액티브 네트워크 기반 세션 추적 및 대응 메카니즘

이수형*, 나중찬*, 손승원*

*한국전자통신연구원, 네트워크보안연구부

Session Tracing and Response Mechanism based on Active Network

Soo-Hyung Lee*, Jung-Chan Na*, Sung-Won Sohn*

*Network Security Department, ETRI

요 약

인터넷 상에서 사이버 공격은 특정 서버에 대해 서비스 요청 패킷을 플러딩 시킴으로써 상용 서비스의 제공을 방해하는 패킷 형태의 공격과 특정 호스트에 연결 설정을 통해 침입함으로써 특정 정보의 획득이나 변경을 목적으로 하는 세션 설정 형태의 공격이 있다. 본 논문에서는 로컬 도메인 보호에 치우쳐 있는 현재의 네트워크 보안 메카니즘에 비해 공격자에 대해서 강력한 대응을 가능하게 하는 공격자의 공격 세션 추적 및 차단에 대한 액티브 네트워크 기반의 네트워크 보안 메카니즘에 대해 기술한다.

I. 서론

네트워크 공격 기법의 다양화 및 지능화함에 따라 사이버 공격의 횟수가 증가하고 그 피해의 정도가 점차 커지고 있다. 그 특징으로는 다수의 분산 에이전트를 이용한 특정 상용 서버의 서비스 제공을 마비시키는 분산 서비스 거부 공격의 출현과 해외 해커들의 국내 전산망을 우회 루트로 활용한 사례의 증가 등 사이버 공격행위가 점차 범죄의 수단으로 이용되는 추세에 있다. 이런 환경 변화에 따라 사이버 공격에 대한 기존의 시스템 보안 및 네트워크 보안 메카니즘에 비해 보안 시스템 사용자 지향적이며, 공격자에 대해 능동적이고 강력한 대응이 가능한 네트워크 보안 기술의 개발 필요성이 대두되고 있다.

현재의 네트워크 보안 관리는 보안 대상이 되는 로컬 네트워크 도메인 상에 침입탐지시스템과 방화벽 시스템을 결합하여 운용한다. 이를 통해 해당 도메인으로 이루어지는 공격을 어떻게 효과적으로 탐지하고 해당 공격 트래픽을 차단하여 해당 도메인을 보호할 것인가에 맞추어져 있다. 반면 공격의 경우 분산서비스거부 공격과 같이 연결 설정 없이 다량의 특정 서비스 요청 패킷을 발송하는 UDP 성격의 공격과 특정 시스템에 연결 설정을 하고 이루어진 접속을 통해 해당 시스템의 정보 획득이나 변경을 목적으로하는 TCP 성격의 공격으로 나누어 질 수 있다. 분산서비스 공격의 경우 요청 패킷 발송 시 소스 주소를 거짓 주소를 설정하고, 연결 설정에 의한 공격의 경우에도 공격자 호스트로부터 목표 호스트로 직접 접속하는 것이 아니라 중간에 여러 호스트를 경유하여 접속하게 된다.

따라서 특정 공격에 대한 탐지와 해당 공격 트래픽의 차단이 로컬 네트워크 도메인 상에서 이루어지더라도 공격자는 네트워크에 대한 접근을 계속 유지할 수 있다. 이를 통해 공격자는 다른 목표 시스템에 대한 공격이나 동일한 시스템에 대해서도 공격 기법의 변경이나 경유 호스트의 변경을 통해 제2, 제3의 공격이 가능하게 된다.

만약 공격자의 실제 위치에 대한 추적이 가능하다면 공격이 이루어질 경우 공격자의 실제 위치를 추적하고 공격자를 네트워크로부터 단절시킴으로써 그 이후에 이루어질 수도 있는 모든 공격에 대한 예방 조치를 취할 수 있다. 공격자의 위치를 추적하기 위해서 UDP 형식의 공격과 TCP 성격의 공격에 적용되는 기법이 달라질 수 있다. 일반적으로 네트워크 노드에서 라우팅 패킷에 대한 로그를 남길 경우 두 유형의 공격 모두에 대해서 추적이 가능하나, TCP 성격의 공격의 경우 호스트 사이에 세션 연결이 설정되고 유지되므로 이를 이용하는 것이 효과적이다.

액티브 네트워크는 네트워크 노드에 프로그래밍 기능을 부가함으로써 사용자의 요구 기능의 변화를 네트워크 상에서 원할이 수용할 수 있도록 하기 위해 연구 중인 네트워크 플랫폼이다. 본 논문에서는 액티브 네트워크 기반에서 TCP 형식의 공격이 이루어지는 세션에 대한 추적 및 대응 메카니즘에 대해 다룬다.

2장에서는 관련 연구로써 미국에서 진행 중인 AN-IDR(Active Network Intrusion Detection and Response)에 대해 언급하고, 3장에서 제안

메카니즘에 대해 다룬 후 4장에서 결론을 맺도록 한다.

II. AN-IDR

1. AN-IDR 개요

AN-IDR은 액티브 네트워크 기반으로 글로벌한 네트워크 수준에서 사이버 공격을 탐지하고 역추적하여 네트워크로의 연결성을 단절하는 보안 기능의 구현을 목표로 미국방성 산하 DARPA에서 연구 중인 과제이다. 기본적인 공격자 추적을 위한 메카니즘은 IDIP(Intrusion Detection Isolation Protocol)로 구현된다. AN-IDR에서 사용되는 액티브 프로그램은 적용될 요소 보안 기능별로 특정 노드에 상주하는 경우, 네트워크의 노드를 이동하며 필요에 따라 자기복제 및 변환하는 경우, 여 실행되는 액티브 프로그램, 특정 패킷의 부착되어 특정 노드로 이동하는 경로 상에서 실행되는 경우로 분류되면 세션 추적을 위해서는 마지막 유형의 액티브 프로그램이 사용된다. 다음은 IDIP에서의 추적 및 차단 메카니즘의 기본 개념이다.

- 추적을 위해 네트워크 노드는 자신이 라우팅한 모든 패킷에 대한 로그 정보를 남긴다.

- 실제 추적이 이루어 질 경우 공격 당한 시스템으로부터 인접 네트워크 노드에게 해당 패킷의 라우팅 여부를 질의 라우팅한 네트워크 노드는 다시 인접 노드에게 해당 패킷의 라우팅 여부 질의 공격자의 위치가 파악될 때 까지 반복

- 인접 노드로 추적 요청을 할 경우 자신이 취할 수 있는 대응 방안을 임시적으로 수행

- 트래픽의 차단은 IDIP가 실장된 방화벽이나 패킷 필터링 라우터에게 해당 트래픽을 차단하여 주도록 지시함으로써 수행.

2. AN-IDR에서 세션 추적 방법

[그림 1]에 같이 공격자가 서버X와 서버 Y를 경유하여 목표 시스템 서버 Z에 침입하는 경우 이들 시스템간에 구성되는 세션을 추적하기 위한 방법을 보였다.

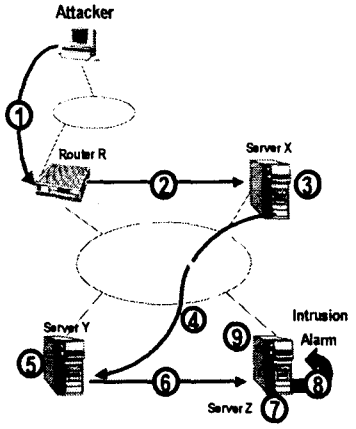

그림 1: AN-IDR 세션 추적 메커니즘

공격자가 서버 X에 대한 연결을 시도할 경우 라우터 R은 해당 연결 설정 요구 패킷에 연결 설정과 관련된 데이터(설정 시작, 종료 호스트 이력)를 설정할 수 있는 프로그램과 해당 데이터를 포함하고 있는 액티브 프로그램인 'escort' 프로그램을 첨부하여 전송한다. 이 후 서버 X에서는 연결 설정과 동시에 'escort'가 설치되어 동작하게 된다.

이후 공격자가 서버 Y로 연결 요청을 하게 될 경우 'escort'는 이전까지의 연결과 관련되 서버 정보를 자신에게 저장한 후 연결 요청 패킷에 자신의 프로그램 복제본을 추가하여 전송하고 서버 Y에서는 서버 X에서의 경우와 마찬가지로 해당 프로그램을 설치하여 운용하게 된다. 이런 절차를 공격자의 연결이 경유되는 모든 서버에서 이루어짐으로써 공격자의 공격 연결이 이루어지게 된 경로 상에 존재하는 모든 서버에 대한 정보를 목표 시스템에서도 관리할 수 있게 된다.

공격이 탐지되면 'escort'에 저장된 정보를 바탕으로 공격자가 네트워크에 접속 지점에 위치하는 라우터 R에 연결 차단 요청을 하게 되고 이를 통해 공격자의 네트워크로의 접속성을 차단하게 된다.

III. 세션 추적 및 차단 메카니즘

세션 추적 및 차단을 위한 하부 플랫폼으로써 액티브 네트워크를 고려하는 이유는 네트워크 노드에서 프로그래밍이 가능하므로, 이를 이용하여 공격자의 경로를 이루는 각 네트워크 세그먼트에서 해당 도메인에 상황을 분석하고 공격 트래픽을 차단하는 메카니즘을 액티브 프로그램이라는 코드의 이동성을 이용하여 수행할 수 있기 때문이다.

하지만 추적 및 차단 메카니즘을 고려할 경우

어는 노드에 액티브 네트워크 기능을 구현할 것인지를 잘 고려하여야 한다. 이는 추후 실제 필드에 도입을 위한 것으로 액티브 네트워크의 실제 구현이 쉽지 않음을 고려하여 액티브 네트워크 기능이 실장될 노드의 수가 최소화되고 기존 백본 네트워크의 변화를 수반하지 않도록 충분히 고려되어야 한다.

[그림 2]는 세션을 추적/차단하기 위한 메카니즘과 그 운용 예를 나타낸 그림이다. 각 로컬 네크워크 도메인마다 보안 기능을 관리할 보안 관리 시스템이 존재하고 이 시스템은 공격자의 세션을 추적하고 차단함에 있어 해당 도메인의 상황을 고려하여 해당 도메인 상에서 적절한 기능을 수행한다. 또한 추적을 위해서는 각 도메인간의 협업 작업이 필수적이고 이를 위해 각 도메인간의 보안관리시스템을 상호 데이터의 교환 및 특정 기능의 수행을 요청할 수 있다.

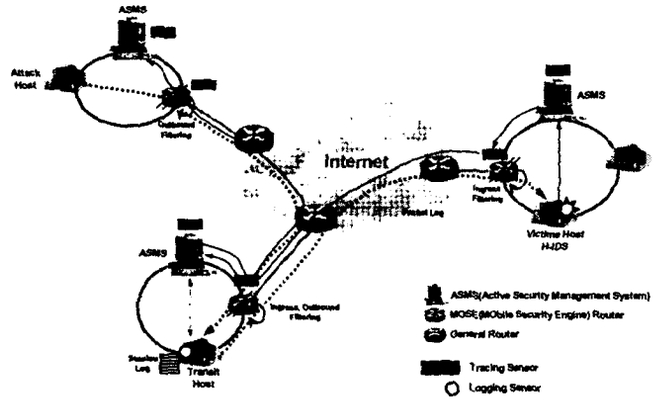

그림2 : 세션 추적 및 차단

세션 추적을 위해 각 호스트에서는 해당 호스트에 로그인한 세션과 타 호스트로 접속해 나간 세션간의 매핑 정보를 관리하고 저장하고 특정 연결에 대한 매핑 정보 요청에 대해 로그 정보를 검색하여 응답할 수 있는 로그 매니저 프로그램이 상주형으로 실행된다. 각 가입자 망이 백본 네트워크로 접속되는 접속점에 위치하는 게이트웨이 라우터는 추적/차단과 관련된 액티브 프로그램을 구현하기 위해 액티브 노드로 구현되었다.

공격이 탐지되면 이를 해당 도메인을 관리하는 보안관리시스템으로 통보하게 된다. 보안관리시스템은 세션을 추적하기 위한 액티브 프로그램인 세션추적센서를 경유 호스트로 파송하게 된다. 세션추적센서는 경유호스트로 이동하는 도중에 액티브 노드인 각 로컬 도메인의 게이트웨이 라우터에서 일차적으로 해당 공격자의 세션을 차단하게 된다. 경유 호스트에 도달한 세션추적센서는 해당 도메인을 관리하는 보안관리시스템으로 이동하여 경유 호스트의 로그 매니저에게 해당 연결에 대한 이전 경유 호스틀 정보를 요청하고 그 결과를 바탕으로 실제 공격자의 위치가 확인될 때까지 위의 과정을 반복하여 수행한다. 공격자의 위치가 파악되면 해당 도메인의 라우터에서 공격자의 트래픽을 차단함으로써 네투워크에 대한 접속성을 차단하게 된다.

[그림 3]는 각 호스트에서 로그 매니저의 전체 기능을 수행하기 위한 모듈의 기능 블록을 보였다. 핵심 블록에는 호스트의 사용자 작업 로그를 수집하고, 수집된 패킷으로부터 네트워크 세션 정보와 시스템 세션 정보를 구축하는 세션데이타수집(SDC) 블록과 이 모듈로부터 사용자 계정 변경

정보를 기록하는 블록(UCR), 해당 호스트로 입출력하는 세션 정보를 기록하는 블록(SDR)이 있다. 외부 타 시스템과의 인터페이스를 위한 통신 블록(SRM)과 세션연결정보 요청을 받아 저장된 정보로부터 해당 데이터를 분석/검색하는 블록(SAS)가 있다. 또한 해당 모듈의 안정성을 보장하기 위하여 통신 데이터를 암호화하고 해당 모듈에서 사용되는 데이터 및 코드의 무결성을 보장하기 위한 블록(DP)과 데이터의 백업 및 삭제와 같은 시스템 관리를 위한 블록(SM)이 있다.

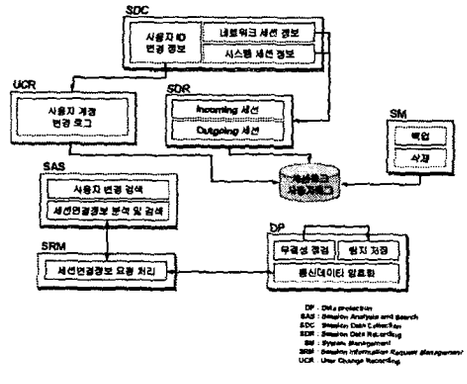

그림 3: 로그 매니저의 기능 블럭

Ⅳ. 결론

지금까지 액티브 네트워크 상에서 세션 설정을 통한 공격에 대한 추적 및 해당 세션의 차단 메

커니즘을 살펴 보았다. 세션 추적이 원할이 이루어지기 위해서는 각 호스트에서의 세션 로그 에이전트의 동작과 그 성능이 관건이고 이를 위한 작업이 현재 진행중에 있는 상태이다. 또한 실제 필드에서 적용되기 위해서는 액티브 네트워크 기능을 구현한 액티브 노드를 어느 범위까지 실제 도입할 수 있을 것인가에 대한 고려가 이루어져야 한다. 또한 각 도메인간의 협업 작업이 필요하게 되므로 서로 상호간의 인증 문제, 자체 교환 데이터의 보안 확보 문제, 각 도메인간의 협업을 이끌어 낼 것인가 하는 행정적인 문제를 해결해 가야 할 것으로 보인다.

현재 프레임워크를 정의하고 각 구성 모듈별 구현을 마쳐 실험실 수준으 테스트베드 상에서 시험이 진행 중인 상태이다. 각 호스트에 실장될 로그 매니저는 하부 플랫폼에 의존적일 수 밖에 없고 현재는 SUN Solaris 플랫폼 상에 구현되어 있는 상태이다. 이런 결과를 실제 필드에 적용하기 까지는 많은 어려움과 해결할 문제가 있을 것으로 생각된다. 하지만 보안에 대한 그 수요나 요구 조건이 점점 더 강화되고 있으므로 실제 적용시 공격자에 대해 강력한 대응 방안을 가짐으로써 보안 분야의 질적 수준을 한 단계 향상 시킬 수 있을 것으로 보인다.

참고문헌

[1] Guy Helmer, Johnny S. K. Wong, Vasant Honavar, Les Miller, Lightweight Agents For Intrusion Detection, Iowa State University, Nov. 27. 2000.

[2] DARPA ITO, Dynamic, Cooperating Boundary Controller , Project Introduction in http://www.darpa.mil/ato

[3] Dan Schneckenberg, Kelly Djahandari and Dan Sterne Infrastructure for Intrusion Detection and Response , DISCEX 2000, Jan. 25 ~ 27, 2000

[4] Peter Mell, Automating Response , UC Davis and Boeing, Intrusion Detection PI Meeting, Feb., 1998

[5] Dan Schneckenberg, Automatic Response to Intrusion , Intrusion Detection PI Meeting, Feb., 1998

[6] Dan Sterne, Active Network Intrusion Detection and Response (AN-IDR) , Boeing and NAI Lab., DARPA FTN PI Meeting, Jul. 20, 2000

[7] Dan Schneckenberg, kelly Djahandari, et. Al., Cooperative Intrusion Traceback and Response Architecture(CITRA) , DISCEX 2001

[8] 이수형, 이승민, 지정훈외 2인, "능동보안기술프레임워크" , NCS2001, 2001. 12. 6 ~ 8