행위기반 SIP DDoS 트래픽 탐지 기법*

이창용, 김환국, 고경희, 김정욱, 정현철
한국인터넷진흥원
e-mail:[chylee, rinyfeel, khko, kjw, hcjung]@kisa.or.kr

SIP DDoS Detection Scheme based-on Behavior

Changyong Lee, Hwankuk Kim, Kyunghee Ko, Jeongwook Kim,
Hyuncheol Jeong
Korea Internet & Security Agency

요 약

SIP 프로토콜은 멀티미디어 통신 세션을 생성, 삭제, 변경할 수 있는 프로토콜로 높은 간결성, 확장성 등 장점을 가지고 있다. 최근 인터넷전화의 대부분이 SIP 프로토콜을 사용하는 등 SIP 프로토콜의 사용이 많이 보편화 되었으나 그만큼 보안에 대한 위협 또한 중요한 문제가 되고있다. SIP는 응용계층 프로토콜로, 기존의 IP기반 보안 기술로는 공격 탐지/차단에 한계가 있을 수 있어 SIP 전용의 보안 기술 및 장비의 개발이 필요하다. 본 논문에서는 SIP 트래픽의 응용계층 정보 통계를 통하여 DDoS 공격 트래픽 행위 특성을 분석하고 이를 정상 트래픽과 구분, 탐지하는 탐지 기법을 제안한다. 제안된 기법은 자체 테스트 망 구축과 SIP DDoS 공격 에뮬레이션을 통해 검증한다.

1. 서론

현재 대부분이 SIP(Session Initiation Protocol)[1] 프로토콜을 기반으로 서비스되고 있는 인터넷전화 서비스는 그 가입자 수가 600만 명을 넘어서며 크게 활성화 되었으며, 최근 스마트폰, 모바일 인터넷전화 서비스의 등장과 함께 더욱 많은 가입자를 확보할 것으로 기대되고 있다. 이 외에도 SIP는 peer-to-peer 통신을 기반으로 하므로 확장성이 좋으며 각종 대화형 응용서비스에 쉽게 적용할 수 있어 향후 활용 가능성이 매우 높다.

반면 서비스 보편화와 함께 보안 위협과 대응방안 또한 크게 이슈가 되고 있는 실정이다. SIP 기반 인터넷전화의 경우 사용자 개인이 사적인 통화 내용을 전달하는 서비스의 특성을 가지므로 그 내용이 도청될 경우 큰 문제가 될 수 있으며, 물리적으로 외부인 접근이 어려운 PSTN과 달리 누구나 쉽게 접근이 가능한 인터넷 인프라를 기반으로 서비스 되므로 언제 어디서든 보안 위협에 노출되어 있다고 볼 수 있다. 인터넷전화는 실시간 음성통화이며 기존의 PSTN의 사용자를 자신의 사용자로 끌어들여야 하므로 PSTN에 비해 보안이 불안정하거나 품질이 떨어질 경우 사업 활성화에도 큰 타격을 입는다. 인터넷전화가 급속도록 확산되고 있는 현재 보안 취약성에 대한 실용적인 대책이 필요하다.

SIP 기반 응용서비스는 INVITE Flooding 등 DDoS 공격, Call-bombing 등 Scan 공격, SPAM, 도청 등 여러 가지 공격에 노출되어 있다. IP망을 기반으로 인터넷 응용서비스 형태로 제공되기 때문에 기본적으로 IP 계층에서 일어날 수 있는 모든 위협을 상속하며, SIP의 특성에 기인한 신규 보안 위협들이 있을 수 있다. 본 논문에서는 이 중 서비스 중단 및 품질 저하를 유발할 수 있는 SIP DDoS 공격 트래픽에 대한 탐지 기법을 제안한다.

본 논문은 다음과 같이 구성된다. 2장에서는 SIP기반 응용서비스의 DDoS 공격, 그리고 이들에 대한 기존 연구를 설명한다. 3장에서는 행위기반 SIP DDoS 공격 탐지 기법을 제시한다. 4장에서는 이에 대한 실험결과를 통해 제시한 기법을 평가하며, 5장에서는 결론을 맺는다.

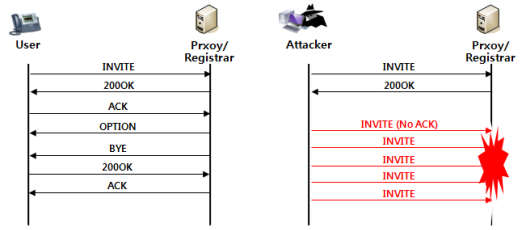
2. 관련연구

DDoS 공격의 경우 기존 IP 응용서비스에 공통적으로 존재하는 위협이다. 하지만 인터넷 전화는 SSW (Softswitch)를 사용하는 트래픽 라우팅 구조를 이용하며 각각의 메소드 별로 수행하는 기능이 달라 특정 메소드만을 SSW에 소량으로 전송하더라도 서비스에 방해를 줄 수 있다. 또한 이러한 공격은 기존의 IP 기반의 탐지 솔루션으로는 탐지가 어려운 문제점이 있다.

기존의 보안 기술들은 IP 트래픽의 5-tuple 정보(근원지 IP, 근원지 port, 목적지 IP, 목적지 port, 프로토콜(TCP, UDP, ICMP)) 를 이용하여 IP 트래픽의 특성을 분석하고 비정상 트래픽을 탐지한다. 하지만 SIP 응용서비스의 경우 IP/port 이외에 응용서비스 제공을 위한 식별자인 URI(Uniform Resource Identifier)를 추가로 사용하며 SIP 트래픽의 전송 패턴 또한 5-tuple 정보 이외에 URI 정보에

* 본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업 일환으로 수행하였음. [KI001850, SIP 기반 응용서비스 보호를 위한 침입대응기술 개발]

영향을 받는다. 하지만, 기존의 보안 기술들은 URI를 인식하지 못해 정확한 SIP 트래픽 패턴 분석 및 비정상 SIP 트래픽 탐지가 불가능하다.



(그림 1) INVITE Flooding

그림 1과 같이 어떠한 메소드를 전송하는지 여부에 따라 정상과 비정상 콜 패턴이 구분될 수 있다. SIP 콜의 경우 INVITE, 200OK, ACK 등 요청/응답 메시지 교환을 통해 콜을 성립하고 통화를 수행한다. 하지만 ACK 메시지 없이 다량의 INVITE 만을 전송하여 서버 자원을 고갈시키는 INVITE Flooding을 이용한 DDoS 공격의 경우 특정 메소드만 다량으로 전송되는 형태를 보인다. IP 헤더 정보만으로 트래픽 행위를 분석할 경우 이러한 공격에 대한 탐지가 어려울 수 있다.

이러한 SIP DDoS 공격에 대해 Liu 등은 시뮬레이션을 통해 SIP DDoS 공격의 패턴 분석을 시도하고 결과를 발표하였고[2], Seifert 등은 SIP DDoS 공격 피해를 완화하기 위한 방법 등을 발표하였다[3]. 하지만, 이들의 연구 결과는 트래픽 자체의 패턴 특성 보다는 DDoS 공격으로 인한 패킷손실 피해를 분석하거나, 피해 예방을 위해 방화벽 등 기존의 보안 기법을 적용하는 방법을 제안한 것으로 SIP 트래픽 특성을 고려한 트래픽 패턴 분석을 통한 SIP DDoS 탐지 기법을 제안한 연구결과는 아직 많이 발표되지 않은 것으로 보인다.

3. 제안하는 기법

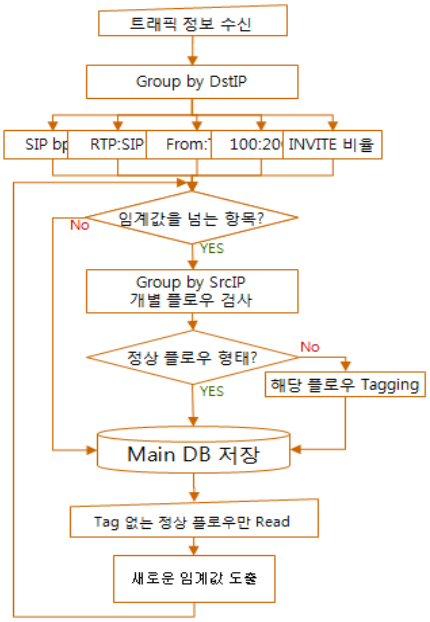
제안하는 기법은 누적된 데이터를 기반으로 정상 SIP 트래픽의 행위 패턴을 분석하고 현재 SIP트래픽의 행위 패턴 분석 결과와 비교하여 트래픽의 비정상 여부를 판단한다. SIP 트래픽은 분석을 위해 수신자 IP 기반으로 그룹핑 작업이 선행되며 각 수신자별로 분석항목을 계산하고 임계값을 초과하는 항목들을 찾아 탐지를 수행한다.

SIP 트래픽의 행위 패턴은 다양한 항목으로 정의 될 수 있으나, 제안하는 기법에서는 총 6가지의 항목을 정의하여 분석하며 이는 크게 3 분류로 구분될 수 있다.

- 사용자 행위 분석
  - 사용자의 분표 형태를 분석한다. 일반적으로 SIP 응용서비스는 1:1 통신을 사용하므로 송신자와 수신자의 분표 비율이 거의 1:1로 일정하다. DDoS형태의 Flooding 공격 발생시 다수의 송신자가 단일 수신자에 트래픽을 집중시키므로 송신자의 비율이 매우 높아진다.
- 콜 행위 분석
  - 정상적인 콜은 INVITE, 200OK, BYE 메시지 등 SIP 메소드들의 교환을 통해 성립되며 각 메소드들의 전송 비율은 어느 정도 일정한 형태를 가진다.
  - INVITE/REGISTER Flooding 등 공격시 특정 메소드의 전송비율이 비정상적으로 폭주한다.

<표 1> SIP 트래픽 행위 분석 항목

구분	상세항목	계산
사용자 행위 분석	From: To 비율	Distinct From count / Distinct To count
콜 행위 분석	INVITE 비율	INVITE count / sum (전체 메소드 count)
	REGISTER 비율	REGISTER count / sum (전체 메소드 count)
	100 Trying : 200 OK 비율	200 count / 100 count
망 상태 분석	SIP bps	sum(SIP in bytes) / (last - 1st timestamp)
	SIP : RTP 비율	(SIP / RTP) in bytes



(그림 2) SIP DDoS 탐지 기법 순서

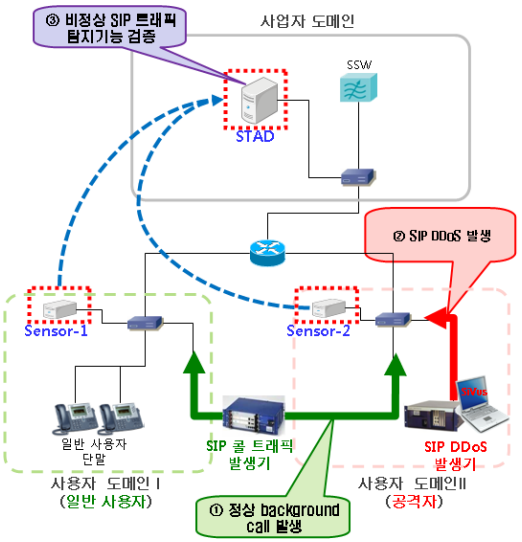
- 망 상태 분석
  - 일반적으로 적용되는 bps 분석을 동일하게 수행한다.
  - 정상 트래픽의 경우 SIP:RTP는 약 1:9의 전송량 비율을 가지나 SIP메시지를 다량 전송하는 Flooding 공격시 SIP트래픽의 비율이 크게 증가한다.

제안하는 기법은 위와 같이 총 6가지의 분석 항목을 통해 SIP 트래픽을 분석하며 분석항목 중 정해진 임계값을 초과하는 항목이 발생할 경우 SIP DDoS 형태 비정상 트래픽으로 탐지한다. 임계값은 각 항목별로 평균값 + α 로

선정하되 α 값은 관리자가 정상 SIP 트래픽 분석 값과 경험을 토대로 선정하기로 한다.

4. 테스트

제안하는 기법의 탐지기능 검증을 위해 다음과 같은 환경에서 기능 검증을 실시하였다.



(그림 3) SIP DDoS 탐지 기법 테스트망

테스트 망은 1개의 사업자 망과 2개의 사용자 망을 모사하여 구성하였으며 사용된 S/W는 다음과 같다.

- 사업자 도메인
  - SSW : Asterisk 1.6
- 사용자 도메인
  - SIP 콜 트래픽 발생기: Abacus 5000
  - DDoS 트래픽 생성기: Sivus, ThreatEX

SIP 콜 트래픽 발생기인 Abacus를 활용하여 600 가입자 망을 구성하였으며 초당 10콜, 콜 길이 10초로 설정, 동시 100 콜을 유지하는 사용자 망을 구성하였다. 모든 콜은 공개 S/W인 Asterisk를 사용하여 구성된 SSW를 통해 이루어지도록 하였다. 공격은 SiVus(DoS)와 ThreatEX(DDoS) 툴을 사용하여 발생하였으며 INVITE 메시지를 초당 50, 100, 500, 1000, 30000 건 전송하는 방식으로 공격을 수행하였다. SiVus를 사용한 공격시 공격에 사용되는 INVITE 메시지들은 전부 동일한 송신자 IP 주소와 From, To 정보를 가지나, ThreatEX를 사용한 공격에서는 모든 INVITE 메시지들이 다른 송신자 IP와 다양한 From 정보를 가진다. 각 도메인 게이트웨이에서 트래픽 미러링을 통해 트래픽 정보를 수집, STAD(SIP Traffic Anomaly Detector)로 명명한 장비에서 분석/탐지를 수행하였다.

우선 공격이 발생하지 않는 정상 상황의 트래픽을 분석한 결과 각 분석항목별 다음과 같은 값을 도출하였다.

<표 2> 정상 SIP 트래픽 특징

동시콜	SIP bps	SIP:RTP	INVITE	REGISTER	100:200	From:To
100	122598	2%	33%	0%	100%	100%

에뮬레이션의 특성상 각 항목들의 시간별 분석 값이 정상 상황에서는 크게 변화하지 않고 어느 정도 일정한 값을 보였다. INVITE 메시지의 경우 전체 중 33%정도의 비율을 유지하였고, 100 Trying 메시지와 200 OK 메시지의 비율이 1:1로 동일했다.

이러한 결과를 토대로 SIP DDoS 탐지를 위한 임계값은 다음과 같이 설정하였다.

<표 3> SIP DDoS 탐지를 위한 임계값

SIP bps	SIP:RTP	INVITE	REGISTER	100:200	From:To
250000	8%	45%	90%	60%	130%

임계값은 정상 SIP 트래픽 분석 결과를 토대로 산정하였으며, SIP bps의 두배인 250000, SIP:RTP 4배인 8%, INVITE비율 45%, REGISTER 비율 90%, 100:200 60%, From:To 130%로 산정하였다.

<표4> SIP DoS 트래픽 행위 분석 및 탐지

공격 패킷	SIP bps	SIP:RTP	INVITE	REGISTER	100:200	From:To
50	152872 /미탐	2% / 미탐	35% / 미탐	0% / 미탐	92% / 미탐	100%/ 미탐
100	158877 /미탐	2% / 미탐	36% / 미탐	0% / 미탐	80% / 미탐	100%/ 미탐
500	158493 /미탐	2% / 미탐	**47% / 탐지**	0% / 미탐	**57% / 탐지**	100%/ 미탐
1000	190930 /미탐	3% / 미탐	**54% / 탐지**	0% / 미탐	**43% / 탐지**	100%/ 미탐
3000	**306093 /탐지**	4% / 미탐	**69% / 탐지**	0% / 미탐	**22% / 탐지**	100%/ 미탐

Sivus를 이용한 DoS 공격 발생시 동시 INVITE 50, 100 건 전송의 경우 탐지하지 못했으나, 실제 공격 자체의 영향력도 매우 작았다. 그 외 동시 500건 이상 전송시 INVITE 비율이 전체의 절반 가까이 늘어나 45%를 넘어서고 콜 성공률에 해당하는 100:200 메시지 비율 또한 절반 가까이 떨어져 탐지가 가능했다.

<표5> SIP DDoS 트래픽 행위 분석 및 탐지

공격 패킷	SIP bps	SIP: RTP	INVITE	REGISTER	100: 200	From: To
50	151976 /미탐	0%*/ 미탐	**99% / 탐지**	0% / 미탐	**0%/ 탐지**	**62%/ 탐지**

ThreatEX를 이용한 DDoS 공격 발생시에는 초당 50건 INVITE 발송만으로도 서비스가 중단되는 피해가 발생하였고, 탐지 또한 성공하였다. SSW가 동일한 INVITE 메시지를 다량 수신하는 DoS 상황과 달리 DDoS 상황에서는 각기 다른 INVITE 메시지를 처리하기위해 발생하는 오버헤드가 커지고, 이에 따라 시스템 자원 고갈로 서비스가 중단된 것으로 파악된다. 이에 따라 콜 성공률이 0%에 가깝게 떨어지고 INVITE 메시지의 비율 또한 99%가까이 치솟는 결과를 보인 것으로 분석된다. DDoS 탐지 테스트의 경우 초당 50건 전송만으로도 서비스가 중단되는 피해가 발생하여 더 이상의 테스트는 의미가 없을 것으로 판단, 수행하지 않았다.

5. 결론

본 논문을 통해 SIP DDoS 트래픽에 대한 행위 분석 방법 및 탐지 방법을 제안하였다. 기존의 IP 기반 탐지 기법이 트래픽 bps, IP/port 정보 등 IP기반의 정보만을 사용하였다면, 제안된 기법은 SIP, RTP 전송 비율, 메소드별 전송량, 응용계층 식별자 등 SIP 특성정보를 고려하여 트래픽 행위를 분석하고, SIP DDoS 트래픽을 탐지한다.

현재 임계값 도출시 관리자의 경험에 의한 주관적 결정이 큰 비중을 차지하고 있으나 향후 연구를 통해 이를 보강하고 미탐율 및 오탐율이 낮은 SIP DDoS 트래픽 탐지 기법에 대한 연구를 계속 진행할 예정이다.

참고문헌

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, “SIP: Session Initiation Protocol”, RFC 3261, 2002.

[2] C.H. Liu and C.L. Lo, "The Simulation for the SIP DDoS Attack," NCM, 2009.

[3] J.P. Seifert, T. Magedanz and E. Rathgeb, "Denial-of-Service Detection and Mitigation for SIP Communication Networks," OPUS, 2009.