DDoS 공격 대응 프레임워크 설계 및 구현

이 영 석*

DDoS Attack Response Framework using Mobile Code

Young-seok Lee*

요 약

사이버 공격의 형태가 나날이 다양해지고 복잡해지는데 반해 기존의 네트워크 보안 메커니즘은 지엽적인 영역의 방어적인 대응에 치중하고 있어 적시에 공격자를 탐지하고 신속하게 대응하는 것이 어려운 실정이다. 본 논문에서는 이러한 문제점을 해결하기 위한 방안으로 광역 네트워크 차원에서 다양한 사이버 공격에 쉽게 대응할 수 있고, 다수의 보안영역 간의 협력을 통해 공격자를 실시간으로 추적하고 고립화할 수 있는 새로운 네트워크 보안 구조를 제안하고자 한다. 제안하는 보안 구조는 액티브 네트워크를 기반으로 하는 이동코드를 포함한 액티브 패킷 기술을 이용하여 위조 IP 공격이나 DDoS(Distributed Denial of Service) 공격에 대하여 자율적이고 능동적으로 대응하는 것이 가능하다. 또한 다수의 보안영역 내의 보안 시스템 간의 협업을 통해 기존의 지엽적인 공격 대응 방식에 비해 보다 광역적이고 일괄적인 보안 서비스를 제공한다. 또한, 본 논문에서는 제안한 공격자 대응 프레임워크의 실험 환경을 구축하고 실험한 결과를 분석함으로써 적용 가능성을 검증 하였다.

ABSTRACT

It has become more difficult to correspond an cyber attack quickly as patterns of attack become various and complex. However, current security mechanisms just have passive defense functionalities. In this paper, we propose new network security architecture to respond various cyber attacks rapidly and to chase and isolate the attackers through cooperation between security zones. The proposed architecture makes it possible to deal effectively with cyber attacks such as IP spoofing or DDoS(Distributed Denial of Service), by using active packet technology including a mobile code on active network. Also, it is designed to have more active correspondent than that of existing mechanisms. We implemented these mechanisms in Linux routers and experimented on a testbed to verify realization possibility of attacker response framework using mobile code. The experimentation results are analyzed.

Keywords : **액티브 네트워크**(Active Network), **분산 서비스거부 공격**(Distributed Denial-of-Service Attack), **공격자 고립**(Attacker Isolation), DDoS, Mobile code.

* 교신저자 군산대학교 정보통신공학과 교수(leeys@kunsan.ac.kr)
접수일자 : 2010년 8월 2일, 수정일자 : 2010년 8월6일, 심사완료일자 : 2010년 8월 20일

Ⅰ. 서 론

네트워크는 컴퓨터 시스템간의 상호접속 및 정보 교환 등 의 편리한 역할을 제공 하지만, 시스템에 대한 불특정 다수의 접근이 가능하기 때문에 시스템 침입자에 의한 보안 사고의 위협을 내포하고 있다. 특히, 네트워크의 물리적인 광범위함, 네트워크 경로 및 사용자의 다양성 등은 네트워크 상에서 특유의 보안 문제를 일으키며, 네트워크 구성요소 중 일부에 문제가 발생하더라도 전체 네트워크에 영향을 미칠 수 있다. 또한 최근 심각한 피해를 입히고 있는 웜 바이러스 형태의 해킹 기법은 수분 내지 수십 분 내에 해당되는 지역이나 공공기관 기간망을 마비시킬 수 있는 피해를 줄 수 있다.

따라서 사이버 공격을 시도하는 침입자에 대해 기존의 네트워크 보안에서 이루어지는 것 보다 좀 더 강력하고 능동적인 대응과 서비스의 품질을 보호하기 위한 보안 기술의 개발이 요구되고 있다.

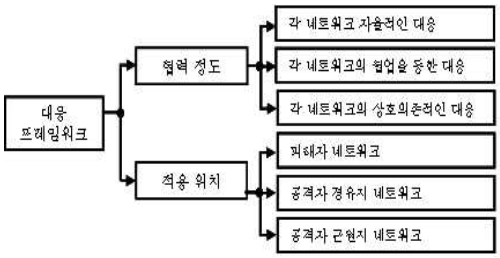
네트워크 인프라 환경은 네트워크 자체의 목적을 최소화하기 위해 지금까지 많은 노력이 진행되어 왔다. 하지만 보안사고의 네트워크 위협에 대한 대응 프레임워크는 아직 현실화되지 않은 문제점들이 있다. 첫째, 기존의 네트워크 보안은 자신의 관리 도메인 내로 침입하는 공격을 어떻게 잘 탐지할 것인가와 탐지된 공격을 어떻게 효율적으로 차단하여 자신의 도메인을 잘 보호할 것인가에 초점이 맞추어져 있다. 이 경우 자신의 도메인에서 파악한 침입자 정보를 바탕으로 자신의 도메인 입구에서만 해당 트래픽을 차단함으로써 침입자는 자유로이 인터넷을 이용할 수 있을 뿐만 아니라, 다른 공격 기술이나 공격 루트를 이용한 제2, 제3의 공격이 이루어 질 수 있다. 둘째, 최근 대부분의 네트워크 공격 형태는 하나의 에이전트에서 하나의 시스템을 공격하는 것이 아니라, 분산된 여러 에이전트에서 하나의 목표 시스템에 패킷을 범람시키는 DDoS 공격이 이루어지고 있다. 그러나 인터넷 관리는 분산화되어 지역적인 정책에 따라 각 네트워크 운영이 되고 있는 실정이다. 이러한 관리 환경은 네트워크 전체 차원에서의 특정한 한 보안 메커니즘 또는 보안 정책으로 보안을 강화하기는 더욱 어렵게 하고 있다. 셋째, 새로운 보안 기능 추가 시에 하드웨어 및 시스템의 교체가 수반되는 등 이종의 보안 장치 간, 이종의 네트워크 간, 이종의 사업자간의 상호 연동의 보안 서비스 환경을 제공하기 어렵고, 사이버 공격에 대응하기 위해 사용자 종단간의 안전하고 효율적인 보안 관리는 한계점이 있다.

이러한 문제점을 해결하기 위해서는 광역 네트워크 차원에서 공격을 탐지하고 대응할 수 있는 네트워크 보안구조와 보안환경 변화에 유연하게 적응할 수 있는 보안 응용 프로그램 구조 및 보안 도메인간의 협업을 통해 일원적인 대응 결정과 분산적인 대응 실행이 가능한 보안 서비스 환경의 구축이 필요하다.

본 논문에서는 이러한 새로운 네트워크 보안 요구사항을 만족하는 보안 프레임워크를 제시하고자 한다. 본 논문에서는 사이버 공격의 대응 기술과 관련된 외국의 연구동향과 국내의 연구개발 현황을 알아보고, 제안하는 이동 코드를 이용한 공격자 대응 프레임워크에 대하여 구체적으로 기술한다. 마지막으로 실험 환경 상에서 제안한 프레임워크의 실험 과정을 기술하고 도출된 실험 결과를 분석하여, 결론을 맺는다.

Ⅱ. 관련 연구

네트워크 인프라의 공격에 대한 효과적인 대응을 위해서는 기존의 네트워크 보안에서 이루어지는 것보다 좀 더 강력하고 능동적인 대응과 사용자 요구에 적합한 고객 지향 서비스를 지원하고 서비스의 품질을 보호하기 위한 대응 프레임워크를 제공해야 한다. 본 장에서는 [그림 2-1]과 같은 관점에서 네트워크 공격자 대응 프레임워크와 관련된 연구를 살펴본다.



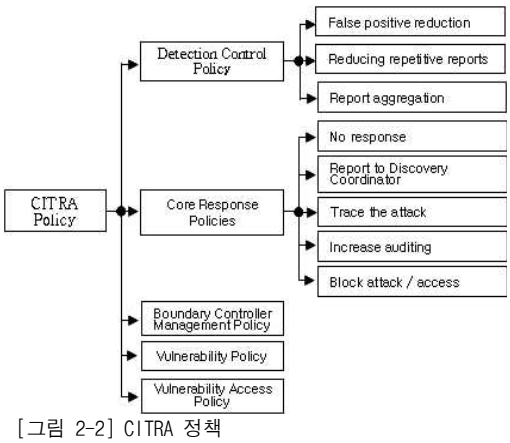
[그림 2-1] 공격자 대응 프레임워크 뷰

1. DARPA's IDIP

IDIP(Intrusion Detection Isolation Protocol)은 침입탐지시스템, 방화벽, 호스트, 보안관리 관련 요소시스템들 간의 협력 작업을 통해 공격자의 실제 위치를 역추적하여 공격자를 네트워크로부터 고립화시키기 위한 프로토콜을 포함한 보안 기반구조로써, 미국 DARPA (Defense Advanced Research Projects Agency) SLSS (Survivability of Large Scale Systems) 프로그램의 일환으로 수행된 연구이다[1]. 그러나 이 프로토콜은 다음의 결점을 갖는다. 첫 번째로 호스트에서 모든 연결에 대한 감시 기능을 수행해야 하며, 둘째 네트워크 도메인상의 모든 네트워크 노드들은 자신이 라우팅하는 모든 패킷에 대해 로그 정보를 유지할 수 있어야 하며, 마지막으로 IDIP가 실제 적용되기 위해서는 프로토콜 스택으로써 구현되어 시스템에 구축되어야 하는 정적인 문제점을 갖는다.

2. DARPA's CITRA

CITRA(Cooperative Intrusion Traceback and Response Architecture)는 공격자 역추적 및 고립화 기능을 프로토콜 형태로 구현하기 위한 목적을 가진 IDIP 과제로부터 시작되었다. CITRA는 DARPA's IDIP의 방법을 그대로 사용하면서 [그림 2-2]와 같은 대응정책을 추가하여 운영하고자 하였다[2].



[그림 2-2] CITRA 정책

이전의 역추적 및 대응이 도메인에서의 공격 경로상 마지막 노드인 경우에는 종료되었던 이전의 연구와는 달리, CITRA는 DARPA의 MCCD(Multi-Community Cyber Defense)과제를 통해 다수의 도메인간의 역추적 및 대응을 위해 확장되었다[3].

3. DARPA's AN-IDR

AN-IDR(Active Network - Intrusion Detection and Response)은 IDIP가 프로토콜로 구현될 경우에 발생하는 기능 변경의 정적인 특성으로 인한 유연성의 부족함과 특정 기능 수행 상에 있어서의 효율성 저하를 해결하기 위해 시작되었다. 이를 위해 IDIP 메커니즘과 액티브 네트워크 기술을 결합하여 상호 운용함으로써 기존의 정적인 IDIP에 이동성(mobility), 유연성(flexibility), 확장성(extensibility)을 부여함으로써 좀더 발전된 침입자 탐지 추적 기능을 수행하고자 하였다[4,5]. AN-IDR의 경우 단순히 공격자의 추적 및 고립화뿐만 아니라, 액티브 패킷을 이용하여 공격용 툴로써 설치된 에이전트 프로그램을 스캐닝하고 해당 에이전트의 실행을 중지시키는 것과 같이 침해된 시스템을 복구하는 기능도 포함하였다.

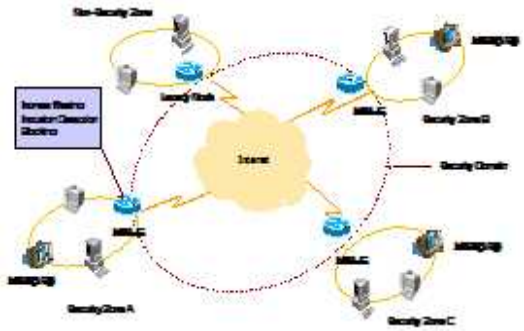
III. 공격자 역추적 프레임워크 설계

본 논문에서 제안된 공격자 대응 프레임워크의 네트워크 구성도는 [그림 3-1]에 도시한 바와 같이 보안관리 영역(Security Zone)의 경계에서 이동코드 처리 및 보안 대응 기능을 제공하는 두 개의 시스템(보안노드와 보안관리서버)으로 구성되며, 두 시스템이 연동하여 하나의 보안관리 영역을 관리하고 제어한다.

각 보안관리 영역은 전체 네트워크 상에 분산적으로 배치되어 상호간의 연동 및 협업을 수행하지만, 이를 위한 별도의 관리 계층은 갖지 않는다. 즉, 모든 보안 제어는 이동코드를 통해 이루어지며 보안관리 영역 간의 상호 연동과 협업 역시 이동코드에 의해 수행된다.

각각의 보안관리 영역은 [그림 3-5]에 도시한 바와 같이 이동코드를 통해 상호 연동함으로써 광역 네트워크 상에 논리적인 보안관리 도메인(Security

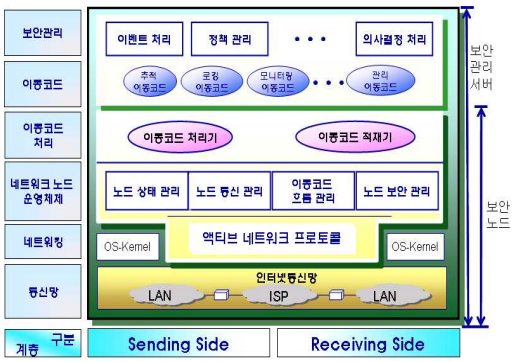
Domain)을 형성한다. 이와 같이 기존의 네트워크(인터넷 백본)에 배치되어 있는 네트워크 시스템의 구성에 대한 변경 없이 새로운 보안 관리 영역을 형성할 수 있는 것이 공격자 대응 프레임워크의 큰 특징 중 하나이다.



[그림 3-1] 공격자 대응 프레임워크 네트워크 구성도

1. 공격자 대응 프레임워크 구성

공격자 대응 프레임워크는 [그림 3-2]에 도시한 바와 같이 보안노드와 보안관리서버로 구성된다. 보안노드 및 보안관리서버에는 이동코드를 수신하고 실행시킬 수 있는 이동코드 처리기가 공통적으로 탑재된다. 또한, 보안관리서버에는 이벤트관리, 의사결정처리 등의 보안관리를 위한 기능과 이동코드 및 정책을 관리하기 위한 저장소가 추가적으로 탑재되며, 보안노드는 이동코드에 의해 네트워크 차원의 대응 기능을 제공한다.



[그림 3-2] 공격자 대응 프레임워크 구성도

보안관리서버는 보안관리 영역 내에 배치된 침입탐지시스템 및 방화벽시스템으로부터 보고된 침입행위에 대하여 이에 적합한 보안 대응을 결정하고, 이를 실행시킬 이동코드를 생성하여 네트워크에 송신함으로써 네트워크 차원의 보안상태를 동적으로 보안제어를 수행한다. 즉, 보안관리 영역 내의 보안노드를 제어함으로써 자신의 보안관리 영역을 관리하며, 다른 보안관리 영역을 관리 하는 보안관리서버와의 협업을 통해 전역적인 네트워크 보안관리 기능을 수행한다. 공격자 대응 프레임워크 상호간의 모든 제어 및 관리는 이동코드에 의해 수행된다.

이동코드는 네트워크에 존재하는 다른 일반 노드에서도 전달될 수 있도록 기존 네트워크에서 사용하는 IP 패킷 형태로 구성한다. 이 IP 패킷을 액티브 패킷라고 하며, 액티브 패킷 헤더는 패킷의 IP 헤더와 ANEP(Active Network Encapsulation Protocol) 헤더로 구성되며, 페이로드에는 이동코드가 포함된다[6]. 'IP Router Alert Option'은 라우터가 패킷의 목적지 주소가 자신이 아닌 패킷을 가로챌 수 있도록 해주는 옵션으로써 일반 IP 패킷과 액티브 패킷을 구분하는 표시자 역할을 위해 활용한다[7].

보안노드는 이동코드처리기, 액티브 패킷을 처리하는 A-Linux 커널, 공격자 대응, 그리고 보안노드 자원을 관리하는 네트워크노드 운영체제 등으로 구성된 구조를 갖는다.

보안 노드는 보안관리 영역의 경계(가입자 네트워크의 에지라우터)에 이동코드처리 기능과 네트워크 차원의 보안대응을 수행하는 기능을 탑재한 시스템이다. 보안노드는 보호하고자 하는 네트워크의 가장 전단에 위치하여 유입되는 네트워크 패킷을 필터링하고 차단하는 기능을 수행한다. 또한, 위조 IP(Internet Protocol) 역추적을 위한 MAC(Media Access Control) 주소 관리 기능과 DDoS 검출을 위한 트래픽 모니터링 기능 등을 제공한다. 이 외에도 전달된 이동코드를 수행하고 다른 네트워크로 송신하거나 보안관리서버로 전달하는 기능도 제공한다.

이동코드는 액티브 네트워크 상에서 보안 기능을 수행하는 일종의 액티브 패킷으로써, 본 논문에서 설계한 이동코드의 종류는 <표 3-1>과 같다.

<표 3-1> 이동코드 종류

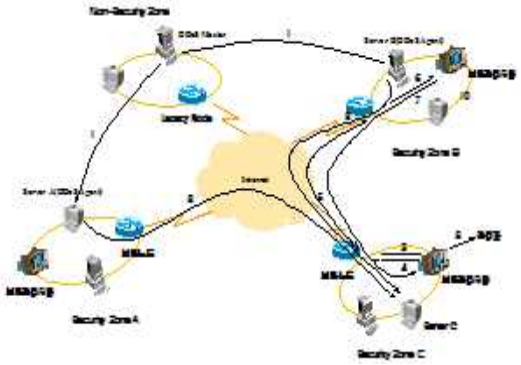
유형	종류	기능
이동형	*Spoofed_IP_Tracing*	IP 패킷의 근원지 주소를 위조하는 위조 IP 공격 대응을 위한 역추적 기능
	DDoS_IP Tracing	트래픽을 세션 별로 조사하여 임계치를 넘는 트래픽을 보내는 노드에 대한 DDoS 추적
	Spoofed_IP_Tracing Complete	위조된 IP 역추적 완료 후 실제 공격자를 네트워크로부터 고립시키는 기능과 역추적 결과를 해당 보안관리서버에게 전달하는 기능
	DDoS_IP_Tracing_Complete	DDoS 공격 역추적 완료 후 실제 공격자를 네트워크로부터 고립시키는 기능과 역추적 결과를 해당 보안관리서버에게 전달하는 기능
	Packet_handling	추적 코드 수신 후, 보안노드에서 침입자로부터 공격이 불가능하도록 패킷을 차단하는 기능과 경유지로 사용되어 차단된 노드의 패킷을 차단을 해제하는 기능
상주형	*Traffic_Monitoring*	도메인 내로 유입되는 트래픽의 이상 변동을 감지하는 기능과 일정 수준을 넘는 트래픽이 발생했을 때 보안관리서버에게 보고하기 위한 기능
	DDoS_Traffic_Detector	트래픽 모니터링의 결과를 보안관리서버에게 전달하는 기능

이러한 이동코드는 네트워크 침입에 능동적으로 대응하기 위한 소프트웨어로써, 액티브 패킷 내에서 실행 가능한 프로그램 코드 형식으로 전달된다. 코드는 이동성 유무에 따라 상주코드와 이동코드로 구분한다. 상주코드는 보안노드에 상주하며 필요에 따라 새로운 코드를 생성하고, 이동코드는 보안노드와 보안관리서버에서 수행되며 코드의 데이터를 변경할 수 있고 다른 보안노드나 보안관리서버로의 이동성을 갖는다.

2. DDoS 공격 대응 메커니즘

DDoS 공격은 수십~수백 개의 시스템이 하나의 목표시스템을 집중 공격함으로써 피해 호스트가 서비스를 제공하지 못하도록 하는 공격 형태를 의미한다. 즉 다량의 호스트들에게 DoS 공격 에이전트를 분산시켜 설치하고, 이들을 중앙에서 제어함으로써 목표 시스템에 일제히 유해 패킷을 전송하도록 하여 시스템의 성능 저하 및 시스템 마비를 유발시키는 공격이다.

본 논문에서 제안된 공격자 대응 프레임워크는 이러한 DDoS 공격을 탐지하고 네트워크 상에 분산되어 있는 DDoS Agent를 찾아 내기 위한 역추적 메커니즘과 유해 패킷을 공격자 근원지에서 고립시키는 보안 서비스를 제공한다. DDoS 탐지 및 공격 대응 메커니즘은 [그림 3-3]과 같은 절차에 의해 수행되며, 각 단계별 수행 기능을 다음과 같다[16].



[그림 3-3] DDoS 탐지 및 공격 대응 메커니즘

① 비 보안영역(Non-Secure Zone)에 위치한 공격자는 보안영역 C 내의 서버 C를 공격하기 위해 DDoS 마스터를 기반으로 보안영역 A와 B에 위치한 서버A와 B에 불법적인 방법을 사용하여 DDoS 에이전트를 설치한다.

② 보안영역 A와 B에 있는 DDoS 에이전트는 보안영역 C에 위치한 서버 C로 DDoS 공격을 시도한다.

③ 보안노드(C) 내의 상주형 Traffic_Monitoring 코드에서 입력 패킷을 분석하여 특정 시간 내에 입력된 전체 패킷의 양이 임계치를 넘는다면 DDoS 공격으로 간주한다. DDoS 공격을 탐지하면 탐지된 결과를 포함하여 보안노드(C)는 DDoS_Traffic_Detector 코드를 생성하여 보안관리서버(C)로 송신한다.

④ 보안관리서버(C)는 DDoS_Traffic_Detector 코드를 수신한 후, DDoS_Traffic_Detector 코드 내의 공격 정보를 분석하여 DDoS_IP_Tracing

코드를 생성하여 보안노드(C)로 전송한다.

⑤ DDoS_IP_Tracing 코드를 수신한 보안노드(C)는 수행환경을 통해 수신된 코드를 실행하여 보안영역 C로 입력되는 패킷들을 분석한다. 만일 특정 발신자 주소들로부터 입력되는 패킷의 수가 일정한 값을 넘는다면, DDoS 공격으로 간주하고 공격 패킷을 전송하는 DDoS 공격 에이전트 수와 동일하게 DDoS_IP_Tracing 코드를 생성한다. DDoS_IP_Tracing 코드들은 DDoS 에이전트(서버 A와 B)들을 목적지 주소로 하여 해당 보안영역으로 전달된다.

⑥ DDoS_IP_Tracing 코드를 포함한 액티브 패킷은 전송 경로에 따라 보안노드(B)에 의해 수신한다. DDoS_IP_Tracing 코드의 실행에 의해 보안영역 C의 서버 C로 나가는 패킷들을 검사한다. 검사한 패킷들이 서버 C의 특정 포트 번호를 공격하는 것으로 판명되면, 보안노드(B)는 서버 B에서 서버 C로 나가는 패킷 가운데 특정 포트 번호를 갖는 패킷들을 Packet_Handling 코드를 통하여 차단한다. 차단 이후에, 보안노드(B)는 DDoS_IP_Tracing 코드의 목적지 주소를 보안관리서버(B)로 변경하고 전송한다.

⑦ 보안관리서버(B)는 DDoS_IP_Tracing 코드를 수신하고, 처리 결과에 따라 DDOS_Tracing_Complete 코드를 생성한다. DOS_Tracing_Complete 코드의 목적지 주소는 DDoS_IP_Tracing 코드 내에 포함된 최초 전송자인 보안관리서버(C)의 주소로 결정된다. 전달 경로 상의 보안노드(B)에서는 DOS_Tracing_Complete 코드 수신 시, 별도의 실행 없이 재전송한다.

⑧ 보안관리서버(C)는 DOS_Tracing_Complete 코드를 수신한 후, 코드 내에 포함된 정보를 분석하여 관리자에게 전달한다.

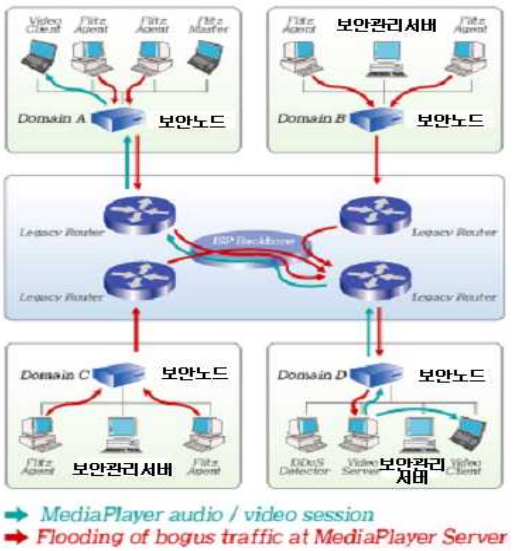
단계 ⑤~⑦은 보안영역 A에도 동일하게 적용되며, DDoS 마스터에 대한 추적 및 대응 기능은 본 논문의 영역 외로 한다[12].

Ⅳ. 실험 및 분석

1. DDoS 공격 대응 시험 절차

DDoS 공격은 목표 시스템의 서비스 제공을 방해하기 위하여 해당 시스템이 처리할 수 없는 요청을 보내는 공격으로써, 무수히 많은 에이전트에서 특정 서비스 요청을 전송하여 부수적으로 해당 네트워크 트래픽을 범람시키는 효과를 가지게 된다. DDoS 공격 툴의 구성은 공격 요청을 보내는 무수히 많은 에이전트와 해당 에이전트에 공격 명령을 시달하기 위한 마스터로 구성된다.

본 시험에서는 Flitz 툴을 이용하여 두개의 보안 도메인 상에 6개의 에이전트를 두고 비디오 스트리밍 서비스를 제공하는 서버를 공격하는 것으로 하였다. 또한 실제 네트워크 상황을 에뮬레이션하기 위해 iperf 툴을 이용하여 3.5M 정도의 백그라운드 트래픽을 생성하였다. 비디오 스트리밍 서비스로는 DVD(Digital Versatile Discs) 드라이브를 네트워크로 연결하여 DVD를 원격에서 구동하였다. [그림 4-1]의 화살표는 실험환경 상에서 DDoS Agent들의 공격 경로를 보여준다.



[그림 4-1] DDoS 공격 시험 구성도

DDoS는 네트워크 기반의 IDS로 탐지하지만, 공격자 대응 프레임워크의 메커니즘을 이용하면 네트워크 기반 IDS가 필요하지는 않다. 즉, 공격자 대응 프레임워크를 구현한 각 도메인의 게이트웨이 라우터인 보안노드에서 네트워크 트래픽을 모니터링하고 이를 바탕으로 경보를 발령하면 실제 트래픽이 과다하게 발생시키는 에이전트 위치를 추적하여 단절하게 된다. 실험에서는 공격이 이루어짐에 따라 비디오 스트링밍 서비스의 품질이 저하되는 것을 보여주었고, 공격자 대응 프레임워크의 동작에 따라 해당 서비스의 품질이 회복되는 것을 보여 주었다. 시험 절차는 다음과 같다.

① 비디오 스트리밍 서비스 제공
② Flitz를 이용한 DVD 서버에 공격
③ 비디오 스트리밍 서비스의 품질 저하 확인
④ 공격자 대응 프레임워크의 구동 및 에이전트의 트래픽을 각 도메인의 게이트웨이에서 차단
⑤ 비디오 스트리밍 서비스 품질의 회복
⑥ 공격 트래픽 차단 확인

2. DDoS 공격 대응 실험 결과

DDoS 공격에 대해 공격자 대응 프레임워크에서 이동코드를 이용한 대응 메커니즘의 코드 수행 시간은 <표 4-1>과 같다. <표 4-1>에서 보듯이, 보안노드(C, B, A)에서는 DDoS_IP_Tracing 코드를 수신하고 DDoS 에이전트로부터 입력 트래픽을 차단하는 기능을 수행하므로 코드 수행 시간이 길다. 그러나, DDoS_IP_Tracing_Complete 코드는 보안노드(C,B,A)에서 별도의 실행 과정 없이 보안관리서버(C)로 전달되기 때문에 보안노드에 실행 부담이 없다.

<표 4-1> DDoS_IP_Tracing 및 DDoS_IP_Tracing_Complete 수행 시간

수행지점	코드종류	1차	2차	3차	4차
보안노드(C)	*DDoS_IP_Tracing*	10478	10933	10509	10747
보안노드(B)	*DDoS_IP_Tracing*	10672	10652	10778	10561
보안노드(A)	*DDoS_IP_Tracing*	10708	10889	10801	10693
보안노드(C)	*DDoS_IP_Tracing_Complete*	30	17	22	29
보안노드(B)	*DDoS_IP_Tracing_Complete*	22	24	27	20
보안노드(A)	*DDoS_IP_Tracing_Complete*	25	28	24	21

DDoS 공격 대응 실험에서 특이한 사항은 무수히 많은 분산된 공격 에이전트인 경우에서 매우 좋은 성능을 나타낼 것으로 예상된다. 이는 동시다발적인 분산된 공격 에이전트에 대한 대응 메커니즘도 공격 에이전트 수와 동일하게 DDoS_IP_Tracing 코드를 생성하여 병렬적으로 수행되기 때문이다.

V. 결 론

본 논문에서는 네트워크 보안 환경 변화에 따르는 요구사항을 반영할 수 있는 확장된 보안 구조로서 액티브 네트워크를 이용한 공격자 대응 프레임워크를 설계하였고, DDoS 공격에 대응하기 위한 메커니즘을 제안하였다. 제안한 공격자 대응 프레임워크는 새로운 공격 기술, 방어 기술의 등장이나 보안 환경 변화에 유연하게 적응할 수 있도록 전체 네트워크 수준에서 수행할 보안 기능을 이동코드 형태로 수행하도록 설계되었다.

제안된 공격자 대응 프레임워크의 적용 가능성을 증명하기 위해 실험환경을 구축하고, 해당 실험환경 상에서 실제 제공되는 서비스와 대표적인 공격 기법을 적용한 상태에서 대응 메커니즘을 실험하였다. 실험 결과에 의하면, 공격자 대응 프레임워크는 기존의 수동적인 침입 차단 및 침입탐지 시스템의 문제점을 해결하고, 동적인 보안 서비스를 제공함을 보였으며, 실제 필드에 적용할 수 있음을 확인하였다.

참 고 문 헌

[1] Dan Schnackenber, Travis Rei, Kelly Djahandar, Brett Wilso, "Cooperative Intrusion Traceback and Response Architecture (CITRA)," NAI Labs Report #02-008 Feb., 2002.

[2] Dan Sterne, Kelly Djahandari, Ravindra Balupari, William La Cholter, Bill Babson, Brett Wilson, Priya Narasimhan, and Andrew Purtell, "Active Network Based DDoS Defense," Proceedings of the DARPA Active Networks Conference and Exposition (DANCE.02), p.193, May 29~30, 2004.

[3] Spyros Denazis, "Overview FAIN Programmable Network and Management Architecture - Draft Ver. 2.0," WP3-HEL-056-D14-FAIN, FAIN Consortium, May 12th, 2005.

[4] B. Chang, D. Kimm Y. Kwon, T. Nam, T. Chung, "Security Management by Zone Cooperation in Active Network Environment," Proc. of the 2002 International Conference on Security Management (SAM'06), p.187-192. 2006,

[5] Stamatis Karnouskos, "Dealing with Denial-of-Service Attacks in Agent-enabled Active and Programmable Infrastructures," IEEE 25th International Computer Software and Application Software (COMSAC 2005), Oct. 8-12, 2005.

[6] Beom-Hwan Chang, Dong-Soo Kim, Hyun-Ku Kim, Jung-Chan Na, Tai-Myoung Chung, "Active security management based on secure zone cooperation," Future Generation Computer Systems, v.20 n.2, p.283-293, February 2004.

[7] D. Kat, "IP Router Alert Option," RFC 2113, IETF, Feb. 1997.

[8] Hyun Joo Kim, Jung C. Na, and Sung W. Sohn, "Response To Distributed Denial-of Service Attack using Active Technology," IMSA2004, Apr. 2004.

저자약력

이 영 석(Young-seok Lee) 정회원

1992년 : 충남대학교 컴퓨터공학과 공학사
1994년 : 충남대학교 컴퓨터공학과 공학석사
2002년 : 충남대학교 컴퓨터공학과 공학박사

1994년~1997년 : LG전자 연구원
2002년~2004년 : ETRI 정보보호연구단 선임연구원
2004년~현재 : 군산대학교 정보통신공학과 부교수

<관심분야> 분산시스템, 정보보호, 이동컴퓨팅