2001 년 한국정보처리학회 추계 학술발표논문집 제 8 권 제 2 호

중간 경유 호스트 탐지에 관한 연구

박재필*, 원유헌*, 서진철*
*홍익대학교 컴퓨터공학과
e-mail : jppark@cs.hongik.ac.kr

A Study on Detecting stepping stone

Jae-Pil Park*, Yu-Hun Won*, Jin-Chul Seo*
**Dept. of Computer Engineering, Hong-ik University

요 약

최근 인터넷 공격의 주류를 이루고있는 징검다리(stepping stone)을 이용한 공격의 개요 및 방법등을 분석하고 이를 효과적으로 탐지할 수 있는 알고리즘을 제시한다. 또한 이렇게 탐지된 사이트들을 실시간으로 모니터링하여 관리 할 수 있는 방법을 개발해보고자 한다.

서론

최근 network 공격자들의 주류를 이루는 공격 방법중에 대표적인 것은 이른바 징검다리(stepping-stone[1]개념을 이용한 익명성(anonymity)의 획득이다.

이 방법은 공격자들이 그들의 공격을 자신의 컴퓨터가 아닌 네트웍 상의 다른 호스트를 매개체로 하여 공격하는 방법이다.

우리는 이러한 징검다리(stepping stone)의 방법을 이용한 공격을 인터넷에 엑세스(access) 할 수 있는 사이트를 모니터링 함으로써 공격이 진행 되는 동안에 실시간으로 탐지 할 수 있는 방법을 본 논문을 통해 개발해 보고자 한다.

본 논문에서 제시한 알고리즘은 네트웍 플로우(network flow)의 주기(period)를 이용한 방법으로 네트웍 트래픽(network traffic)이 암호화 되어있어도 적용할 수 있다.

본 논문에 제시한 알고리즘은 최소한의 시스템 부하로 최대한의 탐지 효과를 내보고자 하는데 그 목적을 두고있다

소 개

최근 들어 네트웍 공격자들을 탐지해내는 가장 중요한 문제는 얼마나 공격자들이 그들의 IP 를 잘 숨기고 있는가가 탐지의 효과와 속도를 좌우하고 있다.

때문에 공격자가 익명성(anonymity)을 얻기 위해 가장 쉽고 많이 사용하는 방법이 바로 징검다리(stepping stone:공격자가 자기 자신의 컴퓨터가 아닌 네트웍 상의 타 호스트를 이용하여 공격을 하는 방법) 기법을 이용한 공격이다.

일반적으로 공격자는 그들이 이용한 호스트들의 순서를 랜덤하게 바꿔 다양한 경로의 공격을 시도함으로써 그 침입경로의 탐지 및 추적이 어렵다.

우리는 이 같은 징검다리(stepping stone)로 이용되는 호스트들을 미연에 탐지해 냄으로써 공격에 사용될지 모를 의심스러운 활동을 감시하고 외부 호스트로의 접속을 검열하여 내부의 공격자를 탐지해 낼 수 있다.

본 논문에서는 징검다리(stepping stone)의 탐지에

대한 논문 Detecting Stepping Stone[1]에 서 언급된 내용중 timing based algorithm 을 응용하여 위 논문과는 다른 방법인 network period 의 데이터 베이스를 구축하고 이를 실시간으로 관리 함으로써 징검다리(stepping stone)에 사용된 호스트들을 탐지해 내고자 한다.

- **Network traffic period 를 이용한 징검다리(stepping stone)의 탐지**

  - 용어정의

    먼저 본 논문에서 제시한 알고리즘의 이해를 돕기위해 알고리즘에 사용된 용어의 정의를 한다.

    1. 징검다리 기법

       징검다리 기법이란 공격자가 자신 고유의 IP 를 속이고 이전에 접근 해두었던 머신(machine)을 통하여 타 호스트를 공격하는 방법이다.

    2. network periods

       본 논문에서는 특별히 TCP 연결상의 키스트로크(keystroke)의 지연시간을 기준으로 네트웍의 흐름이 있었는가 아닌가를 일정시간을 기준으로 판단하여 나눈 주기이다.

    3. 징검다리쌍

       징검다리(stepping stone)으로 연결되어 있는 두 사이트(양방향으로 공격의 기점이 될 수 있는)를 나타낸다.

  - ON/OFF periods

    본 논문에서 제시한 방법을 서술하기 위해 먼저 ON, OFF period 에 대한 정의를 한다.

    OFF period 는 일정시간(T_{idle})이상 데이터의 플로우(data flow)가 없을 경우 이를 OFF period 의 시작으로 정의 한다.

    단 데이터 플로우(data flow)는 항상 새로운 데이터(data)가 운반되었을 경우를 의미하며 데이터(data)의 재전송이나 사이트가 기존의 데이터를 유지하고 있는 경우는 제외한다.

    전송된 패킷(packet)이 비어있지 않은 데이터를 포함하고 있는 경우 OFF period 가 끝나고 ON period 가 시작되는 것으로 정의 하고 ON period 는 다시 일정시간(T_{idle})이상 데이터 플로우(data flow)가 없을 때 끝나는 것으로 정의한다.

위에 언급한 ON/OFF period 에 대한 정의는 TCP 연결시의 키-스트로크(keystroke)시간을 기준으로 하였으며 이는 키-스트로크(keystroke)에 관한 연구[2,3]에 언급된 Pareto distribution 에 정의된 고정된 파라미터값을 이용한다.

이 분포는 다양한 변수를 보이는데 일반적으로 키스트로크(keystroke)중 25%는 500msec 정도의 기간(term)을 갖고 15%

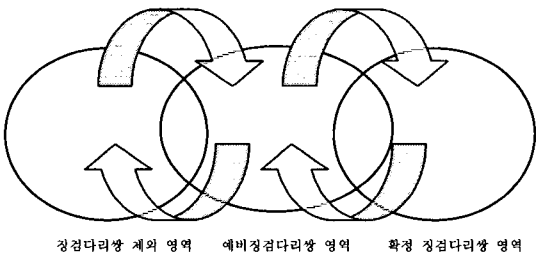
는 1sec, 1.6%는 10sec 이상의 기간(term)을 갖는 것으로 나타났다. 이것은 서로 연관된 트래픽(traffic)들이 종종 눈에띄는 OFF time 을 나타내는 것을 의미한다.

본 논문에서 제시하는 알고리즘의 기반이 되는 정책은 만일 두 사이트 A 와 B 가 서로 징검다리쌍(stepping stone pair)라면 두 사이트 각각의 OFF 피어리드가 끝나는 시점과 ON 피어리드의 시작시점이 서로 연관이 있을 것이라는 가정이 전제가 된다.

따라서 사이트 A 에서 사용자의 키스트로크(keystroke)는 아주 짧은 지연 후에 사이트 B 에 보내지게 될 것이며 이러한 사용자의 키스트로크로 인한 프로그램의 시작과 끝이나 결과물의 출력 등이 유사한 양상을 띄게 될것이다

■ 알고리즘

1. 먼저 모니터하고 있는 사이트들의 OFF period 를 체크하여 ON period 에서 OFF period 로의 전환 시간들의 차이가 δ(control parameter)이하인 두 사이트들을 추려내어 징검다리쌍(stepping stone pair) 후보로 선정. 이 목록을 예비징검다리쌍 영역에 저장 한다.
2. 예비 징검다리쌍 영역에 저장된 각각의 징검다리쌍(stepping stone pair) 후보들에 대하여 그 시점까지의 서로 일치된(오차가 δ 이하인) OFF period 의 수를 두 사이트 중 각 사이트의 총 OFF period 의 수가 보다 작은 사이트의 OFF period 수로 나누어 이를 컨트롤 파라미터인 γ(실험에 의해 값 설정)와 비교
3. 만일 γ 이상일 경우 두 사이트를 징검다리쌍으로 확정 이를 확정징검다리쌍으로 선정하고 확정징검다리쌍 영역으로 이동시켜 저장한다. 또한 이를 네트워크 관리자에게 통고 경고 메시지를 발생시킨다.
   만일 γ 이하일 경우 두 사이트는 징검다리쌍이 아닌 것으로 판정 예비징검다리쌍 영역에서 해제시켜 징검다리쌍 제외영역으로 이동 저장한다.



4. 확정징검다리쌍 영역에 일정시간(실험에 의해 결정)이상 머물게 되면 이를 확실한 징검다리쌍 사이트로 간주 경고를 발생한다.
5. 우리가 본 알고리즘에서 사용한 idle time 은 tcp 연결의 키스트로크 시간(keystroke time)을 기준으로 하였는데 이는 매우 다양한 분포를 나타내기 때문에[2,3] 본 논문에서는 실험에 의한 평균치인 T_{idle}=0.5 초를 사용하였다.
   또한 징검다리쌍 확정 유무에 사용된 γ 는 Detecting Stepping Stone[1]의 실험에서 사용한 결과를 이용하였다

결과

최근 인터넷 공격의 추세는 자기의 신분을 숨긴체 다른 사이트를 이용하여 공격하는 방법이 주류를 이루고 있다.
이처럼 자기의 신분을 숨긴 공격의 대표적인 것들이 바로 징검다리(stepping stone)을 이용한 공격방법이다.
본 논문에서 우리는 이러한 징검다리 공격을 탐지할 수 있는 방법을 네트워크 플로우(network flow)의 피리어드(period)를 이용하여 실시간으로 탐지해 내고 또한 이를 지속적으로 관리 할 수 있는 알고리즘을 개발해보았다.
본 논문에서 언급된 방법과 유사한 알고리즘이 Internet Relay Chat[4] 에서 사용 되었으며 distributed denial-of-service tools[5]에서도 유사한 방법이 언급되어있다.
본 논문은 아직 이론단계의 알고리즘을 제시한 것이기 때문에 논문에서 사용된 실험치 들과 각종 이론들이 실제로 본 논문에서 제시한 알고리즘과 부합하는지를 검증하는 단계가 필요하다.
또한 논문에서 사용된 컨트롤 파라미터들은 추정치가 아닌 실험에 의한 정확하고 통계적인 수치가 사용되어져야만 할 것이다.
나아가서 본 논문의 목적인 징검다리쌍의 탐지에만 머무르지않고 기존에 개발되어진 침입자 역추적 시스템들을 본 논문의 알고리즘과 연관시켜 적절히 사용한다면 좀더 효과적인 역추적 시스템을 개발할 수 있으리라 기대된다. 따라서 본 연구의 최종 목표는 침입자 역추적 시스템이 될 것이다.

참조

[1] "Detecting Stepping Stone" USENIX Security Symposium, Denver, Colorado, August 2000

[2] P.Danzig, S. Jamin, R. Caceres, D. Mitzel, and D.Estrin, "An Empirical Workload Model for Driving Wide-area TCP/IP Network Simulations", Internetworking: Research and Experience,3(1),pp.1-26,1992.

[3] V.Paxson and S. Floyd, "Wide-Area Traffic: The Failure of Poisson Modeling," IEEE/ACM Transactions on Networking,3(3),pp.226-244,June 1995

[4] J. Oikarinen and D. Reed,"Internet Relay Chat Protocol,"RFC1459,Network Information Center, DDN Network Information Center,May 1993.

[5] Computer Emergency Response Team, "Denial-of-Service tools,"CERT Advisory CA-99-17,Dec. 1999.