상태기반 감시기술의 취약점과 위협에 관한 연구

한기문°[1,2], 류재철[2]

[1] 한국과학기술원 사이버보안연구센터, [2] 충남대학교 컴퓨터공학과

A Study for Vulnerabilities and Threats of Stateful Inspection Technology

Ki-Moon Han°[1,2], Jae-Cheol Ryou[2]

[1]KAIST Cyber Security Research Center,

[2]Department of Computer Engineering, Chungnam National University

linuzen@gmail.com, jcryou00@gmail.com

요 약

대부분의 침입차단시스템에서 사용하는 상태기반 감시기술(Stateful Inspection)은 기존 패킷필터 방식이 갖고 있던 세션검사 부재로 인한 한계점을 해결하였다. 하지만 네트워크 트래픽에 대한 상태 변화를 감시 하기 위해 보다 많은 자원을 사용하게 되었고 이로 인한 보안상 문제점이 발생될 가능성이 존재한다. 본 논문에서는 상태기반 감시기술에 대한 신규 취약점을 확인하고 실험을 통해 공격의 실현 가능성을 제시한다.

1. 서론

1990 년대 초 Check Point 가 제안한 상태기반 감시기술(Stateful Inspection)[1]은 오픈소스 및 상용 침입차단시스템은 물론 VPN, 사용기반 과금 시스템 등 네트워크 트래픽 모니터링 기반 시스템에 있어 중요한 기술로 사용되고 있다. 특히 다양한 적용 분야 중 침입차단 분야에 적용 사례가 큰 성과를 보이는데 이는 기존 패킷기반 감시 기술의 한계인 응답 패킷에 대한 별도 접근 통제 규칙 추가 필요 및 FTP 와 같은 파생 세션에 접근 통제 불가 등의 문제점을 해결하고 효율적인 정책관리가 가능하기 때문이다.

상태기반 감시기술에서 현재 상태의 플로우 정보를 저장하는 세션 테이블은 한정된 시스템 자원 안에서 동작하고 이를 사용하는 침입차단시스템은 내부 인프라를 보호하는 장비의 위치 특성상 중요한 공격 목표가 되었다.

본 논문에서는 오픈소스 침입차단시스템인 IPTABLES 를 대상으로 변조된 IP 로 생성된 비정상적인 플로우 정보가 정상 세션으로 인지되는 취약점을 확인하고 실험을 통해 검증하였다.

2. 취약점 및 위협

상태기반 감시기술에서 TCP 프로토콜에 대한 감시는 종단간의 3-Way Handshake 과정을 모니터링하고 정상적인 세션성립(ESTABLISHED)이 이루어지는지 검사하는데, 세션성립 시 타임아웃 값은 시스템 설정에 따라 차이가 있으나 최소 5 분에서 최대 5 일까지로, SYN_RECV, FIN_WAIT 등 다른 상태의 타임아웃 시간보다 일반적으로 크게 설정[2] 된다. 3-Way Handshake 를 거쳐 성립된 세션을 정상적인 호스트간의 연결로 인지하는 것은 그림 1 과 같은 과정[3]을 거치기 때문이다.

그림 1 과 같이 세션을 열기 위해서 출발지 A 는 SYN 플래그가 설정된 패킷에 초기 순서번호(Sequence Number)M 을 부여하여 전송하고 B 로부터 수신한 초기 순서번호 N+1 의 응답번호(Acknowledgement Number)를 설정하여 ACK 플래그가 설정된 패킷에 실어 전송한다. 정상적인 IP 는 목적지 B 로부터 수신된 초기 순서번호 N 을 확인하여 응답번호 N+1 을 포함한 ACK 패킷을 전송할 수 있으나 변조된 IP(Spoofed)는 순서번호 N 이 포함된 패킷을 수신할 수 없기 때문에 세션연결이 불가능하다.

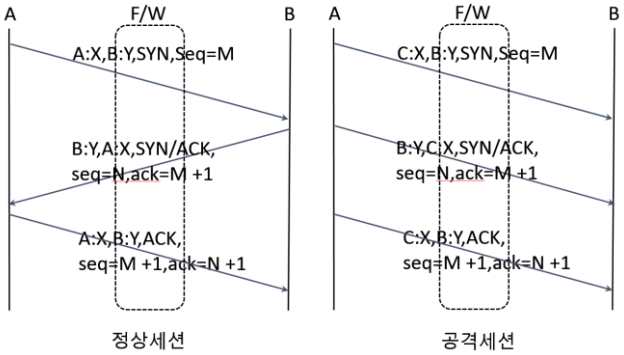

그림 1. 정상 및 공격세션

침입차단시스템과 같이 네트워크 중간에서 세션을 확인하는 상태기반 감시장비의 세션 테이블은 전송되는 패킷의 출발지 IP, 출발지 포트, 목적지 IP, 목적지 포트, 플래그, 순서번호, 응답번호 등을 확인하지만 전송 인터페이스에 대한 검증을 하지 않아 변조된 IP 로 침입차단시스템의 세션을 증가시킬 수 있는 취약점이 존재한다. 그림 1 의 공격세션과 같이 SYN/ACK 플래그가 포함된 두 번째 패킷의 순서번호는 공격자가 임의로 생성할 수 있으므로 공격자는 세 번째 ACK 플래그가 포함된 패킷의 응답번호를 계산하여 전송할 수 있다.

3. 실험 및 검증

제안하는 공격의 실현 가능성을 검증하기 위한 실험 환경은 오픈소스 침입차단시스템인 리눅스 IPTABLES 를 이용하여 구축하였다. 리눅스 머신은 2 개의 네트워크 인터페이스(eth0, eth1)을 갖고 있으며 이는 각각 호스트 A, B 와 연결되어 있다. 침입차단시스템은 서로 다른 A 대역과 B 대역에 대한 라우팅 테이블이 설정되어 있고 디폴트 라우팅은 A 네트워크로 설정하였다.

IPTABLES 의 접근통제 규칙은 FORWARD 체인에 기본 차단 규칙(iptables -P FORWARD DROP)을 설정하고 상태기반 감시를 위한 규칙(iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT)을 설정하였다. 또한, 일반적인 웹 서비스 환경의 HTTP 서비스 허용 규칙(iptables -A FORWARD -p tcp -m tcp --dport 80 -j ACCEPT)을 추가하였다.

공격 방법은 A 호스트에서 B 호스트로 SYN, SYN/ACK, ACK 패킷을 모두 전송하고 이때 출발지 IP 는 C 로 변경하였다.

시험결과는 그림 2 와 같이 iptstate(IPTables State Top)를 사용하여 세션을 확인한 결과 변조된 IP 에서 약 120 시간의 타임아웃 값을 갖는 2 개의 세션이 생성 되었음을 볼 수 있다.

4. 관련연구

네트워크 상태감시를 위해 사용되는 세션테이블은 제한된 시스템 자원 안에서 많은 세션을 관리해야 하므로 이를 사용하는 침입차단시스템은 SYN Flooding, Connection Flooding 과 같은 DDoS 공격의 직접, 간접적인 공격 대상이 된다. Connection Flooding 의 경우 세션성립을 위해 변조되지 않은 실제 IP 를 사용 해야 하므로 대량의 좀비 PC 를 확보해야 하는 어려움 이 있고 변조 IP 로 공격이 가능한 SYN Flooding 의 경우 SYN Cookie 를 사용하거나 SYN RECV 타임아웃 값을 줄여 대응하는 방법[4]들이 제안 되었다.

성능 향상을 위한 세션 테이블 구조개선의 노력[5-7]과 함께 불필요한 미완성 엔트리를 제거 하기

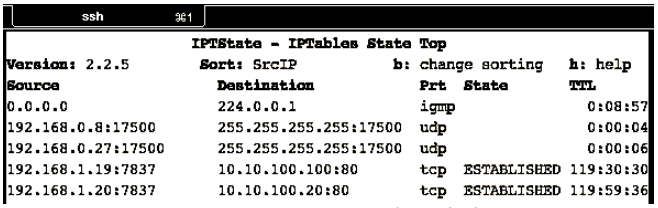

그림 2. IPTABLES 세션현황

위해 적절한 타임아웃 값 설정이 제안 되었으나 취약점을 이용한 정상 세션 연결 시 생성되는 세션테이블의 증가를 막는 데는 한계가 있다.

5. 결론

본 논문에서는 상태기반 감시기술의 취약점을 이용하여 실제 세션이 성립될 수 없는 변조된 IP 로 침입차단시스템의 세션테이블을 증가 시킬 수 있는 위협을 실험을 통해 확인 하였다.

실제 네트워크 환경에서는 3-Way Handshake 의 두 번째 패킷인 SYN/ACK 플래그 패킷의 출발지와 목적지가 변경된 상태에서 변조된 IP 로 라우팅이 불가능하다는 점과 목적지에 SYN 패킷과 부적절한 ACK 패킷이 전달 되었을 때 목적지 서버의 Retry 및 RST 패킷 발생으로 세션 테이블이 초기화 될 수 있는 제약이 있다. 이를 극복하기 위해 내부 네트워크 대역을 사용 하거나 TTL 값을 변경 하는 등 다양한 방법을 연구 중이고 상용 침입차단시스템을 대상으로도 동일한 취약점이 존재하는지 확인이 필요하다.

6. 참고 문헌

[1] Check Point Software Technologies, Ltd. ”Stateful Inspection Technology”, http://www.checkpoint.com/download/public-files/Stateful_Inspection.pdf, Aug. 2005.

[2] Iptables-The state machine, http://www.iptables.info/en/connection-state.html.

[3] Jon Postel, Transmission Control Protocol, https://www.ietf.org/rfc/rfc793.txt, RFC793, Sep. 1981.

[4] Hyogon Kim et al., "TCP 연결의 스테이트풀 인스펙션에 있어서의 보안 약점 최소화 및 성능 향상 방법", 정보과학회논문지 정보통신 제 32 권 제 4 호, Aug. 2005.

[5] Xin Li et al., "Stateful Inspection Firewall Session Table Processing", IEEE ITCC, Apr. 2005.

[6] Mohamed G. Gouda et al., "A Model of Stateful Firewalls and its Properties", IEEE DSN, Jul. 2005.

[7] Noureldien N.A et al.,"A Stateful Inspection Module Architecture", IEEE TENCON, Sep. 2000.