액티브 네트워크 기반의 IP 역추적 시스템

황영철*, 최병선*, 이성현*, 이원구*, 이재광*
한남대학교 컴퓨터공학과*

Active Network-based IP Traceback

Young-Chul Hwang*, Byung-Sun Choi*, Won-Goo Lee*, Jae-kwang Lee*
Dept. of Computer Engineering, Hannam University*

요 약

기존의 정보보호 방식은 시스템 설계 단계부터 반영된 것이 아니기 때문에 서비스 제공 이후에 발생 가능한 다양한 취약점 공격에 대한 효과적인 대응에 태생적 한계를 지니고 있다. 따라서 사이버 공격에 대한 기존의 수동적인 대응에서 벗어나 능동적이고 공격적인 대응을 할 수 있는 기술들이 필요하게 되었다. 본 논문에서는 우선 기존의 망에 적용한 역추적 시스템을 분석한 다음, 정보통신망 자체를 사이버 공격으로부터 보호하며, 정보통신망의 보안 취약점을 없애 해킹이나 정보유출을 원천적으로 차단할 수 있는 능동형 보안 관리 기술인 역추적 시스템을 분석하여 액티브 네트워크 기반의 역추적 시스템을 분석하였다.

1. 서론[1)]

최근의 정보보호 환경에서는 자신의 관리 도메인 내로 침입하게 되는 공격을 어떻게 잘 탐지 할 것인가와 탐지된 공격을 어떻게 효율적으로 차단하여 자신의 도메인을 잘 보호할 것인가에 초점이 맞추어 있다. 따라서 탐지된 침입의 공격자에 대한 대응도 자신의 도메인 경계에서 해당 트래픽을 차단하는 수동적인 방법 이외에는 별다른 방법이 없는 상태이고, 이 경우 자신의 도메인에서 파악한 침입자 정보를 바탕으로 자신의 도메인 입구에서만 해당 트래픽을 차단함으로써 침입자는 자유로이 인터넷을 이용할 수 있을 뿐만 아니라 다른 공격 기술이나 공격 루트를 이용한 제2, 제3의 공격이 이루어 질 수 있다. 반면 인터넷을 이용한 경제 활동 및 그 액수가 점차 증가함에 따라 사이버 공격으로 입게되는 피해는 점차 기업의 생존을 위협하는 수준에 도달하고 있다[1][11]. 따라서 해킹에 능동적으로 대응할 수 있는 기술이 요구된다고 할 수 있으며, 능동적인 해킹 방어를 위한 가장 기본적인 기술로 해커의 실제 위치를 추적하는 역추적 기술을 활용할 수 있어야 한다. 그러나 현재까지 제안된 역추적 기술들은 인터넷이 보유한 다양성을 극복하지 못하여 현재의 인터넷 환경에 적용하는데 어려움이 따른다.

이에 본 논문에서는 해킹으로 판단되는 침입에 대하여 효율적으로 역추적 하기 위해서 액티브 네트워크 기반의 역추적 시스템을 분석한다. 2장에서는 역추적 시스템을 동향을 분석하여 보고, 3장에서는 IDIP에 대해서 분석하였으며 4장에서는 액티브 네트워크 기술을 이용한 역추적 방법인 AN-IDR을 분석하였다. 5장에서는 결론을 맺고 향후 연구방향을 기술하였다.

1) 본 연구는 한국과학재단 목적기초연구 (R01-2002-000-00127-0)지원으로 수행되었음

2. 관련연구

2.1 CIS(Caller Identification System)

CIS(Caller Identification System)는 H.T. Jung에 의해 1993년 제안된 시스템이다. 이 역추적 시스템은 실제 역추적이라기 보다는 미리 사용자가 거쳐온 시스템의 목록을 관리하는 것으로, 정상적인 사용자들이 접속하는 데도 많은 지연을 초래하게 된다. 또한 침입이 발생하기 이전에 수행하는 작업이 많기 때문에, 자원 활용 면에서 비효율적이라고 할 수 있다. 그리고, CIS는 접속을 원하는 사용자가 거쳐온 시스템 각각에 대한 인증을 거쳐가는 시스템마다 요구하므로 이로 인한 네트워크 부하가 크고, CIS에 오고 가는 인증을 위한 메시지의 무결성을 보장하지 못하는 단점이 있다[2].

2.2 SWT(Sleepy Watermark Tracing)

Sleepy watermark 역추적 시스템은 침입에 대한 응답 패킷에 워터마크를 삽입하여 역추적을 수행한다. SWT 기법은 다음과 같은 형태로 이루어진다.
한 네트워크에는 guardian gateway가 존재하고, 이와 연동되어 동작하는 guarded host가 존재한다. 최초 침입이 발생할 때까지는 아무런 추가적인 동작이 진행되지 않은 일반적인 상태로 존재한다. 침입이 발생되면 이는 guarded host내의 IDS에 의해 탐지된다 guarded host의 SWT subsystem의 sleepy intrusion response 모듈의 작동이 시작되고 이때부터 일반 host에 도착되는 패킷에 의한 응답은 watermark enabled application에 의해 작성되기 시작한다. 이는 일반적인 응답패킷에 워터마크를 삽입하여 송신을 시작한다. 이렇게 역추적이 시작되면 이는 guardian gateway의 active tracing 모듈과 연동되어 워터마크가 삽입된 패킷을 찾기 시작한다. 본 SWT 역추적 기법은 공격에 대한 응답 패킷을 이용하여 해커의 위치를 추적하기 때문에 빠르고 정확한 역추적이 가능하다. 그러나, watermark enabled application이 필요하다는 문제로 인해 실제 인터넷 환경에 적용하기에는 큰 문제를 가지고 있다. 또한 해커에 의해 사용되는 연결이 암호화 되는 경우에는 역추적이 전혀 불가능할 수 있다는 단점이 존재한다[1][2].

2.3 ICMP 기반 역추적 시스템

ICMP 기반 역추적 시스템에서는 역추적을 위해 IETF Internet Area의 itrace Working Group에서 표준화 중인 ICMP Traceback Message를 이용하여 역추적을 진행한다.

표 2. 역추적 시스템 분석 및 비교

방식	장점	단점
ICMP 기반	-역추적 성공률이 높다 -암호화되거나 스푸핑된 패킷에 대해 역추적 가능 -IETF 표준화 진행중(ICMP Traceback Message)	- 에이전트 문제
수동 역추적 기술	- 신뢰성 보장	-시간 소용가 많음
CIS를 이용한 역추적	- 특정 도메인내에서 빠른 역추적 가능	- 비표준화, 비현실성
Tumbprint를 이용한 역추적	- 정확한 Tumbprint만 있으면 바른 역추적 가능	- Tumbprint 값의 동기화와 시스템 시간의 정확성을 요구

해당 기술은 수사적 관점에서 해커의 위치를 보다 정확하고 신속하게 파악하고자 하는 공공기관에 적용할 수 있으며, 기업체 및 공공기관 내부망에 설치하여 내부망내의 최초 공격 지점을 찾아 내부망 보호를 위한 기술로 활용할 수 있다[3].

3. IDIP(Intruder Detection and Isolation Protocol)

3.1 IDIP(Intruder Detection and Isolation Protocol)

IDIP는 DC(Discovery Coordinator) 시스템이 해당 도메인의 전체 IDIP 기능을 조율하고 관할하게 되는 'community'와 그 경계를 IDIP가 실장된 시스템으로 이루어지는 'neighborhood'로 이루어진다. 하나의 'community' 내에는 1개의 DC 시스템만이 존재하고, 이 DC 시스템이 해당 'community' 내의 IDIP 기능을 제어, 관할하게 된다. 따라서 'community'는 하나의 독립된 IDIP 관리(administrative) 영역으로 볼 수 있다[7]. 'neighborhood'는 그 경계 안에 IDIP가 실장된 시스템이 존재하지 않는 경우로 IDIP를 구성하는 가장 기초적인 네트워크 요소로 볼 수 있다[4][5]. 그림 1은 IDIP에서의 네트워크 구조를 보여주고 있다.

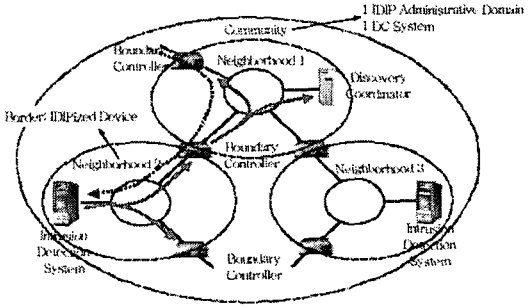

그림 1 IDIP에서의 네트워크 구조

IDIP 네트워크에서 DC는 공격 경로 상에 있는 각 IDIP 노드로부터 상태에 관한 보고를 접수하고 해당 공격에 대한 전체 도메인 상에서의 전체적인 그림을 그리기 위해 각 노드로 접수된 보고 정보를 상호 결합(correlation)하고 각 IDIP가 임시적으로 수행한 대응 방안을 해제하거나 추가적인 대응을 지시함으로써 전체 도메인 상에서의 최상의 대응 방안을 실행하게 된다[6].

3.2 IDIP 메시지

IDIP는 다음과 같은 세 개의 메시지 유형을 지원하면서 공격자 추적 및 대응 기능을 수행한다. 먼저 IDIP는 공격이라고 의심할 만한 연결이 감지되었을 경우 추적(trace) 요청 메시지를 발생한다. 여기에는 공격 이벤트와 해당 연결에 대한 내용이 초함되어 있

다. 이 추적 요청 메시지를 받은 각 IDIP 노드는 이들 정보로부터 자신이 침입 경로 상에 위치하고 있는지를 판단하게 되는데, 자신이 공격 경로 상에 있다고 판단되면 이웃으로 추적(trace) 메시지를 보내기 되는데 보내기 전에 자신을 거쳐간 공격자에 대해 네트워크주소변환(NAT: Network Address Translation)이나 방화벽 프락시(firewall proxy) 등에서 이루어진 경로변경정보(translation record)를 메시지의 끝에 작성해 둠으로써 보다 효율적인 침입자 추적을 보장한다. 또한 자신의 로컬 정책에 따라 해당 공격에 대해서 일시적인 대응을 수행할 수도 있다. 두 번째 메시지는 보고(report) 메시지로 추적 메시지를 받은 각 노드는 DC로 자신이 공격의 경로 상에 존재하는 노드인지를 판단한다. 만약 경로 상에 존재하면 해당 공격에 대해서 대응을 했는지, 어떤 대응을 했는지 등에 대한 정보를 보고하기 위한 메시지이다. 이때 동일한 공격이 반복될 경우 이에 대해서는 하나의 요약된 형태의 메시지가 DC로 전송된다. 마지막으로 지시(directive) 메시지는 보고 메시지를 받은 DC는 이 메시지를 분석한 후, 가장 효과적인 대응 지침을 도출하여 그에 대한 수행을 각 노드에게 지시한다. 이때 실제 사용되는 메시지는 공격에 대해 각 노드들이 취했던 대응 중지를 지시하는 undo 메시지와 취해진 대응에 부가적인 대응 지침의 수행을 지시하는 do 메시지가 있다[6][7].

3.3 공격자 추적 및 대응 기능

액티브네트워크 기반의 역추적 시스템에서 만약 침입이 발생할 경우 먼저 침입탐지시스템이 공격이 발생하였음을 인접 IDIP 노드에게 알리고 공격자의 위치에 대한 역추적을 요청하게 된다. 이때 역추적을 요청하는 것과 동시에 동일 IDIP 노드들에게 대응을 요청하게 된다. 여기에서의 대응이란 해당 도메인의 보안 정책에 따라 해당 도메인에서 수행할 수 있는 대응 방법이 그 후보가 된다. 역추적 요청을 받게 되면 자신이 해당 공격과 관련된 패킷을 라우팅 하였는지(혹은 호스트의 경우 해당 공격과 관련된 TCP 연결이 자신을 경유하여 나갔는지)를 판단하여 그 결과를 DC에게 보고한다. 만약 자신이 공격 경로 상에 존재한다면 자신의 인접 IDIP 노드(피해 시스템 방향은 제외한)에게 공격자에 대한 역추적을 계속 수행해 주도록 요청하게 된다. 만약 자신이 대응 시스템인 경우 해당 도메인의 보안 정책에 따라 임시적으로 해당 공격에 대한 대응을 수행하고 그 수행 결과를 DC에게 보고한다. 이런 역추적 요청의 일련 과정을 공격자의 실제 위치가 파악될 때까지 반복하여 공격자 경로 상의 IDIP 노드들이 수행하게 된다[8][9].

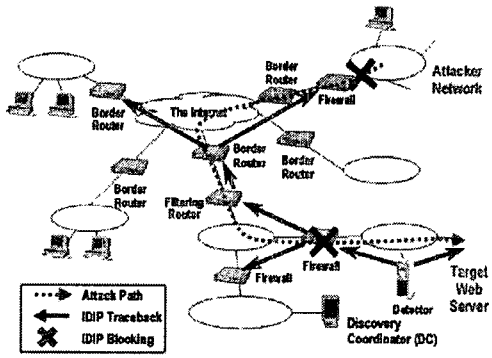

그림 2 추적 결과 및 로컬 대응 결과 보고

4. AN-IDR

AN-IDR은 IDIP가 가지는 정적인 특성으로 인한 유연성의 부족함과 특정 기능 수행상에 있어서의 효율성을 저하를 해결하기 위해 1999년 NAI Lab.과 Boeing 사를 주축으로 하여 DARPA ITO 산하의 Active Network 프로그램 아래에서 수행되었다. 이를 위해 IDIP 메커니즘과 액티브 네트워크 기술을 결합하여 상호 운용함으로써 기존의 정적인 IDIP에 이동성(mobility), 유연성(flexibility), 확정성(extensibility)을 부여함으로써 좀더 발전된 침입자 탐지 추적 기능을 수행하고자 하는 것이다. 따라서 침입자를 탐지 및 추적하여 공격자와 인접한 네트워크 노드에서 공격자의 네트워크에 대한 연결성을 단절함으로써 공격자에 대해 보다 강력한 대응을 하기 위한 목적으로 수행되고 있다[10].

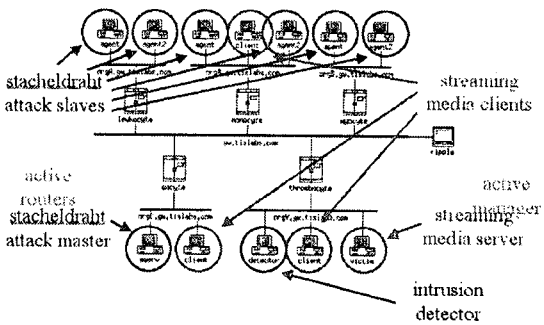

그림 3. 액티브 노드의 구성 및 역할

AN-IDR의 구조는 기존 IDIP의 구조를 그대로 적용하고 있다. 그러나 액티브 네트워크를 기반으로 구성되어 있기 때문에 프로그램들은 네트워크 노드 상의 여러 노드를 이동하고 실행되며, 각 노드에 동적으로 탑재되어 실행되어 진다. TCP 연결기반의 공격에 대한 AN-IDR에서의 공격 추적 메커니즘을 살펴보면

다음과 같다. 우선 다른 호스트로 연결 요청을 할 경우 요청 패킷에 해당 연결 정보를 저장과 다른 호스트에서 해당 연결 상태를 관찰할 코드를 해당 연결 요청 패킷에 첨부하여 전송한다. 이때 첨부하게 되는 액티브 패킷을 'Connection Escort'라 한다. Connection Escort는 처음 연결 시도할 뿐만 아니라, 기 접속한 호스트에서 다른 호스트로 연결을 시도할 경우에도 첨부되어 발생된다. Connection Escort의 첨부는 침입자가 있는 로컬 네트워크에서 백본 네트워크로 접속되는 경계 라우터와 중간 경우 호스트에서 이루어진다. 또한 Connection Escort를 이용한 추적이 이루어지기 위해서는 모든 호스트와 경계 라우터는 액티브 패킷을 인식하고 수행할 수 있는 액티브 노드여야 한다[4][11].

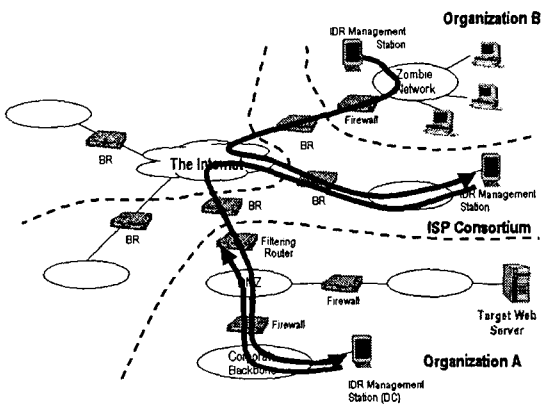

그림 4. AN-IDR 개념

5. 결론 및 향후 연구

기존의 정보보호 방식은 시스템 설계단계부터 반영된 것이 아니기 때문에 서비스 제공 이후에 발생 가능한 다양한 취약점 공격에 대한 효과적인 대응에 태생적 한계를 지니고 있다. 또한 기존의 정보보호 방식에 대한 보안기능이 네트워크 접속점에 위치한 시스템에 구현되어 네트워크 성능 저하를 초래하고 있고, 보안 시스템간의 상호연동이 어려우며 이에 따라 정보보호 인프라 구축이 복잡하고 난이하다고 지적하고 있다[11]. 따라서 본 논문에서는 공격 기법의 고도화에 따라 네트워크 인프라 차원에서 실시간 침입에 대한 탐지 및 역추적 기능을 효율적으로 수행할 수 있는 네트워크 차원의 새로운 보안 기술을 살펴 보았다.

향후 연구로는 ICMP 기반의 역추적 시스템을 분석을 바탕으로 역추적 시스템을 분석 및 설계할 것이며 이를 능동 네트워크 기반으로 발전시켜 새로운 역추적 시스템을 구현하고자 한다. ICMP 역추적 메시지는 현재 IETF internet Area의 itrace Working Group에서 Internet draft로 제출된 상태이며, ICMP 역추적 기법은 라우터에 거쳐 가는 패킷에 대해서 패킷의 일부가 포함된 ICMP 역추적 패킷을 생성하고 목적지 주소로 전송하고, 전송 받은 시스템은 해당 정보를 수집하여, 공격이 검출되면 수집된 정보를 이용하여 해커를 역추적 하는 기법이다. 또한 액티브 네트워크 기술을 이용한 역추적 기법이 실제 적용되도록 하기 위해서 하부 플랫폼에 독립적인 실행 환경을 갖고 이동형 실행 패킷(액티브 패킷)을 적용함으로써 유연성, 확장성을 가지는 능동적인 역추적 시스템에 대한 연구가 이루어져야 할 것이다.

[참고문헌]

[1] 강동호외 3명, "IP 역추적 기술 동향", 주간기술동향, 97-39 한국전자통신연구원

[2] Chun He, Formal Specifications of Traceback Marking Protocols , June 14, 2002.

[3] Steve Bellovin외 2명, "ICMP Traceback Messages", Internet Draft, IETF, February 2003

[4] "차세대 인터넷을 위한 능동 보안 기술 백서", 한국전자통신연구원

[5] 정종민, 이지율, 이구연, "다중 에이전트를 이용한 역추적 시스템 설계 및 구현", 한국정보보호학회 논문지, 제 13권 4호, pp.3-11, 2003. 8

[6] D. Raz, et al., "An Active Network Approach to Efficient Network Management", IWAN'99, 1999

[7] K. Calvert, et al., "Architectural Framework for Active Network", AN Working Group, July, 1999

[8] NAI Labs and Boeing Phantom Works. Intruder Detection and Isolation Protocol (IDIP) Message Layer, NAI Labs Report #02-005, February 2002.

[9] NAI Labs and Boeing Phantom Works. Intruder Detection and Isolation Protocol (IDIP) Application Layer, NAI Labs Report #02-006, February 2002.

[10] Dan Sterne, "Active Network Intrusion Detection and response (AN-IDR)", Boeing and NAI LAB., DARPA FTN PI Meeting, Jul. 20, 2000

[11] 이만영, 손승원, 조현숙, 정태명, 채기준 "차세대 네트워크 보안 기술" 생능출판사, pp.415-430, 2002.11.25