이동형 센서를 이용한 TCP 확장 연결 공격 역추적 메카니즘

손선경*, 방효찬*, 나중찬*, 손승원**

*한국전자통신연구원 정보보호연구본부 네트워크보안연구부 능동보안기술연구팀

**한국전자통신연구원 정보보호연구본부 네트워크보안연구부

The traceback mechanism against TCP extended connection attack using mobile sensor

Seon-Gyoung Sohn, Hyo-Chan Bang, Jung-chan Na, Seung-Won Sohn

Network Security Department, Information Security Technology Division, ETRI

요 약

고도의 기술을 이용한 최근의 사이버 공격을 방어하기 위해서는 자신의 도메인만을 보호하는 현재의 수동적인 네트워크 보안 서비스보다는 액티브 네트워크 기반 하에 침입자의 위치를 역추적하고 침입자의 근원지에서 네트워크로의 접근을 차단하는 능동적인 대응이 필요하다. 본 논문에서는 TCP 기반의 우회 공격인 TCP 확장 연결 공격을 역추적하고 침입자를 네트워크로부터 고립시키는 메커니즘에 대해 기술한다.

I. 서론

최근 인터넷 상에서 발생하는 사이버 공격은 고도의 기술을 이용하여 점차 다양화되고 지능화되고 있다.

이러한 현실에서 현재의 네트워크 보안 서비스는 대부분 자신의 도메인으로 들어오는 공격을 탐지하고 자신의 도메인을 방어하는데 그치고 있다. 따라서 다른 경로나 다른 공격 기법을 이용한 제 2, 제 3의 공격이 가능하다.

이를 해결하기 위해서 네트워크 노드에 프로그래밍을 추가한 차세대 네트워크 플랫폼인 액티브 네트워크 기반 하에 침입자의 위치를 역추적하고 침입자의 네트워크 접근을 차단하는 등의 능동적인 대응을 할 수 있는 능동보안기술에 대한 연구가 진행중이다.

사이버 공격은 크게 특정 호스트에 침입하여 시스템의 상태를 변경시키거나 정보를 획득하기 위하여 여러 호스트를 경유하여 세션이 유지되는 상태에서 공격이 이루어지는 TCP 기반의 공격과, DDoS와 같이 다량의 패킷을 전송하여 서버를 마비시키는 UDP 기반의 공격으로 나눌 수 있다.

본 논문에서는 능동보안기술을 이용하여 TCP 기반의 확장 연결 공격을 역추적하고 그 결과에 따라 침입자를 네트워크로부터 고립시키는 메커니즘에 대해 기술하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 능동보안기술에 대해서 소개하고, 3장에서 침입자 역추적 메커니즘을 기술한다. 마지막으로 4장에서 결론을 맺는다.

II. 능동보안기술

능동보안기술은 프로그래밍이 가능한 보안관리 메커니즘을 생성하고, 이를 이동형 센서 기술을 이용하여 네트워크 노드에 전달하여 능동적인 보안 서비스를 제공하는 기술이다.

능동보안 프레임워크는 액티브 네트워크 기능을 제공하는 능동보안노드와 이를 제어하는 능동보안관리 시스템으로 구성된다.

능동보안노드에는 능동보안 기능을 수행하는 이동형 센서를 수신하고 실행할 수 있는 이동형 센서 엔진이 탑재된다. 이동형 센서 엔진은 이동형 센서에게 하부 시스템에 독립적인 수행 환경을 제공한다. 능동보안관리 시스템은 능동보안관리를 수행하기 위한 능동보안관리 엔진이 추가로 탑재된다.

그림 1은 이동형 센서 엔진과 능동보안관리 엔진의 기능 블록을 나타낸 것이다.

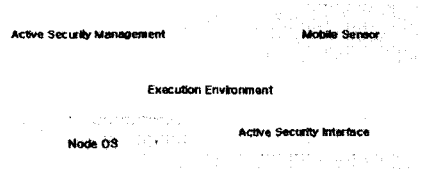

그림 1 능동보안관리 실행환경

능동보안기술은 사이버 공격에 대한 탐지 및 대응 기능을 이동형 센서로 구현하고 보안 취약 지점에 집중 배치하며 침입자의 근원지에서 고립시키는 신속하고 효율적이며 강력한 대응 방안을 제공한다. 그리고 보안 메커니즘이 자동으로 생성, 복제, 소멸되고, 능동적으로 보안 서비스의 프로그래밍이 가능한 능동보안 관리 기술을 제공함으로써 사용자 종단간의 안전한 상호 연동형 서비스 환경을 제공한다. 또한 시스템의 수행 환경 및 네트워크 노드의 수행 환경을 능동화 하여 보안 환경 변화에도 하드웨어나 소프트웨어의 변동 없이 전체적인 보안 도메인 상에서 보안 기능의 업그레이드가 가능하며, 전체 도메인의 보안 구조를 자동으로 재구성함으로써 새로운 사이버 공격에 대하여 즉각적인 대응을 할 수 있다.

III. 침입자 역추적 메커니즘

TCP 확장 연결 공격은 telnet, rlogin, FTP와 같은 TCP 계열의 리모트 접속 서비스를 이용하여 여러 호스트들을 경유한 침투를 시도함으로써 침입자의 위치를 위장한 후 공격을 시도하는 우회 공격이다.

TCP 확장 연결 공격을 역추적하기 위해서는 경유지 노드와 경유지 도메인의 보안관리시스템과의 연계가 필수적이다. 따라서 호스트에서 발생하는 세션을 감시하고 세션에 대한 기록을 남기는 세션 로그 에이전트를 각 호스트에 상주시키고 보안관리시스템에는 세션 로그 매니저를 탑재하여, 특정 세션에 대한 과거 접속 정보에 대한 추적이 가능하게 한다.

그림 2는 TCP 확장 연결 공격에 대한 역추적 과정과 대응, 그리고 역추적의 결과를 통보하는 메커니즘을 나타낸 것이다.

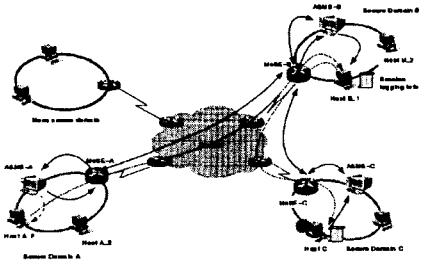

그림 2 침입자 역추적 및 대응

침입이 발생하면 침입 대상 호스트의 침입탐지 시스템에서 보안관리시스템으로 경보를 전달한다. 이 경보에는 침입을 시도한 호스트의 정보와 침입 대상 호스트의 정보가 포함된다. 경보를 받은 보안관리시스템은 역추적을 위한 이동형 센서를 생성하여 침입을 시도한 호스트가 속한 도메인으로 전송한다.

이동형 센서는 목적지로 이동하는 도중 자신의 도메인의 게이트웨이 라우터와 침입을 시도한 호스트가 속한 도메인의 게이트웨이 라우터에서 침입을 시도한 호스트와 침입 대상 호스트와의 세션을 차단한다.

침입자 호스트가 속한 도메인의 게이트웨이 라우터에 도착한 이동형 센서는 현재 도메인의 보안관리시스템으로 이동하여 침입자 호스트와 침입 대상 호스트와의 세션 정보 및 침입 정보를 전달한다.

보안관리시스템은 이동형 센서로부터 전달받은 정보와 침입을 시도한 호스트의 세션 로그 에이전트에 기록된 정보를 비교하여 해당 호스트가 실제 침입자인지 단순히 침입의 우회 경유지로 사용되었는지를 파악한다. 만약 해당 호스트가 경유지로 사용되었다면 보안관리시스템은 세션 로그 에이전트에 기록된 정보를 토대로 새로운 이동형 센서를 경유지 호스트와 세션이 이루어진 호스트가 속한 도메인으로 전송한다.

이러한 역추적을 반복하여 침입자 호스트의 세션 로그 에이전트가 기록한 로그 정보에 더 이상 다른 호스트와의 세션이 존재하지 않으면 해당 호스트를 침입의 근원지로 판단하고, 침입자의 IP를 차단하여 네트워크로의 접근을 완전 봉쇄한다.

침입자 역추적과 그에 대한 대응을 한 후, 침입자 도메인의 보안관리시스템은 역추적에 대한 결과를 통보하기 위한 새로운 이동형 센서를 생성하여 역추적의 역순, 즉 침입이 이루어진 경로를 따라서 전송한다. 역추적 결과 통보를 위한 이동형 센서는 침입 근원지 정보를 각 도메인의 보안관리시스템에 알리고, 경유지로 사용된 호스트와 침입 대상 호스트와의 세션 차단을 해제한다.

IV. 결론

지금까지 능동보안기술을 이용하여 TCP 기반의 확장 연결 공격에 대한 역추적 메커니즘을 기술하였다. 이동형 센서 기술을 이용한 능동보안기술은 공격에 대한 탐지 및 대응을 쉽게 수용하여 이를 동적으로 수행할 수 있으며 침입자 근원지를 역추적하는 과정을 능동화함으로써 침입자에 대한 신속하고 효율적인 대응을 가능하게 한다.

이를 실제 네트워크 보안에 이용하기 위해서는 능동보안관리시스템과 능동보안노드의 안전성 및 이동형 센서에 대한 인증에 대한 연구가 진행되어야 할 것이며, TCP 기반의 공격 이외에 여러 공격에 대한 역추적 및 대응 메커니즘이 연구되어야 한다.

참고문헌

[1] 방효찬, 손선경, 나중찬, 손승원, "액티브 네트워크를 이용한 능동 보안 관리 프레임워크",

COMSW'2002, 2002.

[2] 이수형, 김현주, 나중찬, 송승원, "능동보안 기술에서의 세션 추적 메커니즘", *COMSW'2002*, 2002.

[3] S. Bhattacharjee, K. L. Calvert ad E. W. Zegura, "An Architecture for Active Networking", *In Submitted to IEEE Infocom'97*, 1997.

[4] D. Schneckenberg, K. Djahandari, et Al., "Cooperative Intrusion Traceback and Response Architecture(CITRA)", *DISCEX*, 2001.