제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

우회 경로를 통한 인터넷 연결의 차세대 역추적 모델

한대일*, 안창훈**, 하옥현**, 엄두섭*
*고려대학교 전자컴퓨터공학과
**경찰청 사이버테러대응센터
e-mail:hansolo@korea.ac.kr

A New Trace Model of Internet Indirect Connection

Dae-il Han*, Chang-Hoon An**, Ok-Hyun Ha**, Doo-Seop Eom*
*Dept. of Electronic & Computer Engineering, Korea Univ.
**Cyber Terror Response Center, Korea National Police Agency

요 약

연구와 군사 목적으로 발전한 인터넷은 현재 많은 기업들과 일반인들이 사용하는 현대 사회의 중요한 기반 시설로 자리잡게 되었으며, 아울러 인터넷이 사회에 끼치는 영향이 커짐에 따라 여러 가지 목적으로 자신의 접속 위치를 우회하여 숨기고 인터넷 보안 모델의 취약점을 공격하는 침입자가 증가하고 있다. 따라서, 침입에 사용되는 기술과 그에 대한 대응 기법 또한 보다 복잡하고 정교해 지고 있으나 근본적으로 악의적 침입을 근절하는 능동적인 대응은 미약한 현실이다.

본 논문에서는 인터넷 환경에서 여러 가지 우회 경로를 통해 접근한 침입자의 실제 접속 위치를 효율적으로 추적하기 위해 기존 역추적 연구의 유형과 문제점을 살펴보고 차세대 인터넷 환경에서 활용 가능한 역추적 기법의 모델을 제시한다. 따라서, 기존 역추적 기법의 현실적으로 적용이 어려운 구성과 침입자의 보안 설정에 따른 추적 제한 등의 문제점을 살펴보고 그 해결 방안이 되는 새로운 역추적 시스템의 모델을 제시한다. 그리고, 본 연구에서 제시하는 모델은 기존의 연결 경로를 거슬러 추적하는 기법과 달리 프록시 등 우회 경로를 통해 접근한 침입자에 대해 직접 연결되는 프로토콜을 자동 실행 되도록 구성하여 접근한 침입자의 위치를 파악하는 모델이다. 이 모델을 적용할 경우 실제 적용 가능한 구성과 효율적인 추적 특성을 가지게 되며 구성 비용의 손실 또한 줄일 수 있게 되는 장점을 가지게 된다.

1. 서론

흔히들 현대 사회를 정보화 사회(Information Society)라고 한다. 정보화 사회에 대한 명확한 정의에 있어 다니엘 벨은 모든 것이 정보와 연관되며 정보가 경제 활동에 가장 중요한 자원의 하나로 간주되는 후기 산업 사회(post-industrial society)라 하여 정보화 사회를 기술하고 있다.[1] 실제로 현대 사회에서 정보는 가치 있는 중요한 자원으로 여겨지고 있으며 아울러 가치 있는 정보를 제한 없이 사용하기 위한 침해 활동 또한 활발해 지고 있는 현실이다. 따라서, 가치 있는 정보를 비밀 보관하고 그 정보를 운영하는 시스템의 중요성이 증대되고 있으며 침입에 대한 방어 및 탐지 기술 또한 상대적으로 활발해지고 있다.

최근 인터넷 환경에서 다양한 방법으로 행해지고 있는 시스템 침입에 효율적으로 대응하기 위해서는 기존 방화벽이나 침입탐지시스템과 같은 수동적인 방어 모델의 한계를 극복하여 근본적인 해킹 시도를 줄일 수 있는 능동적인 대응기술이 요구되고 있다. 따라서, 이를 해결해 줄 수 있는 실현 가능한 모델로서 역추적 기술의 연구가 필요하게 되었으나 능동적인 대응 기술로서 현실에 적용 가능한 모델의 연구는 미약한 현실이다. 이는 우회공격에 대한 경로 추적의 기술적인 한계와 공격시스템에 대한 역공격 허용의 문제라는 정책적인 제한에서 기인한다.

따라서, 본 논문에서는 먼저 상대적으로 가치 있는 정보를 침해하는 공격자의 네트워크 주소를 파악하는 기술 연구를 통해 기존 역추적 연구를 분석하

고 정리하며, 아울러 실제 사용가능한 역추적 시스템을 구축하는데 필요한 기법을 연구하는 것이 매우 절실한 상황임을 파악하여 정보의 침해에 대응함에 있어 효율적이고 활발한 대응을 위해 필요한 기술을 분석하도록 한다. 또한, 침해사고 방지 대책의 한계를 극복하는 능동적인 해킹방지 기술의 필요성을 인지하여 해킹시도 자체를 제한 할 수 있는 능동적 해킹 방지 및 검거 기술의 개발을 위해 먼저 새로운 실시간 역추적 모델을의 조건을 제시하고 아울러 다양한 구축을 위한 역추적 시스템의 사례를 제시하여 기존 역추적 기술의 문제점을 극복하는 운영 방안을 제시한다.

2절에서는 기존 역추적 연구의 유형과 그 문제점을 소개하고, 3절에서는 제안하는 역추적 모델의 조건과 그 조건에 부합되는 새로운 역추적 모델을 제한하며 4절에서 결론을 맺는다.

2. 기존 역추적 모델 연구

인터넷 침입에 대한 역추적의 개념은 악의적인 인터넷 접근에 대해 공격자의 실제 네트워크 주소를 탐색하는 메카니즘을 의미한다. 기존 역추적 모델의 유형은 추적 정보를 얻는 형식에 따라 크게 연결 경로 추적을 통해 정보를 얻는 방식과 접속 상태의 상황을 활용하여 정보를 얻는 추적 방식으로 구분 할 수 있다.

연결 경로 추적 모델의 경우 단순히 네트워크 접속 상태 정보를 확인하여 얻은 IP 정보만으로는 우회 경로를 통한 공격에 대한 역추적이 불가능하기 때문에 중간 경유지 즉, 연결고리의 한단계 이전 시스템을 찾아가는 방법이다. 이는 모든 연결점마다 특별한 목적의 에이전트가 존재하거나 역추적을 위한 정보가 제공되는 특정 프로토콜을 사용하여야 한다는 점에서 실용적인 모델의 구현이 어려운 단점이 있다. 한편 우회공격에 대한 접속 상태 상황을 활용한 역추적 모델은 유입되는 패킷을 분석하거나 애플릿과 같은 임의의 모듈을 침입자의 시스템에 삽입하여 추적하는 방법이다. 이 방법은 침입자의 시스템이나 우회경로로 사용되는 시스템의 환경적 요인에 많은 영향을 받으며 역공격 허용 여부에 대한 정책적 제한을 받는다.

현재 알려진 역추적 관련 연구로서 CIS(Caller Identification System)[2], AIAA(Autonomous Intrusion Analysis Agent)[3], Connection Chain, Thumbprints, Sequence Number[4], Self-Extension Monitoring, Sleep Watermark Tracing[5], Packet Header Traceback, Host Agent Traceback, Connection Traceback, IP Packet Traceback[6], Sub-Conclusion, CITRA 등이 있다[7].

2.1 연결 경로 추적 모델

연결 경로간 정보를 역추적하는 추적 모델은 우회침입시 경유하는 지점의 정보를 이용하는 방법이 주된 연구 주제이다. 즉 접속경로를 찾기 위해 연결고리의 한단계 이전 시스템을 찾는 방법으로 중간 경유 라우터를 이용한 방법이 많이 사용된다. 먼저 해킹 당한 시스템의 로그 및 네트워크 연결 정보를 통해 공격 시스템을 파악하고 해당 공격시스템의 로그와 네트워크의 연결정보를 분석하여 이전 공격정보를 분석하는 과정을 반복하게 된다.

현재 연구되고 있는 연결 경로 정보에 기반을 둔 역추적 모델의 종류에는 연결호스트 경로에 기반을 둔 Host-based Trace Back, 라우터 경로에 기반을 둔 Network-based Traceback, 실행 네트워크가 존재한다는 가정하에 정보를 얻는 Active Network based Traceback등이 있다.

연결 경로 역추적 모델을 적용하기 위해서는 각 라우터가 속한 네트워크 또는 각 호스트마다 이전 단계로부터 접속된 로그 정보나 인증 정보를 확인하기 위한 방화벽 또는 특별한 에이전트가 위치하여 작동되거나, 역추적을 위한 별도의 개선된 네트워크 프로토콜이 모든 네트워크상에 존재하여야 한다는 전제조건이 필요하다. 이는 연결 경로상의 모든 네트워크와 호스트로부터 정보나 인증을 얻어야 역추적이 가능하다는 의미이며 역추적 경로상의 한 단계라도 추적이 불가능한 경우 역추적이 불가능하다는 단점이 있다. 따라서, 모든 네트워크와 호스트에서 정보를 얻는 것은 현재의 인터넷 환경에서 적용하기 어려운 현실이다.

2.2 접속 상태 분석 모델

시스템 및 네트워크의 접속 상태에서 정보를 활용한 역추적 모델은 연결 경로 전체에 대한 정보를 얻지 않고 현재 피해를 당하고 있는 상황에서 얻을 수 있는 정보를 바탕으로 침입자 시스템의 네트워크상 실제 위치를 추적하는 모델이다. 일반적으로 패킷의 헤더 정보를 분석하거나 침입시스템의 정보를 얻어내는 모듈을 침입자의 시스템이 다운로드 하도록 하여 정보를 얻는다.

일반적으로 침입 당시 네트워크 연결 정보를 통해 공격자의 네트워크 위치를 파악하는 경우 우회 경로를 통한 침입에 대해 정확한 추적이 어려운 단점이 있으며, 이는 패킷 헤더의 값을 분석할 경우 중간 경유지의 프록시서버의 환경 설정에 따라 정보의 정확성이 결정되기 때문이다. 예를 들어, 프록시 서버를 거친 공격의 경우 네트워크 연결상태만 확인하면 프록시의 네트워크 주소가 나타나게 되고 패킷 헤더를 분석하여도 프록시 서버의 설정이 클라이언트의 IP를 숨기게 되어있는 경우 실제 공격자의 네트워크 위치정보는 나타나지 않는다.

한편, 침입시스템의 정보를 얻을 수 있는 특정 모듈을 자동으로 다운로드 받도록 하는 방식은 사용자의 인터넷 환경에 따라 결과가 변동 되거나 공격 시스템에 대한 역공격이라는 정책적 한계가 존재한다. 공격하는 시스템의 인터넷 설정이 자동으로 애플릿과 같은 구성물을 다운로드 받도록 설정되어 있지 않을 경우 다운로드 전에 확인 메시지를 통해 사용자 승낙을 얻어야 하고 기본적으로 다운로드를 거부할 수 있다. 또한, 불법적인 공격자라도 상대방의 동의 없이 대상 시스템의 정보를 얻을 수 있는 모듈을 삽입하는 것이 현재 정책적인 면에서 허용이 제한되는 어려움을 가지고 있다.

3. 제안하는 차세대 역추적 모델

연결 경로의 정보를 분석하는 모델과 접속상태의 정보를 활용한 역추적 기법이 일부 상품화되어 사용되고 있는 상황이지만 앞서 살펴본 바와 같이 기술적인 면과 제도적인 면에서 제한을 받고 있는 현실이다. 따라서, 이 장에서는 현실적으로 활용 가능하며 정책적인 규제에 대한 영향이 적은 새로운 역추적 모델의 조건을 제시하고 이를 적용할 수 있는 새로운 모델을 제시하기로 한다.

특히, 제안하는 새로운 역추적 모델은 인터넷 환경이 다양해짐에 따라 등장하는 많은 새로운 프로토콜과 서비스를 적극 활용하는 모델로서 향후 다양한 방식의 메카니즘으로 설계 및 사용이 가능하다.

3.1 차세대 역추적 모델의 조건

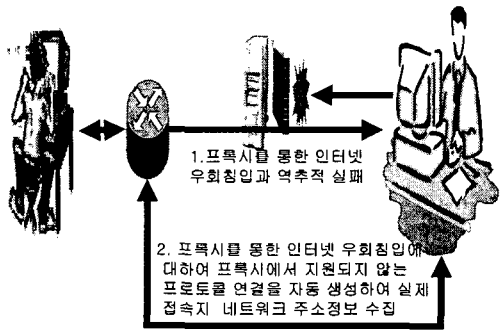
첫째, 기존 역추적 연구에서 현실적으로 활용하는데 문제점으로 지적되고 있는 우회경로상의 모든 네트워크 및 시스템에 정보 수집을 위한 에이전트를 삽입하거나 새로운 프로토콜을 적용하지 않는 방식의 모델이어야 한다. 현재 인터넷에서 대부분 사용되고 있는 TCP/IP 프로토콜이 향후 이러한 단점을 개선할 프로토콜로 전면 대체되지 않을 경우 실제 활용이 어렵기 때문에 이를 제외한 모델을 제안하여야 하며, 따라서 실시간으로 피해를 당하고 있는 시스템에서 필요한 정보를 얻을 수 있어야 한다.

둘째, 정책적인 규제의 대상으로 지적 될 수 있는 정보 수집용 모듈을 공격자의 시스템에 임의로 삽입하지 않아야 한다. 역공격 또한 상대 시스템의 정보를 침해하는 허용되지 않는 행위로 간주될 수 있기 때문에 실제 사용에 있어 규정에 의한 제약을 받을 수 있기 때문이다.

셋째, 위의 두가지 상황을 유지하며 정보를 얻기 위해서는 인터넷 연결이 이루어진 상황에서 서버에 별도의 프로토콜 또는 서비스가 자동으로 실행되어 새로운 직접 연결을 생성해야 한다. 이는 우회 공격의 연결 경로를 추적하기 위해서는 연결 경로상의 모든 네트워크와 호스트로부터 정보나 인증을 얻어야 역추적이 가능하기 때문에 현재 인터넷 환경에서 적용이 어렵기 때문이다.

3.2 새로운 역추적 모델의 적용 사례

아래 (그림 1)은 공격자가 프록시서버를 경유하여 침입하였을 때 연결 경로를 통한 추적이 실패한 경우와 이와 비교하여 프록시서버에서 제공되지 않는 다른 프로토콜을 이용한 새로운 접속을 생성하여 공격자의 실제 네트워크상 주소를 파악하는 모델을 제시하였다.



(그림 1) 차세대 우회침입 역추적 모델

현재 사용되고 있는 프록시서버에서 제공하는 프로토콜과 서비스는 HTTP, Secure, FTP, Gopher 등 기본적인 몇 가지 인터넷 서비스에 한정되고[8] 있기 때문에 여러 가지 프로토콜과 서비스가 지원되고 있는 최근의 환경에서 프록시서버가 지원하지 않는

새로운 인터넷 연결을 생성되게 할 경우 어렵지 않게 공격자와의 직접 연결 상태가 성립된다. 따라서, 새로이 생성된 연결의 네트워크 연결 상태 정보를 확인함으로서 공격자의 실제 네트워크 주소를 파악할 수 있으며 임의로 모듈을 삽입하는 방식이 아니므로 규제의 제한을 받거나 상대 브라우저 설정의 영향을 적게 받는다.

실제 구축의 예를 들어 외부에서 홈페이지 접속 요청이 발생할 경우 첫 화면에 특정 멀티미디어 프로토콜의 컨텐츠가 시작되도록 설정을 해놓은 웹서버는 외부에서 접속시 프록시를 거친 인터넷 접속과 별도록 컨텐츠 재생을 위한 프로토콜을 통한 직접 연결이 생성된다. 이때 네트워크 연결 상태를 확인하면 두 가지 프로토콜이 각기다른 연결을 가지고 있음을 확인하여 우회 접속 여부를 판단할 수 있으며 실제 네트워크 주소를 확인할 수 있다. 한편, 우회 접속 네트워크 주소와 실제 네트워크 주소의 로그를 모두 남겨 둘 경우 차후에도 해당 시간의 침입에 대한 분석이 가능하다. 따라서, 이 모델은 단순히 실시간 역추적뿐 아니라 사후 해당 시간의 프로토콜별 로그를 분석함으로서 접속지를 숨긴 허위 사실의 유포 및 명예훼손의 추적등 여러 가지 활용이 가능하다.

4. 결론 및 향후 연구

본 논문에서는 기존 역추적 연구의 유형과 문제점을 살펴보고 이를 극복하기위한 새로운 인터넷 역추적 모델의 조건을 제시하였으며 아울러, 그 조건에 맞는 별도의 직접 연결 프로토콜 생성 방식의 구축 모델을 제시하였다. 본 고에서 제시한 새로운 방식의 역추적 모델을 적용하여 시스템을 구축할 경우 얻을 수 있는 장점은 다음과 같다.

첫째, 기존 역추적 연구의 문제점을 최소화하는 실제 사용 가능한 모델을 적용하였다.

둘째, 사용을 위한 구축이 용이하며 공격자와의 직접 연결을 생성함으로서 추적의 신뢰성이 높다

셋째, 인터넷 프로토콜과 서비스의 증가에 따라 다양한 형식으로 구축이 가능한 모델이다.

넷째, 임의의 모듈 삽입이 없이 연결 상태를 확인하는 방식으로서 규제의 제한으로부터 받는 영향이 적다.

능동적인 정보보안을 위해 본고에서 제시한 모델을 기존 정보보호연구의 결과와 함께 적용함으로서 보단 견고한 보안시스템이 구축이 가능하다고 생각되며 아울러, 현실적으로 활용가능한 역추적 모델이 될 것이라 생각한다. 향후 본 연구의 내용을 바탕으로 본 고에서 다루지 못한 침입자 시스템의 환경 설정에 따른 역추적 효율의 영향의 분석과 기타 현실적으로 사용 가능한 여러 가지 방식의 새로운 역추적기법의 연구가 진행되어야 할 것이다.

참고문헌

[1] Dinel Bell, The Coming of Post-Industrial Society (N.Y: Basic Books, 1973) pp. 117-118.

[2] H.T.Jung, "Caller Identification System in the Internet Environment", Proceedings of the USENIX Security Symposium IV

[3] 임채호, 원유현, "인터넷 해킹 피해시스템 자동 분석에이전트(AIAA) 및 침입자 역추적 지원 도구 구현", 정보처리학회 논문지, 1999. 11

[4] K. Yoda and H.Etoh, "Finding a Connection Chain for Tracing Intruders", In F. Guppens, Y. Deswate, D. Gollamann, and M. Waidner, editors, 6th European Symposisum on Research in Computer Security - ESORICS 2000 LNCS -1985, Toulouse, France, Oct 2000.

[5] X. Wang, D. Reeves, S.F. WP, and J. Yuill, "Sleepy Watermark Tracing: An Active Network-Vased Intrusion Response Framework", Proceedings of IFIP Conference. on Security, Mar. 2001.

[6] Dawn Xiaodonf Song and Adrian Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback", Computer Science Department, Univ. of California

[7] 서동일, "침입자 역추적 기술 동향", The 8th Network Security Workshop-Korea(NETSEC-KR 2002), 2002. 5

[8] Robert Orfali and Dan Harkey, "Client Server Programming With JAVA and CORBA 2nd", WILEY, 1998