내에 있는 패킷 내용들 중에서 공통부분을 찾아내게 되는데, 실제 구현 역시 매우 쉽고, 동작 또한 빠르기 때문에 많은 곳에서 활용되고 있다. 이렇게 찾아낸 패턴은 Bro [8]와 같은 네트워크 침입 탐지 시스템에서 이용할 수 있는 실제 Signature 형태로 만들어 진다.

Ⅳ. SGS-20 시스템을 이용한 웜 (Worm) 탐지

ETRI에서는 2003년 10Giga급 네트워크 침입 방지 시스템 (SGS-10)을 제작하였고, 2004년에는 20 Giga급 네트워크 침입 방지 시스템 (SGS-20)을 제작하였다. 2004년도에 제작한 SGS-20 시스템은 H/W로 제작된 탐지 시스템으로, 그 내부에 signature를 기반으로 하는 침입 탐지 및 방지 시스템과 더불어 비정상 트래픽을 탐지하는 시스템을 가지고 있다. 이 비정상 트래픽 탐지 시스템은 분산 서비스 거부 공격 (DDOS) 및 웜 공격을 탐지 할 수 있으며 동시에 이를 차단하는 동의 대응이 가능하다.

SGS-20 시스템 내의 비정상 트래픽 감지 기법에서 이용하는 알고리즘은 CPD (Change Point Detection)방식이다. CPD 방식은 특정 Random Process의 변화를 쉽게 찾아 낼 수 있는 것으로 산업공학 및 경영 공학에서 많이 이용되는 것이다. 이 프로젝트에서는 CPD 방식 중에서 CUSUM (Cumulative Sum) 기법을 이용하였고, 동시에 SPC (Statistical Process Control) 기법에서 많이 이용되는 EWMA (Exponential Weighted Moving Average) 기법도 같이 적용하였다.

SGS-20 시스템에서 웜 탐지를 위하여 활용하는 패러미터는 기본적으로 Flow 정보 이다. 먼저, 네트워크 트래픽을 Source IP Address 별로 축약한 Flow별로 정리한 후 이들의 BPS (Bandwidth Per Second)와 PPS (Packet Per Second)값을 정리하였으며, 이들을 방향성을 주어 구분하였다(IN vs OUT). 이 Source IP Address를 기반으로 하는 축약 Flow 정보는 평상시에는 (정상상태) 그리 많은 양을 보이지 않을 것이다. 그러나 만약 웜과 같은 공격이 발생하는 경우 하나의 Source IP Address에서 많은 외부로 향하는 패킷들이 발생할 것이기 때문에 순간적으로 Source IP Address를 기반으로 하는 축약 Flow의 양이 정상 상태에 비해서 갑자기 증가하게 될 것이다. SGS-20 시스템은 이러한 성질을 이용하여 웜을 탐지하도록 하였다. 따라서 먼저, 네트워크 상의 패킷들을 수집하여 Source IP Address를 기반으로 하는 축약 Flow를 생성하였다. 그리고 각 Flow의 세션 정보를 추가로 수집하여 탐지에 정확도를 높이려 하였다. SGS-20 시스템에 적용한 웜을 탐지하기 위한 CUSUM 테스트 알고리즘은 아래와 같은 수식으로 표현된다.

$$C_i = \max[0, x-(u+K)+C_{i-1}] \quad (1)$$

$$C_i = \max[0, (u+K)-x+C_{i-1}] \quad (2)$$

위의 값에서 (1) 식은 Upper CUSUM Value를 나타내고, (2) 식은 Lower CUSUM Value를 나타낸다. 이 때 우리에게 필요한 것은 급격한 증가를 찾아내는 것이기 때문에 (1)식을 이용하도록 한다. (1)식에서 x 값은 시간 축에서 변화하는 BPS와 PPS의 값들을 의미하고, u 값은 target으로 잡은 목표 값을 의미한다. 이 테스트에서 말하는 목표 값이란, BPS와 PPS가 일반적인 값들을 말한다. 따라

서 이 값은 Static하게 정해 질 수도 있으며, 그 외 다른 정상 트래픽 값들에 의하여 Dynamic하게 정해 질 수도 있다. 이 값을 크게 잡는 경우 변화가 크게 생기는 경우에만 탐지가 가능하여, 큰 변화를 잡고 False Positive가 낮아질 확률이 높아지지만, 적은 변화에 민감하게 대처하기 어렵다는 단점이 있다. 그러나 값을 작게 잡는 경우 너무 민감하게 반응할 확률이 높기 때문에 역시 주의하여야 한다. 따라서 이와 같은 가정을 바탕으로 (1)식 내의 u 값을 설정하면 다음과 같다.

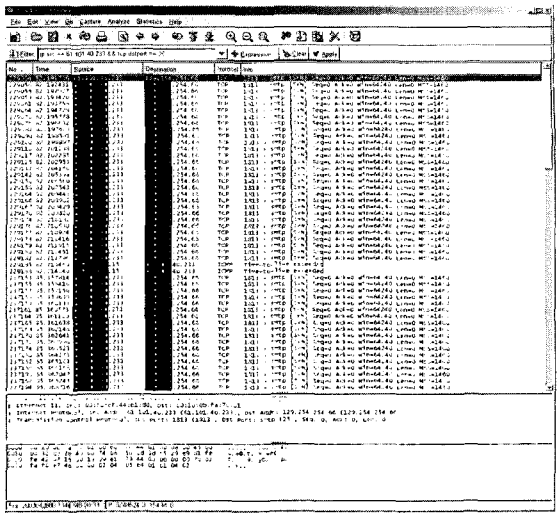
BPS의 경우,

u = (first BPS of Flow(n)) + |Default Value - (first BPS of Flow(n))|/2

PPS의 경우,

u = (first PPS of Flow(n)) + |Default Value - (first PPS of Flow(n))|

그리고 이러한 변수들을 대입하여 얻어진 결과들을 바탕으로 Upper CUSUM Value를 얻게 된다. 이 값들을 시간 순으로 나열하여 계속 증가하는 값을 보인다면 이는 상대적으로 이전에 비하여 BPS나 PPS 값들이 증가하는 것임을 알 수 있다. 따라서 (1)식 값들의 누적 값이 특정 Threshold m 값보다 큰 경우 (즉, BPS나 PPS의 증가가 연속적인 m point만큼 발생), 이를 의심스러운 Flow로 간주하게 된다. 그러나 이 정보 만으로는 정확한 탐지가 어렵게 된다. 일반적으로 네트워크 트래픽의 변화가 심하기 때문에 단순한 양적 비교로는 이것이 공격인지 아니면 단순한 사용자의 패턴 변화인지 알기가 어렵다. 따라서 이를 보완하기 위하여 추가의 정보를 더 분석하게 되었다. BPS와 PPS 외에 추가 정보로 본 시스템에서는 TCP Session 정보를 활용하였다. 일반적으로 TCP Protocol 상태에서 전달되는 Worm이나 DDOS의 경우 그 대상이 불분명하거나, 근원지 IP Address를 숨기는 등의 방법을 이용하기 때문에 TCP Threeway handshake가 완전하게 맺어지는 경우가 거의 없게 된다. 본 시스템에서는 이러한 성질을 이용하여 TCP Session 실패율이 높은 것을 의심하도록 하였다. 따라서 BPS와 PPS 정보를 얻는 것에 이어서 TCP Session 정보들을 수집하여 TCP 연결이 실패하는 비율에 대한 성공하는 비율을 구하게 된다.



〔그림 3〕 SGS-20에서 탐지한 웜의 예제

A = (TCP 연결 실패) / (TCP 연결 성공)

그리고 이러한 비율 값을 마찬가지로 CUSUM 식을 이용하여 변화를 측정하게 된다. 이 때 A 값이 계속 증가하는 패턴을 보이게 된다면 역시 의심스러운 Flow로 간주하게 되고, 위의 BPS와 PPS의 의심스러운 Flow와 일치하게 되면 이를 웜으로 간주하게 되는 것이다. 아래의 그림 3은 SGS-20 시스템을 이용하여 실제로 탐지한 결과를 Ethereal Tool [10]을 이용하여 공격자와 Victim을 알기 쉽게 GUI로 나타낸 것이다.

그림 3에 적용한 것은 실제 국내의 한 연구소에서 직접 실제의 네트워크 트래픽 데이터를 수집한 것을 이용한 것이다. 이 데이터를 SGS-20 시스템에 적용하여 그 결과를 보인 것으로 그림 상에서 보면 특정 Source IP Address에서 특정 서버들로 TCP SYN 스캐닝 패킷을 보내는 것을 알 수 있다.

또한, SGS-20 시스템은 성능 향상을 위해서 기본적인 패킷 수집 및 Flow 생성은 H/W를 제작하여 이용하였으며, 분석은 S/W를 이용하였다. 실제로 Gbps 속도를 내는 네트워크상에서 원활하게 동작하였으며 웜 탐지 역시 원활하게 이루어졌다.

V. 결 론

본 논문에서는 현재 인터넷 보안에서 가장 큰 화제가 되고 있으며 동시에 가장 많은 문제를 일으키고 있는 인터넷 웜에 대해서 알아보았다. 그리고 인터넷 웜을 탐지하기 위한 다양한 방법에 대해서도 알아보

았다. 단순히 웜이 이미 퍼져 나간 후에 웜에 대한 Signature를 생성하여 웜을 탐지하는 것은 이미 네트워크에 많은 피해가 가해진 후에 이루어 질 수밖에 없기 때문에, 그 자체적으로 완전한 해결책이 될 수 없다. 따라서 이러한 문제를 해결하기 위하여 웜으로 생각되는 것을 미리 찾아내서 이를 차단하는 연구가 필요하고 앞으로도 이에 대한 연구가 계속 이루어져야 할 것이다.

참 고 문 헌

[1] D.M. Kienzie and M.C. Elder, "Recent Worms: A Survey and Trends", ACM WORMS'03 Oct 2003, Washington DC, USA

[2] N. Weaver, V. Paxson, S. Staniford and R. Cunningham, "A Taxonomy of Computer Worms", ACM WORMS'03 Oct 2003, Washington DC, USA

[3] Snort, http://www.snort.org

[4] J.Y. Jung, S. Schechter and Arthur W. Berger, "Fast Detection of Scanning Worm Infections", RAID 2004, Sep. 2004, Sophia Antipolis French

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

[6] Cliff Changchun Zou, Weibo Gong, and Don Towsly, "Worm Propagation Modelling and Analysis under Dynamic Quarantine Defense", ACM WORMS'03 Oct 20 03, Washington DC, USA

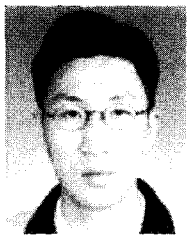
[7] H.A. Kim, Karp Brad, "Autograph: Toward Automated, Distributed Worm Signature Detection", 13th USENIX Security Symposium Aug. 2004

[8] Bro NIDS, http://www.bro-ids.org/

[9] J.Y Jung, V. Paxson, Arthur W. Berger, Hari Balakrishnan, "Fast Portscan Detection Using Hypothesis Testing", IEEE Symposium on Security and Privacy, May. 2004

[10] Ehtereal Tool, www.ethereal.com

〈著 者 紹 介〉



신 승 원 (Seungwon Shin)

1998년 2월 : 한국과학기술원 전기 및 전자공학과 학사 졸업

2000년 2월 : 한국과학기술원 전기 및 전자공학과 석사 졸업

2000년 3월~2002년 11월 : Tmax Soft 연구원

2002년 12월~현재 : 한국전자통신 연구원 정보보호 연구단 네트워크 보안 그룹 보안게이트웨이 연구팀

〈관심분야〉 네트워크 분석, 네트워크 보안

오 진 태 (Jintae Oh)

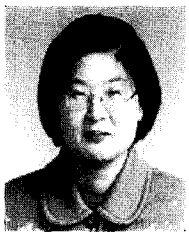
1990년 2월 : 경북대학교 전자공학과 학사 졸업

1992년 2월 : 경북대학교 전자공학과 석사 졸업

1992년 3월~1998년 2월 : 한국전자통신 연구원 선임연구원

2003년 3월~현재 : 한국전자통신 연구원 정보보호 연구단 네트워크 보안 그룹 보안게이트웨이 연구팀

〈관심분야〉 네트워크 보안, 비정상행위 탐지 기술



김 기 영 (Kiyoung Kim)

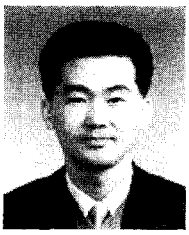
1988년 2월 : 전남대학교 전산통계학과 학사 졸업

1993년 2월 : 전남대학교 전산통계학과 석사 졸업

2002년 2월 : 충북대학교 전자계산학과 박사

1988년 2월~현재 : 한국전자통신 연구원 책임 연구원, 정보보호 연구단 네트워크 보안 그룹 보안게이트웨이 연구팀 팀장

〈관심분야〉 네트워크 보안, 고성능 네트워크 침입 탐지 및 보안



장 종 수 (Jongsoo Jang)

1984년 2월 : 경북대학교 전자공학과 학사 졸업

1986년 2월 : 경북대학교 전자공학과 석사 졸업

2000년 2월 : 충북대학교 박사 졸업

1989년 2월~현재 : 한국전자통신 연구원 책임연구원,
정보보호 연구단 네트워크 보안 그룹 그룹장
〈관심분야〉 네트워크 보안, 정책 기반 보안 관리 기술,
유해정보 차단 기술