SIP-Aware 침입방지 시스템 설계*

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

The Design of SIP-Aware Intrusion prevention System

Jeong-Wook Kim, Hwan-Kuk Kim, KyoungHee Ko, Chang-Yong Lee, DoYoon Ha, HyunCheol Jeong
Security Technology Team, Korea Internet & Security Agency

요 약

인터넷전화는 저렴한 가격과 다양한 서비스를 장점과 번호이동과 같은 정부 정책에 힘입어 급속한 성장을 이루고있다. SIP는 VoIP의 시그널링 프로토콜로서 다양한 부가서비스 제공을 위해 기존의 H.323을 대체하고 있을뿐만 아니라, IMS의 시그널링 제어 프로토콜로 채택되어 향후 SIP기반 응용서비스의 급속한 성장이 예상된다. 하지만 SIP기반 응용서비스는 기존의 IP 망에서 발생되는 보안 위협뿐만 아니라 SIP 특성에 기인한 신규 위협에 의한 피해 사례가 발생하고 있음에도 불구하고, 현재 보안 시스템으로는 이러한 위협에 효과적으로 대응하지 못하고 있다. 본 논문에서는 SIP기반 네트워크 보안 위협에 대해서 설명하고, 이러한 공격을 탐지 및 대응할 수 있는 SIP-Aware 침입방지시스템 설계 및 구조도를 설명한다.

1. 서론

IETF에서 표준으로 제정된 SIP(Session Initiation Protocol)[1]는 시그널링 제어 프로토콜로서 대표적인 SIP 기반 응용 서비스로는 인터넷전화(VoIP)가 있다.

SIP기반 응용서비스는 IP 주소 정보뿐만 아니라, 응용서비스 제공을 위해 URI(Uniform Resource Identifier) 정보와 SIP 프록시 서버를 사용 등으로 인해 기존의 IP 망에서 발생되는 보안 위협을 그대로 상속할 뿐만 아니라, SIP 특성을 이용한 서비스 거부 공격, 통화방해, 과금회피, 도청 등의 신규 보안 위협에 노출되어 있다.

이러한 SIP기반 신규 보안 위협은 비교적 손쉽게 위변조 할 수 있기 때문에 공격이 용이 할뿐만 아니라, 기존의 IP/Port 정보만을 활용하는 보안기술 및 장비로는 효과적으로 탐지 및 대응하기 어렵다.

본 논문에서는 SIP기반 응용서비스 대상 네트워크 보안 위협을 SIP기반 서비스 거부 공격, SIP기반 서비스 오용 공격, 통화방해 및 중단 공격으로 분류하고 분석하여 이러한 공격을 탐지 및 대응할 수 있는 SIP-Aware 침입방지시스템 설계 및 구조도를 설명한다.

2. 관련연구

2.1 SIP 기반 네트워크 보안 위협

* 본 연구는 지식경제부 및 정보통신연구진흥원의 IT성장동력기술개발 사업의 일환으로 수행하였음. [2008-S-028-02, SIP기반 응용서비스 보호를 위한 침입대응기술 개발]

<표 1> SIP기반 네트워크 보안 위협 분류

구분	공격	설명
SIP 서비스 거부공격	시그널링 메시지 기반 DoS	INVITE, Registration flooding 등
	미디어 기반 DoS	RTP flooding 등
	회선자원고갈	DDoS, 비정상 SIP트래픽 폭주 등
	Malformed 메시지 공격	SIP 표준 규격에 벗어나는 공격 패킷을 생성시켜 서버/단말의 오작동 유발
SIP 서비스 오용공격	등록정보변조	SIP SQL Injection 공격 등 사용자 정보 유출
	과금 우회 및 회피	InviteReply, FakeBusy, ByeDelay 등
	INVITE 세션 가로채기	사용자에 301 응답코드 메시지를 발송하여 서비스 이용 방해
	Registration 하이재킹	사용자의 등록 프로세스를 중간에 가로채어 정보 유출을 시도하는 공격
통화방해 및 중단공격	SIP-BYE/Cancel 공격	호 설정/중간 과정에서 통화 세션을 중단/취소하는 공격
	DeRegistration 공격	등록되어 있는 단말을 강제로 등록 해제 시키는 공격
	RTP SSRC collision 공격	Junk RTP 데이터를 생성하여 통화 품질을 저해시키는 공격
	Re-Invite 공격	정상 세션을 종료하고 새로운 세션 성립을 위한 공격

NIST, BSI 등에서는 VoIP 보안위협을 기밀성, 무결성, 가용성에 따라 분류하고 있으며, XMCO, Colorado 대학에서는 네트워크 계층에 따라 분류하고 있다.

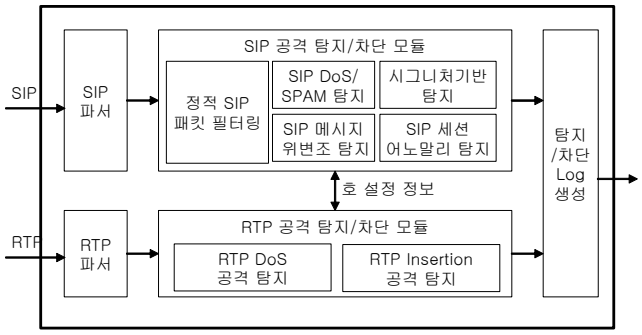
국내의 한국인터넷진흥원에서는 VoIP 보안 위협에 대해 도청, 서비스 거부 공격, 서비스 오용 공격, 세션 가로채기, VoIP 스팸으로 분류하고 있다.

본 논문에서는 SIP기반 응용서비스 대상 네트워크 보안 위협을 공격 특성에 따라 표1과 같이 분류한다.

2.2 기존 연구

현재, VoIP 서비스의 활성화와 함께 SIP 기반의 VoIP 보안을 주제로 많은 연구가 이루어지고 있으며, 연구 결과 또한 발표되고 있다. Chen은 SIP 세션 상태 정보기반 SIP DoS 탐지 시스템[2] 구조를, Geneiatakis 등은 malformed SIP messages[3] 공격을 탐지하기 위한 시스템 구조를, Wu 등은 2004년 SIP-BYE 공격 등 상태 기반 SIP 공격 탐지를 위한 SCIDIVE란 이름의 VoIP 침입 탐지 시스템을 제안하였다[4]. 이러한 공격 탐지 기법 외에도, Kang 등은 VoIP 트래픽의 특성을 분석하기 위한 프로파일링 기법을 제안한 바 있다[5].

3. SIP-Aware 침입방지시스템 설계



(그림 1) SIP 침입방지시스템 구조도

SIP 침입방지시스템의 전체 구조도는 그림1과 같으며, 주요 기능은 아래와 같다.

- SIP/RTP 메시지 파싱 기능 : SIP/RTP 메시지를 수신하여 파싱하고 SIP/RTP 메시지 공격 탐지 모듈로 전송한다.
- SIP 정적 필터링 기능 - 송신자 IP, 수신자 IP, URI/Domain(From, To, Via 필드), Subject 필드의 키워드 등의 블랙 리스트 값을 기반으로 SIP 패킷을 필터링한다.
- SIP DoS/SPAM 탐지 기능 - 송신자IP, 수신자 IP, URI/Domain(From, To, Via 필드), Call-ID, Method, Status Codes 등의 SIP 헤더 정보를 바탕으로 정적 임계치기반 SIP DoS/SPAM을 탐지한다.
- 시그니처기반 탐지 기능 - Positive/Negative 탐지 룰을 비교하여 일치하는 패턴의 SIP 메시지를 탐지/차단한다.
- SIP 메시지 위변조 탐지 - 정상적으로 등록된 사용자의 SIP 메시지 중 INVITE, BYE, CANCEL 메시지를 대상으로 SIP 파서 모듈에서 전송된 SIP 메시지에서 MAC, URI, UA/Max-Forwards 필드 값, 헤더 순서 등을 추출해서, DB에 저장된 초기 SIP 메시지의 값과 비교하여 메시지의 위변조를 탐지/차단한다.
- SIP 세션 어노말리 탐지 기능 - SIP Dialog/Transaction 관리를 통해 유입되는 SIP 메시지의 적합성을 확인하고 부적합한 SIP 메시지를 탐지/차단한다. 트랜젝션 관리는 표준(RFC 3261)의 INVITE/Non-INVITE sever/client transaction에 따라 구성되며, 세션 상태 정보 테이블에 저장된 이전 상태 정보를 바탕으로 유입된 메시지의 적합성을 판단하여 비정상 메시지를 탐지/차단한다.
- RTP DoS 공격 탐지 기능 : 호 설정 정보를 기반으로 호 설정이 이루어지지 않은 RTP Flooding 공격을 탐지/차단하고, RTP Port를 동적으로 관리한다.
- RTP Insertion 공격 탐지 기능 : 이전에 전송된 RTP 패킷의 Timestamps, Sequence 값과 현재 RTP 패킷의 값을 비교하여, RTP Insertion 공격을 통한 통화 방해 공격을 탐지/차단한다.

4. 결론

본 논문에서는 SIP기반 응용서비스에서 발생할 수 있는 보안 위협에 대해서 분류하고 이러한 공격을 탐지 및 대응하기 위한 SIP-Aware 침입방지시스템 설계에 초점을 맞추어 기술하였다. 현재 본 시스템은 구현을 완료하고 연구망에서 시범 운영 중이며, 향후 SIP 공격 탐지/차단 기능 고도화를 통해 기능 및 성능을 향상시킬 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] Eric Y. Chen "Detecting DoS Attacks on SIP Systems", 1st IEEE Workshop on VoIP Management and Security, 2006, April 2006.

[3] 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

[4] 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 DSN'04, Florence, Italy, 2004

[5] 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.