情 報 保 護 學 會 誌
第17卷 第5號, 2007. 10

# VoIP 보안 취약점 공격에 대한 기존 보안 장비의 대응 분석 연구

박진범*, 백형구*, 원용근**, 임채태**, 황병우*

요 약

초고속 인터넷의 보급 확산과 IT 기술의 급격한 발전으로 우리 사회에서 인터넷 이용이 보편화를 넘어 필수적인 요소로 자리 잡고 있다. 이러한 현상에 따른 이용자 증가로 인해 최근 들어 패킷 망에 음성을 실어 보내는 VoIP(Voice Over Internet Protocol) 기술이 주목을 받고 있다. 이 기술로 인해 저렴한 통신비용 및 다양한 부가 서비스의 제공 가능성에 따라 새로운 비즈니스 모델이 증가할 것으로 예상되고 있다. 그러나 VoIP 서비스는 기존 인터넷망에서 발생할 수 있는 보안 취약성 뿐만 아니라 인터넷 전화 트래픽 통과 문제 및 VoIP 스팸이나 도청 같은 기존에 없었던 새로운 형태의 보안 이슈들이 많이 발생할 것으로 예상한다. 본 논문에서는 VoIP 신규 보안 위협을 분석하고, 분석된 보안 위협을 바탕으로 VoIP 공격 패킷 발생 도구를 구현하여 실제 공격 시 기존 보안 장비 시스템의 대응 여부에 대해서 기술하고자 한다.

## Ⅰ. 서 론

최근 인터넷의 급속한 발달과 폭발적인 확산에 따라 인터넷 이용이 보편화를 넘어 필수적인 요소로 자리 잡아 현재 광대역 통합망(Broadband Convergence Network: BcN)의 핵심 서비스로 자리 잡고 있는 VoIP는 IP망 경유를 통한 저렴한 통신비용 및 다양한 부가 서비스의 제공 가능성에 따라 새로운 비즈니스 모델이 증가할 것으로 예상되는 서비스이다.

VoIP 시스템은 기존의 전화 송수화기, 회의 장치(Conferecing Unit), 모바일 유닛 등을 비롯해 다양한 형태를 갖고 있다. 최종 사용자가 갖춰야 할 장비 말고도 VoIP 시스템은 호 처리기(Call Processor)/호 매니저, 게이트웨이, 라우터, 침입차단시스템, 프로토콜 등을 비롯한 다수의 구성요소를 포함한다. 이들 구성요소 중 대부분은 데이터 네트워크에서도 각 구성요소에 해당하는 컴포넌트가 있지만, VoIP 성능을 위해 일반 네트워크 SW/HW를 기반으로 특정 VoIP 구성요소가 추가 보완되어야 한다. 현재 인터넷의 확산에 따라 네트워크를 통한 외부 침입의 가능성이 더욱 커졌고, 내부 사용자에 의한 정보 유출 및 파괴 등이 계속 증가하고 있는 추세이다. 각종 보안 시스템을 이용하여 컴퓨터 시스템 및 네트워크를 보호하지만 해킹 기법 또한 지능화, 다양화 되어 단순한 접근제어나 침입차단만으로는 VoIP 단말 IP의 유동적인 변동과 미디어를 위한 Port의 동적 할당 등으로 인해 동적으로 구성 가능한 파라미터를 가진 네트워크에는 동적 구성 파라미터의 실행할 곳이 많이 존재 하므로, 침입자에게 잠재적으로 공격에 취약한 요소를 광범위하게 노출 시키게 되어 실제적으로 VoIP 보안 사양을 만족시키기가 힘들어지고 있다. [1]

이에 보다 안전한 VoIP 서비스 제공을 위해서는 VoIP 프로토콜의 보안 특성과 기존 IP 기반 환경에서 현재 알려진 취약점 및 잠재적인 보안 위협 유형을 이해하고 신규 VoIP 보안 위협의 특징을 정확히 분석을

본 연구는 정보통신부 및 정보통신연구진흥원의 IT 신성장동력 핵심기술개발사업의 일환으로 수행하였음.
2006-S-043-02, VoIP 정보보호기술

* (주)유너스 ({bbackbum, hgpaek, bwhwang}@uners.co.kr)
** 한국정보보호진흥원 ({ygwon, chtim}@kisa.or.kr)

하여 신규 VoIP 보안 기능에 대한 요구사항을 도출할 필요성이 있다. 따라서 본 논문에서는 VoIP 신규 보안 위협을 분석하고, 분석된 VoIP 보안 위협을 테스트 및 검증하기 위해 실제적으로 공격 패킷 발생기를 구현하여 실제 공격 시 기존 보안 장비 시스템의 침입 및 차단의 대응 여부에 대해서 기술하고자 한다.

## Ⅱ. VoIP 보안 위협

정보통신부는 VoIP 정보보호 추진대책'을 마련하여 VoIP 정보보호에 대한 위협을 다음과 같이 5가지로 분류하여 기술대책을 제시하면서 향후 VoIP 정보보호 가이드라인 제정 및 주요 정보통신 기반시설 지정 등의 방안을 추진할 계획임을 밝혔다. [표 1]는 VoIP 정보보호 위협의 구분에 대한 내용이다.[2]
기본적으로 VoIP 서비스 환경은 기존 IP 기반 망에서 발생하는 위협을 모두 고려 할 수 있지만, 본 장에서는 VoIP 정보보호 위협 구분으로 분류 되는 VoIP 보안 위협 중 대표적인 위협들에 대해서 살펴보고자 한다.

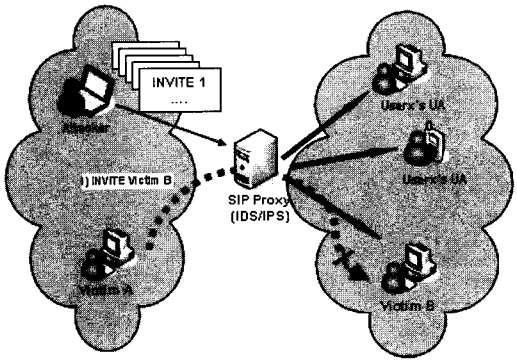
〔표 1〕 VoIP 정보보호 위협 구분

| 분 류 | 내 용 |
|---|---|
| 도 청 | LAN(Local Area Network) 및 WAN(Wide Are Network) 구간에 대한 도청, 단말 도청 |
| 서비스 거부 공격 | 시스템 및 회선 자원 고갈, 통화방해 및 중단, 해킹을 통한 시스템 장애 |
| 서비스 오용 공격 | 등록정보 변조, 관리상의 오류공격, 시스템 해킹을 통한 설정 변경 |
| 세션 가로채기 | Invite 세션 가로채기, SIP Registration Hijacking |
| VoIP 스팸 | Call/IM/Presenve 스팸,비싱 |

### 2.1 서비스 거부 공격

DoS(Denial of Service) 공격은 사용자나 기관이 인터넷상에서 평소 잘 이용하던 자원에 대한 서비스를 더 이상 받지 못하게 되는 상황을 가리킨다. VoIP 서비스에서 DoS는 일반적으로 전체 인터넷 서비스를 방해하거나 특정 VoIP 음성 서비스가 정상적으로 동작을 하지 못하게 하고, 네트워크 접속 및 서비스 등이 일시적으로 제 기능을 발휘하지 못하게 하는 것이다. 최악의 경우 수백만 명이 접속하는 인터넷 전화의 동작이 멈추는 경우도 생겨날 수 있다.

#### 2.1.1 Invite/Registration Flooding

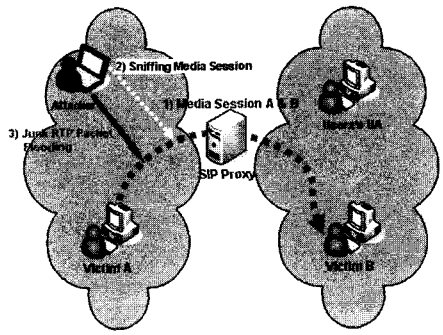



〔그림 1〕 Invite Flood 공격

기존 IP망의 TCP 연결 상에서의 SYN Flood와 유사한 공격 유형이다. 기존 IP망의 보안 요소인 TCP 공격 이외에 일반적인 UDP 서비스 시에도 DoS 공격에 취약하다. 1분에 수 천 개의 다량의 INVITE SIP 메시지를 보내어 공격 대상 사용자는 지속적으로 전화벨이 울리게 되어 사용자의 Softphone이 다운되는 등, 정상적인 업무가 불가능하게 되고, Proxy Server의 과다한 Response 응답으로 인해 회선 자원의 고갈을 야기 시키게 된다. Registration Flood 경우도 공격자에 의한 임의의 가상 사용자에 대한 지속적인 Registration 요청으로 인해 Proxy Server 및 Registrar의 시스템 자원을 고갈 시키게 된다.[3]

#### 2.1.2 RTP Flooding

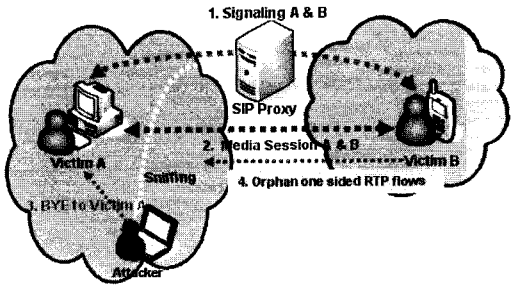
SIP를 이용한 초기 호 접속 설정 관련의 Signal을 두 사용자(User Agent)간 상호 교환을 한 후 실질적으로 음성 및 비디오 등 media 전송에 관련 있는 RTP 패킷을 이용한 공격 방법으로 Garbage header 와 payload를 RTP packet 안에 변경 및 주입 시켜 유효하지 않는 Junk RTP 패킷을 다량으로 보냄으로서 실제 콜 실행을 지연시키고 통화 품질을 저하 시키거나 Softphone을 reboot 시키는 공격 유형이다.




〔그림 2〕 RTP Flood 공격

### 2.1.3 BYE 메시지 공격

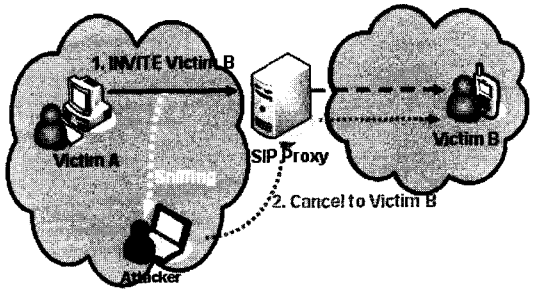
SIP signaling packet은 평문 텍스트로 구성이 되므로 위·변조를 쉽게 할 수 있다. 공격자가 합법적인 사용자의 INVITE message를 Sniffing 하여 To/From Tag, Call-ID 등 규격에 맞는 위조 BYE message를 생성한 후 두 사용자(User Agent) 간의 정상적인 호 세션이 이루어 졌을 경우 공격자는 SIP의 위조된 BYE message를 임의의 공격대상(Victim A)에게 요청을 하여 현재 이루어지고 있는 통화를 강제적으로 종료시키는 공격 유형이다.[7]




〔그림 3〕 BYE 메세지 공격

### 2.1.4 CANCEL 메시지 공격

BYE 메시지 공격과 유사한 방식으로 두 사용자(User Agent)간의 통신이 이루기 위한 세션 요청으로 INVITE message 혹은 이전에 요청을 했었던 Request message에 대한 취소를 할 경우 사용자는 Cancel Message를 요청하게 된다. 공격자는 공격대상(Victim A)이 세션 설정을 요청 할 경우 공격대상(Victim B) 에 대한 200 OK 응답 메시지를 받기 전에 위조된 Cancel Message를 보내게 되어 정상적인 통신이 이루어 지지 못하게 하는 공격 유형이다.




〔그림 4〕 Cancel 메세지 공격

### 2.1.5 De-Registration 공격

공격자가 현재 REGISTER 되어 Online 되어 있는 공격대상자들로 하여금 강제적으로 De-Register를 하여 해당 사용자들의 Registration 정보를 주기적으로 삭제 시킬 수 있는 공격이다.

[그림 5]는 일반적으로 사용자가 로그아웃 등, 현재 자신의 접속을 끊고자 할 경우 Proxy Server에 전송하는 REGISTER 메시지를 나타낸다.

```
REGISTER sip:192.168.0.200 SIP/2.0
Via: SIP/2.0/UDP 192.168.0.11;branch=puW0KrfUL1zdLC
From: 9080<sip:9080@192.168.0.200>;tag=pKVkGUaWij
To: 9080 <sip:9080@192.168.0.200>
Call-ID: VDrWudtzz1Rh@192.168.0.11
CSeq: 123456 REGISTER
Contact: *
Max_forwards: 70
User Agent: X-Lite release 1011s stamp 41150
Content-Type: application/sdp
Expires: 0
Content-Length: 0
```

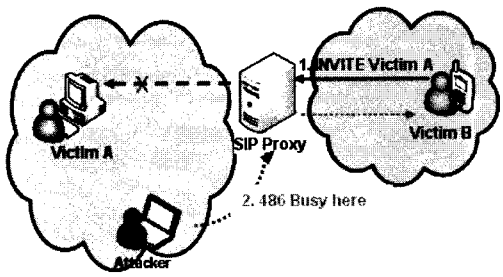
〔그림 5〕 De-REGISTER 메시지

### 2.1.6 Response Code 공격

[그림 6]과 같이 공격자는 다른 공격대상(Victim B)의 INVITE 요청에 대해서 요청 대상(Victim A)이 현재 Busy 상태임을 알리는 위조의 486 Busy here 응답 메시지를 공격대상(Victim B)에게 재전송 시켜 실제적으로 정상적인 세션이 이루어 지지 못하도록 하는 공격 유형이다.[4]

### 2.2 서비스 오용 공격

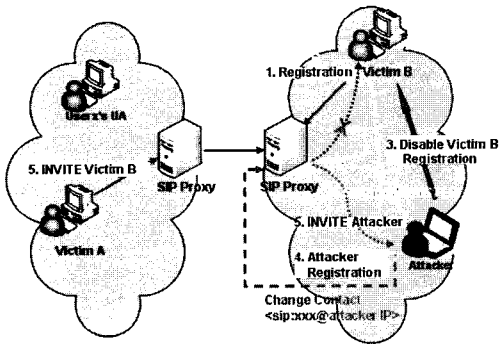
정상적인 사용자의 등록정보를 조작하거나 추가시켜 인증을 받지 않은 사용자를 정상적인 사용자처럼 등록해 서비스를 이용하는 공격이라 할 수 있다.




〔그림 6〕 Response Code 공격

#### 2.2.1 Registration Hijacking

공격자가 정상적인 사용자(Victim B)의 합법적인 REGISTER 메시지의 정보를 이용하여 실제 유효한 사용자로 가장하여 위치 정보의 내용을 담고 있는contact 정보란에 자신의 주소를 변경 후 등록하여 SIP registrar가 잘못된 정보로 업데이트 되어 실제적인 해당 사용자(Victim B)에게 call 세션 접속 요청을 하면 변경된 공격자의 주소로 call 이 전달 되게 하는 공격 유형이다. [5-6]



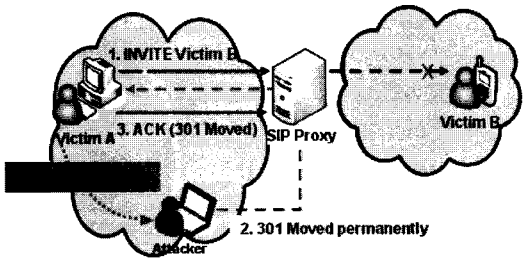

〔그림 7〕 Registration Hijacking

### 2.3 세션 가로채기

호 설정 과정이나 사용자 등록 과정에 공격자가 개입해 사용자의 세션 제어권한 등을 획득하는 공격이며, 이를 통해 도청, 서비스 오용공격 등 2차적인 공격을 유발할 수 있다. [그림 7]의 Registration Hijacking 공격도 세션 가로채기의 한 공격 분류라고 할 수 있다.

#### 2.3.1 Session Hijacking

일종의 Redirect Sever의 기능에 대한 공격으로 공격




〔그림 8〕 Session Hijacking

대상(Victim A)이 한 사용자에게 INVITE 메시지를 요청하였을 경우 요청 사용자의 정보 위치가 바뀌었음을 알리기 위해서 공격자는 위조된 301 Moved Permanently 응답 메시지를 강제로 전송하여 공격 대상(Victim A)은 301 Moved Permanently 응답 메시지의 변경된 공격자의 주소로 다시 INVITE 요청을 하여 공격자는 세션을 가로 채어 통화 정보 및 음성 통화 내용을 도청 할 수 있고 사용자간의 통화를 강제 종료 할 수 있는 2차적인 공격을 유발 할 수 있는 공격 유형이다.[3]

## Ⅲ. 테스트 및 검증

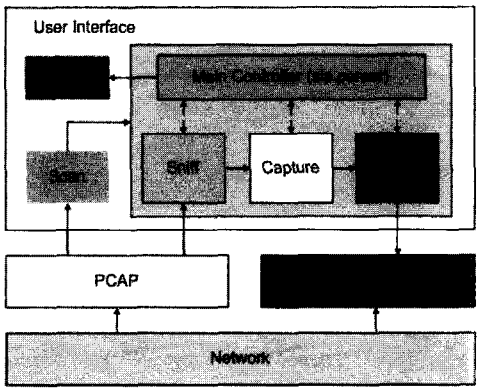
2장에서 살펴본 VoIP 보안 위협을 바탕으로 실제 테스트 및 검증을 하기 위한 VoIP 공격 패킷 발생 도구를 구현하여 공격 시 기존 보안 장비 시스템의 대응 여부에 대해서 분석해 보았다.

### 3.1 VoIP 공격 패킷 발생 도구 구현

VoIP 보안 위협의 실제 테스트 및 검증을 하기 위한 VoIP 공격 패킷 발생 도구를 구현하여 공격 시 기존 보안 장비 시스템의 대응 여부에 대해서 분석해 보았다.

〔표 2〕 공격 패킷 발생 도구 실행 환경

| OS | | Microsoft Window XP |
|---|---|---|
| Compiler | | Microsoft Visual studio VC++ 6.0<br>Microsoft Platform SDK 2003 |
| Additional Libraries | Sniff | Pcap for win32 |
| | Generate | Libnet for win32 |
| | SIP Parser | Libosip2-2.2.2 |



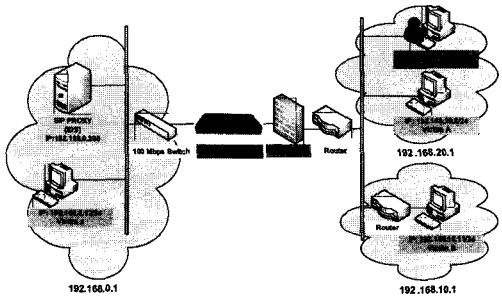

〔그림 9〕 시스템 구성 요소

[표 2]에서는 공격 패킷 발생 도구 실행 환경을 나타내고 있다. [그림 9]는 전체적인 시스템 구성 요소를 보여 주고 있고, 각 시스템 구성 모듈에 대한 자세한 기능들은 다음과 같다.

- User Interface : 사용자에게 공격 명령이나 각 모듈을 위한 parameter를 입력 받고, 결과를 보여준다.
- Main Controller : 사용자로 받은 입력에 대하여 해당 모듈을 호출하여 처리하거나, 모듈의 결과를 분석하여 사용자에게 보여준다. 각 모듈을 control 한다.
- Sniff : 사용자가 지정한 IP/PORT에 맞는 SIP packet을 감시한다.
- Capture : 각 공격유형에 맞는 SIP Packet을 capture한다.
- Generate : 각 공격에 해당하는 SIP Message를생성 한다.
- Scan : 해당 범위의 모든 host를 scan하여 현재공격 가능한 SIP host를 찾는다.
- PCAP : Promiscuous mode로 kernel을 동작시켜network의 모든 packet을 감시한다.
- LIBNET : Generate모듈을 통해 만들어진 공격packet을 network을 통해 전송한다.
- Log : 각 모듈의 동작을 log로 남긴다.

### 3.2 테스트 환경

VoIP 공격 패킷 발생 도구를 이용하여 실제 테스트 및 검증을 하기 위한 전체적인 테스트 베드 구축 사항은 [그림 10]과 같다.




〔그림 10〕테스트 베드 구성도

#### 3.2.1 Proxy Server와 SIP UA

본 논문 테스트 시 SIP 기반의 VoIP 통신을 이용하였다. 이를 위해 서비스를 해주는 SIP Proxy Server가 필요하다. 본 공격 시나리오 테스트 시 iptel.org 에서 공개용으로 제공해 주고 있는 SER (SIP Express Router)를 사용하였다. [8] SER Proxy server는 각 사용자(User Agent)에 대한 location 정보를 MySQL과 연동하여 Database 관리를 하여 동작하고 있다. 또한, 테스트 시 사용자(User Agent)및 공격 대상(Victim)으로 사용하기 위한 SIP UA softphone은 X-Lite version 3.0와 sjphone을 사용하였다.[9-10]

#### 3.2.2 기존 보안 장비 시스템

- 공개 IDS : 현재 공개 S/W 중 가장 대표적인 침입 탐지 시스템으로 패킷 캡처 라이브러리 libcap을 사용하여 패킷을 캡처하고, 수집된 패킷이 사전에 정의된 침입 탐지 Rule들에 일치하는 네트워크 트래픽을 감시, 기록, 경고할 수 있는 기능을제공해 주고 있다.[11]
- 상용 IPS : NIPS(Network Intrusion PreventionSystem)의 기능을 갖춘 보안 장비로 식별 및 인증, 접근 통제와

컨텐츠 필터링에 대한 접근 제어, 웜 바이러스 차단, 메일 바이러스 차단, 세션Shaping (P2P차단), 무결성, 감사기록 및 추적, 경보, 원격관리 및 통합 관리, 다양한 해킹 방지 등과 기본적인 Flooding, DoS 공격의 차단 기능을제공해 주고 있다.

· 상용 Firewall : 네트워크 액세스 보안 정책을 실행하고, 패킷필터링 방식인 상태 검사 기법과 Application Proxy를 결합한 강력한 Hybrid 형태의 통합 보안 시스템 성능을 제공해 주고 있다.

〔표 3〕 Invite Flooding 공격 분류

| 공격자 정보(IP/Port) | From 정보 | To 정보 |
|---|---|---|
| 고정 IP/Port | 고정 | 고정 |
| | 고정 | 동적 |
| | 동적 | 고정 |
| | 동적 | 동적 |
| 동적 IP/Port | 고정 | 고정 |
| | 고정 | 동적 |
| | 동적 | 고정 |
| | 동적 | 동적 |

## 3.3 테스트 및 검증

### 3.3.1 Invite/Registration Flooding

총 10,000개(초당 약400개)의 위조된 Invite/Register 메시지를 Proxy Server에 전송을 하였다. [표 3]와 같이 VoIP 보안 위협 특성상 Application 상의 SIP 메시지(To/From)의 위조와 함께 공격자의 동적 및 고정 IP/Port로 분류하여 공격을 시도 하였다. 특정 공격 대상은 지속적인 Invite 요청에 벨이 계속 울리게 되어 Softphone이 다운되는 등 정상적인 통화를 할 수 없게 되었다. 또한, Proxy Server는 해당 요청 메시지에 대해서 지속적인 응답 메시지를 전달함으로서 정상적인 콜 지연 처리, 시스템이 다운되는 현상이 발생 하였다.

공개 IDS 및 상용 IPS는 특정 고정 IP/Port로 부터의 비정상적인 패킷 전송률에 대해서는 일부 탐지 및 차단이 가능하였으나, 공격자가 실질적인 사용자의 IP Spoofing으로 공격시 정상적인 사용자를 공격형 패킷으로 차단을 하는 오 탐지 결과를 나타내었다. 또한, 동적인 IP/Port로 변조된 공격 패킷에 대해서는 탐지 및 차단이 불가능 하였다.

### 3.3.2 RTP Flooding

공격자(Attacker)는 [그림 2]와 같이 특정 공격 대상의 콜 세션이 성립되어 정상적으로 RTP 패킷으로 음성 통화를 주고받는 상태의 RTP 패킷을 Sniffing 하여 RTP의 Source/Destination IP와 port 및 SSRC 등의 정보를 수집한다. 수집된 정보를 바탕으로 RTP Header 정보 중 Timestamp, Sequence Number, SSRC (Synchronization Source identifier) 값을 해당 공격자 RTP 정보와 일치하는 위조된 유효하지 않는 Junk RTP 패킷을 다량으로 전송한다. 위조된 RTP 패킷의 삽입으로 인해 공격대상은 심각한 통화 품질의 저하 및 SSRC의 충돌로 인해 Softphone이 다운이 되는 현상이 발생하게 된다.

상용 IPS 및 Firewall 은 공격자가 유효하지 않는 Juck RTP 패킷을 다량으로 보낼시 해당 임계치 값(초당 50회)보다 초과 하는 경우의 패킷에 대해서 차단이 가능하였으나 다음과 같은 오탐율을 보여 주고 있다.

· 공격자의 Source IP 가 공격대상(Victim) IP와 동일할 경우 : 정상적으로 콜 세션 중인 공격대상의IP에 대해서 공격 패킷으로 오탐지 및 차단을 하여 정상적인 공격대상의 RTP packet을 전달 할수 없다.

· 공격자의 Source IP가 공격 대상(Victim) IP와 다를 경우 : 해당 임계치값 (초당 50회)보다 초과 되는 RTP 패킷에 대해서 차단 및 대응

### 3.3.3 BYE 메시지 공격

[그림 3]과 같이 공격자(Attacker)는 초기 사용자들간의 세션 연결을 위한 SIP Signaling 관련 메시지들을 Sniffing 하여 현재 콜 세션을 종료의 의미를 지닌 위조된 BYE 메시지를 생성하기 위해 필요한 정보(From/To Tag, Call-ID)들을 수집한다. 공격자는 Proxy Server를 가장하여 공격대상(Victim A)에게 위조된 BYE 메시지를 전송하여 공격대상(Victim A)는 Victim B로 부터의 통화 종료 메시지로 착각하여 현재 통화를 종료하게 된다. 다른 공격 대상(Victim B)는 강제적 통화종료를 인지하지 못하고 지속적으로 RTP 패킷을 전송하게 된다. 기존 보안 장비에서는 탐지 및 차단의 대응을 하지 못한다.

#### 3.3.4 CANCEL 메시지 공격

공격 대상(Victim A)의 모든 Invite 메시지에 대해 공격자(Attacker)는 위조된 Cancel 메시지를 보내어 상대방 사용자와 정상적인 콜 세션 성립이 이루어 질 수 없다.

#### 3.3.5 De-Registration 공격

공격자(Attacker)는 특정 공격 대상(Victim A)의 REGISTER 메시지에 대해서 Sniffing을 하여 위조된 De-Register 메시지를 생성하기 위한 정보들을 수집한다. [그림 5]와 같이 수집된 정보를 이용하여 Contact :* 와 Expire :0의 필드 값 정보를 조작하여 Proxy Server에게 전송을 한다. Proxy Server는 공격대상(Victim A)의 접속을 끊고자 하는 De-Register 메시지로 인식을 하여 location 정보에서 삭제를 하게 된다. 이로 인해 공격 대상(Victim A)에게 통화 요청을 하여도 404 Not Found라는 메시지를 Proxy Server로부터 전달 받게 되어 정상적인 콜 세션을 성립 할 수 없게 된다.

#### 3.3.5 Response Code 공격

공격대상(Victim A)에게 전달되어 지는 Invite 메시지에 대해 공격자(Attacker)는 현재 busy 상태임을 알리는 486 Busy Here의 위조된 메시지를 재전송하게 되어 공격대상(Victim A)는 모든 통화 요청에 대해서 정상적으로 전달 받을 수 없게 된다.

#### 3.3.6 Registration Hijacking

공격자(Attacker)는 사용자 등록에 사용되는 REGISTER 메시지 중 위치정보를 담고 있는 Contact 정보를 공격자 IP로 변경해서 위조된 REGISTER 메시지를 Registrar에 전송하여 공격대상(Victim B)에게 걸려 오는 전화를 가로챌 수 있다.

[그림 7]과 같이 Registration Hijacking 공격을 하기 위한 절차는 다음과 같다.

- 공격자는 공격 대상(Victim B)에 대한 등록요청의 REGISTER 메시지를 Sniffing 하여 필요한 정보를 수집하여 변조된 등록 메시지를 생성한다.
- 정상적인 사용자 공격 대상(Victim B)에 DOS 및 De-Registration 공격을 실시하여 사용자 등록을 해제 시킨다.
- 공격자는 합법적인 사용자의 등록 이전 요청을덮어 쓰기 위해 Expire 주기보다 더 짧은 주기로 REGISTER 요청들을 반복해서 발생시켜 등록 race-condition을 발생시킨다.
- 합법적인 사용자의 등록 메시지에 위치정보를 담고 있는 Contact 정보를 공격자 IP로 변경해서 위조된 REGISTER 메시지를 전송한다.
- 공격대상(Victim B)로 걸려오는 모든 전화는 변경된 공격자 IP주소로 전달되어 모두 가로챌 수있다.

#### 3.3.7 Session Hijacking

공격자(Attacker)는 공격을 하기 위한 Sniffing 동작 경우 공격대상(Victim A)이 통화 시도 메시지인 Invite 메시지를 요청하였을 경우 서버를 가장하여 통화요청 대상의 위치 정보가 바뀌었다는 변조된 301 Moved Permanently 메시지를 공격자 IP주소를 변경하여 전송하여 통화를 가로챌 수 있다. [그림 8]과 같이 공격대상(Victim A)은 공격자에게 통화요청을 다시 하게 되어 공격자는 Proxy Server로 가장을 하여 실제 수신자에게 Invite 메시지를 전달하여 통화는 정상적으로 이루어지지만 호 설정은 공격자를 경유하여 이루어지기 때문에 BYE 메시지 공격 등 2차적인 공격을 시도할 수 있게 된다.

### 3.4 테스트 결과

지금까지 살펴본 내용과 같이 신규 VoIP 보안 위협은 기존 인터넷망의 OSI 4 layer 인 TCP/IP 계층에서의 취약점을 이용한 공격들이 주요 요소를 이루는 데비해 SIP 프로토콜 등 Application 계층의 취약점을 이용한 위협요소들이 존재하고 있다.

서비스 거부 공격의 Flooding 공격 유형들은 비 정상적인 패킷 트래픽으로 인하여 기존보안 장비에서 일부의 대응이 가능하였지만 그 외 공격 유형들은 SIP 메시지의 대량성보다는 지능적인 단일 패킷의 Application 계층 조작으로 의한 공격으로 인하여 기존 보안 장비에서는 탐지 및 차단에 대한 대응을 할 수 없는 것을 확인하였다. [표 4]은 테스트 후 각 공격 유형별 기존 보안 장비의 침입 및 차단의 대응 여부를 보여주고 있다.

(o : 차단 가능 △: 차단 가능/오탐지 x: 차단 불가)

〔표 4〕 기존보안 장비 공격 대응 여부

| 공격 유형 | 공격 정보 | | | 대응 여부 | | |
|---|---|---|---|---|---|---|
| | | | | 공개 IDS | 상용 IPS | Firewall |
| INVITE/ Registration Flooding | 고정 IP/Port | 고정 | 고정 | △ | △ | x |
| | | 고정 | 동적 | △ | △ | x |
| | | 동적 | 고정 | △ | △ | x |
| | | 동적 | 동적 | △ | △ | x |
| | 동적 IP/Port | 고정 | 고정 | x | x | x |
| | | 고정 | 동적 | x | x | x |
| | | 동적 | 고정 | x | x | x |
| | | 동적 | 동적 | x | x | x |
| RTP Flooding | 위조된 RTP 삽입 | | | x | △ | x |
| BYE 공격 | 위조된 BYE 메시지 | | | x | x | x |
| Cancel 공격 | 위조된 CANCEL 메시지 | | | x | x | x |
| De-Registration 공격 | 위조된 REGISTER 메세지 | | | x | x | x |
| Response Code 공격 | 위조된 486 Busy Here 메세지 | | | x | x | x |
| Registration Hijacking | 위조된 REGISTER 메세지 | | | x | x | x |
| Session Hijacking | 위조된 301 Moved Permanently 메세지 | | | x | x | x |

## Ⅳ. 결 론

본격적인 국내 상용화 서비스 확산을 앞두고 있는 시점에서 지금까지 살펴본 내용과 같이 신규 VoIP 보안 위협은 기존 인터넷 그러나 VoIP 시스템은 기존 인터넷에서 발생하고 있는 각종 취약점을 이용한 공격뿐만 아니라 인터넷 전화 트래픽 통과 문제 및 VoIP 스팸이나 도청 같은 기존에 없었던 새로운 형태의 보안 이슈들이 많이 발생할 것으로 예상됨에 따라 안정적인 VoIP 서비스를 제공하기 위한 연구가 필요한 시점이다. [12]

본 논문에서는 안전한 VoIP 서비스 환경의 구축을 위하여 신규 VoIP 보안 위협의 특징을 정확히 분석하여 실제 테스트 및 검증을 하기 위한 VoIP 공격 패킷 발생 도구를 구현하여 기존 보안 장비의 대응 능력을 분석하였다. 이러한 분석을 바탕으로 새롭게 발생되는 보안 위협에 대해 VoIP 보안 기능의 요구사항을 도출할 필요성이 있고 인터넷전화 서비스의 안전한 서비스 환경구축을 위해 고려해야 하는 정보보호 취약성 및 위협에 대한 효율적인 대응 방안에 대해 기간·별정통신사업자·관련 제품 개발자·망 관리자에게 그 지침을 제공할 수 있는 기반이 될 것이다. 또한 일반 사용자에게는 인터넷전화 서비스에 대한 보안의식을 향상시킬 수 있는 계기가 되어 향후 VoIP 서비스가 대중화될 경우에 발생할 수 있는 각 요소별 보안 취약성 및 위협에 대비하여 보다 안정적인 서비스를 제공하는데 기여할 수 있을 것으로 기대 된다.

## 참고문헌


[1] 구자현, "VoIP 서비스 보안 취약성 분석", 한국 정보보호학회지, 제16권 1호, pp.59-63, 2006

[2] 한국정보보호진흥원, "VoIP 정보보호 가이드", Dec 2005

[3] Mark .Collier, "Voice Over IP (VoIP) Denial ofService (DoS) ", SecureLogix Corporation, 2005

[4] M. Mogno, I.Petrilli, M.Listanti, "Vulnerability inIMS-Internet interworking". INFOCOM Dept.http://www.telematica.polito.it/cour-mayeur06/papers/32-B.4.1.doc

[5] http://www.securityfocus.com/infocus/1862

[6] Mark .Collier, "VoIP Vulnerabilities Registration Hijacking", SecureLogix Corporation, 2005

[7] Muhammad Sher, Shaoke Wu, "Security Threats and Solutions for Application Server of IP Multimedia Subsystem (IMS-AS)", MonAM 2006 Workshop

[8] SIP Express Router, http://www.iptel.org/

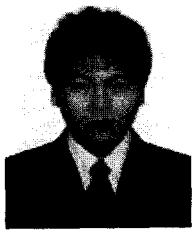
[9] X-lite, http://www.counterpath.com/

[10] SJ Labs, http://www.iptel.org/

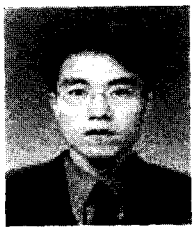
[11] Snort, http://www.snortl.org/

[12] NIST, "인터넷전화(VoIP) 구축시 보안 고려 사항", 2005.12

## 〈著者紹介〉



**박 진 범 (Jin-Bum Park)**
정회원
2003년 2월 : 호서대학교 정보통신학과 졸업
2005년 2월 : 호서대학교 정보통신 응용기술 사업과 석사
2005년 3월~현재 : (주)유너스 개발팀 대리
관심분야 : 네트워크 보안, VoIP, 통신공학, 정보보호, BcN

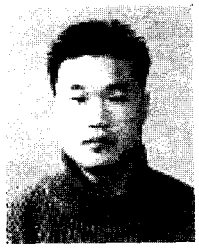


**백 형 구 (Hyung-Goo Paek)**

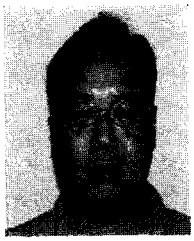
2000년 2월 : 부경대학교 전자계산학과 졸업
2q002년 2월 : 부경대학교 산업대학원 전산정보학과 석사 졸업
2004년 2월 : 부경대학교 일반대학원 전자계산학과 박사 수료
2004년 6월 ~ 2005년 1월 : (주) 나드소프트 연구소장
2005년 2월 ~ 2006년 12월 : (주) 엔지엠랩 책임연구원
2007년 1월 ~ 현재 : 유너스 개발과장
관심분야 : 네트워크 보안, 해킹, 인터넷 정보보호, 데이터베이스

**원 용 근 (Yong-Geun Won))**

2003년 2월 : 중앙대학교 전자전기공학부 졸업
2005년 7월 : 한국정보통신대학교 영상처리공학 석사 졸업
2005년 7월~현재 : 한국정보보호진흥원 응용기술팀
관심분야 : 정보보호, DRM, Watermark



**임 채 태 (Chae-Tae Im)**
2000년: 충남대학교 컴퓨터과학과 졸업
2003년 : 포항공과대학교 컴퓨터공학과 졸업
2003년 ~ 현재 : 한국정보보호진흥원 응용기술팀
관심분야 : 정보보호, 이동통신, 네트워크



**황 병 우 (Byoung-Woo Hwang)**

1998년 2월 : 포항공과대학교 전자계산과 졸업
1998년 2월 ~ 2000년 2월 : 시큐어소프트
2000년 3월 ~ 2002년 3월 : 엠브릿지 과장
2002년 5월 ~ 2002년 9월 : (주)모빌탑 과장
2002년 10월 ~ 2003년 9월 : 넷세이프 차장
2003년 11월 ~ 2006년 10월 : (주) 엔지엠랩 개발 이사
2006년 11월 ~ 현재 : (주)유너스 개발 이사
관심분야 : 네트워크 보안, 시스템 보안, 인터넷 정보보호, BcN