IP 역추적을 위한 액티브 네트워크 기법 적용 방안

최병선* · 이성현*· 이재광*
*한남대학교 컴퓨터공학과

Active Network for IP Traceback

Byung-sun Choi* · Seoung-hyeon Lee *· Jae-kwang Lee*
*Dept. of Computer Engineering Hannam University
E-mail : bschoi@netwk.hannam.ac.kr

요 약

컴퓨터 기술의 발달과 더불어 인터넷의 발전은 고속화되어 왔다. 이에 따라 데이터 전송 속도의 과속화와 대용량의 데이터 전송 등의 기술이 증가되고 이로 인해 업무 효율을 향상됨에 따라 시스템 및 네트워크 차원에서 보안 기능에 대한 요구도 날로 증가하고 있다. 따라서 본 논문에서는 정보통신망 자체를 사이버 공격으로부터 보호하며, 정보통신망의 보안 취약점을 없애 해킹이나 정보유출을 원천적으로 차단할 수 있는 능동형 보안 관리 기술인 역추적 시스템을 분석하고 액티브 네트워크 기반의 역추적 시스템을 분석 및 설계하였다.

ABSTRACT

Advance of computer technique becomes efficient of business in recent years. It has become high-speed data transmission and large data transmission. Network and computer system need to increasingly security because advance of computer technique. So this paper analyzes IP Traceback system that prevent cyber attack as hacking and security vulnerability of network. And this paper design IP Traceback system that based on active network.

키워드
IP Traceback, IDIP, AN-IDR, 액티브 네트워크

Ⅰ. 서 론[1)]

컴퓨터 기술의 발달과 더불어 인터넷의 발전은 데이터 전송 속도의 과속화와 대용량의 데이터 전송 등의 기술을 증가시켜 업무 효율을 향상시키고 생활의 질을 높여 주며 국가 경쟁력을 강화시켜주는 긍정적인 효과를 가져온 반면, 인터넷의 확장으로 인하여 외부의 시스템 불법 침입, 중요 정보의 유출 및 서비스 거부 공격 등의 역기능들이 계속해서 증가되어 그 피해가 심각한 수준이다.

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 경제활동 및 그 액수가 점차 증가함에 따라 사이버 공격으로 입게되는 피해는 점차 기업의 생존을 위협하는 수준에 도달하고 있다. 따라서 해킹에 능동적으로 대응할 수 있는 기술이 요구된다고 할 수 있으며, 능동적인 해킹 방어를 위한 가장 기본적인 기술로 해커의 실제 위치를 추적하는 역추적 기술

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

을 활용할 수 있어야 한다. 그러나 현재까지 제안된 역추적 기술들은 인터넷이 보유한 다양성을 극복하지 못하여 현재의 인터넷 환경에 적용하는데 어려움이 따른다[1].

이에 본 논문에서는 해킹으로 판단되는 침입에 대하여 효율적으로 역추적 하기 위해서 액티브 네트워크 기반의 역추적 시스템을 설계한다. 2장에서는 역추적 시스템을 동향을 분석하여 보고, 3장에서는 액티브 네트워크와 IDIP, AN-IDR에 대해서 분석하였으며 4장에서는 액티브 네트워크 기술을 이용한 역추적 방법을 제시하고 5장에서는 결론을 맺고 향후 연구방향을 기술하였다.

II. 관련연구

1. 호스트 기반 역추적 시스템

1.1. 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].

1.2 AIAA

AIAA(Autonomous Intrusion Analysis Agent) 시스템은 침해를 당한 서버의 해킹 피해 분석과 추적을 위한 로그 분석을 에이전트를 이용해 자동화한 역추적 시스템이다. AIAA 시스템은 침입자가 거쳐온 경유 시스템의 관리자의 도움을 받아 AIAA를 설치하고, 이 시스템에서 바로 이전의 침입경로와 해킹 흔적을 분석하고 다시 이전의 침입 시스템으로 분석을 옮겨가서 최종 경유지 서버까지 거슬러 간다.

본 시스템은 역추적 경로상에 존재하는 시스템들의 관리자의 도움을 받아 설치하기 때문에 역추적을 완료하기까지 많은 시간이 필요하게 된다. 또한 역추적 경로상에 존재하는 모든 시스템에 직접 접속해야 하기 때문에 만약 관리자와의 협조가 불가능하여 시스템으로의 접근이 불가능한 경우 역추적 자체가 불가능할 수도 있다[2].

2. 네트워크 기반 역추적 시스템

2.1 Thumbprints based algorithm

Thumbprint란 말 그대로 지문을 의미한다. Thumbprint를 이용하는 방법은 역추적 시스템 전체를 의미하는 것이 아니라 역추적을 위해 공격자의 시스템으로부터 공격 대상 시스템까지의 연결 체인을 구성하는 알고리듬이다. 본 알고리듬은 연결 체인에 속하는 호스트들이 속한 네트워크 상에 송수신되는 데이터를 수집하여 비교한다. 그러나 패킷이 암호화되거나 터널링되어 패킷의 내용이 변경되는 경우, 해당 연결 체인을 구성할 수 없는 경우가 발생할 수 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[3][4].

III. 액티브 네트워크

1. 액티브 네트워크(Active Network)

사용자의 네트워크 요구 기능을 수행하기 위해 프로그램 코드를 전송 및 실행함으로써 통신망에 새로운 서비스를 신속하고 경제적으로 도입하고 망 자원들을 보다 적절하게 활용할 수 있도록 하는데 목표를 두고 연구되고 있는 분야가 액티브 네트워크 분야이다. 기존의 네트워크는 이를 이용하는 응용 및 사용자가 네트워크 환경에 스스로 적응하게 하면서 서비스를 제공하는 것과는 달리 액티브 네트워크는 사용자의 요구에 맞추어 서비스를 제공한다.

이러한 액티브 네트워크 운영 환경은 기존의 네트워크 노드가 단순히 패킷을 저장한 후 포워딩(store and forward) 하는 식의 단순한 네트워킹 기능을 하는 것과는 달리 액티브 네트워크는 사용

자가 원하는 프로그램을 패킷을 통하여 전송하여 실행하거나 네트워크 노드에 미리 설치된 프로그램 중에서 해당 기능을 실행(store-compute-forward)함으로써 사용자가 원하는 네트워크 기능을 이용하게 된다.

이처럼 네트워크 노드에서 라우팅과 같은 단순한 기능에서 벗어나 네트워크 종단간에서만 이루어지던 여러 가지 에러 처리 및 흐름 제어와 같은 복잡한 기능 혹은 그 외 사용자가 원하는 기능을 네트워크 노드에서 수행할 수 있다는 것은 사용자나 네트워크 망 자체에 유연성뿐 아니라 여러 많은 장점들을 제공할 수 있다[5].

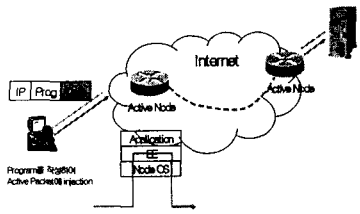

그림 1. 액티브 네트워크 운영환경의 예

2. IDIP(Intruder Detection and Isolation Protocol) 분석

IDIP는 침입탐지 시스템, 방화벽, 호스트, 보안 관리 관련 요소 시스템들 간의 협력 작업하기 위한 프로토콜을 포함한 보안 기반 구조이다. IDIP의 네트워크 구조는 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 하나의 DC 시스템만이 존재하고, 이 DC 시스템이 해당 'community' 내의 IDIP 기능을 제어, 관할하게 된다. 따라서 'community' 는 하나의 독립된 IDIP 관리 영역으로 볼 수 있다. 'neighborhood' 는 그 경계 안에 IDIP가 설정된 시스템이 존재하지 않는 경우로 IDIP를 구성하는 가장 기초적인 네트워크 요소로 볼 수 있다.

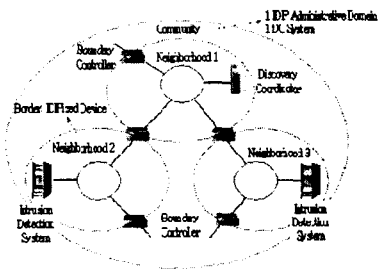

그림 2. IDIP 에서의 네트워크 구조

3. AN-IDR(Active Network-Intrusion Detection and Response) 분석

AN-IDR의 구조는 기존 IDIP의 구조를 그대로 적용하고 있다. AN-IDR 구조에서 드러나는 변화는 AN-IDR의 보안상 관리 도메인을 계층적 구조로 가져가고 있다는 점이다. 이는 현실적으로 침입자를 추적하고 대응하기 위해서는 여러 관리 도메인을 지나 정보를 교환하거나 특정 시스템을 제어할 필요가 있는데, 각 망 사업자나 네트워크 서비스 제공 사업자들이 자신의 망을 다른 사업자에게 제어권을 넘기지 않을 것에 대한 방안으로 고안된 것으로 보인다. 즉, 실제 필드에서 적용하기 위해 각 사업자는 자신이 관리하는 도메인에 대한 AN-IDR 관리 및 제어를 수행하고, 각 사업자들이 자신의 도메인에서 수행한 대응 방법을 조율하며, 정보를 공유하기 위해서 상위계층을 도입함으로써 각 사업자의 고유 권한을 침해하지 않으면서도 전체 AN-IDR의 기능을 수행할 수 있게 된다.

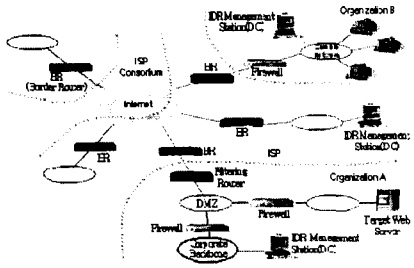

그림 3. AN-IDR의 네트워크 구조

IV. 액티브 네트워크 기반의 역추적

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 보고한

다. 이런 역추적 요청의 일련 과정을 공격자의 실제 위치가 파악될 때까지 반복하여 공격자 경로 상의 IDIP 노드들이 수행하게 된다.

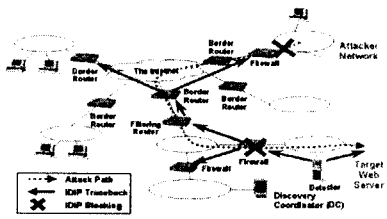

그림 4. 추적 결과 및 로컬 대응 결과 보고

V. 결 론

방대한 네트워크 인프라의 확보와 이를 바탕으로 한 폭발적인 인터넷 사용자의 증가는 실제 물리적 공간에서의 세상과는 전혀 다른 인터넷이라는 사이버 공간을 창출하게 되었고, 이러한 사이버 공간에서는 전 세계의 현실공간의 모든 정보가 생성 및 저장, 유통됨으로써 실생활에서 수행할 수 있는 대부분의 일들을 온라인 상에서 진행할 수 있게 되었다. 그러나, 이러한 정보화 사회는 긍정적인 측면이 있는 반면에 부정적인 측면도 대두되게 되었다[6]. 특히 부정적인 측면은 개인 생활의 파멸을 초래할 수도 있을 뿐만 아니라, 국가적인 안보의 위협까지 초래할 수 있다. 대표적인 부정적 측면은 인터넷을 통한 해킹, 악성 웜과 바이러스의 유포, 지적 재산권의 침해, 사이버 범죄에의 이용, 대규모 네트워크에 대한 가용성 고갈 등을 열거할 수 있으며, 이는 최근 발생한 "1.25 인터넷 대란" 을 보면 쉽게 알 수 있다. 따라서 본 논문에서는 이러한 침입에 대한 대응을 위해 액티브 네트워크기반의 역추적 시스템을 분석 및 설계하였다.

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

[2] S. Savage, D. Wetherall, A. karlin, and T. Anderson, Network Support for IP Traceback , IEEE/ACM transactions on networking, vol. 9, No. 3, June 2001.

[3] R. Stone, CenterTrack: An IP overlay network for tracing DoS floods , in Proc, 2000 USENIX Security Symp., pp.199~212, July 2000.

[4] D. Song and A. Perrig, Advanced and authenticated marking schemes for IP Traceback , in Proc. IEEE INFOCOM, vol. 2, pp. 878-886, April 2001.

[5] "차세대 인터넷을 위한 능동 보안 기술백서", 한국전자통신연구원, P137~139, 2001.5.15

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