제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

RTP Packet을 활용한 SIP 기반 INVITE Flooding 탐지 기법

이성민, 김강석, 홍만표
아주대학교 일반 대학원 지식정보보안학과
bapam@hanmail.net, kangskim@ajou.ac.kr, mphong@ajou.ac.kr

SIP-based Invite Flooding Detection using RTP Packet

Sungmin Lee, Kangseok Kim, Manpyo Hong
Dept. of Knowledge Information Security, Graduate School of Ajou University

요 약

인터넷이 발전함에 따라 기존의 PSTN(Public Switch Telephone Network)망이 감소하고 VoIP 서비스가 증가하고 있다. VoIP 서비스가 기존의 인터넷을 기반으로 서비스가 되어 보안문제까지 같이 떠안게 되었다. 이에 VoIP상의 다양한 공격에 대한 분석 및 효율적인 탐지 방법이 연구 되고 있다. 본 연구에서는 공격 중에서 SIP 상에서의 INVITE Flooding 공격에 대해 분석하고, 기존의 탐지 알고리즘을 연구하여 오탐율이 개선된 탐지 알고리즘을 제안한다.

1. 서론

최근 인터넷이 발달함에 따라 기본의 PC만으로 활용하던 것에서 생활 전반으로 파고 들어와 통합 멀티미디어 서비스로 진화하기 시작했다. VoIP도 이러한 발달로 인하여 나타나게 된 서비스 중 하나로 기존의 PSTN망을 사용하여 단순히 음성 전화만을 사용하던 시대에서 인터넷망을 통하여 단순 음성 통화 및 영상 통화, 메시지, 멀티미디어 영상 서비스까지 제공하게 되었다. 이로 인하여 사용자는 다양한 콘텐츠로 인하여 선택의 폭은 넓어졌지만, 이러한 발전으로 인한 부작용도 발생되었다. 이러한 기술의 대부분은 인터넷을 기반으로 상용화 되어 서비스되기 때문에 보안에 대한 문제까지 같이 떠안게 되었다. 또한 악의적인 목적, 즉 금전적 이득이나 경쟁사와의 승리 등의 목적을 가지고 하는 공격이 증가함에 따라 피해규모도 증가하고 있는 실정이다. 더욱이 공격의 방법도 더욱 다양해지고 있는 것이 현실이어서 대책이 시급하다.

본 논문에서는 여러 공격 중 대상 서버와 사용자간의 정상적인 서비스가 이루어지지 못하도록 사용자의 세션 연결 방해 및 서버에 자원을 소모시키는 INVITE Flooding 공격을 탐지하는 개선된 방법을 제안한다.

논문의 section 2에서는 SIP(Session Initiation Protocol)와 INVITE Flooding 공격을 분석하고, 기존에 사용되었던 알고리즘을 설명한다. section 3에서는 사용되었던 알고리즘을 향상시키는 방안을 제시한다. section 4에서는 논문에서 제안한 기법에 대한 결론과 향후 연구 방향으로 구성하였다.

2. 관련연구

2.1 SIP

SIP는 VoIP 서비스를 이용하기 위한 Signaling Protocol로, 주로 세션을 설정하고 제어하는데 사용되는 사용된다. 다양한 서비스를 제공할 수 있고, H.323 프로토콜보다 구현 및 확장이 쉽다. SIP 메시지는 클라이언트 측에서 발생시키는 Request 메시지와 서버 측에서 발생시키는 Response 메시지로 구분할 수 있다. Request 메시지는 INVITE 메시지, ACK 메시지, BYE 메시지 등이 있고, Response 메시지는 200OK 메시지와 180 Ringing 메시지 등이 있다. HTTP 프로토콜의 메시지와 같은 텍스트 기반으로 헤더와 바디로 이루어져 있고, 구조는 server-client 모델로 이루어져있다. 주요 구성요소로는 UA(User Agent), Proxy Server, Redirection Server, Location Server, Registrar Server가 있다[2].

2.2 INVITE Flooding Attack

INVITE Flooding 공격은 일종의 DoS 공격으로 정상적인 INVITE 메시지를 대량으로 서버에 전송하여 원활하지 못하도록 과부하를 일으키는 공격이다. TCP의 SYN Flooding 공격과 유사한 형태를 나타내고 있다[5]. 정상적인 많은 수의 INVITE 메시지들이 서버로 전송되기 때문에 서버의 시스템 자원을 고갈되어 사용자에 대한 정상

적인 서비스가 불가능하게 되고 공격이 진행되는 동안 공격 대상의 전화벨이 지속적으로 울리게 되어 일반 업무의 진행에도 지장을 초래할 가능성이 있다[5].

2.3 CUSUM (Cumulative Sum)

change point detection 이론에 근원을 둔 비정상 탐지 알고리즘으로 예상 값에서 샘플 값의 편차를 누적 합으로 구한 후 time serises에 대한 평균을 이용하여 변화를 탐지하는 알고리즘이다.

같은 간격의 단위 시간으로 이루어진 일정 기간 동안 관찰을 한다. x_n, n=1,2,...은 n번째 시간 간격 이내에 수집된 INVITE 메시지의 수이고 μ_n은 시간 n시간 동안의 평균 INVITE 메시지의 수신비율이라고 한다. μ_n 값은 지수적 가중이동 평균(EWMA: exponentially weighted moving average)을 이용하여 계산한다[6].

$$\mu_n = \beta\mu_{n-1} + (1-\beta)x_n$$

이때 β는 지수적 가중이동 평균의 요소이고 μ_0의 값은 x_1이 된다. 이때 x_n의 값은 non-stationary 하기 때문에 다음 과 같은 방정식으로 전환한다.

$$\tilde{x}_n = \frac{x_n}{\mu_{n-1}}, \quad n \geq 1$$

CUSUM 알고리즘은 다음과 같은 회귀 방정식으로 구해질 수 있다.

$$y_n = \max\left(0, y_{n-1} + \tilde{x}_n - a\right), \quad y_0 = 0$$

여기서 공격 발생 시에 $\widetilde{x_n}$-a의 값은 큰 양의 값이 된다. 이때 a의 값은 다음과 같으며,

$$a = E_{est}(\tilde{x}_n) + \eta.\sigma_{est}(\tilde{x}_n)$$

η은 표준편차의 수, $\sigma_{est}(\widetilde{x_n})$은 정상 트래픽의 표준편차이다. 임계치값은 ρ가 우리가 탐지하려는 구간을 반영하여 $\rho.\sigma_{est}(\widetilde{x_n})$ 형태로 구해진다. 구해진 임계치의 값보다 가중 평균의 값이 클 경우 공격을 인식하게 된다.

3. CUSUM 알고리즘 기법에 RTP 패킷 덤프를 적용한 SIP Invite Flooding 탐지 방법

기존의 CUSUM 알고리즘은 INVITE 메시지의 수만 활용하여 공격을 탐지하기 때문에 정상적인 사용자의 증가로 인해 트래픽이 증가하여 네트워크가 혼잡한 상황과 SIP Flooding 공격 인한 상황의 구분탐지가 어렵다. 그러므로 사용자가 많아질 경우 공격으로 잘못 인식하여 정상적인 서비스의 이용이 어려워질 우려가 있지만, 그러한 상황을 방지하기 위하여 임계치를 높이면 공격 탐지의 시간이 늦어질 우려가 있다[1].

제안 방식은 그림 1.의 구조 같이 공격 대상인 UA와 SIP Proxy Server가 포함되어 있고 VoIP 트래픽이 합쳐져 인터넷으로 연결되어 있는 Router의 앞에서 기존의 CUSUM 알고리즘에 INVITE 메시지만 적용하여 공격을 탐지하는 것 이외에 RTP(Real Time Transport Protocol)

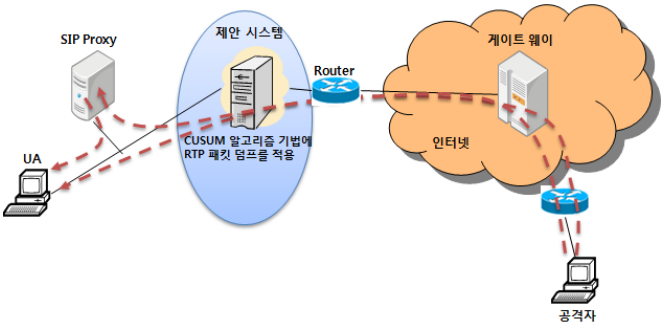

그림 1. 제안 시스템

패킷의 데이터를 이용하여 INVITE Flooding 공격을 탐지하도록 한다.

RTP는 SIP 세션이 연결 되고 그 다음 멀티미디어 데이터 전송을 실시간으로 지원하는 프로토콜이다. 실시간이라는 RTP의 특징을 이용하는 방법으로 INVITE 메시지의 수집 시간과 동일한 시간동안 전송되는 RTP 패킷을 활용한다. RTP 패킷 구조는 아래 그림 2.의 형태로 이루어져 있다. RTP 패킷은 헤더와 데이터 부분으로 구성되어 있는데 헤더 부분의 SSRC(Synchronization source)필드의 값을 활용한다. SSRC 필드는 32bits의 크기로 이루어져 있으며, 동시화 소스를 의미한다[7]. SSRC 필드들은 무작위로 설정되지만 동일한 세션에서 전송되는 RTP 패킷들의 SSRC필드 값은 동일한 값을 가지도록 지정되어 있다. 따라서 각기 다른 값을 갖고 있는 SSRC필드의 종류의 수를 파악해 보면 RTP 세션의 수를 구할 수 있다.

이때 패킷을 직접 캡쳐하여 분석하지 않고 dump를 생성하여 분석한다. dump를 생성하는 이유는 패킷을 직접 분석하게 되면 서버의 과부하를 발생시킬 수 있기 때문에 과부하를 감소하기 위한 방안으로 dump를 사용한다.

V	P	E	CC(4bits)	M	PT(7bits)	Sequence number(16bits)
Timestamp (32bits)						
Synchronization source (SSRC) identifier (32bits)						
Contributing source (CSRC) identifier (variable)						
Data (variable)						

그림 2. RTP 패킷 구조

Section 2.3.에서 설명되었던 n 시간 간격으로 수집한 RTP dump의 데이터 중에서 SSRC의 값을 분석하여 해

당 시간에 연결되어 있는 RTP 세션의 수가 구해진다. 구한 RTP 세션의 수를 INVITE 메시지와 동일하게 CUSUM 알고리즘을 적용한다.

공격을 받지 않는 정상적인 상태의 VOIP 통신이라면 세션을 설정하기 위해 INVITE 메시지를 전송하게 되고 요청을 정상적으로 받아들여 하나의 세션이 이루지게 된다. 즉, 네트워크의 상태가 불안정하거나 혼잡으로 인한 재전송과 같은 경우를 제외한다면 하나의 INVITE 메시지에 하나의 세션이 설정되는 것이다. 하지만 실제 환경에서는 재전송과 같은 예상하지 못하는 상황이 발생할 수 있기 때문에 CUSUM 알고리즘을 적용하여 비교하는 것이다.

CUSUM 알고리즘에 나타나는 두 가지의 결과를 비교하여 INVITE Flooding 공격의 여부를 확인할 수 있다.

INVITE에 해당하는 CUSUM 값이 임계치를 초과하였을 때 RTP 세션에 해당하는 CUSUM 값이 임계치를 초과하지 않았다면 INVITE 메시지와 세션의 수가 비례하지 않고 INVITE 메시지만 과도한 양이 전송되기 때문에 INVITE Flooding 공격으로 탐지가 되고, INVITE 메시지에 해당하는 CUSUM 값과 RTP 세션 수에 해당하는 CUSUM 값 모두 임계치를 초과하였다면 INVITE 메시지만큼 세션이 형성되어 있는 것으로 많은 수의 사용자로 인한 네트워크 혼잡을 나타낸다.

따라서 기존의 INVITE 메시지의 수와 RTP 메시지를 이용하여 SIP Flooding 공격을 탐지할 뿐만 아니라 RTP Foolding 공격도 탐지가 가능하다. 또한 기존의 문제였던 네트워크혼잡으로 인한 오탐율을 감소시킬 수 있다.

5. 결론

인터넷의 발달과 활용도가 넓어지면서 기존의 PSTN망은 감소하고 VoIP에 대한 기술의 발전 및 보급이 크게 증가하는 추세이다. 그에 따라서 VoIP에 대한 다양한 공격도 크게 증가하는 결과가 나타나고 있다. 이에 본 논문에서는 기존에 CUSUM을 활용한 INVITE Flooding 공격 탐지 방법에서의 FAR을 개선하기 위해 RTP 패킷의 SSRC 필드의 값을 이용하는 방법을 제안하였다.

제안된 방식은 네트워크 혼잡시 INVITE Flooding 공격에 대해 탐지 가능하지만 RTP dump를 사용함으로써 시스템에 부하가 되는 부분에서 탐지 속도에 대한 문제가 발생할 여지가 있다. 향후에는 시스템 부하의 해소와 본 논문에서 제안한 방법을 발전시켜 VoIP에서 발생하는 패킷과 트래픽의 유형을 분석하여 한번에 다양한 공격을 탐지할 수 있는 방안으로 연구하고자 한다.

참고문헌

[1] 아주대학교 산학협력단, “응용계층(SIP, RTP) 기반 보안위협 모델링 연구”, 한국정보보호진흥원, 2008. 12.

[2] Hongli Zhang, Zhimin Gu, Caixia Liu, Tang Jie, “Detecting VoIP-specific Denial-of-Service Using Change-Point Method“, Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on, Feb. 2009.

[3] “SIP의 이해”, http://www.NExpert.net.

[4] 윤성렬, 하도윤, 정현철, 박석천, “SIP 환경에서의 DDoS 공격 탐지를 위한 확장된 TRW 알고리즘 검증”, 멀티미디어학회 논문지 제 13권 제 4호 2010. 4.

[5] 한양대학교 산학협력단, “SIP기반 보안위협에 따른 품질 영향평가 방법론 연구“, 한국정보보호진흥원, 2008. 12.

[6] 류제택, 류기역, 노병희, “발생 메시지의 상한값을 고려한 SIP INVITE 플러딩 공격 탐지 기법연구”, 한국통신학회논문지, 2009. 8.

[6] Yacine Rebahi, Muhammad Sher,Thomas Magedanz, ″Detecting Flooding Attacks Against IP Multimedia Subsystem (IMS) Networks″, IEEE Intern′l Conf. Computer Systems and Applications 2008 (AICCSA′2008), Mar, 2008

[7] 민상원, “차세대 통신망의 IMS와 VoIP″, 홍릉과학출판사, 2011. 6.