VoIP 이상 트래픽의 플로우 기반 탐지 방법
(A Flow-based Detection Method for VoIP Anomaly Traffic)

손 현 구 † 이 영 석 ††
(Hyeongu Son) (Youngseok Lee)

요 약 SIP와 RTP를 기반으로 한 인터넷 전화 서비스가 널리 보급되고 있다. 이와 함께 VoIP 전화 연결 지연, 방해, 종료 및 음성 통화 품질 감소 등의 피해를 주는 VoIP 이상 트래픽들이 등장하기 시작했다. 국내 대부분의 VoIP 응용들은 현재 표준으로 정의되어 있는 보안 프로토콜을 사용하지 않고 있어 공격자가 패킷을 쉽게 스니핑하고 사용자의 정보 및 헤더 정보를 얻을 수 있을 뿐만 아니라 이상 트래픽을 쉽게 생성시킬 수 있다. 본 논문에서는 무선랜 상에서 SIP/RTP 패킷 스니핑을 통하여 CANCEL, BYE DoS 및 RTP 플러딩 이상 트래픽의 생성 방법과 플로우 기반 트래픽 모니터링을 통하여 VoIP 응용 이상 트래픽 탐지 방법을 제시한다. 실제 상용 VoIP 망에서 실험한 결과 이들 이상 트래픽을 97% 탐지하였다.
키워드 : VoIP, 플로우, 이상 트래픽, IPFIX, 탐지

Abstract SIP/RTP-based VoIP services are being popular. Recently, however, VoIP anomaly traffic such as delay, interference and termination of call establishment, and degradation of voice quality has been reported. An attacker could intercept a packet, and obtain user and header information so as to generate an anomaly traffic, because most Korean VoIP applications do not use standard security protocols. In this paper, we propose three VoIP anomaly traffic generation methods for CANCEL;BYE DoS and RTP flooding, and a detection method through flow-based traffic measurement. From our experiments, we showed that 97% of anomaly traffic could be detected in real commercial VoIP networks in Korea.
Key words : VoIP, Flow, Anomaly traffic, IPFIX, detection

1. 서 론

전세계적으로 PSTN을 대체하는 인터넷 기반의 전화 서비스(VoIP: Voice over IP)가 널리 보급되고 있다. 대표적인 국내 VoIP 응용 서비스 사업자인 LG 데이콤, 삼성 네트웍스, SK 텔링크 및 KT등에서는 SIP(Session Initiation Protocol)[1]와 RTP(Real-time Transport Protocol)[2]를 이용한 인터넷 전화를 출시하여 보급하고 있으며, 2009년 8월 현재 전체 가입자 수는 500만명을 돌파하였다. 전체 가입자 중 50%인 250만명은 2009년에 가입한 것으로 나타났으며, 현재 가입자가 지속적으로 증가하고 있다[3].

SIP와 RTP 기반의 인터넷 전화가 널리 보급됨에 따라 이들 서비스를 방해하기 위한 다양한 이상 트래픽들이 나타나고 있다. 이에 대응하기 위하여 방송통신위원회에서는 2009년 방통 융합 5대 핫이슈로 'VoIP 보안 위협 및 대책'을 제시하였다. 또한, 국내 보안 업체인 안철수 연구소에서도 VoIP 보안을 2009년 7대 보안 이슈로 발표하였다[4,5].

인터넷 성능 저하 및 특정 서비스를 방해하기 위한 DoS(Denial of Service), DDoS(Distributed DoS), 웜(Worm) 및 포트 스캐닝 등은 VoIP 응용 서비스의 품질을 저하시킬 수 있다. 또한, VoIP 응용 서비스에서 전화 연결 지연, 통화 품질 감소 등을 초래할 수 있다. 최근 VoIP 응용 서비스를 직접 방해하기 위한 이상 트래픽들이 등장하고 있다. 국내에서 사용하고 있는 SIP

· 본 연구는 2008년도 충남대학교 학술연구비의 지원에 의하여 연구되었음
† 학생회원 : 충남대학교 컴퓨터공학과
hgson@cnu.ac.kr
†† 정 회 원 : 충남대학교 컴퓨터공학과 교수
lee@cnu.ac.kr
(Corresponding author임)
논문접수 : 2010년 2월 9일
심사완료 : 2010년 4월 13일

정보과학회논문지: 정보통신 제37권 제4호(2010.8)

와 RTP 기반의 VoIP 서비스에 대해서 공격자가 쉽게 이상 트래픽을 생성시켜, 사용자의 전화 연결 강제 취소 및 종료 등을 발생시킬 수 있다.

이상 트래픽으로부터 VoIP 응용 서비스를 보호하기 위하여 다양한 보안 프로토콜이 제안되었다. 패킷 암호화를 위하여 SRTP(Secure RTP)[6], IPSec(IP Security)[7], TLS(Transport Layer Security)[8]등이 제안되었으며, 사용자 인증을 위한 인증 방법이 SIP 표준에 제시되어 있다. 하지만, 국내 상용 VoIP 응용 서비스를 실험한 결과 표 1처럼 패킷 암호화를 위한 프로토콜을 적용하지 않고 있으며, 사용자 인증을 위한 인증 필드만을 사용한다. 이와 같은 경우 VoIP 트래픽에 대한 기밀성과 무결성을 보장하기 어렵기 때문에 보안 취약점을 보이게 된다[9].

표 1 국내 VoIP 서비스 제공자의 보안 프로토콜 적용 현황

보안 프로토콜 / 사업자	SIP 인증	TLS	IPSec	SRTP
myLG070	○	×	×	×
삼성 wyz 070	○	×	×	×
SK 텔링크	○	×	×	×

최근 무선랜을 기반으로 한 VoIP 전용 단말이 널리 보급되고 있다. 무선랜의 경우 대부분의 사용자가 암호화를 사용하지 않은 상태로 사용하기 때문에 공격자가 쉽게 트래픽을 스니핑할 수 있다. 따라서 본 논문에서는 무선랜 기반의 VoIP 환경에서 VoIP 트래픽을 스니핑하여 이상 트래픽을 생성하고 이를 탐지하는 방법을 제안한다. 실제 사용되는 VoIP 트래픽은 패킷 암호화가 적용되어 있지 않기 때문에 이상 트래픽을 쉽게 생성시킬 수 있으며, 본 논문에서는 이를 이용하여 CANCEL/BYE DoS와 RTP 플러딩 이상 트래픽을 생성한다. 생성된 이상 트래픽으로 사용자 간에 전화 통화 시도 취소 및 전화 통화 강제 종료, 음성 통화 품질 저하 등을 초래하였다.

[10]에서는 플로우 기반 트래픽 모니터링을 이용한 VoIP 응용 이상 트래픽 탐지 방법을 제시하였다. 플로우 기반 트래픽 모니터링을 이용하여 VoIP 트래픽 모니터링을 수행하기 위해 IETF에서 표준으로 정의된 IPFIX(IP Flow Information eXport)[11]를 사용하였다. 하지만 VoIP 응용 이상 트래픽을 탐지하는 방법만을 제시하고 있을 뿐 이에 대한 실험결과가 제시되어 있지 않다.

본 논문에서는 [10]에서 제시된 VoIP 이상 트래픽 탐지 방법을 기반으로 무선랜 상에서 발생하는 VoIP 이상 트래픽 탐지 방법과 실험 결과를 보인다. VoIP 트래픽 모니터링은 [10]에서 제시한 IPFIX를 이용하며, 무선 VoIP 단말과 무선 액세스 라우터 사이에서 수행된다. 본 논문에서 생성한 이상 트래픽은 정상적인 VoIP 환경에서 사용되는 트래픽과 매우 유사하기 때문에 SIP와 RTP 헤더 정보 외에 다른 계층의 헤더 정보를 이용한 탐지 방법을 제시한다. CANCEL DoS 이상 트래픽 탐지를 위하여 SIP 헤더 뿐만 아니라 802.11 MAC 헤더의 내용을 이용하였으며, BYE DoS 이상 트래픽 탐지는 SIP 헤더 및 RTP 트래픽 정보를 이용한다. 또한, RTP 플러딩 이상 트래픽은 RTP 헤더의 순서번호와 SSRC(Synchronization source) 값을 이용하여 탐지한다. 이 세 가지 이상 트래픽 탐지 방법을 이용하여 실제 VoIP 네트워크에서 실험하여 97%의 탐지 정확도를 확인할 수 있었다.

2. 관련연구

[12]에서는 NetFlow v9을 이용하여 VoIP 트래픽을 모니터링하고, VoIP 이상 트래픽들을 탐지할 수 있는 방법을 제시하였다. [12]에서 VoIP 트래픽 모니터링을 위하여 사용된 메트릭들만을 이용하여 정상 트래픽과 유사한 이상 트래픽을 탐지하는 것은 쉽지 않다. [13]에서는 VoIP 트래픽이 네트워크상에서 쉽게 스푸핑 될 수 있으며, 패킷 암호화 프로토콜을 사용하여도 공격자가 같은 암호화 프로토콜을 사용하여 이상 트래픽을 생성할 수 있음을 보였다. 또한 인증된 SIP 메시지와 인증이 되지 않은 메시지를 구분을 통해 이상 트래픽을 탐지하는 방법도 제시하였다. 하지만 이 방법은 공격자가 스니핑한 정상 트래픽으로부터 인증 필드를 가져와 사용한다면 이를 탐지하는 것은 쉽지 않다.

[14]에서는 플로우 기반 트래픽 모니터링인 표준인 IPFIX를 이용한 VoIP 트래픽 모니터링 방법을 제안하였다. 이 논문에서는 SIP 트래픽으로부터 헤더의 필드 내용과 SDP(Session Description Protocol)[15]에 음성 트래픽 송수신을 위하여 포함되어 있는 IP 주소 및 포트번호를 모니터링하고 RTP 트래픽으로부터 QoS 메트릭들을 모니터링한다. 하지만 이들 모니터링 필드들을 이용하여 정상 트래픽과 유사한 이상 트래픽을 탐지하는 것은 쉽지 않다.

[16]과 [17]에서는 VoIP 응용 이상 트래픽 탐지를 위한 방법들을 제시하였다. [16]에서는 SIP 트래픽을 모니터링하여 정해진 규칙에 따라 이상 트래픽 유무를 탐지한다. 하지만 [16]에서 제시한 이상 트래픽 탐지 방법은 VoIP 트래픽 해킹을 통해 패킷의 내용을 복사하여 이상 트래픽을 생성할 경우 탐지하기 어렵다는 단점을 가진다. 또한, [17]은 일정 시간 동안 모니터링된 트래픽의 패킷 수를 통해 Hellinger Distance(HD) 값을 계산하고

HD 값이 1에 가까워 지면 이상 트래픽으로 탐지하는 방법이다. 하지만 [17]에서 제시된 탐지 방법은 VoIP 트래픽의 패킷 수만으로 이상 트래픽을 탐지하고 있어 VoIP 응용에서 많은 패킷을 이용한 이상 트래픽이 아닌 1~2개의 적은 패킷을 이용한 이상 트래픽 탐지는 어렵다.

3. VoIP 응용 이상 트래픽 생성

본 장에서는 무선랜을 이용한 VoIP 응용 이상 트래픽 생성 방법을 설명한다. 무선랜을 사용하는 대부분의 국내 VoIP 응용들은 패킷 암호화가 적용되어 있지 않기 때문에 공격자가 정상 트래픽을 스니핑하여 이상 트래픽 생성이 용이하다. 보안을 위하여 SIP 표준에서는 인증 필드를 제공하고 있지만, 대부분의 SIP 메시지들은 이 필드를 사용하지 않는다. 또한 인증 필드를 사용하더라도 패킷 암호화가 되어있지 않기 때문에 공격자가 쉽게 인증 필드의 내용을 복사한 후 이상 트래픽에 사용 가능하다. VoIP 응용 이상 트래픽은 정상 VoIP 트래픽을 스니핑한 후 복사한 필드를 통해 생성되므로, 평상시 사용되는 VoIP 트래픽의 내용과 매우 유사하다. 본 논문에서는 3가지 VoIP 응용 이상 트래픽을 생성한다.

3.1 CANCEL DoS 이상 트래픽

SIP에서 사용되는 request 메시지들 중에서 CANCEL 메시지는 전화 연결을 요청하는 사용자가 상대방과의 전화 연결을 취소할 때 사용된다. 이 메시지를 공격자가 생성하여 전송하면 전화 연결을 요청하는 사용자의 의도와는 상관없이 전화 연결 시도가 강제로 취소된다.

그림 1은 CANCEL DoS 이상 트래픽 생성 과정과 이상 트래픽을 수신받은 프록시 서버의 응답 메시지를 보여준다. 그림 1에서 VoIP 단말 1이 INVITE 메시지를 프록시 서버에 보내면(a), 공격자는 이를 스니핑하여 SIP 헤더 필드와 VoIP 단말의 IP 주소 등을 복사한다.

CANCEL 이상 트래픽을 생성하기 위해서 인증 필드는 필요하지 않다. 따라서 저장된 INVITE 메시지 내용 중 인증 필드를 제외한 나머지 필드를 이용하여 CANCEL DoS 이상 트래픽을 생성한다. 생성된 이상 트래픽은 SIP 헤더 뿐만 아니라 IP 및 UDP 헤더의 내용도 실제 CANCEL 메시지와 동일하다.

생성된 CANCEL DoS 이상 트래픽은 그림 1처럼 VoIP 단말 1이 아닌 프록시 서버로 전송된다(b). 프록시 서버는 공격자가 보낸 트래픽이 정상적인 CANCEL 메시지와 같은 것으로 판단하고, VoIP 단말 1에 전화 연결 시도가 취소되었음을 알리는 'Request Terminated'라는 메시지를 VoIP 단말 1에게 전송한다(c). 이를 수신한 VoIP 단말은 전화 연결 시도를 강제로 취소한다.

3.2 BYE DoS 이상 트래픽

BYE SIP request 메시지는 사용자간에 연결된 전화를 종료하기 위하여 사용된다. 공격자가 BYE DoS 이상 트래픽을 생성하여 사용자에게 전송하면 이를 수신한 VoIP 단말의 전화는 연결이 종료되고 상대의 VoIP 단말은 전화가 종료된 것을 인지하지 못하고 음성 트래픽을 계속 전송하게 된다.

그림 2는 BYE DoS 이상 트래픽 생성과정을 보여준다. 공격자는 VoIP 단말 1과 액세스 포인트 사이에서 VoIP 트래픽 스니핑을 수행한다. VoIP 단말 1이 전화 연결을 위하여 INVITE 메시지를 프록시 서버에 전송하면(a), 공격자는 이 트래픽을 스니핑하여 SIP 헤더 필드의 내용을 저장한다. 프록시 서버는 전화 연결이 성공했다는 OK 메시지나 Session Description 메시지를 VoIP 단말 1에 전송하면(b), 공격자는 이 메시지도 스니핑하여 SIP 헤더 필드의 내용을 저장한다. 두 메시지 모두 패킷 암호화가 되어있지 않기 때문에 SIP 헤더의 내용을 추출하여 저장하는 것은 어렵지 않다. BYE 메시지는 전화 연결 종료를 위하여 사용자의 인증이 필요하다. 따라서 BYE DoS 이상 트래픽의 헤더 필드는 저장된 INVITE와 OK/Session Description 메시지의 SIP 헤더 내용을 이용하여 구성되며, 이중 인증 필드는 INVITE로부터 추출된 것을 사용한다. 생성된 BYE

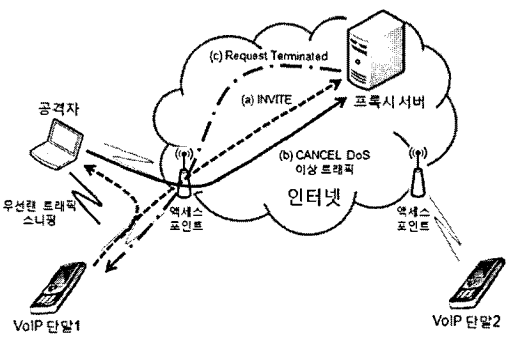

그림 1 CANCEL DoS 이상 트래픽 생성과정

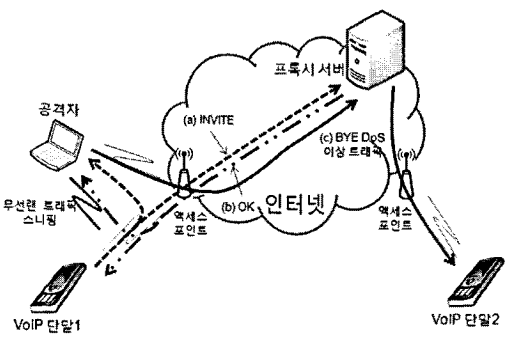

그림 2 BYE DoS 이상 트래픽 생성과정

DoS 이상 트래픽에서 출발지 IP 주소는 공격자가 VoIP 단말 1의 IP 주소를 스푸핑하여 사용한다. 생성된 BYE DoS 이상 트래픽은 프록시 서버로 전송되고(c), 이를 수신한 프록시 서버는 정상적인 BYE 메시지와 동일하다고 판단하여 VoIP 단말 2로 전송한다. BYE 메시지를 수신한 VoIP 단말 2는 VoIP 단말 1이 전화 연결 종료를 위해 이 메시지를 전송한 것으로 간주하고 전화 연결을 종료시킨다.

3.3 RTP 플러딩 이상 트래픽

RTP 트래픽은 사용자 간에 연결된 콜에서 사용자의 음성을 전송하기 위하여 사용된다. 음성 통화를 위해서 사용되는 RTP 트래픽도 패킷 암호화를 사용하지 않기 때문에 공격자가 이를 스니핑하여 얻은 IP 주소와 포트 번호 및 RTP 헤더 정보를 이용하여 이상 트래픽 생성이 가능하다. 공격자는 스니핑된 RTP 패킷을 이용하여 사용자의 음성이 인코딩 되어 있는 페이로드를 임의로 변경한 이상 트래픽을 생성하거나, 같은 RTP 패킷을 대량으로 생성할 수 있다. 이들 이상 트래픽은 전화 통화하는 사용자에게 임의의 소리가 재생될 수 있도록 하거나, 전화 통화의 품질을 떨어뜨리거나 차단하는 피해를 유발한다. 본 논문에서는 스니핑한 RTP 패킷을 복사하여 RTP 플러딩 이상 트래픽을 생성한다.

그림 3은 공격자가 RTP 플러딩 이상 트래픽을 생성하는 과정을 보여준다. VoIP 단말 1과 VoIP 단말 2 사이에 전화가 연결된 후 RTP 트래픽이 양방향으로 전송된다(a). 공격자는 VoIP 단말 1에서 VoIP 단말 2로 전송되는 RTP 패킷을 스니핑하여 RTP 헤더 정보 및 IP 주소, 포트번호를 추출하여 저장한다. 이 정보들을 이용하여 실제 사용되는 RTP 트래픽과 유사한 RTP 플러딩 이상 트래픽을 생성하여 음성 트래픽 중계 서버를 경유하여 VoIP 단말 2로 전송한다(b). RTP 플러딩 이상 트래픽의 발생으로 VoIP 단말 1과 VoIP 단말 2 사이의 음성 트래픽 전송 품질이 저하되거나 통화가 차단되는 피해가 발생한다.

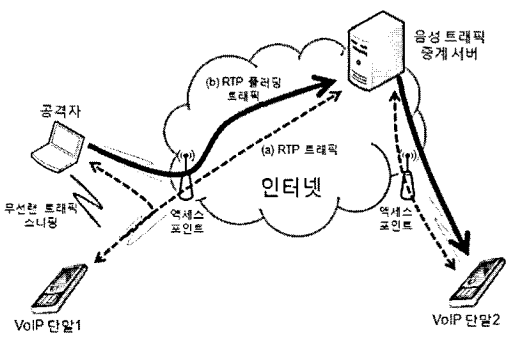

그림 3 RTP 플러딩 이상 트래픽 생성과정

4. VoIP 이상 트래픽 탐지

본 논문에서는 VoIP 응용 이상 트래픽 탐지를 위하여 플로우 기반 트래픽 모니터링 방법을 사용한다. 그림 4는 트래픽을 모니터링하고 VoIP 이상 트래픽을 탐지하는 구조를 보여준다. 이상 트래픽 탐지 구조는 액세스 포인트와 IPFIX 플로우 수집기 및 VoIP 트래픽 분석기로 구성된다. 액세스 포인트에서는 무선랜 트래픽을 캡쳐하고 이를 플로우 형태로 관리한 후 IPFIX 플로우 형태로 IPFIX 플로우 수집기로 전송한다. IPFIX 플로우 수집기및 VoIP 트래픽 분석기는 IPFIX 플로우를 수신하고 이를 디코딩하여 트래픽 모니터링 결과를 데이터베이스에 저장한다. 데이터베이스에 저장된 트래픽 모니터링 결과를 이용하여 VoIP 트래픽 분석 및 이상 트래픽을 탐지한다.

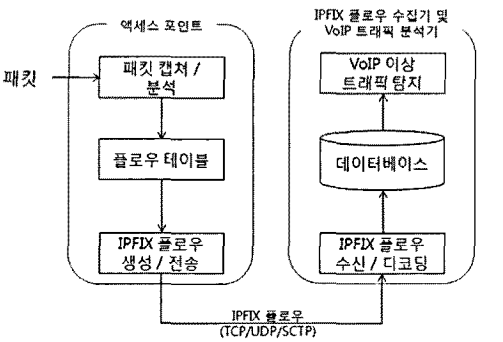

그림 4 IPFIX 플로우를 이용한 트래픽 모니터링 및 이상 트래픽 탐지 구조

그림 4의 구조를 기반으로 본 논문에서 생성한 3가지 이상 트래픽에 대한 탐지 방법을 제시한다. 생성된 VoIP 이상 트래픽은 무선랜 상에서 정상적인 VoIP 트래픽을 스니핑하여 SIP와 RTP 헤더의 필드들을 복사하여 생성되기 때문에, 정상적인 VoIP 트래픽에서 사용되는 필드들과 매우 유사하다. 하지만, 기존에 제시된 이상 트래픽 탐지 방법 등[11,12,16,17]은 본 논문에서 생성된 이상 트래픽을 탐지하기 어렵다. 따라서 본 논문에서는 VoIP에서 사용되는 SIP와 RTP 헤더 외에 다른 계층의 헤더 정보과 트래픽 통계 정보를 이용한 탐지 방법을 제시한다.

4.1 CANCEL DoS 이상 트래픽 탐지 방법

CANCEL DoS 이상 트래픽은 사용자가 상대방과 통화를 시도할 때 이를 방해하여 전화 연결을 강제로 취소시킨다. 이 때 공격자가 생성하는 CANCEL DoS 이상 트래픽은 스니핑된 SIP INVITE 메시지에서 SIP 패킷 헤더 필드들을 복사하여 생성되므로 정상적인

CANCEL 메시지에서 사용되는 SIP 패킷 헤더의 필드의 내용과 대부분 일치한다. 따라서 SIP 패킷의 헤더만으로는 정상과 이상 CANCEL 트래픽을 구분하기 어렵다.

본 논문에서는 CANCEL DoS 이상 트래픽을 탐지하기 위하여 무선랜에서 사용되는 802.11 MAC 헤더 필드 중 출발지 MAC 주소와 순서번호를 사용한다. 출발지 MAC 주소를 사용하는 것은 공격자가 전송하는 CANCEL DoS 이상 트래픽이 공격자의 MAC 주소를 사용할 수 있어 이를 비교하기 위함이다. 하지만, 잘 알려진 이상 트래픽 중에 출발지 MAC 주소를 스푸핑하여 이상 트래픽을 전송하는 것도 있다. 따라서 본 연구에서는 출발지 MAC 주소를 스푸핑하여 이상 트래픽을 전송할 경우를 대비하여 출발지 MAC 주소를 비교한 후 순서번호를 이용한 탐지 방법을 제시한다.

CANCEL 이상 트래픽 탐지를 위하여 802.11 MAC 헤더의 순서번호와 출발지 MAC 주소를 사용한다. 왜냐하면 공격자에 의해서 전송되는 CANCEL DoS 이상 트래픽의 IP, UDP 및 SIP 헤더 내용이 정상 CANCEL 메시지의 SIP 헤더 내용과 동일하기 때문이다. 따라서 본 연구에서 제시한 CANCEL DoS 이상 트래픽 탐지 과정은 일반적으로 사용되는 유선상의 라우터에서 트래픽 모니터링된 결과를 이용한 탐지가 어렵다. 따라서 802.11 MAC 헤더를 볼 수 있는 단말과 액세스 포인트 사이에서 트래픽 모니터링된 결과를 이용하여 이상 트래픽을 탐지할 수 있다.

본 연구에서는 출발지 MAC 주소가 같은 경우 순서번호를 비교하여 CANCEL DoS 이상 트래픽을 탐지한다. 순서번호를 이용하여 이상 트래픽을 탐지할 때 CANCEL 메시지가 모니터링되기 이전 플로우의 마지막 순서번호와 CANCEL 메시지의 순서번호 차이가 N 이상인 경우에 이상 트래픽으로 간주한다. 본 연구에서는 N의 값을 5로 설정하고 이상 트래픽을 탐지한다. 실험 결과 이전 패킷과 CANCEL 메시지의 순서번호 차이가 대부분 5 이상 발생하지 않았기 때문이다.

그림 5와 그림 6은 CANCEL 메시지가 정상일 때와 이상일 때 이전 패킷들과의 802.11 MAC 헤더 순서번호의 차이를 보여준다. CANCEL 메시지가 정상적으로 VoIP 단말로부터 생성되면, 이전 플로우의 마지막 순서번호와의 차이는 그림 5처럼 '5' 이하가 된다. 하지만 그림 6과 같이 CANCEL DoS 이상 트래픽이 발생한 경우는 CANCEL 메시지의 순서번호와 이전 플로우의 마지막 순서번호의 차이가 매우 크다는 것을 알 수 있다. 따라서 본 논문에서 CANCEL DoS 이상 트래픽을 탐지하기 위하여 실제 환경에서 구현할 때는 순서번호 차이의 기준을 '5'로 하였다.

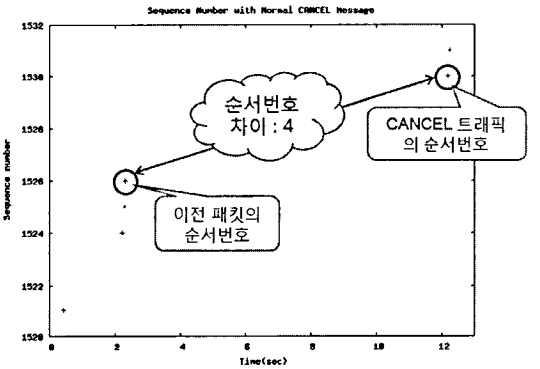

그림 5 정상 CANCEL 트래픽의 순서번호 차이

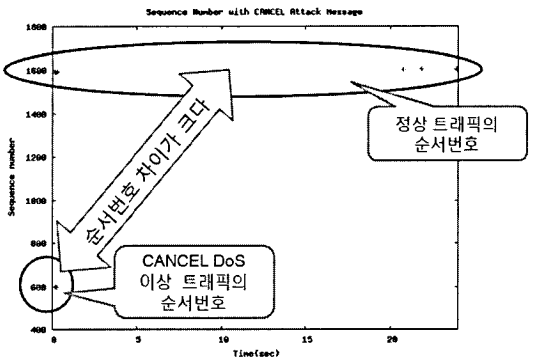

그림 6 CANCEL DoS 이상 트래픽 발생시 정상 트래픽과의 순서번호 차이

4.2 BYE DoS 이상 트래픽 탐지 방법

BYE DoS 이상 트래픽은 사용자 간 전화 통화 중에 일방적으로 한 사용자의 전화 통화를 종료시키게 한다. 이때 BYE DoS 이상 트래픽은 공격자가 무선랜을 사용하는 VoIP 응용에서 송수신되는 SIP 메시지들 중 INVITE와 OK 또는 Session Description 메시지를 스니핑하여 생성된다. 특히, BYE 메시지의 SIP 헤더는 사용자의 인증을 위하여 전화 연결시 사용된 인증 키를 포함한다. 공격자는 INVITE 메시지로부터 인증 키값을 얻어 BYE DoS 이상 트래픽을 생성한다. BYE DoS 이상 트래픽도 스니핑된 정상 SIP 트래픽을 이용하여 생성되므로 정상 BYE 메시지에서 사용된 헤더의 내용과 매우 유사하다. 따라서 기존에 제안된 BYE DoS 이상 트래픽 탐지 방법을 적용하기 어렵다. 본 연구에서는 BYE DoS 이상 트래픽을 탐지하기 위하여 RTP 트래픽을 모니터링한 결과를 이용한다.

본 연구에서 BYE DoS 이상 트래픽을 탐지하기 위하여 모니터링된 RTP 플로우의 타임스탬프를 이용한다. BYE 트래픽이 발생한 후 한 방향의 RTP 트래픽이 일

532	11.091487	168.188.46.123	123.142.134.167	RTP	PT=ITU-T G.711 PCMA, SSRC=0xC35D836, Seq=60530, Time=47040
533	11.110255	168.188.46.123	123.142.134.167	RTP	PT=ITU-T G.711 PCMA, SSRC=0xC35D836, Seq=60531, Time=47200
534	11.114599	123.142.134.22	168.188.46.123	SIP	Request: BYE sip:7082687729@192.168.1.101:5060;maddr=168.188
535	11.130573	168.188.46.123	123.142.134.167	RTP	PT=ITU-T G.711 PCMA, SSRC=0xC35D836, Seq=60532, Time=47360
536	11.151188	168.188.46.123	123.142.134.167	RTP	PT=ITU-T G.711 PCMA, SSRC=0xC35D836, Seq=60533, Time=47520
537	11.217930	168.188.46.123	123.141.134.22	SIP/SDP	Status: 200 OK, with session description
538	11.228063	123.142.134.22	168.188.46.123	SIP	Request: ACK sip:7082687729@192.168.1.101:5060;maddr=168.188
539	11.454392	168.188.46.123	123.142.134.22	SIP	Status: 200 OK

그림 7 정상 BYE 트래픽과 RTP 트래픽의 타임 스탬프

정 시간 이후에도 계속 발생한다면 이 BYE 메시지는 이상 트래픽으로 간주된다. BYE 메시지를 전송하고 난 직후의 RTP 트래픽에 대한 타임스탬프 정보를 이상 트래픽 탐지 알고리즘에 적용하지 않는 이유는 실제 환경에서 BYE 메시지가 발생한 후에도 2~3개의 RTP 패킷이 전송되었기 때문이다. 따라서 그림 8에 제시된 것처럼 N초 후에 RTP 트래픽이 존재할 경우 모니터링된 BYE 메시지는 이상 트래픽으로 간주된다.

BYE 이상 트래픽 탐지를 실제 환경에서 구현하기 위해 본 논문에서는 N을 1로 설정한다 왜냐하면 대부분의 VoIP 응용이 BYE메시지를 전송한 후 RTP 트래픽을 전송하지만 그림 7처럼 RTP 트래픽이 0.5초 이내에 전송되었기 때문이다.

4.3 RTP 플러딩 이상 트래픽 탐지 방법

RTP 플러딩 이상 트래픽은 사용자간에 전화 통화의 품질을 떨어뜨리거나 차단시킨다. 본 논문에서는 이 이상 트래픽 탐지를 위하여 RTP 헤더의 SSRC와 순서번호를 이용한 방법을 제시한다.

RTP 헤더의 SSRC 값은 사용자 간에 전화통화를 하는 동안 변경되지 않는다. 따라서 모니터링된 RTP 플로우 내에서 SSRC 값이 바뀐 적이 있다면 이는 RTP 이상 트래픽이 발생한 것이다. 하지만 공격자가 RTP 패킷을 스니핑하여 이상 트래픽을 생성하므로 정상 트래픽의 RTP 헤더에 포함되어 있는 SSRC값을 사용하게 되면 이상 트래픽을 탐지하지 못한다. 따라서 본 연구에서는 RTP 헤더의 순서번호를 사용한 이상 트래픽 탐지 방법을 추가한다.

RTP 헤더의 순서번호를 이용하여 이상 트래픽을 탐지하기 위하여 모니터링된 RTP 플로우 내에서 첫번째, 마지막 패킷의 순서번호와 최대, 최소 순서번호를 비교한다. 그림 10에서 순서번호를 이용하여 이상 트래픽을 탐지할 경우 2가지가 존재한다. 이는 RTP 헤더에서 순서번호는 2 바이트를 사용하여 0~65,535까지 사용 가능하기 때문에 순서번호가 65,535를 넘어가게 되면 다시 '0'부터 시작한다. 이 때의 환경을 이상 트래픽 탐지에도 적용하기 위하여 그림 10처럼 순서번호가 65,535를 넘었을 때와 아닐 때 이상 트래픽 탐지를 위한 순서번호 비교를 다르게 제시한다.

5. 실험환경

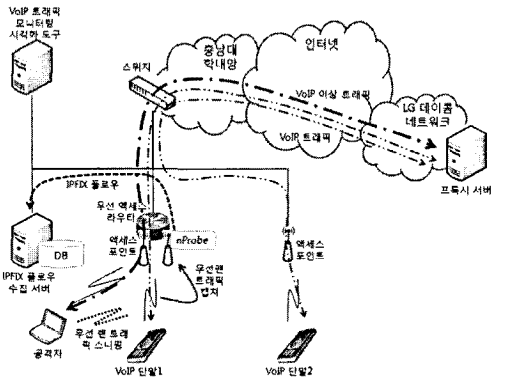

그림 8 VoIP 이상 트래픽 생성 및 탐지를 위한 실험환경

그림 8은 VoIP 이상 트래픽 생성 및 탐지를 위한 실험환경이다. VoIP 이상 트래픽 생성은 VoIP 단말 1과 무선 액세스 라우터의 액세스 포인트 사이에 공격자를 설치하여 무선랜 트래픽을 스니핑할 수 있도록 한 후 공격자가 VoIP 이상 트래픽을 생성하여 프록시 서버로 전송하도록 한다.

VoIP 이상 트래픽 탐지를 위하여 VoIP 트래픽을 IPFIX 기반으로 트래픽 모니터링을 수행하였다. VoIP 트래픽의 모니터링은 VoIP 단말 1과 연결된 무선 액세스 라우터에서 수행된다. 무선 액세스 라우터에서는 802.11을 사용하는 무선랜 트래픽을 모니터링하기 위하여 액세스 포인트로 사용되는 무선랜 인터페이스외에 PCI 타입의 무선랜 카드를 추가로 장착하였다. 이를 이용하여 VoIP 단말 1과 액세스 포인트 사이에 송수신되는 무선랜 트래픽의 모니터링이 가능하다.

본 실험환경에서 사용된 무선 액세스 라우터는 리눅스(커널버전: 2.6.19)를 설치하고 2개의 무선랜 카드(모델명: 3com SL-3055)를 사용하였다. 공격자 PC도 리눅스(커널버전: 2.6.18)이 설치되어 있으며, 트래픽 스니핑을 위한 무선랜 카드(모델명: 시스코 AIR-CB21AG)와 이상 트래픽 전송을 위한 무선랜 카드(모델명: ZIP WLB2154 USB)를 사용하였다. 또한, 인터넷 전화기는 LG 데이콤에서 제공되는 단말을 사용한다. 사용된 VoIP 단말의 모델은 WPU-7700이고, 펌 웨어 버전은 1.5.8 121 C이다.

무선 액세스 라우터에서 트래픽을 모니터링하고 IPFIX 플로우를 생성하기 위하여 수정한 nProbe[18]를 사용하

였다. 수정된 nProbe에는 VoIP 트래픽 및 802.11 무선랜 트래픽을 모니터링하기 위하여 추가된 IPFIX 템플릿을 적용하였다. nProbe를 통해 전송된 IPFIX 플로우는 IPFIX 플로우 수집 서버로 전송되며, 이 서버에서는 IPFIX 플로우를 수신하고 디코딩하기 위하여 802.11 트래픽과 VoIP 트래픽 모니터링 결과를 디코딩할 수 있는 기능이 추가된 libipfix[19]를 사용하였다. IPFIX 플로우 수집 서버에서 트래픽 모니터링 결과를 저장하기 위하여 mysql[20]을 사용하였다.

6. 실험결과

본 장에서는 VoIP 이상 트래픽 탐지 결과를 보여준다. VoIP 이상 트래픽 탐지 결과를 보이기 위하여 본 논문에서는 Precision, Recall 및 F-score를 사용한다[21]. Precision은 탐지된 이상 트래픽 중에 실제 이상 트래픽이 얼마나 있는지를 나타내며, Recall은 전체 트래픽 중에서 이상 트래픽을 얼마나 잘 탐지하는지에 대한 척도를 나타낸다. F-score는 이상 트래픽 탐지 방법의 전체 정확도를 보여준다. 본 논문에서 제시한 세 가지 이상 트래픽을 탐지한 결과 전체 F-score가 97%로 측정되었다. Precision, Recall 및 F-score 계산 방법은 공식 (1)~(3)과 같다.

$$Precision = \frac{True\ Positive}{(True\ Positive + Fase\ Positive)} \quad (1)$$

$$Recall = \frac{True\ Positive}{True\ Positive + False\ Negative} \quad (2)$$

$$F-score = \frac{(2 \times Precision \times Recall)}{(Precision + Recall)} \quad (3)$$

표 2는 세 가지 VoIP 이상 트래픽에 대한 Precision, Recall 및 F-score를 측정한 결과를 보여준다. 본 실험에서 CANCEL DoS 이상 트래픽 탐지를 위하여 89개의 이상 트래픽이 포함된 381개의 CANCEL 플로우를 생성하였다. CANCEL DoS 이상 트래픽 탐지 결과 F-socre가 97.69%로 측정되었다. F-score 계산시에 사용되는 Precision과 Recall은 각각 100%, 95.5%로 측정되었다. 이 실험 결과는 탐지된 이상 트래픽 중에서 이상 트래픽이 아닌 것은 없었지만, 생성된 이상 트래픽 중 일부를 탐지하지 못했기 때문이다. 본 논문에서 CANCEL DoS 이상 트래픽을 탐지하기 위하여 [22]에 제시된 방법을 수정하여 이용하였다. [22]에서는 출발지 MAC 주소가 스푸핑된 이상 트래픽을 탐지하기 위하여 본 논문에서 적용한 것처럼 802.11 MAC 헤더의 순서번호를 이용하였다. [22]에서는 모든 802.11 패킷의 순서번호 차이를 계산하여 이상 트래픽을 탐지하여 높은 정확도를 보였지만, 본 논문에서는 IP 패킷들 사이의 순서번호를 이용하여 탐지하기 때문에 [22]에서 제시된 정확도와 차이를 보였다. 따라서 더 정확한 CANCEL DoS 이상 트래픽 탐지를 위하여 순서번호의 차이로 설정되는 값을 적절히 조절할 수 있는 방법이 필요하다.

BYE DoS 이상 트래픽은 전체 755개의 BYE 플로우를 생성하였으며, 118개의 BYE DoS 이상 트래픽이 포함되어 있다. BYE DoS 이상 트래픽 탐지 결과 F-score가 96.13%로 측정되었다. 측정 결과에서 Recall은 94.92%로, 118개의 이상 트래픽 중에서 112개의 이상 트래픽만을 탐지하였다. 또한 Precision은 97.39%로 탐지된 이상 트래픽 중에서 일부 정상 트래픽이 이상 트래픽으로 분류되는 결과를 보였다. 이와 같은 오차의 발생은 BYE DoS 이상 트래픽 탐지시 RTP 트래픽의 타임스탬프와 연동하여 탐지하기 때문에 이 시간을 조절하면 본 논문에서 제시한 탐지 방법을 이용하여 정확하게 BYE DoS 이상 트래픽을 탐지가 가능하다.

RTP 플러딩 이상 트래픽은 810개의 RTP 플로우 중에 103개가 포함되어 있다. 이를 탐지한 결과 F-score가 98.09%로 측정되었다. 측정된 F-score의 결과에서 Recall은 100%로 전체 이상 트래픽을 모두 탐지하였지만, Precision은 96.26%로 일부 정상 트래픽을 이상 트래픽으로 오인하였기 때문이다. 이와 같은 이유는 RTP 플러딩 이상 트래픽 탐지에서는 RTP 헤더의 순서번호를 모니터링한 결과를 이용하기 때문에 이를 계산할 때 일부 트래픽이 정상 트래픽으로 오인되는 결과도 있었다. 순서번호의 비교를 정확하게 비교할 수 있도록 수정한다면 본 논문에서 제시한 RTP 플러딩 이상 트래픽 탐지 방법을 이용하여 정확한 탐지가 가능할 것으로 기대된다.

7. 결 론

국내에서 사용되는 대부분의 SIP/RTP 기반의 VoIP 응용들은 패킷 암호화를 통한 보안 정책을 사용하지 않기 때문에 공격자가 패킷 스니핑을 통한 이상 트래픽 생성이 용이하다. 또한 무선랜 환경에서 사용가능한

표 2 VoIP 이상 트래픽 탐지 결과

공격 종류	총 플로우 수	공격 플로우 수	Precision(%)	Recall(%)	F-score(%)
CANCEL DoS	381	89	100.00	95.50	97.69
BYE DoS	755	118	97.39	94.92	96.13
RTP 플러딩	810	103	96.26	100.00	98.09
총 계	1,946	310	97.72	96.77	97.24

VoIP 응용들이 널리 보급되고 있어 액세스 포인트와 VoIP 단말사이에서 공격자가 쉽게 VoIP 패킷을 스니핑하고 이상 트래픽 생성이 가능하다. 본 논문에서는 실제 VoIP 네트워크상에서 정상 VoIP 트래픽을 스니핑하여 CANCEL/BYE DoS 및 RTP 플러딩 이상 트래픽을 생성하였다. 또한, 생성한 이상 트래픽을 탐지하기 위한 방법을 제시하였다.

생성한 이상 트래픽을 탐지하기 위하여 본 논문에서는 IETF에서 플로우 기반 트래픽 모니터링 표준으로 제시한 IPFIX를 이용하여 트래픽 모니터링을 네트워크상에서 수행하였다. 수집된 트래픽 정보를 이용하여 VoIP 응용 이상 트래픽 탐지 방법을 제시하였다. 본 논문에서 제시한 이상 트래픽 탐지 방법은 SIP/RTP 헤더 정보, 트래픽 통계 정보 및 802.11 MAC 헤더 정보를 사용하였다.

본 논문에서 제시한 플로우 기반 이상 트래픽 탐지 방법을 이용하여 VoIP 이상 트래픽을 발생시키는 공격자의 IP 주소를 관리하여 향후 이 IP에서 발생하는 이상 트래픽 탐지 및 사전 차단에 유용할 것으로 예상된다. 하지만 본 논문에서 생성한 이상 트래픽은 패킷 암호화가 되지 않은 정상 VoIP 트래픽으로부터 사용자의 정보를 추출하여 생성되기 때문에 TLS, IPSec 및 SRTP와 같은 패킷 암호화 기술의 도입이 필요하다. 패킷 암호화 기술을 적용하면, 공격자가 정상적인 사용자의 정보의 추출이 쉽지 않기 때문에 정상적인 사용자인것처럼 VoIP 패킷 생성 및 전송 방지가 가능하다.

본 논문에서 제시한 VoIP 이상 트래픽 탐지 방법은 네트워크상의 라우터나 스위치로부터 트래픽을 모니터링하고 이를 이상 트래픽 탐지 서버내의 데이터베이스에 저장한 것을 이용한다. 따라서 이상 트래픽이 탐지되는 시점은 트래픽을 라우터에서 수집하고 이상 트래픽 서버로 전송하는 시간이 반영되기 때문이 이 시간만큼 사용자가 VoIP를 사용하는 순간과 차이가 발생한다.

참 고 문 헌

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

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

[3] http://www.asiae.co.kr/news/view.htm?idxno=2009093011543343825.

[4] 정재훈, "인터넷전화(VoIP) 보안위협 및 대책", KTOA (한국통신사업자연합회), 통신연합 47호, 2008. 11.

[5] http://kr.ahnlab.com/company/pr/comIntroKoNDView.ahn?B_SEQ=143229.

[6] M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman, "The Secure Real-time Transport Protocol(SRTP)," IETF RFC 3711, Mar. 2004.

[7] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol," IETF RFC 2401, Nov.

[8] T. Dierks, E. Rescorla, "The Transport Layer Security (TLS) Protocol," IETF RFC 5246, Aug. 2008.

[9] D. Geneiatakis, T. Daguklas, G. Kambourakis, C. Lambrinoudakis, S. Gritzalis, K. S. Ehlert, D. Sisalem, "Survey of Security Vulnerabilities in Session Initiation Protocol," *IEEE Communications Surveys & Tutorials*, vol.8 no.3, pp.68-81, 2006.

[10] H. Son, Y. Lee, "An Anomaly Traffic Detection Method for VoIP Applications using Flow Data," PAM 2009 Student Workshop, Apr. 2009.

[11] J. Quittek, T. Zseby, B. Claise, and S. Zander, "Requirements for IP Flow Information Export (IPFIX)," IETF RFC3917, Oct. 2004.

[12] C. Lee, H. Kim, K. Ko, J. Kim, H. Jeong, "A VoIP Traffic Monitoring System based on NetFlow v9," *International Journal of Advanced Science and Technology*, vol.4, pp.1-9 Mar. 2009.

[13] K. Darilion, "Analysis of a VoIP Attack," IPCom, Oct. 2008.

[14] S. Anderson, S. Niccolini, D. Hogrefe, "SIPFIX: A Scheme For Distributed SIP Monitoring," *IEEE IM*, pp.382-389, June 2009.

[15] J. Rosenberg and H. Schulzrinne, An Offer/Answer Model with the Session Description Protocol (SDP), IETF RFC 3264.

[16] A. Lahmadi, O. Festor, "SecSip: A Stateful Firewall for SIP-based Networks," *IEEE IM*, pp.172-179, June 2009.

[17] H. Sengar, H. Wang, D. Wijesekera, S. Jajodia, "Detecting VoIP Floods Using the Hellinger Distance," *IEEE Transactions on Parallel and Distributed systems*, vol.19, no.6, pp.794-805, June 2008.

[18] L. Deri, "nProbe: an Open Source NetFlow Probe for Gigabit Networks," TERENA Networking Conference, 2003.

[19] libipfix, http://ants.fokus.fraunhofer.de/libipfix/.

[20] mysql, http://www.mysql.com/.

[21] C. Goutte and E. Gaussier, "A probabilistic Interpretation of Precision, Recall and F-score, with Implication for Evaluation," ECIR, *LNCS 3408*, pp. 345-359, 2005.

[22] F. Guo, and T. Chiueh, "Sequence Number-based MAC Address Spoof Detection," in *Proceedings of 8th International Symposium on Recent Advances in Intrusion Detection(RAID 2005)*, Sep. 2005.

손 현 구

2007년 충남대학교 전기정보통신공학부 컴퓨터전공 학사. 2009년 충남대학교 컴퓨터공학과 석사. 2009년~현재 충남대학교 컴퓨터공학과 박사과정. 관심분야는 인터넷 트래픽 측정, 이상 트래픽 탐지 등

이 영 석

1995년 서울대학교 컴퓨터공학과 학사 1997년 서울대학교 컴퓨터공학과 석사 2002년 서울대학교 컴퓨터공학부 박사 2002년~2003년 University of California, Davis 방문연구원. 2003년~현재 충남대학교 전기정보통신 공학부 컴퓨터전공 부교수. 관심분야는 차세대 인터넷, IPv6, 인터넷 트래픽 측정 및 분석