Sync Flooding IPS 구현 방안

한미란* · 김근희** · 강영모*** · 김효정**** · 김종배○

*,**,***,****,○숭실대학교

E-mail : kjb123@ssu.ac.kr

요 약

본 논문에서는 정보시스템을 공격하는 여러 공격 기법 중, 대표적인 서비스 거부 공격 기법인 Sync Flooding 공격 기법에 관해 연구하여, 시스템 성능 저하 및 마비의 근본원인을 탐지하고 이를 기반으로 최근 새롭게 등장하는 Sync Flooding 공격 방어를 위한 기법을 설계하려 한다. Sync Flooding 공격 기법은 DoS공격으로 서버의 자원(resources)를 고갈시키는 네트워크 트래픽 flooding 기법이 특징이다. 이러한 보안 취약점 해결하기 위한 방어 정책 수립과 공격 시나리오에 따른 방어 기법을 제안 한다.

키워드

DoS, DDoS, Sync Flooding, IPS

Ⅰ. 서 론

Sync Flooding 공격의 개념이 알려진 지는 오래 되었지만 간단하게 실행할 수 있는 공격 툴이나 소스가 배포되면서 공격이 빈번하게 발생되고 있다. 따라서 본 논문에서는 Sync Flooding의 원리에 대해 분석하고, 대처 방안을 도출하고, 공학적 원리를 기반으로 설계하여 서비스 거부 공격을 예방하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 기반으로 현행 Sync Flooding Attack 공격 구조에 대해 분석하고, 예방 방법에 대해 설계한다. 3장에서는 Sync Flooding 탐지 기법 과 IPS 시스템 아키텍처 분석에 대해 연구하고, 본 논문에서 제안하는 방어 기법을 설계하였다. 4장에서는 Sync Flooding 방어기법을 구현 및 실험을 통해 해결방안을 도출한다. 마지막으로 5장에서 결론 및 향후 연구 방향에 대해 기술하였다.

Ⅱ. 관련 연구

기본적인 Flooding은 Tcp/IP 네트워크 프로토콜의 설계를 이용하는 공격이다. TCP, UDP, ICMP같은 예상되는 프로토콜의 연결은 해커가 쉽게 공격할 수 있는 환경은 만들어 준다. 예를 들어 Sync Flooding 공격은 TCP/IP의 3-Way handshake 원리를 기법으로 한다. 기본 원리는 SYN 요청, SYN+ACK 응답, 응답에 대한 ACK로 작동한다. 이와 같은 원리는 SYN 요청에 대한 응답으로 ACK를 주는 방법을 악용하여, SYN요청을 unix 시스템의 자원(Limit)의 한계 값인 1024 이상에 SYN 요청을 하게 되면, 요청에 대한 응답으로 ACK가 1024가 발생하게 되어, 시스템의 한계 자원을 초과하여 더 이상 접속이 불가능 하게 된다. 이런 현상으로 인하여 시스템은 더 이상 서비스를 제공할 수 없게 된다. 이로 인해 시스템은 서비스 거부 공격에 대상이 된다. 서비스 거부 대상은 접속 자원 초과 및 접속 log Queue 임계치를 초과하게 되어 더 이상 새로운 접속을 받아 들 일 수 없게 된다.

이러한 Flood의 공격에 종류는 Smurf 공격, SYN 공격, UDP 공격, ICMP 공격, CGI request 공격, Authentication 서버 공격[1]등이 있으며 다음은 Sync Flooding Attack 공격에 대해 좀 더 자세한 원리를 알아보도록 한다.

2.1 Sync Flooding Attack의 원리

Sync Flooding는 DoS(denial-of-service)공격의 하나로 공격자가 타켓 시스템으로 SYN패킷을 보내서 큐용량을 넘치게 하는 네트워크 공격방법이다. 각각의 패킷이 타켓 시스템에 SYN-ACK응답을 발생시키는데, 시스템이 SYN-ACK에 따르는 ACK를 기다리는 동안, backlog 큐로 알려진 큐에 모든 SYN-ACK응답을 넣게 된다. 이것이 보통 TCP three-way handshake방식이다. 서버가 SYN에 응답하지 않는데도 무차별적으로 SYN패킷을 발생시켜서 LAN을 마비시킬 수도 있다.[2]

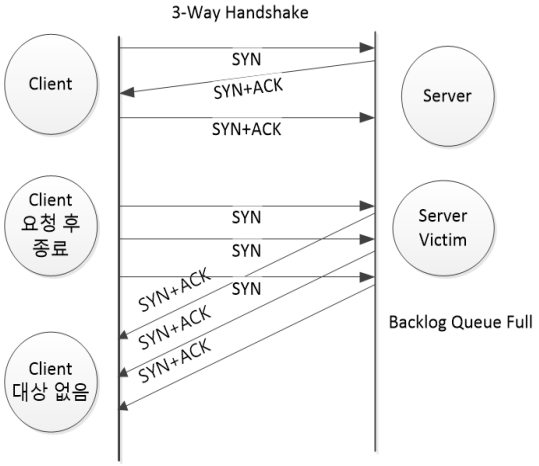

그림 1. 3-Way Handshake 원리와
Sync Flooding 개념도

위의 [그림 1]은 Client 와 Server 간에 3-Way Handshaking을 정상 처리하는 원리이다.

1단계는 클라이언트는 서버에게 접속을 요청하는 SYN 패킷을 보내고 2단계 서버는 요청을 받고 클라이언트에게 요청을 수락한다는 SYN+ACK 패킷을 발송한다. 마지막 3단계 클라이언트는 서버에게 ACK를 보내고 이후로 연결이 되면 본격적으로 데이터가 교환된다.

Sync Flooding 공격 방법은 위의 원리를 이용한 것으로 Client에서 다수의 연결 요청 후 종료를 통해 Server Victim 시스템에서 Client 에 SYN+ACK를 송신하지 못하여, Server Victim 시스템에 Backlog Queue Full 발생으로 시스템이 더 이상 새로운 요청을 처리하지 못하게 되는 원리이다.

2.2 TCP header 구조 분석

offsets	Octet	0				1				2	3
Octet	Bit	1 ... 7				8 ... 15				16 ...23	24 ... 31
0	0	Source port								Destination port	
4	32	Sequence number									
8	64	Acknowledgment number(if ACK set)									
12	96	Data offset	Reserved 0 0 0	N S	C W R	U R G	A C K	P S H	R S T	S Y N	F I N	Window Size
16	128	Checksum								Urgent pointer(if URG set)	
20	160	Options(if data offset>5. Padded at the end									

그림 2. TCP header 구조[3]

위의 [그림 2]에 TCP Header 구조를 분석한 결과 TCP Header에 구성은 송신 포트, 수신 포트, 시퀀스 번호, ACK 번호, Data offset, Control bit, Window size, Checksum, Urgent Pointer, Options로 구성되어있다. TCP Header Control-flag주요 정보로서 URG, ACK, PSH, RST, SYN, FIN으로 구분된다. 이중 Syn Flooding 의 중요 flag는 SYN과 ACK, FIN으로 SYN에 대한 응답 flag인 ACK 메시지가 Backlog Queue에 남게 되어 Queue 가 가득차게 된다.

2.3 Backlog Queue Full 해결 방안[5]

2.3.1 백 로그 큐 메모리 사이즈 증가

서비스 거부가 시작하게 되는 Backlog Queue가 가득차서 다른 접속요구를 받아들이지 못하기 때문에 Backlog Queue의 Size를 늘려주면 된다.

Backlog queue 증가를 위한 방법은 다음과 같다. 첫 번째, 커널 시스템 정보중에 tcp max syn backlog 사이즈를 확인하다. 두 번째, 확인 된 Backlog Queue 사이즈를 확인 후 ACK 1개에 대한 사이즈 X 최대 허용 세션수 만큼에 Backlog Queue 사이즈를 지정하게 되면 된다.

```
#cat /proc/sys/ipv4/tcp_max_syn_backlog
#sysctl -w net.ipv4.tcp_max_syn_backlog=[값]
```

그림 3. Backlog Queue의 Size 값 코드

하지만 backlog queue사이즈를 증가로 Sync flooding 공격을 예방하는 데는 한계가 있을 뿐만 아니라 임시적인 대책일 뿐 근본적인 해결방안이 아니다. DDos 와 같은 대량의 서비스 거부 공격으로 인한 Sync flooding 은 backlog Queue 메모리가 증가하여 시스템에 취약점이 노출되는 것은 시간 문제일 뿐이다.

2.3.2 Syscookies 기능 활성화 방안

Three-way handshake진행과정을 다소 변경하는 것으로 Alex Yuriev와 Avi Freedman에 의해 제안되었는데, TCP 헤더의 특정한 부분을 뽑아내어 암호화 알고리즘을 이용하는 방식으로 Three-way Handshake가 성공적으로 이루어지지 않으면 더 이상 소스 경로를 올라가지 않는다. 따라서 적절한 연결 요청에 대해서만 연결을 맺기 위해 리소스를 소비하게 된다.

```
#cat /proc/sys/net/ipv4/tcp_syscookies
-> 1(활성화), 0(비활성화)
#sysctl -w net.ipv4.tcp_syncookies=1
```

그림 4. syscookies 사용코드

Ⅲ. Sync Flooding 방어 기법 및 제안 아키텍처 구성

3.1. TCP Header 정보 분석

IPS(Intrusion Prevention System)은 네트워크상에서 발생하는 침입에 대해 탐지 보고 및 예방하는 보안 시스템이다. 따라서 외부의 악의적인 공

격에 대한 탐지 방법과 방어 기법이 중요한 기술 요소이다. 본 논문에서는 TCP Header에 Control-Flag 정보를 기반으로 Syn Flooding 공격을 탐지하고, 방어 기법은 Control-Flag 관리를 통해 방어 정책을 수립하여 방어하도록 제안 한다.

표 1. TCP Header Control-Flag 정보

Flag	설 명
URG	Urgent Pointer.
ACK	Acknowledgement.
PSH	This flag means Push function
RST	Reset the connection
SYN	This flag means synchronize sequence numbers
FIN	No more data from the sender

위의 [표 1]에 Control-Flag 는 2byte로 표현 되며 6가지 유형으로 분류된다. 첫 번째, URG는 Urgent data 전송에 경우 데이터에 마지막 offset Pointer 위치 값에 대한 Flag이다. 두 번째, ACK 는 SYN 요청에 대한 Acknowledgement 응답 구분 Flag 이다. 세 번째, PSH 는 PUSH 기능 플레그 값으로 데이터 전송 대기시간 없이 전송하는 구분 Flag 이다. 네 번째, RST 는 네트워크 연결에 대한 회복할 수 없는 에러인 경우 RESET 정보를 가진 Flag 값이다. 다섯 번째, SYN는 synchronize sequence 번호를 의미하는 Flag 이다. 마지막으로 FIN는 발신 정송자로부터 더 이상 데이터가 없다는 정보 Flag 이다. 위와 같은 TCP Header Control-Flag 정보기반으로 세션별 Flag 건수를 모니터링하게 되면, Sync Flooding 공격에 유무를 판단할 수 있게 된다. 비정상 세션에 대한 Flag인 FIN-WAIT, TIME-WAIT 발생 건수가 모니터링 대상이 된다.

3.2. Sync Flooding 방어 정책 및 IPS 아키텍처 구성

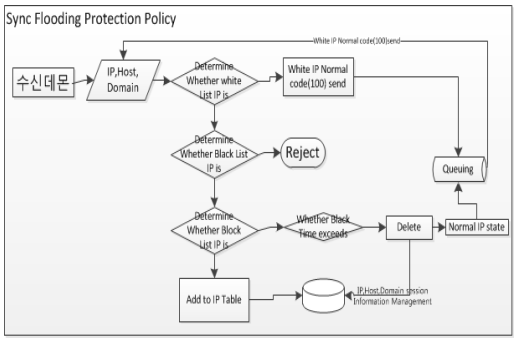

그림 5. Sync Flooding 방어 정책

위의 방어 정책은 외부로부터 들어오는 정보를 기반으로 크게 White List 와 Black List 로 구분한다. 접근 정보를 관리하기 위해 자료구조는 환형 링크 리스트를 이용하였다. 이를 통해 정보 탐색 속도 시간을 향상 시킬 수 있다.

White List는 접속 건수를 기록 후 즉시 통과 시키게 된다. 하지만 기준시간대비 최대처리기준건수를 초과할 경우 악의적인 공격으로 판단하여, Block List 대상으로 관리된다. Block List 관리 대상 정보는 사용자가 수립한 보안 정책을 기반으로 일시적인 차단 또는 영구적인 차단을 수행한다.

위의 보안 정책의 가장 특징은 발송지 공격에 대해 신속하게 탐지하는 것이 가능하다는 것이다. 이는 요청 발송정보를 기반으로 판단하며, 보안 정책 수립에 따라 유연하게 세션 제어하는 것이 가장 큰 특징이라 할 수 있다.

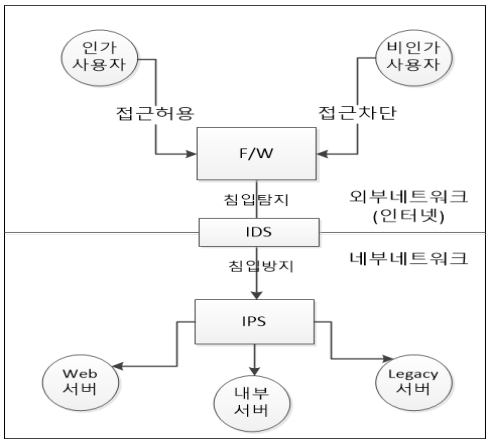

그림 6. IPS 제안 아키텍처

위 [그림 6] 는 IPS(Intrusion Prevention System) 아키텍처로서 외부 네트워크와 내부 네트워크를 기준으로 구분된다. 외부 네트워크를 통해 들어오는 패킷을 내부 네트워크에 존재하는 IPS 시스템이 이상접속 및 서비스 거부 공격들을 예방하는 역할을 하게 된다. 제안하는 [그림 3]에 Sync Flooding 방어 정책을 IPS시스템 내부 방어 정책에 적용하게 되면 외부의 악의 적인 공격에 대해 효과적으로 방어 할 수 있게 된다.

IV. 결론 및 향후 연구 과제

IPS 시스템에 적용 할수 있는 Sync Flooding 방어 정책 설계를 기반으로 IPS 아키텍처에 적용한 결과 외부의 악의적인 DDos 및 Sync Flooding 공격에 대해 효과적으로 방어가 가능하게 되었다. IPS 시스템의 가장 중요한 기술 요소는 외부의 침입 탐지에 대한 정확한 식별과 이를 기반으로 방어하는 기술이 가장 중요한 기술 요소 기술이다. 향후 연구에 과제는 외부의 악의적인 공격에 대해 다양한 실험을 통해 Sync Flooding 공격을 효과적으로 방어하는 기법에 대해 연구하려 한다.

참고문헌

[1] 이연호, 김범재, 이남용, 김종배 , “DDoS 대응 지표 프레임워크 개발”, 한국디지털콘텐츠학회논문지, ISSN 1598-2009, 03/2010, Volume 11, Issue 1, pp. 79 - 89
[2] D.DeepthiRani,T.V.SaiKrishna,G.Dayanandam, Dr.T.V.Rao,“TCP Syn Flood Attack detection Prevention“, IJCTT Vol.4 Issue 10 Oct. 2013
[3] Mitko Bogdanoski ,“Analysis of the SYN Flood Dos Attack“, I.J. Computer Network Information Security DOI: 10.5815/ijcnis. 2013.08.01.
[4] 김근희, ” 데이터 전송 방법 및 이를 적용한 주식 체결 시스템 “,대한민국 등록번호 제 10-1458436호 2014.10.30
[5] http://blog.naver.com/nobless_05/50082436157