한국컴퓨터정보학회 하계학술대회 논문집 제18권 제2호 (2010. 7)

계층적 방어를 위한 침입탐지 시스템 설계

구민정°, 한우철**, 장영현***
°(주)넷플라이, **대림대학, ***배화여자대학
e-mail: ok999@hanmail.net, wchan@daelim.ac.kr, baewhaoa@paran.com

Design of an Intrusion Detection System for Defense in Depth

Min Jeong Koo°, Woo Chul Han**, Young Hyun Chang***
°Research Institute, NETFLY Co., LTD
**Dept. of Computer Information, Baewha Women's University
***Dept. of Industrial Management, Daelim University

● 요 약 ●

2000년 대규모 DDoS 공격이래, 2009년 7월 7일 국가주요정부기관 및 인터넷 포털, 금융권 등의 웹사이트 대상으로 1차, 2차, 3차로 나누어 대규모 사이버 공격이 발생하였다. 지속적으로 발전되는 행태를 보이고 DDoS 공격에 대해 본 논문에서는 계층적인 침입탐지시스템을 설계하였다. 네트워크 패킷을 분석하기 위해 e-Watch, NetworkMiner등의 패킷, 프로토콜 분석도구를 이용하여 TCP/IP의 Layer별 공격을 분석한 후 패킷의 유입량, 로그정보, 접속정보, Port, Address 정보를 분석하고 계층침입에 대한 방어를 수행하도록 설계하였다. 본 논문은 DDoS(Distributed Denial of Service)에 대한 패킷 전송에 대해 계층적인 방어를 통해 보다 안정적인 패킷수신이 이루어진다.

키워드: 침입탐지(Intrusion Detection), 계층적 방어(Defense in Depth), OSI 7계층(OSI 7layer)

I. 서론

2000년대 초반 아마존, 야후, 이베이, E-트레이드등 유명 인터넷 사이트들의 침해로 12억 달러의 경제적 손실이 발생된 이래, 7·7 DDoS 대란은 2009년 7월 7일~ 7월 10일까지 만 3일 동안 진행된 DDoS 공격으로 국내·외 주요 웹사이트에 동시 다발적으로 접속 장애를 발생시켰으며, 7월 10일 0시를 기준으로 악성코드(인터넷 웜)에 감염된 PD에 대한 파일 파괴 및 부팅 에러가 일어나 추가적 이용자 피해가 발생되어 현대경제연구원은 363억원~544억원의 경제적 손실을 추정하고 있다[1]. 또한 DDoS 공격은 금전적인 피해를 넘어 불이익, 경쟁, 보복, 이념의 차이를 표현하고 주장하기 위한 종교적, 정치적 사이버 시위 그리고 국가간의 분쟁에서 선제공격으로 이용되고 있으므로 중요한 과제라 볼 수 있다. 이에 본 논문에서는 네트워크 패킷을 분석하기 위해 e-Watch, NetworkMiner등의 패킷, 프로토콜 분석도구를 이용하여TCP/IP의 Layer별 공격을 분석한 후 패킷의 유입량, 로그정보, 접속정보, Port, Address 정보를 분석하고 계층침입에 대한 방어를 수행하도록 설계하여 안정적인 패킷 전송이 이루어 질 수 있도록 계층적 방어를 위한 침입탐지시스템을 설계하였다[3].

II. 관련 연구

1. 관련연구

대규모 인터넷공격에 대응하기위해 ISP에서도 각종 네트워크장비와 보안솔루션을 적용하여 네트워크 모니터링과 침입을 차단하고 있으나, 광대역 네트워킹 환경에서 안전한 방어는 어려운 실정이다. 따라서 기존의 방어 기법과 제안한 계층적 방어의 침입탐지의 차이를 분석한다.

1.1 기존의 침입탐지 기술

1) ACL(Access Control List)

IP주소, 서비스포트, 컨텐츠 차단을 수행하며, 네트워크 장비의 부담을 줄이기 위해서는 접근통제를 위한 별도의 ASIC화된 모듈이 필요하다. 그러므로 장비의 접근통제 정책을 업데이트하기 위한 별도의 스크립트가 필요하다[2].

2) Null0 라우팅(블랙홀 라우팅, 블랙홀 필터링)

이동 중인 패킷들을 Null0라는 가상 인터페이스에 포워딩하여 drop 시키는 기술이다. 포워딩 기능을 사용하며, L3의 필터링만 제공하므로 서비스포트제공, L4·L7의 필터링이 불가능하다.

3) uRPF(unicast Reverse Path Forwarding)

단순한 IP Spoofing을 차단하는 기술로써, 라우터가 수신한 패킷의 송신지 IP를 확인하여 Reverse Path가 존재하는지 확인한다. 그러나 다수의 경로(비대칭 망구조)인 경우, 적용 한계가 있다.

4) Rate-Limit 기술(Rate Filtering)

일정단위시간 동안 일정량이상의 특정 서비스패턴을 가진 패킷이 유입되는 경우 차단하는 기술이며, Cisco에서는 CAR(Commit Access Rate)로 구현하며, flooding공격시 Bandwidth제한에 사용된다. 전용모듈이 없을 경우, 라우터의 과부하를 유도한다.

5) NegtFlow

Cisco에서 개발되었으며, Traffic Flow Analysis를 통해 소스 및 대상주소, 각 flow의 Byte수, 패킷수, 유입인터페이스, 업스트림피어정보등을 모니터할 수 있다. 그러나 네트워크장비에 대한 접근이 주어져야 분석이 가능하다.

6) Firewall, IPS(INtrusion Prevntion), L7 스위치등 기존의 보안장비도 DDoS에 대한 차단과 추적기능이 있으나, 전체의 ISP 망을 제어할 수 없다.

III. 제안한 계층적 방어를 위한 침입탐지 시스템 설계

1) 방화벽과 DMZ는 외부공격으로부터 웹서버, 이메일 게이트웨이, 네트워크 서버, 안티바이러스서버 DNS서버를 배치하여 침해를 방지한다.

2) 방화벽으로 유입된 침입트래픽의 경우, Application,Transport, Internet, Network 계층별로 공격을 분석하여 IDS로 전송하여 IDS는 공격의 특성 세부적으로 검출하고(신종포함) 보안정책을 방화벽으로 업데이트하고 공격패킷을 폐기한다. 정상패킷의 경우, 다음 노드로 전송하여 침입을 방지한다.

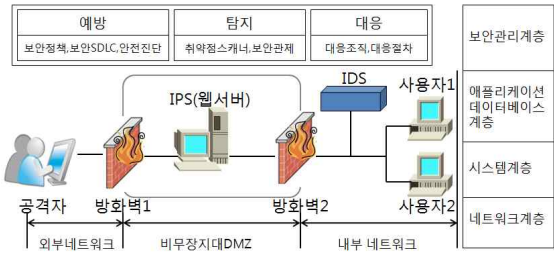

그림1. 계층적 방어의 침입탐지 시스템

Fig 1. An Intrusion Detection System for Defense in Depth

3) 응용계층의 응용프로그램은 개발자에 의해 취약점이 고려되지 않으므로 통신당사자간의 상호인증이 이루어 지도록 프로그램을 설치하여, 다소 처리시간이 지연되어지만, 안정화를 높였다.

IV. 결론

패킷이 유입되면, 방화벽을 이용하여 각 계층별 침입의 유형을 검출하여 IDS로 전송하고 IDS는 공격을 특성을 세부적으로 검출하여 보안정책을 방화벽에 전송함으로써 공격패킷의 검출에 대비하였으며, 응용계층에 상호 인증프로그램을 구동하여 신뢰성을 높였다.

참고문헌

[1] 배성훈, '7.7 DDoS 사고' 대응의 문제점 재발방지 방안, 국회입법조사처, 2009. 12. 1

[2] "Design and Implementation of Security Protocol for Home-Network", Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing, 2009. SNPD '09. 10th ACIS International Conference, IEEE, pp.220-224, September 2009.