정보 은닉을 통한 Stego-tracing

김지현*, 이문호*

*전북대학교, 전자정보공학부

Stego-tracing with Information Hiding

Ji-hyun Kim*, Moon-ho Lee*

*Division of Electronics and Information Engineering Chonbuk National Univ.

요 약

본 논문에서는 자료 파일에 위치 추적 모듈을 삽입하여 공격자에 의해 자료 유출 사고 발생 시에 유출된 자료 및 자료를 유출한 공격자 그리고 불법 복제되어 유포되는 자료와 불법 사용자를 추적할 수 있는 시스템을 제안한다. 제안한 역추적 시스템은 부가적인 역추적 모듈의 설치를 필요로 하지 않으며 공격자가 이용한 중간 경유지 시스템을 고려할 필요가 없다.

I. 서론

방화벽(Firewall)은 다른 네트워크 사용자들로부터 사설 네트워크의 자원을 보호해주는 보안 제품으로, 외부인이 자신의 공개되지 않은 자원에 접근하는 것을 막고, 내부 사용자가 외부 자원에 접근하는 것을 통제하기 위해 내부 네트워크와 인터넷 사이에 설치된다. 주로 TCP/IP protocol header 정보를 이용하여 외부로부터의 접근을 통제하며 content filtering을 통해 정교한 접근 제어 기능을 수행한다. 침입탐지시스템(IDS)은 로컬 네트워크 또는 호스트에 위치하여 보다 정밀한 유/출입 데이터에 대한 분석을 수행하며 네트워크를 통한 공격이나 시스템에 대한 불법접근을 탐지하는 2차 방화벽 기능을 수행한다. 침입방지시스템(IPS)는 불법 침입, 분산서비스거부공격(DDoS) 등의 비정상적인 이상신호를 발견 즉시 인공 지능적으로 적절한 조치를 취한다는 점에서 방화벽이나 침입탐지시스템과 차별성을 갖는다.

이러한 보안 제품은 차단과 탐지와 같은 수동적인 방어에 중점을 두고 있다. 더욱이 최근에는 이러한 보안 제품을 우회하는 공격 기법이 늘어나고 있으며 이 경우에는 적절한 조치를 취하지 못한다. 이에 따라 공격에 대해 보다 적극적인 대응과 근본적인 방지를 위해 침입자 역추적 기술이 연구되고 있으며, 공격에 유연한 대응 방안으로 침입 감내 기술 등이 연구되고 있다.

본 논문에서는 중요 자료 파일에 위치 추적 모듈을 삽입함으로써, 해커에 의해 자료 유출 사고 발생 시에 유출된 자료와 자료를 유출한 해커 그리고 불법 복제되어 유포되는 자료 및 불법 사용자를 추적할 수 있는 시스템을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 역추적 시스템에 대해서 설명하고, 3장에서는 제안한 역추적 시스템의 구성과 각 모듈의 기능 및 동작 과정에 대해서 서술하고, 4장에서는 제안한 역추적 시스템의 구현과 동작에 대해 설명하고 마지막으로 6장에서는 결론을 맺고 향후 연구에 대해 언급한다.

II. 역추적 시스템

역추적 시스템이란, 인터넷과 같은 사이버 상에서 공격자의 실제 위치를 추적하는 시스템으로 공

† 이 논문은 정보통신부 대학정보통신 연구센터 지원사업의 지원 및 한국소프트웨어진흥원의 관리로 수행되었음.

격 기법에 따라 역추적 기술도 달라지며 IP 패킷 역추적과 Connection 역추적으로 나눌 수 있다.

1. IP 패킷 역추적

IP 패킷 역추적 기술은 그림 1과 같이 분산 서비스 거부 공격(DDoS)과 같이 주로 공격자가 IP 스푸핑 기술을 사용하여 거짓 IP 주소를 담고 있는 패킷의 실제 송신지를 추적하는 방법으로 IETF iTracing Working Group에서 표준화를 진행 중인 ICMP Traceback과 라우터의 패킷 마킹 기능을 이용하는 Packet Marking 기술이 이에 속한다.[1][2]

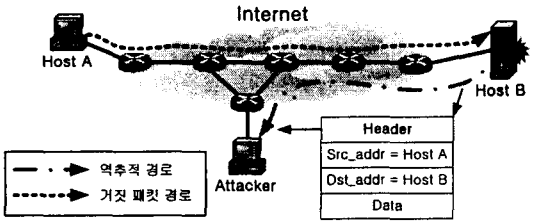

그림 1: IP 패킷 역추적.

2. Connection 역추적

Connection 역추적 기술은 그림 2와 같이 공격자가 최종 공격 대상 시스템에 접근하는 과정에서 여러 중간 경유지 시스템을 경유하는 공격을 추적하는 방법으로, 시스템 상에 역추적 모듈을 설치하여 로그 분석을 통하여 역추적 하는 호스트 기반 역추적과 네트워크 상에 송수신되는 패킷으로부터 정보를 추출하여 역추적 하는 네트워크 기반 역추적으로 나누어진다. 따라서 네트워크 기반 역추적 시스템은 모든 송수신 패킷을 감시할 수 있는 위치에 역추적 모듈이 설치되어야 한다.

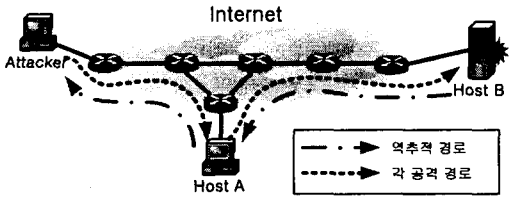

그림 2: Connection 역추적.

호스트 기반 역추적 기술에는 AIAA(Autonomous Intrusion Analysis Agent), CIS(Caller Identification System) 등이 있으며, 네트워크 기반 역추적 기술에는 IDIP(Intrusion Detection & Isolation Protocol), SWT(Sleepy Watermarking Tracing) 등이 있다.[3][4][5][6]

III. 제안한 역추적 시스템

제안한 역추적 시스템은 그림 3과 같이 정보 은닉 모듈, 위치 추적 모듈, 그리고 정보 처리 모듈로 구성되어 있다.

그림 3: 제안한 역추적 시스템 구성도

1. 정보 은닉 모듈

정보 은닉 모듈은 중요 자료 파일에 위치 추적 모듈을 삽입하는 기능을 수행하여 해커에 의해 유출된 자료 파일이 실행될 때, 동시에 위치 추적 모듈이 Background Job으로 자동 실행될 수 있도록 한다. 이는 해커로 하여금 위치 추적 모듈이 동작하는 것을 인지하지 못하도록 하기 위함이다.

정보 은닉 모듈은 FileMerge와 Controller로 구성되는데,

FileMerge는 그림 4와 같이 Controller와 위치 추적 모듈(Traceback)을 Data 파일에 삽입하여 새로운 파일을 생성한다. 이 때, Controller와 위치 추적 모듈(Traceback) 그리고 Data 파일의 사이즈를 구해서 새로운 파일의 마지막에 기록한다. 이는 FileMerge에 의해 생성된 파일이 공격자 시스템에서 실행될 때, Controller에 의해 위치 추적 모듈(Traceback)과 Data 파일을 추출하기 위함이다.

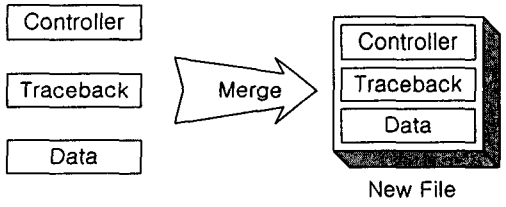

그림 4: 위치 추적 모듈 삽입.

Controller는 그림 5와 같이 FileMerge에 의해 생성된 새로운 파일로부터 위치 추적 모듈(Traceback)과 Data 파일을 추출하여 Data 파일을 Foreground Job으로 실행시키고, 위치 추적 모듈의 존재를 숨기기 위해 Background Job으로 실행시킨다. 이 때, FileMerge에 의해 기록된

Controller와 위치 추적 모듈(Traceback) 그리고 Data 파일의 사이즈를 가지고 추출할 수 있다.

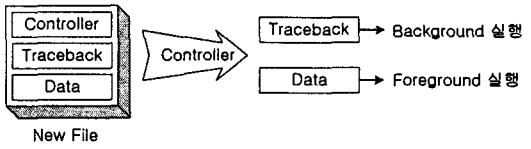

그림 5: Controller.

2. 위치 추적 모듈

위치 추적 모듈은 해커로부터 존재를 감추기 위해 Background Job으로 실행되며, 정확한 공격자 역추적을 위해 다양한 로컬 시스템 정보 및 네트워크 정보를 수집하여 자료 파일을 유출당한 서버에게 전송하는 기능을 수행하며, 이 때 수집되는 정보에는 Host Name, IP 주소, MAC(Media Access Control) 주소, Subnet Mask, Gateway, DNS(Domain Name Server) 등이 있다.

위치 추적 모듈에 의해 수집된 공격자 위치 정보는 그림 6과 같이 자료를 유출당한 시스템에게 전송된다.

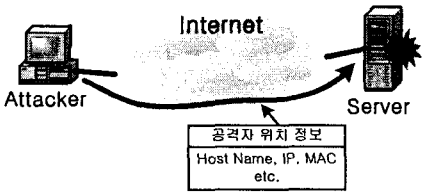

그림 6 : 위치 추적 모듈.

3. 정보 처리 모듈

정보 처리 모듈은 그림 7과 같이 위치 추적 모듈에 의해 전송된 정보를 수신하여 파싱(parsing)하여 화면에 출력하여 시스템 관리자에게 보고하고 수신된 공격자의 시스템 및 네트워크 정보를 로그 파일로 저장한다.

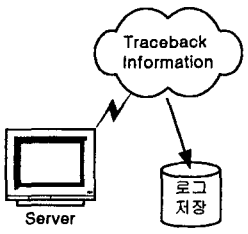

그림 7 : 수신 정보 출력 및 로그 저장.

IV. 구현

본 논문에서 제안한 시스템은 Application 레벨에서 동작하며 윈도우즈 플랫폼 상에서 동작하도록 구현되었다.

그림 8은 정보 은닉 모듈인 FileMerge를 실행한 모습으로 Controller와 위치 추적 모듈을 삽입할 파일을 선택하는 대화창을 보여준다.

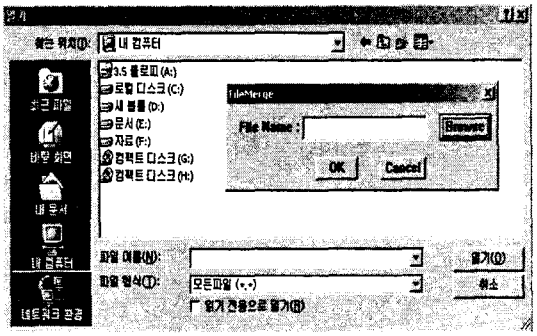

그림 8: 위치 추적 모듈 삽입.

FileMerge의 실행 결과로는 Controller와 위치 추적 모듈이 삽입된 새로운 파일이 생성된다.

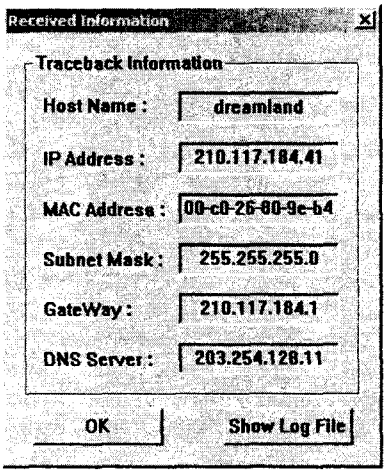

그림 9: 수신 정보.

그림 9는 FileMerge에 의해 생성된 새로운 파일을 실행한 결과로, 자료를 유출당한 서버에서 위치 추적 모듈에 의해 수집되어 전송된 공격자의 시스템 및 위치 정보를 수신하여 출력하는 모습이다. 또한 서버에서 수신한 공격자 정보는 자동으

로 로그 파일로 저장되어 Computer Forensics에 사용할 수 있다.

V. 결론 및 향후 과제

본 논문에서 제안한 역추적 시스템은 공격자가 위치 추적 모듈이 삽입되어 있는 자료 파일을 유출해서 실행시켜야만 추적이 가능하다. 하지만, 기존의 역추적 시스템이 네트워크 전반에 걸쳐 역추적 시스템을 설치해야만 공격자 추적이 가능한 반면에 제안한 역추적 시스템은 단독으로 동작이 가능하다. 즉, 공격자에 의해 사용된 중간 경유 시스템을 고려할 필요가 없다. 또한 공격자가 유동 IP를 사용하거나 사설 네트워크 내부에 위치하고 있을 경우에도 추적이 가능하다.

제안한 역추적 시스템은 현재 공격자 정보를 전송할 때 임의의 포트를 통해서 데이터를 전송한다. 만약, 공격자가 방화벽 내부에 위치하고 있을 경우에는 데이터 패킷이 방화벽에서 차단될 수 있다. 이를 해결하기 위해서 웹서비스에 사용되는 80번 포트를 이용해 데이터를 전송하는 방안과 수신된 데이터를 단순히 출력하고 파일로 저장하는데 그치지 않고, 부재중인 관리자에게 신속하게 통지할 수 있도록 이메일 또는 SMS 문자 서비스를 통해서 전달할 수 있는 방안을 향후 연구한다.

참고문헌

[1] Allison Mankin, Dan Massey, Chien-Lung Wu, S. Felix Wu, Lixia Zhang, "On Design and Evaluation of Intention-Driven ICMP Traceback", Proceedings of IEEE International Conference on Computer Communications and Networks, 2001.

[2] Dawn X. Song and Adrian Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback", Proceedings of InfoCom, 2001.

[3] Chaeho Lim, "Semi-Auto Intruder Retracing Using Autonomous Intrusion Analysis Agent", FIRST Conference on Computer Security Incident Handling & Response, 1999.

[4] H. T. Jung, "Caller Identification System in the Internet Environment", Proceedings of the USENIX Security Symposium IV, 1993.

[5] D. Schnackenberg, K. Djahandari, and D. Sterne, "Inforastructure for Intrusion Detection and Response", Proceedings of the DARPA Information Survivability Conference and Exposition, 2000.

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

[6] 이수형, 나중찬, 손승원, "액티브 네트워크 기반 세션 추적 및 대응 메카니즘", CISC 2002 Proceedings, Vol.12, No.1, 2002.

[7] 침입자 역추적 기술 동향, ETRI.