액티브 네트워크 기반의 위조 IP 공격 대응 메커니즘

이영석[O] 방효찬 나중찬
한국전자통신연구원
{yslee[O], bangs, njc}@etri.re.kr

Traceback Mechanism for Spoofed IP Attack on Active Network

Youngseok Lee[O] Hyochan Bang Joongchan Na
Active Security Technology Research Team, ETRI

요 약

최근 인터넷을 통한 사이버 공격의 형태가 다양해지고 복잡해지면서 효과적인 탐지 및 대응이 어려워지고 있다. 특히 UDP 계열의 DoS, DDoS 공격에서 IP 패킷 내의 근원지 IP 주소를 타인의 IP 주소로 위조하여 공격하는 경우 패킷의 실제 송신자를 추적하고 고립화 시키는 것은 불가능하다. 본 논문에서는 이러한 공격에 쉽게 대응할 수 있는 보안 구조로서 액티브 네트워크를 이용한 보안 관리 프레임워크를 설계하고, 위조 IP 공격에 보다 능동적인 대응이 가능한 메커니즘을 제안한다.

1. 서론

컴퓨터의 고성능화, 인터넷의 보급 및 웹 등의 새로운 네트워크 어플리케이션의 등장에 의해 네트워크 컴퓨팅이 비약적으로 발전하지만, 네트워크 상에서 노드 간의 통신 기반이 되는 네트워크 프로토콜의 발전은 느리게 진행된다. 이는 네트워크 간의 상호운용성을 확보하기 위한 프로토콜 표준화가 새로운 기술 개발에 비해 매우 늦은 속도로 진행되기 때문이다. IETF, ISO 등 표준화 단체에 의한 표준화 작업에는 많은 노력과 시간이 소요되며 프로토콜이 규정 되어도 실제 네트워크 상에 적용되어 운용되기까지는 더욱 많은 기간이 필요하다. 이러한 인터넷 상에서의 문제를 해결하기 위하여 DARPA(Defense Advanced Research Project Agency)에서는 유연하고, 고기능을 제공하는 네트워크를 실현하기 위한 기술로 액티브 네트워크 개념을 제안했다.

액티브 네트워크[1]는 패킷 스위칭 네트워크를 통해 전송되는 이동 프로그램을 실행할 수 있는 라우터나 스위치를 배치하여, 전송된 액티브 패킷에 포함되어있는 이동 프로그램을 서비스 특성이나 사용자 요구에 따라 적합하게 연산, 처리할 수 있는 네트워크이다. 즉, 사용자에게 네트워크를 프로그래밍하는 능력을 부여하는 네트워크 아키텍처를 액티브 네트워크라고 한다.

본 논문에서는 보안 환경 변화에 따른 요구사항을 반영할 수 있는 보안 구조로서 액티브 네트워크를 이용한 보안 관리 프레임워크를 설계한다. 특히, 제안된 보안 프레임워크 상에서 위조 IP 공격에 능동적인 대응 메커니즘을 기술한다.

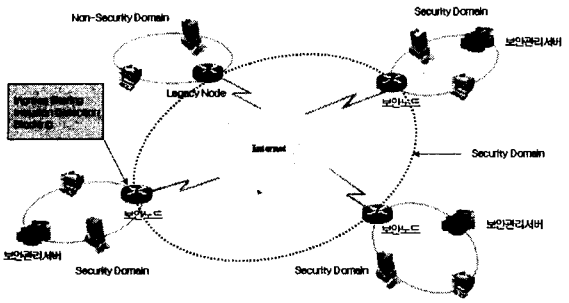
2. 보안 관리 프레임워크

보안 관리 프레임워크는 액티브 네트워크로 구성된다. 액티브 네트워크를 이용할 경우 네트워크 보안이 능동적으로 발전할 수 있는 이유는 크게 다음과 같다[2].

- 네트워크 상의 라우터나 스위치들은 자신에게 전송된 보안 대응 프로그램을 특별한 프로토콜이 없이도 네트워크 처리 단계에서 인식하고 수행할 수 있다.
- 보안 관리자는 각각의 노드에서 필요한 보안 대응 수단을 프로그래밍에 의해 제어 할 수 있다. 즉 네트워크 상에서의 보안 메커니즘을 보다 유동적이고 유연하게 배치, 삭제할 수 있으며, 다수의 네트워크 장비 및 보안장비를 분산 관리할 수 있다.

이는 제품 개발시 탑재된 보안 기능을 정해진 프로토콜에 의해 상호 연동시키며, 제한된 범위에서의 보안 기능만을 제공할 수 있었던 기존의 정적인 보안 메커니즘의 문제들을 해결할 수 있는 새로운 개념의 보안 메커니즘이다. 광역 네트워크 상에 분산적으로 설치되어있는 다수의 보안 노드에 대한 보안 제어 기능과 노드간의 협업 기능을 제공하는 능동적인 네트워크 보안 프레임워크를 제공하기 위해서는 보안 기능의 복잡한 계층 구조화와 이들간의 통신을 위한 다수의 프로토콜이 제공되어야 한다.

액티브 네트워크를 이용한 네트워크 보안 프레임워크에서는 프로토콜 대신 액티브 패킷을 이용하며, 보안 기능 자체를 액티브 패킷 내의 보안 대응 프로그램으로 전송, 실행함으로써 보안 구조를 단순화시키고 네트워크 자원을 절약한다.



[그림 1] 보안 관리 프레임워크

본 논문에서 제안한 보안 관리 프레임워크는 [그림 1]에 도시한 바와 같이 보안 관리 영역의 경계에서 이동형 센서 처리 및 능동 대응 기능을 제공하는 보안 노드와 이를 관제하는 보안 관리 서버로 구성되며, 두 시스템이 연동하여 하나의 보안 관리 영역을 관리하고 제어한다. 각 보안 관리 영역은 전체 네트워크 상에 분산적으로 배치되어 상호간의 연동 및 협업을 수행하며 이를 위한 별도의 관리 계층은 갖지 않는다. 즉, 모든 보안 제어는 액티브 패킷 내에 포함되어 전달되는 이동형 센서를 통해 이루어지며, 보안 도메인 간의 상호 연동과 협업 역시 이동형 센서에 의해 수행된다. [그림 1]에서 보듯이, 각각의 보안 관리 영역은 이동형 보안 센서를 통해 상호 연동함으로써 광역 망 상에 논리적인 보안 관리 영역을 형성한다. 이와 같이 기존의 망(인터넷 백본)에 배치되어 있는 네트워크 시스템의 구성 변경 없이 보안 관리 영역을 형성할 수 있는 것이 큰 특징이다.

보안 노드 및 보안관리 서버에는 이동형 보안 센서를 수신하고 실행시킬 수 있는 이동형 보안 센서 처리 블록이 공통적으로 탑재된다. 또한, 보안관리 서버에는 보안 관리를 위한 기능 블록과 보안 센서 및 정책을 관리하기 위한 저장소가 추가적으로 탑재되며, 보안 노드에는 이동형 센서에 의해 네트워크 차원의 실시간 대응 기능을 제공하는 대응 블록이 추가된다.

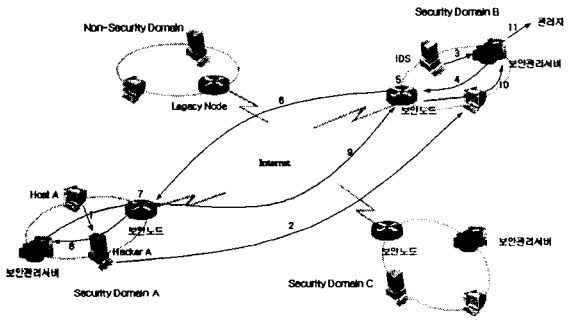
3. 위조 IP 공격 대응 메커니즘

위조 IP 공격에 대한 대응 기능(Spoofed IP trace back)은 해커가 IP 헤더 내의 근원지 IP 주소를 타인의 IP 주소로 위조하여 공격(IP Address Spoofing Attack)한 경우에 패킷의 실제 송신자를 추적하기 위한 역 추적 메커니즘과 해커를 공격자 도메인에서 고립시키는 보안 서비스를 제공한다. 위조 IP 공격은 주로 UDP 계열의 DoS, DDoS, 기타 플러딩(flooding) 계열의 공격에 널리 사용되며, TCP/IP 기반의 네트워크에서는 근원지 IP 주소의 위조 여부를 파악하기 어렵다는 점을 이용한 지능적인 공격 수법이다. 제안된 위조 IP 역 추적 메커니즘은 기존의 네트워크 프레임워크를 수정하지 않고도 이동형 보안 센서를 통해 신속하게 실제 공격자를 검출할 수 있으며 이러한 기능은 지금까지 수동적으로 이루어졌던 침입자 파악 수단보다 자동적이고 능동적인 대응이 가능함을 보여준다. 메커니즘은 다음과 같은 기능을 제공한다.

- 침입 탐지 및 차단을 위해 필요한 기존 보안 장비(NIDS)와의 연동 기능
- 침입 근원지를 파악하기 위한 역 추적 기능, 침입자를 원천 봉쇄하기 위한 침입 근원지 고립화 기능
- 상기 기능의 유기적인 통합 관리를 통한 보안 관리 영역의 보안 상태 복구 기능

위조 IP 공격에 대한 대응 서비스를 제공하기 위하여 보안관리 영역의 망 접속 점(Edge Point)에 설치된 보안 노드에서 Ingress Filtering 기능[3]을 수행하도록 하였다. Ingress Filtering을 통해 해커에 의한 타 도메인의 IP 주소 위조 및 조작을 사전에 방지함으로써 해커에 의한 IP Spoofing 범위를 하나의 보안관리 영역 내부로 한정한다.

[그림 2]는 액티브 네트워크를 이용한 보안관리 프레임워크에서의 위조 IP 역 추적 메커니즘 및 기능 절차를 도식화 한 그림이다.



[그림 2] 위조 IP 공격 대응 단계

제안된 메커니즘은 아래와 같은 절차에 의해 보안 기능을 수행한다.

(단계 1) IP 주소 위장
Secure Domain A에 위치한 해커 A는 같은 도메인에 위치하는 호스트A의 IP주소를 자신의 IP 주소로 위조

(단계 2) 타 도메인에 있는 서버 공격
Secure Domain B에 위치하는 서버 B에게 flood 계열의 DoS(Denial of Service) 공격을 시도

(단계 3) 침입탐지 경보 전달
Secure Domain B에 존재하는 IDS는 공격을 감지하여 침입탐지 경보를 보안관리서버(B)로 송신

(단계 4) 패킷 역추적 센서 전송
보안관리서버(B)는 수신된 침입탐지 경보 데이터를 참조하여 유해 패킷을 송신한 근원지 IP 주소를(Secure Domain A의 호스트A 근원지 IP주소) 목적지 주소로 하여 역추적 센서를 생성하여 전송

(단계 5) 패킷 역추적 센서 실행
패킷 역추적 센서를 수신한 보안노드(B)는 수행환경을 통해 수신된 센서를 실행하여 유해 패킷의 유입을 차단. (보안노드는 해커의 위조 패킷은 물론 IP 주소를 위조 당한 호스트A의 정상적인 패킷까지 차단)

(단계 6) 패킷 역추적 센서 재전송

보안노드(B)는 보안관리서버(B)로부터 수신한 역추적 센서를 목적지 주소로 전송

(단계 7) 패킷 역추적 센서 실행

Secure Domain A의 접속 점에 위치하는 보안노드(A)에서 수신된 센서는 로깅 센서에 의해 기록된 Outgoing Ethernet 프레임 축약 정보를 검색하여 유해 패킷 정보와 일치하는 로그 정보를 추출한 후, 로그 정보에 기록된 MAC 근원지 주소와 ARP table에 저장된 IP 주소를 비교하여 위조 여부 및 실제 근원지 IP 주소를 파악한다. 위조 여부가 판별되면 해당 MAC 주소로부터 유입되는 패킷을 차단

(단계 8) 역추적 센서 실행 결과 보고

역추적 의뢰 정보, 성공 여부, 파악된 근원지 주소 등의 정보를 해당 도메인에 위치하는 보안관리서버(A)로 송신

(단계 9) 침입자 원천봉쇄 결과 보고

보안관리서버(A)는 역추적을 의뢰한 보안관리서버(B)로 최종 역추적 결과보고 센서 전송

(단계 10) 패킷 역추적 보고 센서 수신

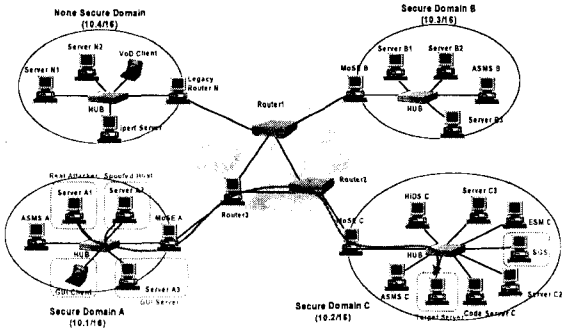
보안노드(B)는 (단계 5)에서 IP 주소를 위조 당한 호스트A의 정상적인 패킷까지 차단한 세션을 복구한 후, 보안관리서버(B)로 역추적 보고 센서 전송

(단계 11) 보안관리자에 통보

보안관리서버(B)는 수신된 역 추적 보고 센서의 정보를 보안 관리자에게 통보한다.

4. 시험

위조 IP(IP Spoofing) 공격은 직접적으로 사용되는 공격 기법이 아니라 다른 공격과 결합되어 사용된다. IP Spoofing을 적용하면 해당 공격을 구성하는 패킷의 근원지 주소(source address)를 다른 시스템의 주소로 속여 전송함으로써 공격이 수행하는 실제 호스트를 속이기 위한 기법이다. 시험에서는 DDoS 공격용 툴이 Flitz를 이용하여 동일 도메인 상에 존재하는 다른 시스템의 주소를 이용하여 도메인 C에 존재하는 서버를 대상으로 ICMP Flooding 공격을 수행하는 것으로 하였다.

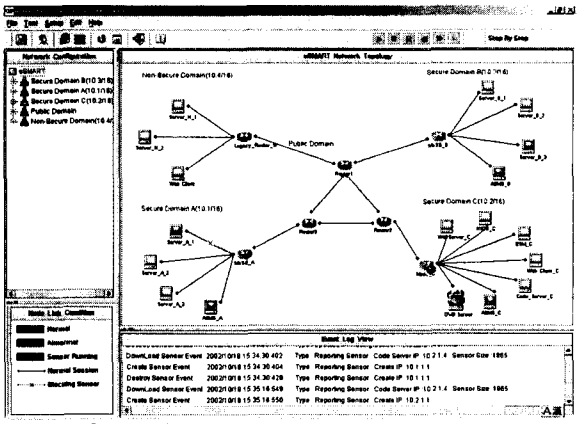


[그림 3] 시험 환경 및 ICMP Flooding 공격

[그림 3]에서 보듯이, 본 시험은 ICMP Flooding 공격과 그에 따른 메커니즘의 구동과 관련된 동작을 GUI 상에서 보여 주는 것으로 하였다. 시험 절차는 다음과 같다.

- Flitz를 이용한 ICMP Flooding 공격 수행
- IDS의 탐지 후, 보안노드 및 서버로 통지
- 대응 메커니즘 구동 및 공격자 호스트 역추적
- 실제 공격자 호스트 MAC 주소 필터링
- 공격자 차단 확인

[그림 4]는 IP Spoofing을 적용한 ICMP Flooding 공격에 대해 공격자 실제 호스트가 차단되었음을 보여 주는 관리자 GUI 화면이다. 그림에서 x 표시된 선은 공격자를 고립화 시키기 위해 기존의 연결된 네트워크를 단절을 의미한다.



[그림 4] ICMP Flooding 공격 대응 결과

5. 결론

본 논문에서는 네트워크 보안 환경 변화에 따르는 요구사항을 반영할 수 있는 확장된 보안 기반 구조로써 액티브 네트워크를 이용한 보안 관리 프레임워크를 설계하고, 위조 IP 공격에 대응하기 위한 메커니즘을 제안하였다. 제안된 구조에서는 기존의 단일 조직 단위의 수동적인 침입 차단 및 침입 탐지 시스템의 문제점을 해결하고, 보다 능동적인 보안 서비스를 제공할 수 있다.

6. 참고문헌

[1] S.Bhattacharjee,K.L. Calvert ad E.W.Zegura, " An Architecture for Active networking" , High Performance Networking(HPN' 97), White Plains, NY, April, 1997.

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

[3] P. Ferguson, D.Senie, " Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing" , IETF RFC2827, May, 2000.