SIP 호 설정 메시지기반 서비스 거부 공격패턴 및 분석시스템에 관한 연구

하도윤, 김환국, 고경희, 이창용, 김정욱, 정현철
한국인터넷진흥원 보호기술팀
{dyha, rinyfeel, khko, chylee, kjw, hcjung}@kisa.or.kr

A Study on Attack Pattern and Analysis System against SIP Signaling Message-based DoS

Do-Yoon Ha, Hwan-Kuk Kim, Kyoung-Hee Ko, Chang-Yong Lee, Jeong-Wook Kim, Hyun-Cheol Jeong

Security Technology Department, Korea Information Security Agency

요 약

인터넷전화의 활성화와 더불어 SIP 프로토콜의 사용이 증가하고 있다. 최근 DDoS 공격이 주요위협으로 이슈가 되고 있으며, 향후 SIP관련 서비스 대상 서비스 거부 공격 위협도 증가할 것으로 예상된다. 본 논문에서는 SIP 프로토콜의 특성을 이용한 SIP서비스 거부 공격들의 유형을 살펴보고, SIP 프로토콜의 특성을 이용한 서비스거부 공격 탐지를 위한 고려사항을 바탕으로 분석시스템 아키텍처를 제안한다. SIP서비스 거부공격의 유형은 분류 기준에 따라 다양할 수 있으나, 본 논문에서는 SIP 프로토콜의 특성을 이용한 공격 기법을 대상으로 한다. SIP서비스 거부 공격 트래픽 분석을 위해 정보수집, 정보분석, 정보관리 기능을 고려한다.

1. 서론

SIP(Session Initiation Protocol)[1]는 멀티미디어 서비스 세션 생성, 수정, 종료를 제어하는 시그널링 프로토콜이다. SIP 기반 서비스는 인터넷 전화, 인터넷 컨퍼런스, 메신저 등이 있다[2]. SIP는 향후 인터넷을 이용한 멀티미디어 서비스의 주요 호 설정 프로토콜로 활용될 것으로 예상된다.

하지만, SIP 기반 응용 서비스는 IP 네트워크를 이용하고 있어, 기존 TCP/IP 환경의 보안 위협을 그대로 상속할 뿐만 아니라 SIP 특성에 기반한 신규 보안 위협도 존재한다. 한국인터넷진흥원(KISA) 및 안철수 연구소는 2008년, 향후 2년 내 현실화될 사이버 위협으로 VoIP, IPTV를 겨냥한 서비스 거부 공격이 등장할 것으로 예측한 바 있다[3].

SIP 기반 응용 서비스는 IP기반의 라우팅과 응용서비스 제공을 위해 URI(Uniform Resource Identifier) 정보와 SIP 프락시 서버를 이용하므로 기존의 IP기반 정보만을 분석하는 보안기술 및 장비로는 효과적인 SIP 공격 탐지 및 대응이 쉽지 않다.

본 논문에서는 SIP 보안위협 중 SIP 특성을 이용한 서비스거부공격의 유형을 분류하고 분석을 위한 고려사항과 분석시스템 아키텍처를 제안한다.

2. 관련연구

Geneiatakis 등은 malformed SIP messages 공격을 탐지하기 위한 시스템 구조를 제안하였다[4]. Wu등은 SIP-BYE 공격 등 상태 기반 SIP 공격탐지를 위한 SCIDIVE란 VoIP 침입 탐지 시스템을 제안하였다[5]. Kang 등은 평균 등록 주기 분석, 송신자와 수신자의 비율 분석 등 VoIP 트래픽의 특성을 분석하기 위한 프로파일링 기법을 제안하였다[6]. 현재 SIP기반 VoIP 보안을 위한 다양한 연구가 진행 중에 있다.

3. SIP서비스 거부공격 유형

SIP 프로토콜은 응용계층의 프로토콜로 IP 계층에서의 트래픽 패턴 분석을 위한 IP 정보와 응용계층에서의 트래픽 패턴 분석을 위한 URI 정보도 통합적으로 고려하여 분석하여야 한다. 또한 각 세션별 식별자인 Call-ID도 함께 고려하여야 한다.

SIP서비스 거부공격의 유형은 분류 기준에 따라 다양할 수 있으나, 본 논문에서는 SIP 프로토콜의 특성을 이용한 공격 기법을 기준으로 분류한다.

3.1 SIP기반 Flooding 공격

Invite Flooding: 공격자가 위조된 Invite 메시지를 다량 전송하여 원하지 않는 다수의 사용자에게 전화 벨이 울리거나 SIP Proxy Server, Soft Switch 등을 대상으로 시스템 자원을 고갈시키거나 오작동을 유발할 수 있다.

Register Flooding: 공격자가 반복적인 register 요청 메시지를 다량 전송하여 정상 사용자가 등록을 하지 못하게 방해하거나 서버에 과부하를 쉽게 발생시킬 수 있다.

RTP Flooding: 공격자가 다량의 음성 메시지를 전송

하여 서비스의 이용 및 사용하고 있는 서비스 지연을 유발할 수 있다.

3.2 비정상 메시지 공격

SIP 메시지들은 텍스트 기반이므로 공격자가 헤더와 바디 부분에 메시지를 위/변조 하여 정상 사용자를 서비스 불능 상태로 만들거나 SIP 서버를 대상으로 오동작을 유발할 수 있다.

3.3 Cancel 공격

SIP 정보를 지속적인 스니핑을 통해 통화 정보(Caller-ID, From, To tag)를 획득하여 위조된 SIP 메시지를 다량 전송하여 정상 사용자의 호 설정을 방해할 수 있다.

3.4 Bye 공격

SIP 정보를 지속적인 스니핑을 통해 통화 정보(Caller-ID, From, To tag)를 획득하여 위조된 SIP 메시지를 다량 전송하여 정상 사용자의 통화를 강제로 종료시킬 수 있다.

4. SIP서비스 거부 공격 탐지를 위한 고려사항 및 분석시스템 아키텍처

4.1 SIP 트래픽 정보수집 기능

SIP 패킷 필터링 기능: 네트워크로부터 모든 패킷을 손실없이 원형 그대로 수집한 후 IP 패킷으로부터 SIP, RTP 패킷을 식별하고 분류한다.

SIP 응용트래픽 정보 수집 기능: 송신자, 수신자 정보, RTP QoS 등 SIP에 특화된 정보를 수집한다.

SIP기반 플로우 생성 기능: 통화 세션 단위 트래픽 정보 통계 및 플로우를 생성한다.

4.2 SIP 트래픽 분석 기능

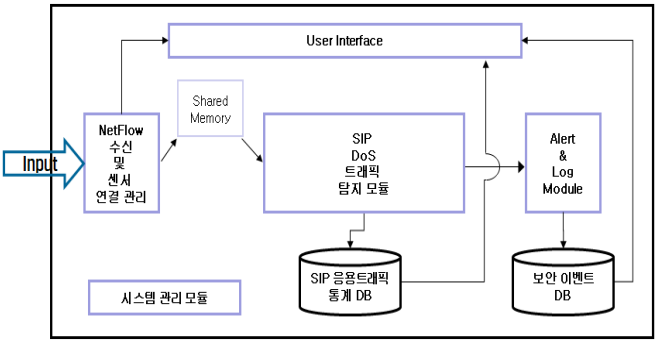
SIP 응용트래픽 행위 분석 기능: SIP 응용서비스 행위 속성별 트래픽을 분석한다.

비정상 SIP 트래픽 탐지 기능: 분석 결과와 수집된 플로우 통계정보를 기반으로 비정상 SIP 트래픽을 탐지한다.

4.3 SIP 트래픽 관리 기능

SIP 트래픽 수집·분석 기능 검증 UI: 관리자에게 현재 트래픽 모니터링 정보, 비정상 트래픽 탐지 정보 및 시스템 환경 설정을 보여주는 화면을 제공한다.

4.4 SIP서비스 거부 공격 트래픽 분석시스템 아키텍처



(그림 1) 시스템 전체 구조도

SIP서비스 거부 공격 트래픽 분석 시스템은 다음의 모듈로 구성된다.

NetFlow 수신 및 센서 연결관리 : 다중지점의 SIP 응용트래픽 수집센서로부터 SIP 기반 플로우를 수신하고 디코딩한다.

SIP DoS 트래픽 탐지 모듈 : Shared Memory로 구성된 SIP 응용트래픽 정보를 대상으로 의심되는 SIP 응용트래픽을 탐지한다.

Alert&Log 모듈 : 비정상 트래픽에 대한 알람 및 Log 기록한다.

User Interface : SIP기반 플로우 및 통계정보, 보안이벤트 Log 조회, 시스템 설정 변경 등 사용자 인터페이스를 제공한다.

시스템 관리 모듈 : 시스템 상태 관리 및 센서 리스트를 관리한다.

5. 결론 및 향후 연구

SIP 프로토콜 사용이 증가함에 따라 SIP관련 서비스 대상 서비스 거부 공격 위협도 증가할 것으로 예상된다. 본 논문에서는 SIP 프로토콜의 특성을 이용한 SIP서비스 거부 공격들의 유형을 살펴보았고, SIP 프로토콜의 특성을 이용한 서비스거부 공격 탐지를 위한 고려사항을 바탕으로 분석시스템 아키텍처를 제안하였다.

향후 전체 트래픽에서 SIP트래픽 정보만 수집을 위한 연구와 프로파일링 기반의 SIP DoS, DDoS 탐지 알고리즘 연구를 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, June 2002.

[2] H. Schulzrinne, S. Casner, R. Frederick and V. Jacobsonm, "RTP: A Transport Protocol for Real-Time Applications", RFC 1889, January, 1996

[3] 길민권, “2년뒤 현실화될 사이버 보안 위협 3종세트,” 보안뉴스, 2008.1.3.

[4] D. Geneiatakis, G. Kambourakis, T. Dagiuklas, C. Lambrinoudakis and S. Gritzalis, "A Framework for Detecting Malformed Messages in SIP Networks", the 14th IEEE Workshop on Local and Metropolitan Area Networks LANMAN), Greece, September 2005

[5] Y. Wu, S. Bagchi, S. Garg, N. Singh and T. Tsai, SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments”, 2004 International Conference on Dependable Systems and Networks (DSN'04), Florence, Italy, 2004

[6] H. Kang, Z. Zhang, S. Ranjan and A. Nucci, “SIP-based VoIP Traffic Behavior Profiling and its Application”, MineNet'07, San Diego, USA, June 2007.