정 보 보 호 학 회 지
제24권 제1호, 2014. 2

TCP/IP 네트워크 프로토콜의 DoS 공격 취약점 및 DoS 공격사례 분석

조 성 현*, 이 택 규**, 이 선 우***

요 약

서비스 거부 공격 (Denial of Service Attack)은 현재 사이버테러와 맞물려 중요한 이슈로 자리 잡고 있다. 응용계층에서부터 네트워크계층에 이르기까지 다양한 프로토콜들의 취약점을 이용하는 DoS 공격은 공격대상을 서비스 불가능 상태에 빠뜨려 작게는 서버다운에서 크게는 국가적인 보안위험을 야기 시키고 있다. 본 논문은 TCP/IP 기반 네트워크에서 DoS 공격에 대하여 취약점이 있는 응용계층, 전송계층, 및 네트워크 계층 프로토콜들의 보안 취약점을 분석한다. 또한 다양한 프로토콜 취약점들을 활용한 기존 서비스 거부 공격 사례를 분석함으로써 궁극적으로는 DoS 공격을 예측하고 공격 발생 시 신속한 대응책을 마련에 활용될 수 있는 정보를 제공하고자 한다.

Ⅰ. 서 론

최근 사이버 공격은 단순한 개인적 이득을 목적으로 이루어지는 범위를 넘어서서 국가 기간망 파괴 혹은 국가 정보 시스템 마비를 목적으로 한 대규모 테러 형태의 공격까지 범위가 확대되고 있다. 이러한 대규모 테러 형태의 사이버 공격에 가장 많이 활용되는 공격 방법이 서비스 거부 (Denial of Service: DoS) 공격이다.

DoS 공격은 특정 시스템의 리소스를 고갈시키거나 대역폭을 고갈시키는 방법을 통해 공격 대상 네트워크를 마비시키는 공격 방법이다[1]. DoS 공격은 MTU (Maximum transmission unit)를 이용하여 큰 사이즈의 Ping 패킷을 서버로 전송하여 재조합하게 만들어 리소스를 많이 소비하도록 만드는 Ping of Death 사례와 같이 특정 서버를 공격하는 형태에서부터 분산 서비스 거부 공격과 홈페이지 변조 및 개인정보를 유출한 6.25 사이버 테러 사례와 같이 조직적인 테러 형태의 공격까지 다양한 형태를 보인다. DoS 공격은 공격자의 선택 및 공격 방법에 따라 분산 서비스 거부 (Distributed DoS: DDoS) 공격[2] 및 분산 반사 서비스 거부 (Distributed Reflection DoS: DRDoS) 공격[3] 등으로 발전하게 된다. 그러나 DoS, DDoS, 및 DRDoS 공격 방법 모두 다양한 프로토콜들의 보안 취약점을 이용하여 공격을 시도하는 공통점을 가진다 [4]-[5]. 가장 대표적인 예가 TCP (Transmission Control Protocol)의 3-way handshaking 절차의 취약점을 이용한 TCP SYN 플러딩 DoS 공격이다. TCP SYN 플러딩은 TCP 3-way handshaking 도중 마지막 ACK를 수행하지 않음으로써 연결된 상태의 접속정보가 쌓여 서버의 리소스를 고갈시키는 공격이다. 그 외에도 응용계층에서의 HTTP (Hyper-Text Transfer Protocol), DNS (Domain Name System), SMTP (Simple Mail Transfer Protocol), SIP (Session Initiation Protocol), SNMP (Simple Network Management Protocol) 등의 프로토콜을 이용한 DoS 공격들이 보고되고 있으며 전송계층의 TCP 및 UDP (User Datagram Protocol), 네트워크

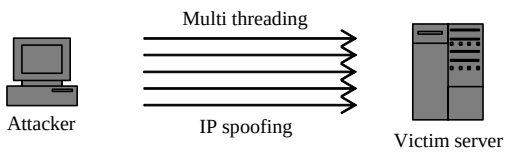
이 논문은 ETRI부설 연구소의 지원을 받아 수행된 것임
이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2010-0023326)
* 한양대학교 공학대학 컴퓨터공학과(chopro@hanyang.ac.kr)
** ETRI부설 연구소(saxophone95@hanmail.net)
*** 한양대학교 공학대학 컴퓨터공학과(yswqq@naver.com)

계층의 ICMP (Internet Control Message Protocol) 등이 DoS 공격에 활용되는 대표적인 프로토콜들이다. 따라서 본 논문에서는 TCP/IP 기반 네트워크에서 응용계층, 전송계층, 및 네트워크 계층의 다양한 프로토콜들에 대한 DoS 공격 취약점을 분석하고자 한다. 또한 각 프로토콜들의 다양한 취약점을 활용한 기존 DoS 공격 사례들을 분석함으로써 향후 예상되는 DoS 공격 형태 및 적절한 대응 방법 등에 대한 기준을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 다양한 DoS 공격 유형을 분석한다. 3장에서는 각 계층별 프로토콜의 DoS 공격 취약점에 대해 상세히 분석한다. 4장에서는 대표적인 국내 DoS 공격 사례를 3장의 분석 내용과 연계하여 소개하고 5장에서는 향후 연구방향 소개 및 결론을 맺는다.

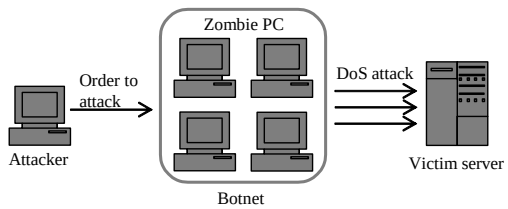
Ⅱ. DoS 공격 유형 분석

DoS 공격은 서버측 리소스를 고갈시키는 플러딩 방식의 DoS 공격이 주를 이뤘으며 네트워크 대역폭을 고갈시키는 DoS 공격사례도 발생되어 왔다. 하지만 현재는 각종 프로토콜들의 보안 취약점을 통해 공격하는 사례가 증가하고 있으며 특히 TCP 세션을 열기 위한 3-way handshaking시 리소스 사용을 이용한 공격이 전형적으로 사용되고 있다. DoS 공격은 [그림 1]과 같이 주로 공격자가 직접 공격 트래픽을 생성하여 대상 시스템을 목표로 하기 때문에 많은 프로세스를 생성하여 트래픽을 생성하여도 현재 발전된 네트워크의 용량과 기본적인 필터링이 수행되고 있는 방화벽을 무력화시키고 대상 시스템에 도달하기에는 무리가 있다.



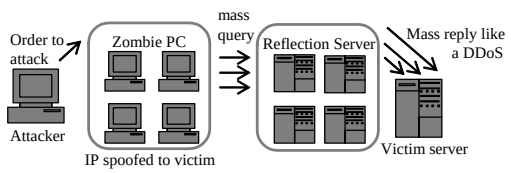
〔그림 1〕 DoS Attack Flow

DDoS 공격과 DRDoS 공격은 DoS 공격의 단점을 보완하여 등장한 새로운 방식의 DoS 공격이다. 공격자가 내린 명령에 따라 DoS공격이 가능한 악성코드를 미리 감염시킨 개인용 컴퓨터 (Personal Computer: PC)를 좀비 PC라 일컫는데, DDoS는 공격자가 수많은 좀비 PC를 통해서 대상 시스템으로 DoS공격을 동시에 일어나게 하는 것이다. DoS 공격처럼 단일 PC에서 다중 쓰레딩 (Threading)을 통한 패킷 생성은 시스템 리소스를 고갈시킬 순 있겠지만 네트워크 대역폭을 고갈시키기는 어려우며 무엇보다 차단이 용이하다. 하지만 [그림 2]에서처럼 DDoS공격은 분산된 수천 혹은 수만 개의 PC에서 DoS공격이 일제히 일어나는 것이기 때문에 통상적으로 한 좀비 PC가 30Mbps 정도의 플러딩 트래픽을 유발할 수 있다고 본다면 약 1000개의 좀비 PC는 30Gbps에 달하는 트래픽을 유발할 수 있다. 또한 DDoS는 공격 유형을 알 수 없고 추적이 불가능하도록 공격 시 사용하게 될 명령들을 암호화하는 방법 등을 동원해 그 근원지를 찾지 못하도록 위장하고 있다.



〔그림 2〕 DDoS Attack Flow

DRDoS는 DDoS 보다 약간 더 발전한 형태의 공격이다. DDoS 공격이 공격자가 좀비 PC를 이용하여 대상 시스템을 공격하는 흐름이라면 [그림 3]과 같이 DRDoS는 공격자가 수많은 좀비 PC를 이용하여 정상 서비스를 제공하는 서버들에게 공격 대상 시스템으로 위장하여 서비스를 요청하는 흐름이다. DDoS와 유사하지만 공격자를 찾는 것은 거의 불가능한 특징을 보인다.



〔그림 3〕 DRDoS Attack Flow

Ⅲ. 프로토콜 보안 취약점 분석

본 장에서는 DoS 공격의 문제점들을 분석하고 방어 및 예방하기 위해 TCP/IP 기반 네트워크 프로토콜들을 계층별로 나누어서 분석한다. 각 프로토콜들이 어떠한

취약점을 가지며 해당 취약점들이 DoS공격에 어떻게 응용되는지 분석하고 해당 공격에 대한 대응법을 개괄적으로 기술한다.

3.1. 응용계층 프로토콜 보안 취약점 분석

응용계층에서 DoS공격에 이용되는 대표적인 프로토콜들은 HTTP, DNS, SMTP, SIP, SNMP 등이 있다. HTTP를 이용하는 DoS공격에는 HTTP GET 플러딩 (HTTP Get Flooding)[5], HTTP CC 공격 (HTTP Cache-Control Attack) 등이 있다. DNS를 이용한 DoS 공격에는 DNS 증폭 DDoS 공격[6]이 있고, SMTP를 이용한 DoS 공격에는 메일 폭탄 (Mail Bomb)공격[7] 등이 있다. SIP를 이용하는 DoS 공격에는 SIP 플러딩 (SIP Flooding)[8]이 있으며 SNMP를 이용하는 공격에는 SNMP DDoS 공격[9]이 있다.

3.1.1. HTTP 보안 취약점

HTTP GET 플러딩은 TCP 3-way hand shaking 과정 이후 HTTP GET 요청을 주기적으로 수행하여 서버가 TCP 세션처리 뿐만 아니라 HTTP 요청작업까지 수행하도록 유도함으로써 서버의 리소스를 고갈시키는 공격의 한 종류이다. 다른 공격들과는 다르게 변조되지 않은 IP로 정상적인 TCP 세션을 유지하고 HTTP GET 요청을 하기 때문에 특징을 찾아 필터링 하기가 어렵다. 그렇기에 해당 공격은 공격 트래픽과 요청 주기 등을 분석해 IP를 차단하는 방법이 효과적이다. 그러나 필터링 정책보다도 낮은 트래픽과 주기를 갖고 수많은 좀비 PC로 공격을 하게 된다면 방어는 쉽지 않을 것이다. 이러한 공격은 주기적으로 프로그래밍 된 동일한 GET 메시지가 생성되기 때문에 HTTP GET 요청에 포함된 URL이 응답한 뒤에도 중복된 파일을 언급하고 있다면 필터링이 가능하다.

HTTP GET 플러딩과 더불어 행해질 수 있는 HTTP CC 공격은 HTTP GET 플러딩의 위력을 증폭시킬 수 있는 부가적인 공격방법이다. 웹서버는 클라이언트에게 웹페이지를 보여줄 때 이미 보여준 페이지에 대해서는 캐시에 저장된 페이지를 보여주도록 하고 있다. 그러나 HTTP의 헤더 값인 Cache-Control 을 No-Cache로 설정하게 되면 동일한 웹 페이지라도 매번 새로운 페이지를 로드하게 된다. HTTP CC 공격은 이러한 취약점을 이용하여 HTTP GET 플러딩 공격 시 헤더의 Cache-Control 값을 No-Cache로 설정함으로써 공격을 증폭시키는 역할을 한다. 이러한 공격은 동적인 페이지에 대하여 콘텐츠를 변경할 때마다 매번 새로운 요청이 일어나므로 더 큰 효과를 가져 오게 된다. HTTP CC 공격 역시 헤더의 Cache-Control 옵션 값을 체크하고 요청횟수에 대한 필터링을 적용한다면 방어가 가능하다.

3.1.2. DNS Query 취약점

DNS 서버는 사용자 PC의 요청에 따라 해당 도메인을 갖고 있는 IP를 반환해 줌으로써 손쉽게 기억할 수 있는 도메인으로 서버에 접속할 수 있도록 도와준다. IP를 얻기 위하여 DNS Query를 만들어 보내게 되면 먼저 로컬 DNS의 Cache를 검사한 다. 테이블에서 해당 내용이 발견되지 않을 시 해당 Query는 Root DNS 서버로 포워딩 되고 순차적으로 차 상위 계층의 DNS 서버로의 Query가 이어진다. 공격자는 이런 Query 순서를 이용하여 공격하고자 하는 서버의 IP로 출발지를 변조한 뒤 DNS 서버에 다량의 좀비 PC 집단 (Zombie PC Network:Bot-Net)[10]을 가지고 Query를 전송하여 그 응답이 모두 대상 서버에 집중되도록 한다. 더불어 공격자는 더 효율적으로 공격하기 위해 RR (Resource Records)를 비정상적으로 큰 값으로 설정하여 기본 Query에 대한 응답 값이 훨씬 더 커지도록 유도한다. 이러한 종류의 공격을 DRDoS라고 부른다. 중간에서 재귀적으로 Query를 전송하는 DNS 서버들이 리플렉터 역할을 해주게 된다. 해당 공격이 성립되는 이유는 로컬이나 인증된 클라이언트로부터의 Query만을 받아야 하지만 공격자의 Bot-Net이 위조한 IP로부터도 정상적으로 Query를 받아들이고 응답하기 때문이다. DNS에서도 마찬가지지만 모든 프로토콜기반 서비스에서 IP Spoofing[11]은 금지되어야 할 사항이다. 하지만 아직도 서비스 팩이 적용되지 않은 windows XP를 사용하는 사용자들이 많이 있고 해당 운영체제를 포함한 다수의 이전 버전 운영체제들은 Row Socket을 사용하기 때문에 IP Spoofing에 사용된다는 것이 보안상 큰 문제점이다.

3.1.3. SMTP 자원 고갈 취약점

SMTP Mail Bomb 공격은 메일서버에 동일하거나 유사한 메일을 자동적으로 생성하여 동시에 수백만 통을 보내 서버의 용량을 초과하게 만드는 공격이다. 이러한 DoS 공격을 통해 메일 서버가 서비스가 불가능한 상태에 빠지게 해 정상적인 메일 송·수신을 방해하게 된다. Mail Bomb 공격은 공격자가 프로그램을 통하여 다량의 메일을 일정한 패턴을 통해 생성하여 발송하게 된다. 그러므로 공격자가 보낸 TCP 패킷을 분석하여 SMTP (25Port)를 확인한 후 데이터가 571 (Unsolicited email refused), 550 (Requested action not taken: mailbox unavailable), 501 (Syntax error in parameters or argument), 554 (Transaction failed)인지 확인하여 동일한 데이터를 보내는 메일의 횟수를 카운트해 필터링 하는 방법이 있다. 탐지된 내용을 토대로 방화벽에서 발송자의 IP 주소를 차단하고 공격자에게 Reset 패킷을 보내어 더 이상 메일이 송수신되지 않도록 해 공격을 방어할 수 있다.

3.1.4. SIP 자원 고갈 취약점

SIP 플러딩 공격은 공격자가 SIP 서버 및 사용자 에이전트에 SIP메시지를 대량으로 생성하여 전송하는 것으로 DoS 공격에 가깝다고 볼 수 있다. 해당 공격을 받은 SIP 구성요소는 SIP 요청에 대한 응답이 불가능 하게 되어 서비스 거부 상태에 빠지게 된다. SIP 프로토콜은 TCP와 UDP 모두에 사용 될 수 있기 때문에 공격 대상에게 리소스 고갈이나 대역폭 고갈을 모두 야기 시킬 수 있다. 해당 공격은 메시지 분석을 통해 중복되는 요청을 필터링 하고 해당 IP 주소를 차단하는 방법으로 방어가 가능하다.

3.1.5. SNMP 인증 (certification) 취약점

NMP DDoS 공격은 SNMP의 인증 취약점을 이용해 IP Spoofing 및 데이터 수정을 통해 DDoS 공격을 대상 시스템에 시도한다. 프로토콜은 UDP상에 정의된 프로토콜로 네트워크 관리자가 성능을 관리하고 네트워크 문제점을 찾기 위해 활용된다. 하지만 일부 버전은 데이터가 텍스트 형태로 전송되며 소스 IP에 대한 검증이 이루어지지 않아 위험에 노출되어 있다. 또한 SNMP 프로토콜은 프린터, 라우터, IP 카메라, 센서 및 기타 인터넷을 이용하는 기기들이라면 거의 다 지원하고 있어 더욱 더 거대한 Bot-Net을 구성해 공격할 수 있는 가능성을 내포하고 있다. SNMP DDoS 공격은 SNMP 서비스를 사용하지 않는다면 해당 프로토콜을 차단함으로써 예방이 가능하다.

3.2. 전송계층 프로토콜 보안 취약점 분석

전송계층에서 DoS공격에 이용되는 대표적인 프로토콜에는 TCP, UDP 등이 있다. TCP를 이용한 DoS 공격에는 TCP SYN, NULL, FIN, ACK, PUSH, RESET, URG 플러딩과 각종 플래그를 통합시킨 XMAS 플러딩이 있고 TCP DRDoS 공격이 있다. UDP 공격으로는 UDP 플러딩, UDP Checksum 에러, Snork 공격, UDP Loop-back 등이 있다.

3.2.1. TCP 3-way handshaking 취약점

TCP 플래그 플러딩 공격은 클라이언트가 서버에 TCP 헤더 속 플래그를 각 SYN, NULL, FIN, ACK, PUSH, RESET, URG 중 하나로 설정하여 대량의 패킷을 보내면 서버는 이를 처리하기 위해 대부분의 자원을 소모하게 되고 정상적인 서비스를 하지 못하게 된다. 이러한 공격은 잘 알려져 있기 때문에 기본적으로 방화벽에서 필터링이 가능하다. 때문에 공격자는 여러 가지 조합으로 공격을 시도하며 XMAS 플러딩은 FIN, URG, PUSH, RST 등의 조합을 갖고 있는 플러딩 공격 중 하나라고 볼 수 있다. 탐지는 서버에서 대상 플러그들에 대한 다양한 조합으로 만든 필터링 테이블을 토대로 일정량의 공격 인정 횟수 이상의 공격이 단위시간당 들어오게 되면 탐지한다. 그 후 해당 연결을 RESET으로 끊고 IP 주소를 차단하는 방법으로 방어 및 대비가 가능하다.

3.2.2. TCP Reflection 취약점

TCP DRDoS 공격은 IP Spoofing을 통해 좀비 PC의 IP를 공격대상 IP로 위조하여 TCP 연결을 임의의 서버로 시도함으로써 해당 TCP 연결에 대한 응답이 모두

공격대상으로 집중되는 공격이다. 공격대상은 위조된 연결을 끊기 위해 RST 메시지를 보내지만 시스템이 느려져 모두 응답할 수 없는 상태에 빠진다. 임의의 서버는 공격대상으로부터 응답이 없는 것을 패킷이 유실되었다고 생각해 3회 정도 재전송 하게 되어 공격이 더욱 증폭되게 된다. 이러한 공격은 경유지 서버에서 완료되지 않은 TCP 연결을 찾아 해당 IP를 차단하는 방법이 있고, 좀 더 근본적인 해결방안은 IP Spoofing을 ISP (Internet Service Provider) 자체에서 출입이 불가능 하도록 필터링 하는 것이다.

3.2.3. UDP 트래픽 고갈 취약점

UDP 플러딩은 좀비 PC가 UDP 프로토콜을 이용하여 서버에 더미 데이터를 주기적으로 전송하여 서버의 대역폭을 고갈시키는 DoS 공격이다. 이러한 플러딩 공격은 특정 포트로 패킷이 주기적으로 날아오게 되면 패킷의 수를 카운트하여 필터링이 가능하다. 더불어 불필요한 UDP 서비스를 중지하고 라우터 등에서도 필터링 정책을 세워둔다면 효과적으로 차단이 가능하다. 동일한 방법으로 임의의 비정상적인 UDP 패킷을 보내어 공격 대상 시스템의 서비스를 방해하는 UDP Checksum 에러 공격에도 대응이 가능하다.

UDP Snork 공격과 UDP Loop-back 공격은 UDP의 보안상 취약점을 이용하여 공격자가 목적지를 135 포트로 정하고 소스를 7 (Echo), 19 (Chargen), 135 로 정해서 패킷을 보내 서로가 끊임없이 통신을 하도록 유도하는 공격이다. UDP Loop-back 역시 비슷한 유형으로 포트를 조작하여 전송하게 되면 서로 끊임없는 통신을 하게 되어 리소스 및 네트워크 대역폭을 고갈시킨다. 해당 공격들은 불필요한 UDP 서비스를 차단하고 공격자의 IP주소를 차단하여 방어가 가능하다.

3.3. 네트워크계층 프로토콜 보안 취약점 분석

네트워크계층에서 DoS공격에 이용되는 대표적인 프로토콜은 ICMP가 있다. 세부적인 공격 방법으로는 ICMP Unreachable Storm, ICMP Ping of Death, ICMP Checksum error, ICMP Smurf, Ping Sweep 등이 있다[12].

3.3.1. ICMP 자원 고갈 취약점

ICMP Unreachable Storm 공격은 공격자가 연속적으로 ICMP의 Port Unreachable 프레임을 보내서 시스템의 성능을 저하시키거나 마비시키는 공격을 말한다. 해당공격은 패킷에서 ICMP를 분석한 뒤 소스 및 목적지 IP 주소가 도달할 수 없는 IP 주소이면 공격으로 간주할 수 있다. 이 또한 패킷 횟수를 카운트하여 공격인정 시간 내에 임계값 이상의 공격이 이뤄지면 필터링을 통하여 감지가 가능하고 ICMP (ECHO) 서비스를 Close함으로써 해결이 가능하다.

비슷한 유형의 공격으로 ICMP Ping of Death 공격이 있다. Ping 패킷은 일반적으로 56 bytes 크기이며 이 크기를 의도적으로 크게 하여 전송하는 것은 RFC 791 규정을 위반하는 것이다. 그러나 Ping 패킷을 IPv4에서 허용하는 65,535 bytes 크기로 만든 후 이를 56 bytes 크기로 fragmentation 하여 전송하는 것은 가능하다. 이렇게 Ping 패킷을 전송하는 경우 공격 대상 시스템은 해당 패킷을 reassemble하는데 자원을 소모하여 버퍼 오버플로 등으로 인해 시스템의 정상작동이 불가능해진다. 이 공격은 공격자로부터 보내진 패킷을 분석하여 ICMP 타입이 ECHO이고 ECMP (Equal Cost Multi-Path routing) 메시지 데이터의 크기가 1024 byte 이상인지 확인한 후 필터링 한 뒤 ICMP 서비스를 Close함으로써 해결이 가능하다. 이와 비슷하게 ICMP Checksum Error공격 또한 비정상적인 패킷을 대상서버에 보냄으로써 과부하를 일으키는 공격이지만 동일한 방법으로 필터링이 가능하다.

3.3.2. ICMP 트래픽 고갈 취약점

ICMP 스머프 공격은 공격자가 대상 서버 및 네트워크에 오버로드를 발생시켜 정상적인 서비스를 하지 못하게 하는 공격이다. 공격자가 ICMP 패킷의 소스 IP 주소에 공격대상 서버의 IP 주소를 설정하고 임의의 Broadcast 주소로 ICMP ECHO 패킷을 발송하면 이를 수신한 경유지 서버는 동시에 대상서버에 응답을 하게 한다. 대상 네트워크 트래픽은 기하급수적으로 증가 되고 서버에 과부하가 발생하게 된다. 탐지방법은 공격자가 보낸 패킷에서 ICMP를 분석하여 ICMP 타입이 REPLY인지 확인한 뒤 소스 IP의 변조여부를 확인해

공격자가 보내는 패킷의 횟수를 카운트하여 공격인정 시간 내에 공격인정 회수이면 ICMP 스머프 공격으로 탐지할 수 있다. 해당 공격은 ICMP (ECHO) 서비스를 Close 함으로써 방어가 가능하다.

위와 비슷한 방법으로 Ping 스윕 공격은 ICMP 프로토콜을 이용하여 해당 네트워크가 정상적으로 작동하는지 여부를 확인하는 Ping 테스트와 ICMP 브로드 캐스팅을 통한 네트워크 오버로드 발생이 주목적인 공격이다. 해당 공격들은 패킷 분석 시 ICMP의 타입이 ECHO일 경우 필터링을 통하여 차단이 가능하며, ICMP (ECHO) 서비스를 Close 함으로써 방어가 가능하다.

Ⅳ. 대표적인 DoS 공격 사례

최근 국내 DoS 공격 사례들을 살펴보면 DoS 공격의 한 트렌드인 APT (Advanced Persistent Threat) 공격과 맞물려 시도된 것들이 많이 발견되었다. 최근 대표적인 DoS 공격 사례로는 2003년도 1월 25일에 발생한 인터넷 대란, 2009년도 7월 7일과 2011년 3월3일에 발생한 DDoS 공격, 2013년 3월 20일과 6월 25일에 발생한 복합적인 사이버테러를 들 수 있다. 초기에 발생한 DDoS 공격은 그 목적과 수단의 강도가 깊지 않았지만 2009년부터 이뤄지는 DDoS 및 DRDoS는 그 목적이 뚜렷하고 DDoS만이 아닌 다른 루트로의 공격이 더해진 복합적인 공격양상을 띄고 있다는 것이 특징이다. 본 장에서는 최근 발생한 주요 DoS 공격들에 대해 개괄적으로 분석한다.

4.1. 2009년 7월 7일 DDoS 공격

해당 공격은 HTTP GET 플러딩 공격을 이용하여 대한민국의 상당수가 이용하고 있는 포털 사이트의 이메일 서버와 인터넷 뱅킹 서비스를 제공하는 은행 사이트들을 공격한 사례이다[13]. 7.7 DDoS의 Zombie PC 수량은 대략 20만대 내외로 추정되었으며 해당 악성코드를 감염시킨 경로는 피어-투-피어 파일 공유 사이트에 업-로드된 파일 일부에 삽입되어 유포된 것으로 알려졌다. 공격에 활용된 PC의 주소는 대부분 국내 IP로 3만대의 IP는 지속적인 HTTP GET 플러딩을 매우 높은 횟수로 시도하였다. 공격 절차는 악성코드가 심어져 있는 파일인 perfvwr.dll이 서비스로 등록되어 uregvs.nls에 하드 코딩 된 웹사이트로 GET 플러딩 공격을 수행하였고 파일을 읽어 들이면서 버퍼에 저장하는 순서를 보였다. 1차 공격이 이뤄진 뒤 전용 백신 등이 공급되어서 안정화가 빠르게 진행되었다.

4.2. 2011년 3월 3일 DDoS 공격

해당 공격은 UDP 플러딩, ICMP Ping of Death, HTTP CC 공격을 통해 국내 공공기관과 포털, 금융 기관을 공격한 사례이다[14]. 3.3 DDoS 공격은 7.7 DDoS처럼 국내 웹-하드를 이용한 점과 DDoS 대상 리스트 및 공격 시나리오들이 매우 유사하며, 하드디스크 파괴 기능(msvcr90.dll 불필요 등) 강화 등 여러 문제점을 보완한 면을 보이고 있다. 이전 공격과 다른 특징은 공격 계획들이 이미 악성코드에 포함되어 유포되었다는 점이다. 7.7 DDoS의 분석을 토대로 빠르게 대응이 이루어진 3.3공격은 악성코드에 계획된 공격일정과는 다르게 도중에 하드디스크를 파괴하는 명령과 백신다운로드 사이트 접속을 막는 명령을 실행하였다. 하드디스크를 파괴하는 공격이 동반되어 전체적으로 시스템을 복구하는 데는 오랜 시간이 소요되었다.

4.3. 2013년 6월 25일 사이버 테러

해당 공격은 DNS 증폭 DDoS 공격을 이용하여 청와대 홈페이지 및 정부 기관의 홈페이지를 공격한 사례이다[15]. 해당공격은 국내 특정 파일공유 (웹-하드) 사이트의 설치프로그램 변조를 통해서 유포되었다. 악성파일은 정상적인 웹-하드 셋업 파일을 변조하여 설치 시 악성파일이 함께 설치하도록 압축되어 있었다. 공격당한 홈페이지에 업로드 된 공격 과정의 패킷을 추적하여 확인한 결과 “정부 통합 전산 센터”의 DNS (gcc.go.kr)에 무작위로 생성한 도메인 질의를 통해 DoS 공격을 수행한 것이 확인되었고 동시에 공격자는 웹 사이트 변조를 통해 유출한 신상정보를 업로드 해 놓았다. 해당공격은 웹사이트의 악성코드 감염루트를 차단하고 DNS 서버를 복구하는 것으로 일차적인 대응책이 세워졌다.

Ⅴ. 결론

DoS공격은 대부분 그 목적이 분명하고 공격 대상 시스템이 존재하기 때문에 대부분 수주 혹은 수개월 동안 준비하여 공격하는 것이 일반적이다. DoS 공격 준비 기간 동안에는 악성코드를 배포하여 공격에 활용될 좀비 PC를 확보한 후 준비 과정이 끝나면 대상 시스템으로 사이버 공격을 가하게 된다. 이러한 일련의 과정에서 다양한 프로토콜의 보안 취약점들이 사이버 공격 수단으로 사용되어 지고 있다. 이에 본 논문에서는 기존 DoS 공격에 사용 되어진 각 프로토콜별 보안 취약점에 대해 분석하였다. 또한 최근 국내에서 있었던 대표적 DoS 공격을 각 프로토콜별 보안 취약점과 연계하여 분석하였다.

본 논문에서 기술한 TCP/IP 기반 네트워크 프로토콜 보안 취약점 및 각 취약점 별 기본적인 대응방법은 DoS 공격을 일정부분 예방하거나 DoS 공격 발생 후 신속한 대응책 수립에 활용될 수 있을 것으로 기대된다. 그러나 본 논문에서 분석한 취약점 및 대응법들은 기존 발생되었던 DoS 공격에서 알려진 내용이라는 한계점을 가진다. TCP/IP 기반 네트워크상의 프로토콜들은 현재까지 DoS 공격에 활용된 보안 취약점 외에도 무수히 많은 취약점을 내포하고 있다. 따라서 이미 알려진 취약점들에 대한 대응만으로는 미래의 DoS 공격을 효과적으로 예방하기는 어려운 것이 현실이다. 향후 각 프로토콜들의 보안 취약점에 대한 분석 연구가 보다 적극적이고 심도 있게 수행 되어야 한다. 또한 이러한 연구 내용을 기반으로 DoS 공격을 비롯한 사이버 공격을 사전에 예방하거나 공격 발생 시 신속한 대응이 이루어질 수 있는 국가적 매뉴얼 작성 등의 후속 작업 등이 향후 연구 과제로 시급히 수행 되어야 할 것으로 사료된다.

참고문헌

[1] G. Loukas and G. Öke, "Protection against denial of service attacks: a survey," The Computer Journal, vol. 53, pp. 1020-1037, 2010.

[2] M. Li, J. Li, and W. Zhao, "Simulation study of flood attacking of DDOS," in Proc of International Conference on Internet Computing in Science and Engineering 2008, pp. 286-293.

[3] H. Tsunoda, K. Ohta, A. Yamamoto, N. Ansari, Y. Waizumi, and Y. Nemoto, "Detecting DRDoS attacks by a simple response packet confirmation mechanism," Computer Communications, vol. 31, pp. 3299-3306, 2008.

[4] W. Liu, "Research on DoS attack and detection programming," in Proc. of Third International Symposium on Intelligent Information Technology Application 2009, pp. 207-210.

[5] J. Nazario, "DDoS attack evolution," Network Security, vol. 2008, pp. 7-10, 2008.

[6] G. Kambourakis, T. Moschos, D. Geneiatakis, and S. Gritzalis, "Detecting DNS amplification attacks," in Critical Information Infrastructures Security, ed: Springer, 2008, pp. 185-196.

[7] M.-J. Chen, K.-P. Chien, C.-Y. Huang, B.-C. Cheng, and Y.-S. Chu, "An ASIC for SMTP Intrusion Prevention System," in Proc. of IEEE International Symposium on Circuits and Systems 2009, pp. 1847-1850.

[8] F. Huici, S. Niccolini, and N. d'Heureuse, "Protecting SIP against very large flooding DoS attacks," in Proc. of Global Telecommunications Conference 2009, pp. 1-6.

[9] J. Yu, H. Lee, M.-S. Kim, and D. Park, "Traffic flooding attack detection with SNMP MIB using SVM," Computer Communications, vol. 31, pp. 4212-4219, 2008.

[10] Z. Zhu, G. Lu, Y. Chen, Z. J. Fu, P. Roberts, and K. Han, "Botnet research survey," in Proc. of 32nd Annual IEEE International Computer Software and Applications 2008, pp. 967-972.

[11] I. Mopari, S. Pukale, and M. Dhore, "Detection and defense against DDoS attack with IP spoofing," in Proc. of International Conference on Computing, Communication and Networking 2008, pp. 1-5.

[12] J. Udhayan and R. Anitha, "Demystifying and rate limiting ICMP hosted DoS/DDoS flooding attacks with attack productivity analysis," in Proc. of IEEE International Conference on Advance Computing Conference 2009, pp.

558-564.

[13] H. Y. Youm, "Korea's experience of massive DDoS attacks from Botnet," ITU-T SG, vol. 17, 2011.

[14] S.-H. Kang, K.-Y. Park, S.-G. Yoo, and J. Kim, "DDoS avoidance strategy for service availability," Cluster Computing, pp. 1-8, 2013.

[15] J. Eom, " The Active Deterrence Strategy of Cyberwarfare for Cyber Security," Journal of Security Engineering, vol. 10, 2013.

〈저자소개〉

조 성 현 (Sunghyun Cho)
정회원

1995년 2월 : 한양대학교 컴퓨터공학과 공학사
1997년 2월 : 한양대학교 컴퓨터공학과 공학석사
2001년 8월 : 한양대학교 컴퓨터학과 공학박사
2001년 9월~2006년 : 10월 삼성종합기술원 및 삼성전자정보통신연구소 전문연구원
2006년 10월~2008년 2월 : Stanford University,Postdoctoral Visiting Scholar
2009년 9월~2012년 8월 : 경상대학교 컴퓨터과학과 조교수
2012년 9월~현재 : 한양대학교 컴퓨터공학과 부교수
<관심분야> 차세대 이동통신 시스템, 차세대 무선랜 시스템, 자동차 통신, 무선네트워크 보안

이 택 규 (LEE TAEK KYU)
정회원

1999년 2월 : 아주대학교 전자공학과 공학사
2001년 2월 : 아주대학교 전자공학과 공학석사
2003년 2월 : 고려대학교 전파공학과 공학박사 수료
2013년 2월 : 충남대학교 컴퓨터공학과 공학박사 수료
2003년 3월 : ~현재 : ETRI 부설연구소 선임연구원
<관심분야> 사이버 보안관제, DDoS 공격 탐지 및 대응

이 선 우 (Seonwoo Yi)
학생회원

2013년 2월 : 한양대학교 컴퓨터공학과 공학사
2013년 3월~현재 : 한양대학교 컴퓨터공학과 공학석사 재학
<관심분야> 피어-투-피어 스트리밍 서비스, 프로토콜 보안