정책기반 네트워크 보안구조에서 IP Encapsulation을 이용한 실시간 침입자 추적 기술

이광희° 안개일 장종수 최훈
한국정보통신연구원 보안게이트웨이연구팀, 충남대학교
{khlee63734°, fogone, jsjang}@etri.re.kr, hchoi@ce.cnu.ac.kr

The Intruder Traceback technology using IP Encapsulation on Policy-based Network Security Architecture

Lee KwangHee° An Gaell Jang JongSu
Electronics and Telecommunications Research Institute, Security Gateway Research Team

요 약

본 논문에서는 고도로 지능화고 복잡한 공격으로부터 광대역 네트워크를 보호하기 위한 정책기반 네트워크 보안구조와 능동적 네트워크 보안 기술의 핵심인 실시간 침입자 추적 기능의 효율적인 통합 방안을 제시하기 위해 필요한 구성요소를 정의하고 이들간의 통신 프로토콜을 확장하여 정책기반 네트워크 보안구조에 적합한 실시간 침입자 추적 기술로서 IP Encapsulation을 이용한 실시간 침입자 추적 알고리즘을 제시한다.

1. 서 론

인터넷은 가상생활환경의 제공과 정보공유 환경의 제공, 가상 업무환경의 제공 등과 같은 생활의 편의성을 제공하고 있지만 누구나 쉽게 접근할 수 있는 개방망 환경으로 인한 해킹, 바이러스 유포, 지적 재산권의 침해, 사이버 범죄에의 이용 등과 같은 정보화 역기능의 위험도 만만치 않은 것이 현실이다. 이러한 사이버 공격은 더욱 분산반사서비스거부(DRDoS : Distributed Reflected Denial of Service) 공격과 같이 더욱 지능화되고 있으며 그 대상도 개별 시스템에서 광대역 네트워크로 확대되고 있다. 이렇듯, 네트워크에 대한 사이버 공격 양상이 점차로 복잡해지고 광역화됨에 따라 네트워크에 존재하는 각 보안 시스템 간의 상호 결합적 운용을 통해 전체 네트워크 차원에서 공격자에 대한 대응도 기존의 수동적 대응에서 능동적이고 통합적인 네트워크 보안 방안이 요구되어 진다.

정책기반 네트워크 보안구조는 기본적으로 IETF의 PBNM (Policy-Based Network Management) 구조[1]를 따르며 PBNM 구조에서 PMT(Policy Management Tool)와 PDP (Policy Decision Point) 역할을 수행하는 CPCS(Cyber Patrol Control System) 시스템과 PEP(Policy Enforcement Point) 역할을 수행하는 SGS (Security Gateway System) 시스템으로 구성된다[2].

침입자 역추적 기술은 크게 두 가지로 분류할 수 있다. 대규모의 IP Spoofing 패킷을 생성하는 근원지를 찾기 위한 IP Traceback 기술과 인터넷에 연결된 컴퓨터를 징검다리 호스트(Stepping Host)로 이용하여 자신을 숨기는 침입자를 추적하기 위한 Connection Traceback 기술이다. 침입자 역추적 기술은 능동적 네트워크 보안 기술의 핵심이며 공격자의 공격시도 자체를 제한한다. 본 논문에서 정의하고자 하는 실시간 침입자 역추적 기술은 Connection Traceback 방식으로서 공격자는 자신을 숨기기 위해 IP Spoofing을 하지않고 다수의 Stepping 호스트를 통한 Interactive TCP connection을 이용하여 피해시스템을 공격한다고 가정한다.

본 논문에서는 고도로 지능화고 복잡한 공격으로부터 광대역 네트워크를 보호하기 위한 정책기반 네트워크 보안구조와 능동적 네트워크 보안 기술의 핵심인 실시간 침입자 추적 기능의 효율적인 통합 방안을 제시하기 위해 필요한 구성요소를 정의하고 이들간의 통신 프로토콜을 확장하여 정책기반 네트워크 보안구조에 적합한 실시간 침입자 추적 기술로서 IP Encapsulation을 이용한 실시간 침입자 추적 알고리즘을 제시한다.

2. 관련 연구

2.1 정책기반 네트워크 보안구조 (Policy-based Network Security Architecture)

정책기반 네트워크 보안구조는 기본적으로는 PBNM 구조를 따르지만 세부적으로는 많은 기능을 추가하고 확장해야 한다. PBNM 구조는 네트워크 관리를 목적으로 하고 정책기반 네트워크 보안구조는 네트워크 보안을 목적으로 하기 때문에 어떠한 확장 없이는 그대로 적용할 수가 없기 때문이다. 네트워크 보안 관점에서 PBNM 구조의 PCIM 모델, COPS, LDAP 프로토콜의 확장과 침입보고를 위한 IAP(Intrusion Alert Protocol)의 도입이 필요하다. 정책기반 네트워크 보안구조에서 정의하고 있는 CPCS 시스템과 SGS 시스템이 제공하는 주요 서비스는 다음

과 같다.

- CPCS 시스템 : 보안정책 관리 및 전달, 침입분석 및 대응정책 수립, SGS 시스템 관리
- SGS 시스템 : 보안정책 집행, 침입 탐지/차단 기능 제공, 관리 정보 제공

정책기반 네트워크 보안구조의 간단한 네트워크 구성을 개념적으로 표현해 보면 다음과 같다.

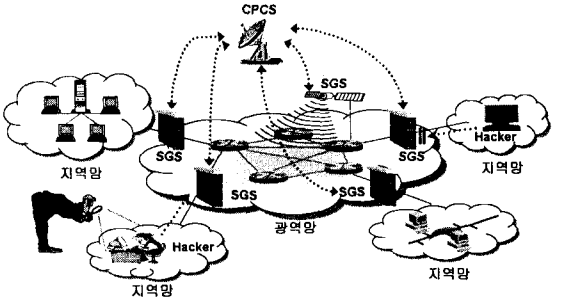

그림 1 정책기반 네트워크 보안구조 개념도

2.2 침입자 역추적 기술 (Intruder Traceback Technology)

침입자 역추적 기술은 크게 두 가지로 분류할 수 있다. 대규모의 IP Spoofing 패킷을 생성하는 근원지를 찾기 위한 IP Traceback 기술과 인터넷에 연결된 컴퓨터를 징검다리 호스트(Stepping Host)로 이용하여 자신을 숨기는 침입자를 찾기 위한 Connection Traceback 기술이 있다.

IP Traceback은 데이터를 전송하는 라우터에서 침입자 추적을 위한 정보를 제공하고 침입을 발견한 피해시스템은 라우터에서 제공하는 추적 정보를 이용하여 공격 경로 그래프(Attack Graph)를 생성하여 침입자를 추적하는 기술이며 서비스 거부 공격에서처럼, TCP/IP의 단점인 IP Spoofing을 이용한 대량의 패킷 생성 호스트 발견을 목표로 하며 경우에 따라선 침입자와 가장 가까운 에지 라우터를 찾는 기술이다. Connection Traceback 기술은 침입자가 자신을 숨기기 위해 인터넷에 연결된 다수의 컴퓨터를 이용한 공격에서 침입자에 의해 공격에 이용된 컴퓨터(Stepping host)를 발견하고 최종적으로 침입자가 사용하고 있는 컴퓨터를 찾기 위한 기술이다. 침입자가 Telnet과 같은 Interactive TCP connection을 이용하여 네트워크에 연결된 다수의 컴퓨터를 통해 피해시스템을 공격하려 할 때 침입자 추적을 위해 효율적인 Connection Chain 구성 방안이 가장 중요한 이슈가 된다. 이러한 Connection Traceback 기술에는 ThumbPrint[3], Timing based algorithm[4], Sequence number deviation[5] 등이 대표적인 기술이다.

ThumbPrint는 네트워크 모니터와 같은 네트워크 감시 장비에 적용할 수 있는 네트워크 방식의 TCP connection 추적 기법이며 패킷의 컨텐트 기반 방식이며 컨텐트 요약 데이터(24byte/min/connection)를 이용하여 TCP connection 연관성 분석을 수행하는 기법이다

Timing based algorithm는 " 같은 connection chain에 속하는 TCP connection은 같은 데이터 전송 기간(ON period), 데이터를 전송하지 않는 기간(OFF period)를 갖는다" 라는 개념을 이용하여 연관성 분석을 수행한다.

Sequence number Deviation 기법은 TCP connection이 두 시스템 간에 연결될 때 Initial sequence number 협상 후 실제 데이터 전송이 일어날 때 협상된 Sequence number에 데이터 길이를 더해서 전송하는 것을 이용해 연관성 분석을 수행하는 기법이다.

이러한 기법들은 연관성 분석을 위한 데이터를 수집하는 네트워크 장비들간의 매우 적은 오차의 클럭 동기화를 요구하며 전송데이터 오류에 의해 발생하는 데이터 재전송(Retransmission)에 의해 TCP connection 연관성 분석이 영향을 받는다.

3. 정책기반 네트워크 보안구조에서 IP Encapsulation을 이용한 실시간 침입자 추적 기법

정책기반 네트워크 보안구조에서 인터넷에 연결된 다수의 징검다리 호스트들의 Interactive TCP 연결을 통해 하나 혹은 다수의 SGS에 의해 보호되는 피해시스템을 공격하는 공격자를 실시간 추적하기 위해 IP Encapsulation을 이용한 실시간 침입자 추적 기법을 정의하며 구성요소의 확장을 통해 수행된다.

- CPCS 시스템 : 보안정책 관리 및 전달, 침입분석 및 대응정책 수립, SGS 시스템 통합관리, SAT 시스템 관리, 실시간 침입자 추적 정보 분석
- SGS 시스템 : 보안정책 집행, 침입 탐지/차단 기능, 관리 정보 제공, 실시간 침입자 추적을 위한 Tracker Packet 생성 및 제거, 침입자 추적 정보 보고
- SAT (Subnet Attacker Tracer) : 서브넷에서 침입자 추적을 위한 TCP Connection의 연관성 분석, ADI 삽입, 추적 패킷 재 생성, 침입자 추적 정보 보고
- 추적 패킷(Tracker Packet) : 공격에 의한 응답 패킷을 IP Encapsulation을 통해 생성된 침입자 추적 패킷
- IAP (Intrusion Alert Protocol) : 침입자 추적 정보를 CPCS에 보고 하기 위한 통신 프로토콜
- ADI (Attacker Detection ID) : TCP 연관성 분석에 이용되는 문자열로서 32bit 난수발생 숫자이고 사용자는 인식할 수 없는 가상 공백 문자열(Virtual NULL String)로 표현됨

정책기반 네트워크 보안구조에서 실시간 침입자 추적을 위해 피해 시스템에서 공격자로 응답 패킷을 이용하여 침입자 추적을 수행하므로 침입자 추적 기능이 항상 활성화 되어 있는 것이 아니라 침입자 추적 패킷의 수신을 통해 활성화되며 공격자 추적 패킷은 피해시스템이 공격에 의한 응답 패킷을 공격자로 전송할 때 SGS에서 이 패킷을 캡쳐하여 생성한다. 이때 외부 IP 헤더의 정보는 응답 패킷에서 추출하여 구성하며 발신지 주소는 SAT나 SGS에 의해 침입자 추적 정보를 보고하기 위해 CPCS의 IP

주소가 되며 목적지 주소는 응답 패킷의 목적지 주소가 된다. 내부 IP Header는 이 패킷이 침입자 추적 패킷임을 나타내기 위해 TTL 필드를 255로 설정하고 헤더 체섬 필드는 침입 타입 정보를 나타내며 발신지 주소는 나중에 일반 응답 패킷으로 변환하기 위해 응답 패킷의 발신지 주소로 설정되며 목적지 주소는 CPCS에서 침입자 추적에 부여한 침입자 추적 ID 정보가 설정된다. 따라서 기존의 침입자 추적 기법과는 달리 클럭 동기화를 요구하지 않으며 TCP 재전송에 영향을 받지 않는다.

침입자 추적 패킷의 구조는 다음과 같다.

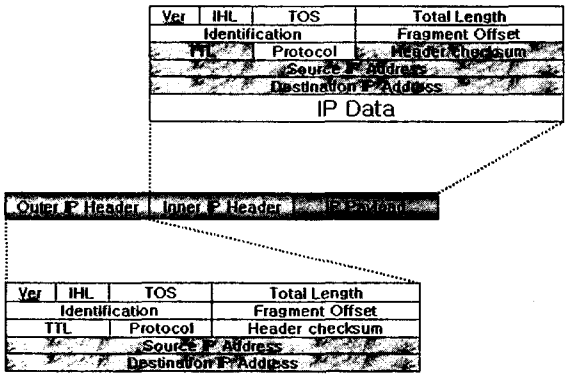

그림 2 침입자 추적 패킷의 구조

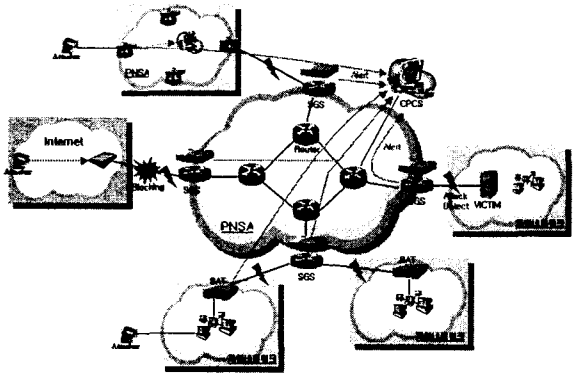

그림 3 정책기반 네트워크 보안구조에서 실시간 침입자 추적 과정

그림 3은 정책기반 네트워크 보안구조에서 실시간 침입자를 추적하는 과정을 나타내고 있다. 공격자는 하나의 CPCS에 의해 관리되는 정책기반 네트워크 보안구조에 인터넷을 통하거나 지역네트워크, 또는 다른 정책기반 네트워크 보안구조에서 공격을 시도한다.

① 정책기반 네트워크 보안구조내의 SGS에서 피해시스템에서 공격이 발생했음을 검출한다.

② SGS는 CPCS에게 공격타입, 피해시스템에 관한 정보를 보고하고 침입자 추적 ID를 CPCS로부터 부여 받는다.

③ SGS는 피해시스템으로부터의 응답 패킷을 캡춰하여 추적 패킷을 부여 받은 침입자 추적 ID를 이용하여 생성 후 일반 라우팅에 따라 전송한다.추적 패킷의 목적지주소에 따라 L3 라우팅을 통해 정책기반 네트워크 보안구조의 다른 SGS에게 전달된다.

④ 추적 패킷을 전달 받은 SGS는 미리 설정되어 있는 포워딩할 네트워크 정보를 이용하여 대응을 판단한다. 인터넷 전송해야 한다면, 추적 패킷의 목적지 주소로부터 오는 모든 패킷에 대한 Blocking을 수행하며 다른 정책기반 네트워크 보안구조나 지역네트워크로 전달한다면, CPCS에 추적 패킷 수신을 보고하고 다시 목적지 주소에 따라 L3 포워딩을 수행한다.

⑤ SAT에서 추적 패킷을 수신하면 모니터링 테이블(Target Host, ADI, Timeout)을 생성하고 일반 응답 패킷을 생성 후 패킷의 페이로드에 ADI를 삽입하여 전송한다. Target host에서 생성되는 TCP connection 트래픽을 모니터링하여 패킷에 ADI가 포함되었는지 검사한다.

⑥ SAT에서 Target host의 트래픽 중 Timeout 전에 ADI 포함 패킷을 검출하면 CPCS에게 이 호스트가 징검다리 호스트로 이용되었음을 알리고 다시 Tracker 패킷을 생성 후 L3 포워딩하며 Timeout 동안 검출되지 않으면 이 호스트가 공격자 호스트임을 CPCS에게 보고한다.

4. 결 론

본 논문에서는 정책기반 네트워크 보안구조에서 IP Encapsulation을 이용한 실시간 침입자 추적을 위해 CPCS, SGS, IAP의 확장하였으며 지역 네트워크내에서 침입자 추적을 위한 네트워크 모니터인 SAT를 정의하였다. 본 논문에서 정의한 IP Encapsulation을 이용한 실시간 침입자 추적 기법은 정책기반 네트워크 보안구조에 적합한 실시간 침입자 추적기법이며 응답 패킷의 침입자 추적 패킷화로 기존의 침입자 추적 기법이 요구하는 클럭 동기화나 TCP connection의 재전송에 따른 문제를 해결하였다. 그러나, TCP 연관성 분석을 위해 패킷의 컨텐트를 이용하므로 컨텐트를 암호화하는 TCP 연결 공격은 지원할 수 없으며 이는 향후연구과제로 남긴다.

5. 참고 문헌

[1] Dinesh C. Verma, " Policy-Based Networking : Architecture and Algorithms" , New Riders Publishing, 2001

[2] 김기영 외 3명, " 정책기반 네트워크 보안구조 및 설계" , JCCI 2002, 2002.4.24

[3] S. Staniford-Chen, " Holding Intruders Accountable on the Internet" , In Proceedings of IEEE Symposium on Security and Privacy, 1995

[4] Yin Zhang, " Detecting Stepping Stones" , In the Proceedings of the 9th USENIX Security Symposium, 2000.8

[5] Kunikazu Yoda, " Finding a Connection Chain for Tracing Intruders" , 6th ESORICS, 2000.10