2002년 한국정보처리학회 춘계학술발표논문집 제9권 제1호

정책기반 네트워크보안 프레임워크에서의 네트워크 침입자 역 추적 메커니즘

방효찬*, 나중찬*, 장종수*, 손승원*
*한국전자통신연구원 네트워크보안연구부
e-mail : bangs@etri.re.kr

Network intruder trace back mechanism in a Policy-based network security management framework

Hyo-Chan Bang*, Jung-Chan Na*, Jong-Su Jang*, Sung-Won Son*
*Dept. of Network Security
Electronics and Telecommunications Research Institut

요 약

본 논문에서는 정책기반의 네트워크 보안 프레임워크 내에서 동작하는 침입자 역 추적 방안을 제안하고, 필요한 기능 구성요소에 대해 논한다. 제안한 역 추적 방안에서는 라우터, 스위치 등과 같은 기존의 네트워크 노드에서 tracing 기능을 직접 수행하지 않고도 위조된 유해 패킷의 송신 근원지 파악이 가능하다. 특히 정책기반의 네트워크 보안 프레임워크 내의 구성요소(보안제어서버, 보안게이트웨이)만으로 근원지 주소를 파악할 수 있기 때문에 망 구성 환경에 영향을 받지 않으며 네트워크 서비스 성능에 영향을 끼치지 않고도 침입 근원지를 파악하여 대응 할 수 있는 능동적인 보안 기능이 가능하다.

1. 서론

최근, 인터넷이 사회에 침투하여, 교육, 연구, 기업 등 많은 분야에서 이용되고 있으며, 이를 위한 정보통신 인프라도 급속히 비대해지고 있다. 이와 더불어 네트워크 침해사고 및 특정 호스트에 대한 서비스 방해 등과 같은 네트워크 상의 부정행위도 급증하고 있는 실정이다. 특히 이러한 사이버 공격으로 인한 경제적인 손실과 개인의 피해가 해마나 급증하고 있어 사이버테러에 대한 대응 방안이 시급히 요구되고 있다.

이에 대한 대책으로서 방화벽(Firewall)에 의한 접근제어 및 침입탐지시스템(IDS)에 의한 부정행위 검출 기술이 급속히 보급되고 있다. 그러나, 방화벽과 침입탐지시스템은 사전에 설정된 침입탐지 패턴과 보안정책에 따라 동작하는 정적인 기능만을 제공하고 있으며, 장비간의 상호 연동 및 통합운용의 어려움으로 인해 광역 네트워크 환경에서의 사이버테러에 대한 일관된 대응 방안을 제공하기에는 한계가 있다.

이러한 문제점을 해결하기 위해 네트워크 자원에 대한 운용 및 보안 관리를 공통된 정책에 따라 일관적으로 자동제어 하고 보안 장비간의 상호 운용성과 통합보안관리 기능을 제공하기 위한 정책기반의 네트워크 보안 프레임워크를 제안해 왔다[1,2].

정책기반의 네트워크 보안 프레임워크는 네트워크 접속 점에서 네트워크 침입 검출 및 대응이 운용자의 개입 없이 자동으로 수행되어 유해 패킷에 대한 일관된 대응이 가능하지만, 시스템 간의 연동을 통해 해커의 위치를 실시간으로 검출하여 네트워크로부터 고립시키거나 위조된 발신자 주소를 파악하여 실제 공격자의 위치를 추적하는 등 자율적이고 능동적인 구조는 제공하지 못하고 있는 실정이다. 또한, 인터넷을 경유한 네트워크 부정 행위를 조기에 검출하고, 침입 근원지를 파악하고자 하는 네트워크 침입자 역 추적 시스템에 대한 관심이 높아감에 따라 이에 대한 연구가 활발히 진행되고[3,4,5] 있지만 실제 망에 적용하기에는 scalability 측면에서 어려움이 있다.

본 논문에서는 상기의 문제점을 해결하기 위한 방

안으로 정책기반의 네트워크 보안 프레임워크 내에서 동작하는 침입자 역 추적 프레임워크를 제안하고, 역 추적을 실현하기 위해 필요한 기능 구성요소를 설계하였다.

2 정책기반의 네트워크 보안 프레임워크에서의 역 추적 구조

2.1 근원지 주소 역 추적 구조

네트워크 상에서 온라인으로 근원지 주소를 파악하기 위해서는 nslookup 또는 whois 등의 명령어를 사용하여 수동적으로 특정 IP 주소에 대한 정보를 수집하는 방법[7]이 있다. 그러나 근원지 주소는 쉽게 위조될 수 있으며, 이를 악용한 Flood 공격과 OOB 공격 등의 침입 유형은 상기 방법으로는 실제 근원지 주소의 추적이 불가능하다. 따라서 위조된 근원지 주소에 대한 효과적인 역 추적을 위해서는 IP 주소에만 의존하지 않는 새로운 역 추적 메커니즘이 필요하다.

본 논문에서는 이러한 문제를 해결하기 위한 방안으로 Ingress Filtering 기능과 Ethernet Frame 축약정보 관리 기능 및 trace audit 기능을 제안하고 그림 1 에 도시한 바와 같이 정책기반 네트워크보안 프레임워크 내의 보안게이트웨이(이하 SGS: Security Gateway System)에 이들 기능을 구현한다.

그림 1 은 정책기반의 네트워크 보안 프레임워크의 기능요소를 나타낸 것이다. 각 보안제어서버(이하 SCS: Security Control Server)는 망 경계에 위치하는 SGS 가 관리하는 네트워크의 프리픽스(IP 어드레스 범위)를 관리하고 있기 때문에 유해 패킷 검출을 통해 수신된 침입경보데이터의 근원지 IP 주소 필드를 참조하여 역 추적을 의뢰해야 하는 SGS 를 검색 할 수 있다. 역 추적을 의뢰 받은 SGS 는 상기 기능을 통해 실제 근원지 주소를 파악하고 역 추적을 의뢰한 SCS 로 그 결과 값을 송신한다.

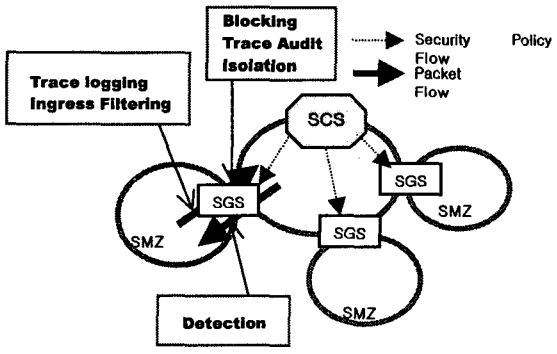

그림 1. 정책기반 네트워크 보안 프레임워크

2.2 근원지 주소 역 추적 아키텍처 요구사항

본 논문에서 제안하는 역 추적 아키텍처의 요구조건을 아래에 정리한다.

가) 정책기반 네트워크보안 프레임워크에서 동작한다.
나) 보안 관리 도메인 계층별로 보안제어 서버가 동작하고 상호 간의 연동이 보장되는 환경에서 동작한다.
다) 네트워크 접속 점에 위치하는 보안게이트웨이가 Ingress Filtering 기능을 수행한다.
라) 부정행위자의 발신 근원지 정보로 유해 패킷 송신자의 호스트 IP 주소를 검출하는 역 추적 기능을 수행한다.
마) 유해 패킷의 근원지 주소가 위조된 주소인 경우에도 실제 패킷 송신자의 IP 주소를 추적하는 기능을 수행한다.

2.3 역 추적 아키텍처 기본방침

가) 계층적 역 추적 관리 범위

인터넷은 대규모의 개방형 네트워크이기 때문에 역 추적을 위한 제어와 추적에 필요한 정보를 하나의 관리서버에서 일원 관리하는 것은 불가능하다. 또한 보안 관리 방침이 상이한 도메인 간에 추적 메커니즘을 계승시키기는 것 또한 어려움이 따른다. 따라서 역 추적 관리 범위로서 정책기반 보안관리 네트워크(PSMN: Policy-based Security Management Network)의 개념을 도입하여 추적의 제어와 정보 관리를 PSMN 별로 분산시켜 수행하고 각각의 PSMN 을 계층화 시켜 관리하는 아키텍처를 제안한다.

나) PSMN 내의 추적제어

PSMN 내에서 통일적인 보안 정책에 의한 역 추적 및 관련 정보를 집중적으로 관리하기 위한 보안제어서버(SCS)를 도입한다.

다) PSMN 간의 추적제어

추적 범위가 단일 PSMN 을 넘어설 경우 PSMN 간의 추적 상태파악, 추적 계속 판단 등의 전체적인 추적 상태 관리 및 PSMN 상호 간의 정보 교환 중개 등을 위한 최상위 보안제어서버(GSCS)를 도입한다.

3 정책기반의 네트워크 보안 프레임워크에서의 역 추적 기능

3.1 역 추적 기능 요소

Ingress Filtering 기능은 SGS 로 유입되는 outgoing packet 의 근원지 IP 주소가 SGS 가 관리하고 있는 네트워크 주소 범위를 초과한 경우, 즉 위조된 IP 주소인 경우에는 해당 패킷을 차단한 후 보안관리자에게 통보한다. 네트워크 경계에 위치하는 SGS 에서 Ingress Filtering 기능을 지속적으로 수행함으로써 해커가 다른 사이트의 IP 주소를 위조하고 있는 지를 실시간으

로 검출할 수 있으며, 위조된 패킷을 사전에 차단함으로써 침입자의 부정 행위 의도를 사전에 방지할 수 있다. Ingress Filtering 기능은 내부 망 안에서의 근원지 IP 주소 위조는 검출할 수 없으나 IP 주소 위조 가능 범위를 하나의 SGS 관리 도메인으로 축소시킬 수 있다.

Ethernet Frame 축약정보 관리 기능은 SGS 로 유입되는 모든 Ethernet Frame 으로부터 해당 프레임 내의 IP 패킷을 특정할 수 있는 기본 정보 만을 추출하여 일정기간 임시 저장하는 기능을 수행한다. 일반적으로 IP 헤더 내의 근원지 IP 주소는 해커에 의해 간단히 위조가 가능[7]하나 Ethernet Frame 내의 MAC 주소와 같은 데이터링크 층의 정보는 라우터 등의 중계장치에 의해 프레임 전송 시에 해당 네트워크 장치의 MAC 주소로 변환되기 때문에 사전에 위조하기는 어렵다. 따라서 데이터 링크 층의 정보와 IP 헤더 내의 정보를 함께 축약한 Ethernet Frame 축약정보는 유해 패킷을 송신한 실제 근원지를 추적하기 위한 유용한 정보로 활용할 수 있다.

Trace audit 기능은 유해 패킷 정보로부터 실제 근원지를 파악하는 역 추적 기능을 수행한다. Trace audit 는 역 추적 의뢰 시 전송되는 유해 패킷 정보에 포함되어 있는 IP 헤더 내용과 SGS 에 임시 저장된 Ethernet Frame 축약정보 내의 IP 헤더 내용이 일치하는 Ethernet Frame 축약정보를 검출한다. 검출된 로그정보의 근원지 주소 위조 여부를 판정하기 위해 ARP 주소 목록을 통해 IP 근원지 주소와 MAC 근원지 주소 조합이 일치하는 가를 판단한다. 일치되는 항목이 검출되지 않은 경우에는 근원지 IP 주소가 위조된 것으로 판단하여, SGS 의 ARP 캐시로부터 Ethernet Frame 축약정보의 근원지 MAC 주소에 실제 할당되어 있는 IP 주소를 검출한다.

3.2 통신 메시지

역 추적 아키텍처에 있어서 송수신 되는 모든 통신 메시지는 COPS Protocol 을 이용한다[8]. 표 1 은 역 추적에 필요한 각 메시지 및 내역을 정리한 것이다.

표 1. 통신 메시지 일람

메시지 명	개 요
Alert	SGS 가 탐지한 유해 패킷에 대한 경보 데이터를 SCS 로 통보하기 위한 메시지
trace request	SCS 가 SGS 로 침입자 역 추적을 의뢰하기 위한 메시지
trace result	SGS 가 SCS 로 역 추적 결과를 송신하기 위한 메시지
trace outcome	SCS 가 보안관리자에게 역 추적 결과를 통보하기 위한 메시지
PSMN trace request	PSMN 간에 침입자 역 추적을 의뢰하기 위한 메시지
PSMN trace result	PSMN 간에 역 추적 결과를 전달하기 위한 메시지

SCS 는 인접 PSMN 의 SCS 로부터의 역 추적 의뢰에 대하여 자신이 관리하는 PSNM 내에서 추적을 수행할 것인가를 판단하고, 필요에 따라서는 거부할 수 있으며 보안정책에 따라 추적을 제한할 수 있다. 역 추적 최종 수행 결과는 trace outcome 메시지에 의해 보안관리자에게 통보된다.

3.3 Ethernet Frame 축약 정보

Outgoing Ethernet Frame 축약 정보는 SGS 로 유입되는 모든 Outgoing Ethernet 프레임으로부터 SGS 가 trace audit 기능을 수행하기 위해 필요한 최소 정보를 추출하고 구조화한 데이터이다. 그림 2 는 Ethernet 프레임에서 검출해야 하는 축약정보 내용을 나타낸 것이다. 축약된 정보는 SGS 의 메모리 버퍼에 기록되며, 데이터 사이즈는 실제 패킷과 비교하여 매우 작고 일정시간 동안만 임시 저장되기 때문에 자원을 보다 효율적으로 사용할 수 있다.

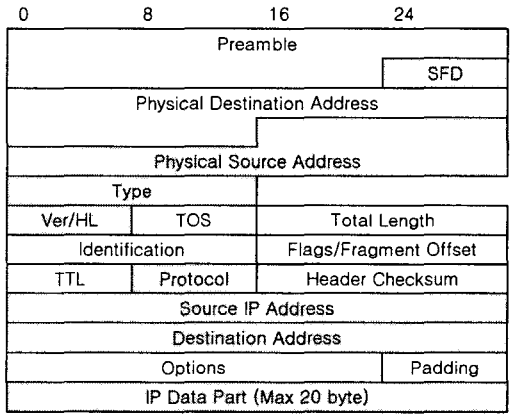

그림 2. Ethernet 프레임 축약정보(색칠 부분)

3.4 역 추적 기능 Flow Work

그림 3 은 정책기반 네트워크보안 프레임워크에서 SGS 에 의한 유해 패킷 검출로부터 침입자의 실질적인 근원지 IP 주소를 파악하기까지의 일련의 흐름을 나타낸 그림이다. 아래에 각 기능요소 및 흐름을 정리한다.

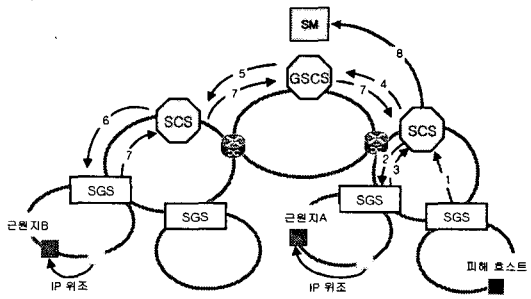

그림 3. 역 추적 기능 Flow

1. 타겟 사이트의 망 접속 점에는 네트워크기반 침입 탐지 기능을 수행하는 SGS 가 설치되어 있다[2]. SGS 는 유해 패킷이 검출되면 해당 패킷의 정보와 위반내역을 축약한 경보데이터를 생성하여 자신이 속해있는 PSMN 의 SCS 로 송신한다.
2. SCS 는 수신된 경보데이터의 보안등급이 역 추적을 요구하는 경우, 해당 경보데이터의 근원지 주소를 근거로 유입 점(특정 SGS)을 검출하여 해당 SGS 에게 역 추적을 지시한다.
3. SGS 는 trace audit 기능을 통해 근원지 IP 주소를 검출한 후 추적결과를 SCS 로 송신한다.
4. 추적 범위가 해당 PSMN 을 벗어난 경우 상위 SCS(GSCS)로 역 추적을 의뢰한다. 이때 2 항에서 수신한 경보데이터를 파라메타로 전송한다.
5. GSCS 는 자신이 관리하고 있는 SCS 를 통해 특정 유입 점(SGS)을 검출하고, 해당 SGS 를 관리 하는 SCS 로 역 추적을 의뢰한다.
6. SGS 는 trace audit 기능을 통해 근원지 IP 주소를 검출한 후 추적결과를 SCS 로 송신한다.
7. SCS 는 자신이 위치하는 PSNM 영역 내에서 역 추적을 수행한 결과를 종합하여 GSCS 를 경유해 추적을 의뢰한 SCS 로 송신한다.
8. 최초에 추적을 의뢰한 SCS 는 최종적인 추적결과를 보안관리자에게 통보한다.

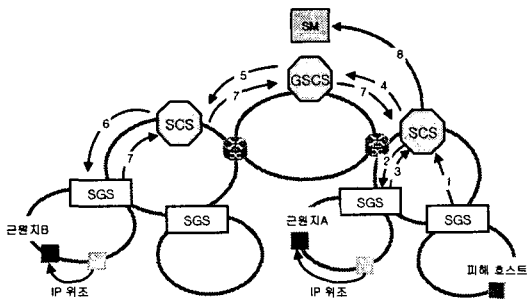

그림 3. 역 추적 기능 Flow

4. 결론

본 논문에서는 정책기반의 네트워크보안 프레임워크 내에서 동작하는 침입자 역 추적 메커니즘을 제안하고, 역 추적을 위해 필요한 기능 구성요소에 대해 논했다. 제안한 아키텍처는 라우터 및 스위치 등과 같은 기존의 네트워크 노드에서 tracing 기능 및 로깅 기능 등을 직접 수행하지 않고도 위조된 유해 패킷의 송신 근원지 파악이 가능하다. 특히 정책기반의 네트워크보안 프레임워크 내의 구성요소(SCS, SGS)만으로 근원지 주소를 파악할 수 있기 때문에 기존의 망 구성 환경에 영향을 주지 않는다. 또한, 네트워크 서비스 성능에 대한 영향을 최소화 하면서 침입 근원지를 파악하고 침입자를 네트워크로부터 고립시키는 등의 능동적인 보안기능이 가능하다.

향후 역 추적 소요 시간 측정 및 축약정보 버퍼링 유효 한계 값 계산 등의 유효성 검증 연구를 통해 제시한 아키텍처를 실제 네트워크에 적용하기 위한 방안을 모색해 갈 예정이다.

5. 참고문헌

[1] 방효찬,김명은,장종수,"PBNM 최신동향 분석을 통한 정책기반의 네트워크보안제어 기술 제안",NCS2000

[2] 방효찬 외 3 인, "보안정책모델을 적용한 네트워크 보안제어서버 구조", 한국정보처리학회 2001 추계학술대회지

[3] DARPA ITO, "Dynamic, Cooperating Boundary Controller, Project Introduction in http://www.darpa.mil/ito

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

[5] K,Kokubo, H.Watanabe, S.Matsuda, et al. "A study of unauthorized access tracing system" in Proceeding of the 60th National Convention of IPSJ, March 2000

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

[7] E.Amoroso, "Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace back, Traps and Response", Intrusion.Net Books, Sparta, New Jersey, 1999

[8] RFC2748," The COPS(Common Open Policy Service) protocol