액티브코드 기반의 실시간 역추적 시스템

지정훈° 남택용 손승원
한국전자통신연구원 정보보호연구본부 네트워크보안연구부
(jhjee°, tynam, swsohn)@etri.re.kr

Active Code based Real-Time Traceback System

Junghoon Jee° Taekyong Nam, Sungwon Sohn
Network Security Department, Information Security Research Division, ETRI

요 약

본 논문에서는 액티브코드를 이용한 실시간 역추적시스템에 대하여 논한다. 본 시스템은 우회공격의 연결특성을 이용하여 TCP 응용프로그램의 응답메시지에 액티브코드를 덧붙였다. 덧붙여진 액티브코드는 침입자의 근원지 소스측으로 실시간 이동하면서 네트워크 중간노드에서 침입자의 공격에 유연하게 대응한다. 또한, 본 시스템에서는 데이터은닉기법을 적용하여 중간 경유호스트에서 별도의 역추적 시스템을 도입할 필요가 없도록 기존의 환경에 투명성을 부여하였다. 이러한 방법을 통해, 기존의 호스트기반역추적 시스템의 신뢰성문제와 deployment 문제를 해결하였다. 본 시스템을 통하여 기존의 네트워크환경에 최소한의 변경으로 침입자의 공격에 실시간적이며 능동적인 대응을 할 수 있다.

1. 서 론

인터넷의 개방성으로 인해 인터넷에 연결된 기관내부의 시스템에 대한 사이버 공격의 위험 또한 늘어나고 있다. 더욱이 인터넷은 패킷 스위칭 방식과 단순 패킷 전송에 기반하고 있어서 네트워크 침입자의 발생시 해당 침입자를 추적하는데 많은 어려움을 야기시킨다[1].

대부분의 네트워크 침입자들은 자신의 위치를 숨기기 위해서 여러 시스템을 우회하여 목적 시스템을 공격한다. 이러한 우회공격에서는 해당 침해사실이 발견되더라도 침입자의 근원지 소스를 파악할 수 없으므로 침입자로부터의 차후 공격을 완전히 근절할 수 있는 방안이 없다.

본 논문에서는 우회공격의 연결특성을 이용한 실시간 역추적기법에 대하여 논한다. 우회공격에서는 침입자가 여러 호스트를 경유하더라도 실제 침입자의 패킷과 그에 대한 응답의 패킷은 침입자의 호스트로부터 여러 경유호스트를 거쳐 대상 목적지호스트에 전달된다. 이러한 점을 고려하여 본 논문에서는 대상 목적지 호스트에서 응답시 액티브코드를 덧붙이도록 한다.

액티브코드는 이동코드의 형식을 가지며, 일반 응답메시지의 payload 에 덧붙여져서 여러 경유호스트를 거치며 침입자의 호스트측으로 전달된다. 또한, 액티브코드는 네트워크 중간노드인 라우터에서만 실행되며 중간 경유호스트에서는 은닉됨으로써 호스트에 대한 신뢰문제와 실행환경의 deployment 문제를 해결한다.

본 논문의 구성은 다음과 같다. 2장에서는 본 시스템의 설계가이드라인에 대해서 살펴보고 3장에서는 역추적시스템의 구조에 대하여 기술한다. 4장에서는 관련연구를 살펴보고 5장에서 결론을 맺는다.

2. 설계가이드라인

본 시스템은 아래와 같은 점을 고려하여 설계되었다.

- 우회공격의 연결특성 이용

우회공격의 경우 침입자가 여러 호스트를 경유하여 목적지 대상 호스트에 침입한다. 이러한 경우, 침입자의 명령라인상에서의 명령은 침입자의 호스트로부터 경유호스트를 거쳐 대상 목적지까지 전달된다. 또한, 이러한 명령에 따른 응답메시지도 대상 목적지에서 경유호스트를 거쳐 침입자의 호스트까지 전달된다. 본 논문에서는 이점에 주목하여 응답메시지의 조작을 통해서 침입자를 추적하도록 한다. 이러할 경우, 기존의 호스트에서의 세션매칭 등의 기법등이 불필요하게 되어 매우 효과적이다.

- 네트워크기반의 역추적

우회공격의 경우 경유호스트는 이미 침입자로부터 침해를 당한 시스템이다. 이러한 시스템에 설치된 보안모듈에 근거하여 역추적하는 것은 시스템의 신뢰성을 떨어뜨린다. 본 논문에서는 상대적으로 침해가 적은 네트워크 중간노드인 라우터측에 역추적 시스템을 지원하는 모듈을 설치하도록 한다. 이러한 방식으로 중간 경유지의 호스트의 도움없이 역추적을 수행할 수 있다.

- 이동 코드기술의 적용

Sleepy watermark 시스템[2] 에서는 침입자의 명령에 따른 응답메시지에 watermark 정보를 덧붙여서 네트워크 라우터단에서 watermark 를 식별하여 라우터들간의 메시지교환에의한 역추적을 수행하였다. 본 논문에서는

이동코드를 응답메시지에 덧붙임으로써 역추적 수행에 자율성을 부여하였다. 덧붙여진 액티브코드는 경유라우터단에서 패킷 블록킹등의 기능을 수행하며, 침입자 호스트 부근의 경계라우터에서 침입자를 고립시킨다.

- 경유호스트에 대한 투명성 제공

침입자의 공격은 글로벌네트워크차원에서 발생되고 있는 상황이다. 이러한 상황에 대응하기위하여 역추적을 지원하기 위한 모듈을 인터넷에 연결된 모든 호스트에 설치할 수는 없는 상황이다. 또한, 경유호스트에서 기존에 사용하고 있던 응용의 변경을 요하면 안된다. 본 논문에서는 경유호스트에 어떠한 역추적 모듈을 설치하지 않음과 동시에 기존의 호스트에 설치된 응용에도 전혀 영향을 주지 않도록 데이터은닉기법[3]을 이용하였다. 이러한 방식으로 본 역추적 시스템은 피해 대상호스트와 네트워크상의 보호영역의 경계라우터단에만 설치를 요한다.

- 실시간 역추적 시스템

대부분의 네트워크침입은 침입발생시 많은 시간이 경과하면 거의 역추적이 불가능하다. 가급적 빠른 시간내에 역추적이 수행될수록 역추적 성공률은 높아진다. 본 논문에서는 이러한 점에 주목하여 침입자의 침투가 이루어지는 동안에 실시간적인 역추적을 수행하도록 한다. 침입자의 명령에 실시간 대응하는 응답메시지에 액티브코드를 덧붙임으로써 실시간 역추적을 수행한다.

3. 시스템구조

3.1 전체구조

본 논문에서 제안한 추적시스템의 전체구조는 다음 그림 1과 같다. 각 네트워크도메인의 경계라우터에는 액티브코드를 실행시킬수 있는 엔진을 갖는다. 이러한 엔진은 기존의 라우터내에 이식되거나 게이트웨이의 형식으로 설치될 수 있다.

피해호스트에는 침입을 탐지하는 기능과 침입사실의 발생시 액티브코드를 생성하여 메시지에 전달하는 모듈이 설치되어있다. 피해호스트의 기존 TCP 기반 서비스는 이러한 기능을 위하여 변경되어야한다.

침입자의 호스트와 경유호스트간과 경유호스트와 피해자의 호스트사이에는 독립적인 TCP 연결을 가지며, 중간 경유호스트에서는 두개의 연결간의 설정된 세션을 통해 데이터전달기능만을 수행한다.

침입자 호스트로부터의 침투명령이 경유호스트를 거쳐 피해호스트에 전달되면 피해호스트에서는 응답메시지에 액티브코드를 덧붙여전달한다. 액티브코드는 전달되면서 네트워크상의 액티브 실행엔진에서 패킷블록킹등의 기능을 수행한다. 주목할 점은 전체 인터넷의 모든 노드에서 액티브 실행엔진을 제공할 필요가 없다는 점이다. 액티브코드의 블록킹등의 과정을 통해서 그림 2 와 같이 물리적인 네트워크 토폴로지상에서 침입자에 대항하기위한 논리적인 신뢰네트워크가 동적으로 구성된다.

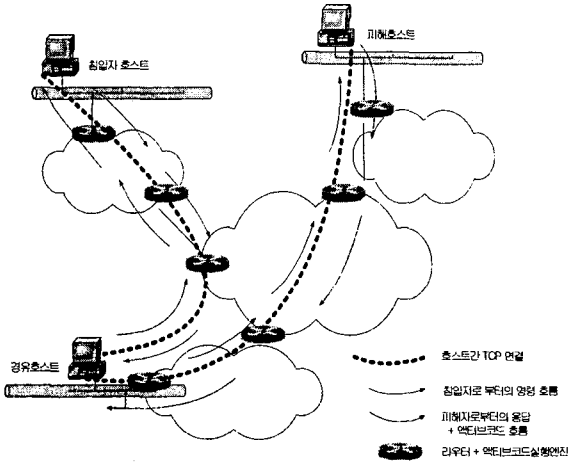

그림 1. 전체구조

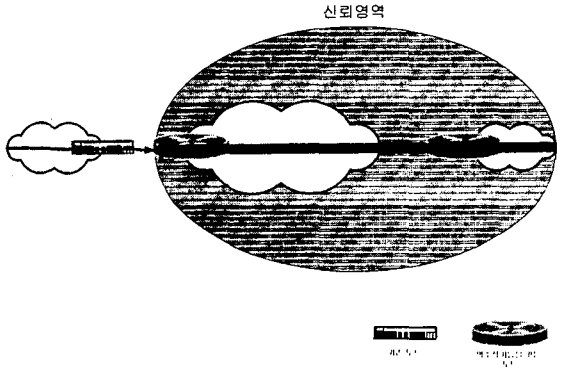

그림 2. 역추적시스템에 의한 신뢰네트워크

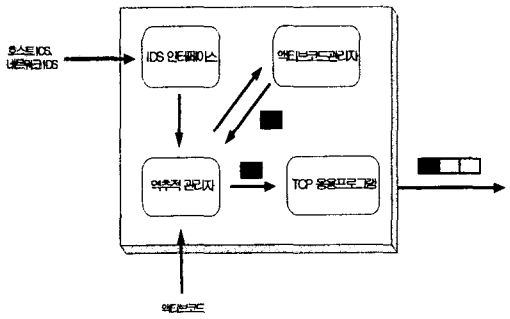

그림 3. 역추적 시스템 구조

3.2 역추적 시스템 구조

호스트를 보호하기 위하여 설치되는 역추적 시스템의 구조는 그림 3과 같다. 역추적 시스템은 역추적관리자, IDS 인터페이스, 액티브코드관리자와 TCP 응용프로그램으로 구성되며 각각은 아래와 같은 기능을 수행한다.

- 역추적관리자

네트워크로 전달된 액티브코드로부터 역추적관련정보를 전달받는다. 이러한 정보에는 현재 역추적노드 및 각 노드에서의 대응결과등이 있다.

- IDS 인터페이스

네트워크 IDS 와 호스트 IDS 로부터 침입발생정보를 전달받는다. 전달받은 정보를 역추적관리자측으로 전달한다.

- 액티브코드관리자

액티브코드를 관리한다. 역추적 관리자에서의 액티브코드 요청시 적합한 액티브코드를 역추적 관리자측에 전달한다.

- TCP 응용프로그램

역추적관리자의 요청에 의해 응답메시지에 액티브코드를 덧붙여서 연결된 호스트로 메시지를 전달한다.

4. 관련연구

CIS (Caller Identification System) [4] 은 우회공격에 대한 추적방안을 제시한 선도적인 연구다. 해당 연구에서는 기존의 TCP Wrapper [5] 를 확장한 ETCPW (Extended TCP Wrapper) 고안하여 사용자가 시스템에 접근하기 전에 이전 경로상의 모든 시스템에 질의하여 경로를 확인함으로써 침입자의 경로위조를 원천적으로 봉쇄한다. 하지만, 해당 연구는 시스템에서 사용자의 세션정보관리에 대한 구체적인 명시가 없고 침입자의 재사용공격에 대한 대처방안이 없다는 단점을 갖는다.

AN-IDR (Active Networks Intrusion Detection and Response) 프로젝트 [6] 에서는 사용자의 연결 요구 패킷에 escort 라는 프로그램을 덧붙임으로써 침입자의 우회공격을 추적하는 메커니즘을 제시하였다. 해당 연구는 침입자를 추적하기 위하여 액티브 네트워킹기술을 도입한 새로운 접근방식을 보여주었으나 다음과 같은 문제점을 갖는다. 첫째, 일반 사용자의 적법한 연결을 포함하여 모든 연결요구패킷에 대하여 프로그램을 덧붙이는 것은 상당한 부담을 초래한다. 둘째, 네트워크 라우터에서 프로그램을 덧붙이기 위해서는 해당 라우터에서 계층 4 또는 5 에서 프로세싱을 수행해야 한다. 이것은 라우터의 고속화를 위해서 더욱 낮은 계층에서 패킷을 전달하는 추세에 비추어 비 효율적이라 할 수 있다. 마지막으로 사용자 레벨의 프로그램을 통하여 시스템에서 세션을 추적하는 구체적인 방 안이 제시되지 않았다.

IDA (Intrusion Detection Agent) 시스템 [7] 은 이동에이전트기술을 침입자의 추적에 적용하였다. 해당 연구는 자동화된 이동에이전트객체를 통하여 추적을 수행하여 관리자의 부담을 덜고 보다 침입에 대한 즉각적인 추적을 수행할 수 있다는 점에서 가치가 있으나 추적의 범위가 특정 네트워크 도메인내로 한정되고 시스템에서 사용자의 세션관리에 대한 명확한 방안이 제시되지 않은 단점을 갖는다.

응답메시지에 watermark 를 덧붙임으로써 역추적을 수행한 Sleepy watermark 시스템[2] 은 우회공격의 연결특성을 고려하였다는 점에서 주목할 만하다. 하지만, 네트워크 중간노드에서 watermark correlation 에 따른 부담, watermark 의 유일성 보장문제, 역추적을 위한 중간노드간의 메시지교환에 따른 부하등이 지적된다.

5. 결론

본 논문에서는 액티브코드에 기반한 실시간 역추적 시스템을 제시하였다. 본 시스템은 우회공격의 연결특성을 이용하여 TCP 응용프로그램의 응답메시지에 액티브코드를 덧붙였다. 데이터은닉기법을 적용하여 중간 경유호스트에서 별도의 역추적 시스템을 도입할 필요가 없도록 기존의 환경에 투명성을 부여하였다. 따라서 본 시스템은 기존의 호스트기반역추적 시스템의 신뢰성문제와 deployment 문제를 해결한 네트워크기반의 역추적시스템이며 침입자를 효과적으로 추적하기위하여 실시간적인 역추적을 수행한다.

참고문헌

[1] F. Buchholz et al., " Packet Tracker," CERIAS Final Report, available at http://www.cerias.purdue.edu/traceback/.

[2] Xinyuan Wang et al., " Sleepy Watermark Tracing: An Active Network-based Intrusion Response Framework" , IFIP Conference on Security, 2001.

[3] W. Bender, D. Gruhl, N. Morimoto and A. Lu. Technique for Data Hiding, IBM Systems Journal, Vol. 35, Nos. 3&4, 1996.

[4] H. Jung et al., " Caller Identification System in the Internet Environment," UNIX Security Symposium IV Proceedings, pp. 69-78, 1993.

[5] W. Venema, " TCP Wrappper, Network Monitoring, access control, and booby traps," In Proceedings of the USENIX Security III Symposium, pp. 85-92, 1992.

[6] D. Schnackenberg et al., " Cooperative Intrusion Traceback and Response Architecture (CITRA)," DISCEX' 01 Proceedings, pp. 56-68, 2001.

[7] M.Asaka et al., " A Method of Tracing Intruders by Use of Mobile Agents," INET'99, 1999.