VoIP 공격 탐지기술

연재순서

1. 행위기반 봇넷 탐지기술
2. 알려지지 않은 스파이웨어 탐지기술
3. VoIP공격 탐지기술
4. 알려지지 않은 신종 인터넷 웜 탐지기술
5. 악성코드 사전 탐지기술
6. IP 스푸핑 탐지기술

Voice over IP(이하 VoIP)는 저렴한 요금과 국제 전화의 용이성 등으로 인하여 그 사용률이 급증하고 있다. 이 VoIP에서 전화 연결을 맺을 때 사용하는 Session Initiation Protocol(이하 SIP)에서 일어날 수 있는 위협을 논하고 그에 대한 탐지 방법을 알아본다.

글 · 서동원 고려대 컴퓨터보안연구실 연구원, 이희조 고려대 교수

요즘 들어 050, 030, 070으로 시작하는 전화를 받아보지 못한 사람은 거의 없을 것이다. 위의 국번들은 모두 VoIP 서비스 사업자들이 사용하는 번호로서 정부 및 여러 가지 서비스 업체들이 주로 사용한다.

이런 국내 VoIP 서비스 시장은 2009년까지 연평균 성장률 54%를 기록해 2009년에는 9689억원 규모를 형성할 것으로 전망된다. 이런 추세는 전 세계적으로도 비슷해서 2008년에는 VoIP 서비스 사용자들이 약 2억명이 될 것으로 예상했다. 또한 VoIP 서비스는 전화뿐만 아니라 원격 화상 회의, 인스턴트 메시지, SMS 등의 기술들과 결합하고 기존의 인터넷망을 이용함으로써 국내 전화는 물론 국제 전화까지도 무료 혹은 아주 저렴한 가격에 제공함으로써 진화를 거듭하고 있다. 그런데 이것은 다른 관점에서는 VoIP 서비스가 앞으로 여러 보안 문제에 직면하게 된다는 것과 다름이 아니다.

사실 VoIP 소프트웨어의 취약성을 점검해주는 툴들이 몇몇 있기는 하지만 이들 대부분은 단순히 여러 예상되는 취약성들을 나열하여 보고서 형식으로 보여 주는 것이 그친다. 이러한 취약성들로부터 안정적인 VoIP 서비스를 위해서는 현재의 서비스를 방해하지 않으면서도 특정 위험 요소들을 탐지할 수 있는 VoIP 서비스 디자인이 필수적이라고 할 수 있다. 본문에서는 VoIP 중에서 SIP를 이용한 서비스의 이해를 도울 수 있는 배경 지식과 일어날 수 있는 위협들을 알아보고 이 위협에 어떻게 대처할 수 있는가에 대해 알아보도록 하겠다.

SIP-VoIP 배경지식

우선 VoIP 서비스라고 앞에서 언급하다가 SIP를 이용한 VoIP 서비스에 초점을 맞춘다고 했는데 도대체 SIP가 무엇이고 어떤 역할을 하는지 궁금할 수도 있을 것이다. 이에 대해 간단히 설명을 하면, 우선 VoIP 서비스는 쌍방간의 접속을 통한 미디어 서비스인 만큼 연결을 맺기 위한 규약(프로토콜)이 필요하다. 바로 이 연결 프로토콜중의 한 표준이 Session Initiation Protocol, 즉 SIP인 것이다. 다른 대표적인 VoIP 연결 프로토콜로는 H.323이 있다. SIP는 H.323보다 연결을 맺는 과정이 간단하고 HTTP처럼 패킷의 헤더정보가 일반 텍스트로 되어있어서 쉽게 인터넷 환경에 적용을 할 수 있다는 이점이 있다.

또한 H.323보다 연결 부하가 적다는 점 때문에 많은 기능들을 제공해야하는 현재의 VoIP 사업자들에게는 SIP가 매력적인 프로토콜로 자리매김을 하고 있다. 두 프로토콜에 대한 자세한 비교와 정보는 Packetizer라는 사이트의 VoIP웹페이지에서 에서 얻을 수 있다.

그러면 앞에서 설명한 연결 프로토콜은 SIP를 사용한다고 했

을 때, 연결 후에 사람의 음성을 전달 할 프로토콜도 필요할 것이다. 그것이 바로 Real-time Transport Protocol(RTP)이다. SIP는 연결의 맺고 끊음을 담당하는 반면에 RTP는 멀티미디어 데이터(음성, 영상등)의 전송을 담당하는 프로토콜이다. 이해를 돕기 위해 SIP-VoIP 서비스에서 전화의 연결과정에 대해 간략하게 살펴보기로 하자.

그림1에서 보면 UAC(User Agent Client)가 UAS(User Agent Server)에게 전화를 요청(INVITE)한다. UAS가 INVITE 메시지를 받게 되면 Ringing 메세지를 전송함으로써 INVITE 메시지의 수신을 알린다. 후에 UAS가 전화 요청을 수락하면 OK 메시지를 UAC에게 전송하고 서로 간에 ACK를 주고받음으로써 세션 연결은 성립이 된다.

그 후에는 RTP가 미디어 스트림의 전송을 도맡아서 처리하게 되고 어느 한 쪽이 BYE 메시지를 전송하게 되면 세션 연결은 종료된다. 어떻게 생각하면 당연하고 간단한 일들을 SIP와 RTP라는 두 규약에 따라서 왠지 복잡하게(?) 처리하는 것 같기도 하다. 하지만 이것이 끝이 아니다. 오늘의 요점인 SIP 메시지의 내부를 한 번 들여다보면 더욱 복잡하다는 것을 알 수 있다.

SIP의 여러 메시지 중 INVITE 메시지의 내용을 보면 메시지 헤더 부분에는 누가 누구에게 어떤 메시지 종류(여기서는 INVITE)를 보내고자 하는지, 메시지 바디부분에는 RTP로 미디어 스트림 전송 시에 오디오 코덱의 종류와 사용할 포트 정보가 있다.

이에 대한 자세한 정보는 RFC 3261과 RFC 2237 문서에 정리되어 있다. 여기서 한 가지 주목할 만 한 점은 TCP/IP 등 다른 네트워크 프로토콜들과는 다르게 메시지의 헤더와 바디가 일반 문자로 되어있다는 것이다. 이것은 서비스의 구현에 편리하게 작용할 수도 있지만 보안상으로는 취약할 수도 있다.

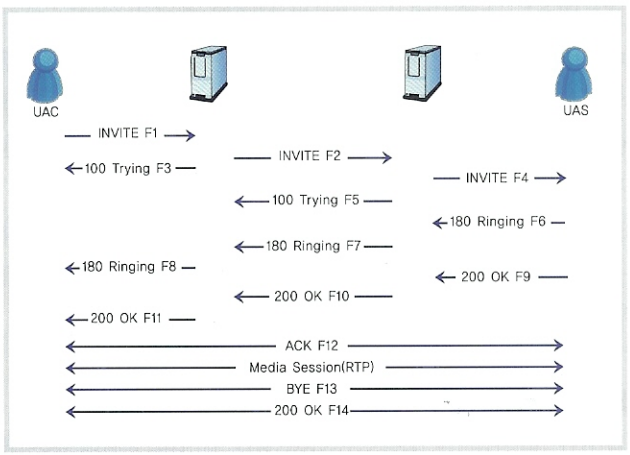

그림 1. SIP 연결 과정

위협 모델

SIP-VoIP 서비스에서는 어떠한 위협들이 있을 수 있는지 알아보자. 사실 VoIP 서비스는 앞에서 말한 것처럼 SIP와 RTP가 서로 역할을 나누어 맡고 있기 때문에 그 위협 또한 SIP 기반 위협, RTP 기반 위협 두 가지로 나누어 볼 수 있다. 본문에서는 SIP 기반 위협들을 다루기로 하고 RTP 위협들에 대한 것들은 간단히 언급만 하기로 한다.

① SIP 기반 위협

우선 SIP 기반 위협들은 크게 비정상 메시지 공격(Malformed message attack), SIP 플러딩 공격(SIP flooding attack), 스푸핑 공격(Spoofing attack), 이렇게 세 가지로 나누어 볼 수 있다.

- 비정상 메시지 공격 : SIP의 헤더와 바디 내용이 일반 문자로 되어있다는 점을 이용하여 다른 문자들로 삽입, 변조 혹은 삭제하는 것이다. 예를 들면 엄청난 수의 공백 문자를 넣어 오버플로우 예외를 발생시킨다거나 특수문자(한자어나 non-ASCII)를 넣어 이에 대응하지 못하는 VoIP 서비스의 오동작을 유발할 수 있다.
- SIP 플러딩 공격 : SIP 메시지를 대량으로 보내어 VoIP 사용자나 사업자가 정상적인 서비스를 이용 혹은 제공하지 못하게 하는 것으로, 일반 네트워크에서 DoS(Denial of Service)와 비슷한 개념이라고 볼 수 있다. 하지만 연결 요청, 즉 INVITE 메시지 플러딩인 경우 수신자의 전화기가 불통이 될 뿐만 아니라 전화 벨이 계속 울리는 등 아주 난처한 상황을 유발 할 수도 있기 때문에 그 심각성이 높다.
- 스푸핑 공격 : 발신자의 IP나 URI(Uniform Resource Identifiers, VoIP 서비스에서는 ID와 같은 개념)를 변조하여 공격자의 신분을 숨기거나 변조하는 것을 말한다. 사실 이 위협은 IP를 사용하는 모든 서비스에서 겪는 것이므로 다른 여러 논문에서 그 대응 방안들을 언급하고 있다. SIP-VoIP에서의 위협과 대처법에 초점을 맞추기로 한 본 문의 범주에는 벗어나므로 다루지 않기로 하겠다.

② RTP 기반 위협

- RTP 플러딩 공격 : 미디어 스트림을 대량으로 수신자에게 전송시켜 정상적인 서비스 이용을 방해한다.
- VoIP Spam : SPIT(Spam over Internet Telephony)으로 알려진 VoIP Spam 공격은 요즘들어 빠르게 확산되고 있다. 상업적인 목적으로 자동화 시스템을 이용하여 불특정 다수에게 다량의 전화 연결을 시도하는 것이다.
- MITM(Man-In-The-Middle) : 공격자가 송신자와 수신자의 중간에 위치하여 도청, 감청등을 행한다.

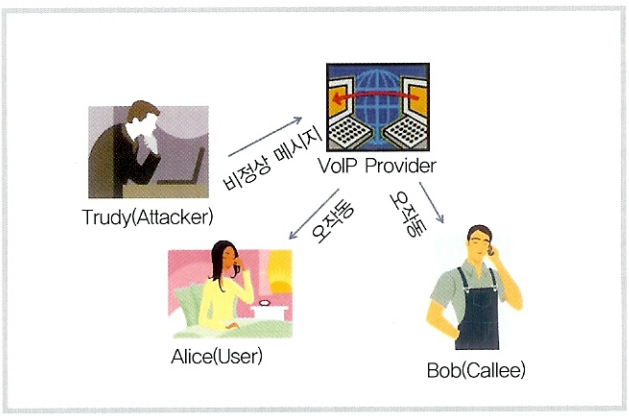

그림 2. 비정상 메시지 공격의 예

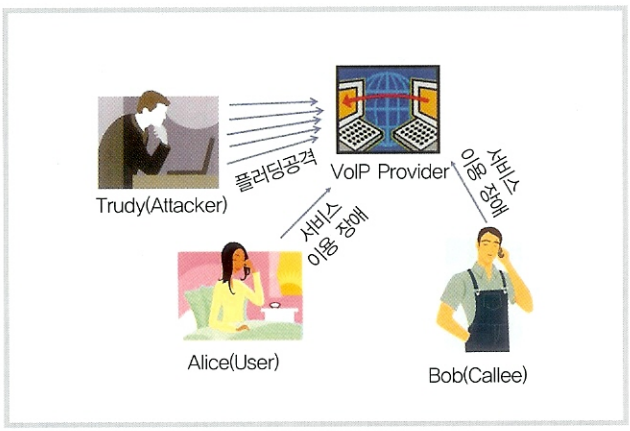

그림 3. SIP 플러딩 공격의 예

SIP-VoIP 위협 탐지 방법

앞에서 나열한 위협들 중에서 SIP 기반 위협에는 크게 세 가지가 있고 그 중 본문에서 초점을 맞출 비정상 메시지 공격과 SIP 플러딩 공격에는 어떠한 대처법이 있을 수 있는지 알아보자.

우선 위의 두 가지 공격에 대해 탐지할 수 있는 메카니즘의 모듈들과 순서는 각 호스트에서 SIP 패킷이 송수신될 때마다 비정상 메시지인지 판별이후 정상적인 SIP 형태를 갖춘 패킷들만을 분석하여 그 SIP 패킷이 어떤 세션 소속인지를 판단한다. 그 후에는 해당 세션에 과도한 메시지의 송수신이 있었는지 판단하여 해당 SIP 패킷을 통과 시킬 것인지 차단할 것인지를 결정하게 된다. 각 모듈에 대한 설명은 아래와 같다.

① Malformed SIP detection module
- 해당 SIP 패킷이 올바른 형태를 갖추고 있는지 룰 매칭 엔진에서 검사를 하게 된다. 룰 매칭 엔진은 정규 표현식을 이용하여 해당 패킷을 정해진 규칙과 비교 검사한다.

② Session management module
- 해당 SIP 패킷을 분석하여 어느 세션에 속한 패킷인지를 판단한다. IP 주소, URI, 포트번호등으로 판단하며 처음 송수신되는 SIP 패킷이라면 새 세션을 만들게 된다.

③ SIP flooding detection module
- 해당 SIP 패킷이 속한 세션에서 과도한 SIP 메시지 송수신이 있는지를 State transition model과 상한 기준선(Threshold)을 사용하여 판단한다.

④ Error management module
- 해당 SIP 패킷의 검사 결과를 토대로 패킷의 통과, 사용자에게 경고, 패킷의 차단 중 어떤 것을 실행할 것인지 판단한다.

사실 위의 4가지 모듈중에서 ②와 ④는 ①과 ③의 원활한 작동을 위한 부가적인 모듈이다. 따라서 본 메카니즘의 탐지 핵심 모듈이라 할 수 있는 ①과 ③의 설명을 자세히 하도록 하겠다.

Malformed SIP Detection Module

비정상 메시지인지 여부를 판단하는 이 모듈에서 가장 중요한 아이디어는 RFC 3261에서 규정한 250여 가지가 넘는 ABNF(Augument Backus-Naur Form)규칙들을 컴퓨터 언어에 적용할 수 있도록 정규 표현식으로 바꾸는 것이다.

예를 들면 RFC 3261의 SIP 규칙 중에 port=1*DIGIT이라는 것이 있다. 이 의미는 포크는 한 자리 이상의 숫자로 이루어져야 한다는 것이다. 이것을 정규 표현식으로 바꾸면 port=/d+가된다.

당연한 이야기 일지 모르지만 이러한 규칙들이 여러 개 합쳐져서 하나의 혹은 여러 개의 SIP 메시지들의 형태를 잡아주게 되는 것이다. 하지만 이 규칙에도 오류가 있다는 것을 이미 발견한 사람도 있을 것이다. 그것은 바로 포트 번호는 0~65535의 범위 내에서 존재한다는 것이다. 그래서 포트 규칙을 보다 안정성 있게 바꾼 식은 port=/d{1,5}이다.

포트번호는 숫자이면서 1~5자리 이내의 수여야 된다는 것이다. 물론 이 식도 99999와 같은 예외 가능성도 있기 때문에 완벽한 것은 아니다. 하지만 숫자이기만 하면 무조건 가능한 (심지어는 음수까지도) 원래의 RFC 규칙에 비한다면 훨씬 안전하다고 말할 수 있다.

표 1은 RFC 3261의 여러 규칙들을 위와 같은 아이디어를 적용하여 보안성 있는 정규 표현식으로 바꾸어 본 것들이다. 해당 규칙에 대한 원래 식들은 RFC 3261에 기술되어있다.

SIP Flooding Detection Module

과도한 SIP 메시지 송수신이 있는지를 검사하기 위해서는 보통 허용 상한선(Threshold)를 두고 그 선을 초과했는지 여부

표 1. Secure SIP 규칙 예

Secure RFC3261 regular expressions
user:((#alphanum#|₩_|₩-){1,12})
callid:(#ASCII#{1,50}(₩@(₩₩₩.*){1,32})?)
SIP_Version:((SIP₩/₩d₩.₩d){7,9})
extension_method:(#ASCII_NAME#{1,20})
protocol_version:(₩d{1,2}₩.₩d{1,2})

〈출처: 2006 국가정보보호백서, 국정원, 정보통신부〉

를 보고 판단하게 된다. 하지만 SIP에서는 여러 종류의 메시지가 있고 이 종류에 따라서 플러딩 검사를 하는 것이 효율적이 되는데 이를 이용하기 위해 RFC 3261에 있는 State transition model을 사용했다.

이러한 State transition model은 INVITE 메시지 송신 경우, INVITE 메시지 수신 경우, Non-INVITE 메시지 송신 경우, Non-INVITE 메시지 수신 경우의 네 가지로 나누어지는데 본문에서는 첫 번째 경우만 소개했다. 나머지 경우에 대한 State transition model은 RFC 3261에 자세히 기술되어 있다.

실험 및 관련 연구

비정상 메시지 탐지 실험을 하기 위해 인터넷의 공개 자료인 PROTOS test-suite:c07-sip를 사용했다. 이 테스트 자료는 SIP와 SDP 비정상 메시지를 4,527개 정도를 담고 있으며 실험에서는 그중 SIP 비정상 메시지인 2,426개를 실험 자료로 사용했다.

전체 비정상 메시지 탐지 개수를 원래 RFC 규칙과 Secure 규칙을 비교해 본 결과 Secure 규칙을 적용한 것이 원래 RFC 규칙보다 더욱 좋은 탐지율을 보인다는 것을 알 수 있었다.

SIP 플러딩 공격을 재연하기 위해서 직접 SIP 패킷을 발생시키는 툴을 제작, 사용했고 공개 소프트웨어인 SiVuS를 사용했다.

SIP 패킷 전송 속도, 즉 pps(packet per second)를 다르게 했을 때 각각 몇 초 뒤에 플러딩 공격을 탐지하는지에 대한 허용 상한선은 8로 하였는데 이것은 State transition model의 시작서부터 끝까지 최대 8개의 SIP 메시지를 허용한다는 뜻이다.

이 8이라는 수치는 그동안의 정상적인 VoIP 서비스를 모니터링 한 통계를 토대로 허용 상한선을 책정하게 되며 이 상한선은 네트워크의 상태에 따라 동적으로 변하도록 했다. 1pps의 경우에는 전송속도가 매우 느리기 때문에 플러딩 공격으로 간주할 수 없고 그 다음으로 느린 3pps의 경우 약 2.4초 후에는 탐지되는 것을 알 수 있다.

사실 3pps도 플러딩 공격으로 간주하기에는 그 속도가 느리다고 할 수 있지만 이 경우에도 2.4초 후에 탐지된 다는 것은 VoIP 서비스를 제공하기에 무리가 없음을 의미한다.

이와 관련 연구로는 우선 Intrusion Detection System(IDS, 침입 탐지 시스템)이라는 것이 있는데 이것의 대표적인 예로는 Snort라는 아주 유명한 공개 IDS가 있다. Snort는 일반 네트워크 침입 탐지 시스템으로서 6,000여개가 넘는 룰을 제공하는 무료 소프트웨어이다. 하지만 Snort는 VoIP에 특화된 룰을 아직 제공하지는 않을 뿐더러, 패킷 기반의 탐지여서 세션 단위로 탐지가 이루어져야하는 VoIP 서비스에는 바로 적용하기에는 무리가 있다.

비정상 메시지를 탐지하는 기존 연구도 물론 있어왔다. 대표적으로 D. Geneiatakis 등의 연구가 있는데 이 연구에서는 SIP 메시지의 공통점을 토대로 특정 SIP 메시지가 꼭 포함해야할 것, 패킷 길이의 제한등의 SIP 메시지 포맷의 큰 틀을 제안했다. E. Chen등의 연구에서는 본 연구에서 제안한 것처럼 RFC 3261의 State transition model을 사용하여 플러딩 공격을 탐지하는 방법을 선보였다.

위의 두 연구는 각각의 VoIP 위협을 탐지할 수 있지만 본 연구는 두 개의 위협을 동시에 탐지할 수 있는 방법을 제시했으며 실제적인 사용을 위해 기존 RFC 규칙을 강화하고 정규 표현식을 도입하였으며 플러딩 탐지시 네트워크 상황을 반영한 동적 상한선을 두었다는 점에서 차이가 있다.

네트워크 종단점과 중간의 SIP Proxy에 적용

이 글에서는 요즘 높아진 인터넷 보급률을 바탕으로 그 입지를 넓혀가고 있는 VoIP 서비스 중, 앞으로 대부분의 VoIP 서비스에서 사용하게 될 SIP의 취약성과 그 탐지에 대해 알아보았다.

탐지를 하기 위해서 크게 네 개의 모듈로 구성된 메카니즘을 제안했고 이 중 비정상 메시지 탐지는 정규 표현식을 이용, SIP 플러딩 탐지는 State transition model을 사용한다는 것이 핵심적인 내용이었다.

실험 결과 비정상 메시지 탐지는 원래 RFC 규칙 보다 제안한 Secure 규칙이 26% 높은 탐지율을 보였으며 플러딩 공격도 최대 2.4초 안에 탐지함으로써 기존 VoIP 서비스에 방해가 되지 않음을 보였다. 기본적으로 실험은 호스트에서 행해졌지만 이것은 실험 결과 도출의 용이함을 위한 것이었고 본 메카니즘은 네트워크의 종단점뿐만 아니라 중간의 SIP Proxy등에도 적용되어 VoIP 서비스를 좀 더 강건하게 만들어 줄 수 있을 것이다.