디지털산업정보학회 논문지 제7권 제2호-2011년 6월

SIP 플러딩 탐지 차단 실험방법에 대한 연구

최 희 식* · 박 재 표** · 전 문 석***

An Experimental Study on the Method of Detection and Blocking against SIP Flooding

Choi, Hee Sik · Park, Jae Pyo · Jun, Mun Seog

〈Abstract〉

Privacy IP hacking problems such as invasion of privacy, password cracking, voice wiretapping and internet over charged occurred, because VoIP internet voice phone service gradually spread. This thesis attempted to attack the VoIP service network by application. First use application to spoof IP address then attempted wiretap the VoIP service and sends a lot of messages to disturb service movement. At this point, we connected VoIP soft terminal, so we can operate real-time filtering operator to block the SIP Flooding offence by monitor the traffic and detect the location where it got attacked. This thesis used experiment to prove it is possible to detect the offence and defend from SIP Flooding offence.

Key Words : VoIP, SIP Flooding, Detection, Hacking, Internet Phone

Ⅰ. 서론

본 논문에서는 초고속통신망의 발달과 정부의 적극적인 육성정책으로 인터넷 사용자가 급증함에 따라 현재 가정은 물론 정부 및 일반기업, 행정기관에서도 VoIP 서비스 기반 환경을 구축하여 VoIP를 채택하고 바꾸어 나가는 추세이다.

인터넷 전화는 기존 인터넷 망을 기반으로 저렴하게 이용할 수 있을 뿐만 아니라 다양한 부가 서비스 혜택까지도 함께 누릴 수 있다는 장점으로 이용자가 늘고 있는데 반해 보안 위협에 대한 대책 수준은 아직 미비하여 VoIP 관련 전용 보안장비가 없어 공공기관의 VoIP 보안 대책 마련에 어려움이 있었다. 최근에는 가정용 VoIP는 무선랜 해킹으로 도청은 물론, 개인정보까지 침해된 사고와 제3국과 무단 통화를 시도한 인터넷전화 해킹 사고가 발생하였다.

본 논문에서는 SIP 보안 프로토콜의 취약한 Flooding 공격을 효과적으로 탐지하여 사전에 공격을 차단할 수 있도록 보안 문제점을 시사하여 해결 방안을 연구하고자 한다. 먼저, II절에서는 VoIP 정의 및 구성요소에 대해서 소개하고, III절에서는 위협 요소 및 공격방법 대해 살펴보고, IV절에서는 SIP 기반 트래픽 탐지 실험, V절에서는 결론을 통한 제시로 본 논문을 마무리 하고자 한다.

* 숭실대학교 대학원 컴퓨터학과 박사과정
** 숭실대학교 정보과학대학원 교수(교신저자)
*** 숭실대학교 컴퓨터학과 교수

Ⅱ. 관련연구

2.1 VoIP 정의

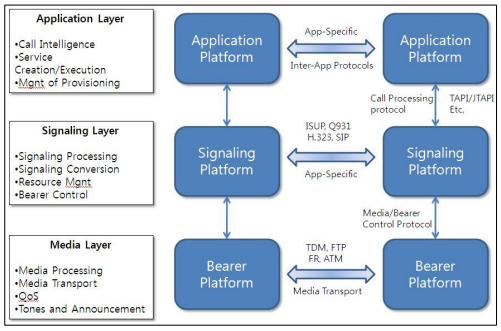
VoIP는 Voice over Internet Protocol의 약자로 지금까지 PSTN 네트워크를 통해 이루어졌던 음성 서비스를 Internet Protocol이라는 IP를 이용해 여러 가지 다양한 서비스를 제공하는 기술을 말한다. 즉, VoIP 서비스는 IP 계층을 이용한 음성 서비스 기술을 상대방 수신 측에 안전하게 전달하는 전송하는 서비스로 기술적으로는 아날로그의 신호를 디지털 신호로 변환시키는 패킷 망을 의미한다[1]. 이 때 IETF(Internet Engineering Task Force)에서 채택하고 있는 프로토콜로는 SIP(Session Initiation Protocol)라는 것이 있는데 이는 멀티미디어 통신에 있어 세션이나 호(Call)을 관리하고, IP망에서 음성 데이터를 안전하게 전송하는 응용 계층의 제어 프로토콜[2]로 멀티미디어 데이터 전송 자체보다는 Signaling을 통한 멀티미디어 통신 관리에 중점적인 역할을 맡고 있다.

2.2 VoIP 시스템의 구성요소

VoIP 시스템을 구성하는 계층은 <그림 1>과 같이 크게 3개의 계층으로 나눌 수가 있는데 응용 계층(Application Layer), 신호 계층(Signaling Layer), 매체 계층(Media Layer)으로 나누어 지며 그 역할에 대한 설명은 아래 <표1>과 같다[1, 3, 4].

<표 1> VoIP Layer

Layer	특징
Application Layer	서비스의 생성/수행 기능, 지능화된 호 처리, 서비스 관리 등을 수행한다.
Signaling Layer	호 처리, 호 변환, 자원관리, 매체 제어 등을 담당한다.
Media Layer	실제 데이터 처리 및 전달 또는 변형, 품질 보장 톤 발생 기능 등을 담당하며 음성 데이터 RTP 프로토콜을 이용하여 패킷으로 전송한다.



<그림 1> 시스템 구성 요소

2.3 SIP(Session Initiation Protocol)

SIP 프로토콜은 멀티미디어 세션이나 콜을 생성하거나 변경하고 해제할 때 사용하며, 패킷 교환 망에서 회선 교환망의 호 제어가 가능하도록 세션을 제어[5]하고 멀티미디어 컨퍼런스, VoIP, 원격 교육 등이 가능하도록 다양한 서비스와 결합하여 유연성과 확장성을 제공하고 있다. 또한 SIP 프로토콜은, SMTP(Simple Mail Transfer Protocol), e-Mail, HTTP(Hyper Text Transfer Protocol) 등과 같이 웹 기반에서 동작하고 있으며, SIP 클라이언트와 SIP 서버는 일반 클라이언트 서버 구조처럼 동일한 구조를 취하고 있는데 SIP 클라이언트와 SIP 서버의 역할은 다음과 같다[6].

2.3.1 SIP 클라이언트(Client)

① UAC(User Agent Client) : 세션 종단에 위치하며 전화를 먼저 거는 UA로써, 요청 메시지를 보내는 역할을 한다[7].

② UAS(User Agent Server) : UAC의 요청을 수신하고 응답하는 UA로써, 응답 메시지를 보내는 역할을 한다[7].

2.3.2 SIP 서버(Server)

① Proxy Server : 하나 이상의 Client 또는 서버와 통신

하며 UAC로부터 SIP 콜을 받아 호 요청을 중계하는 역할을 수행한다[4].

② Register Server : 사용자의 에이전트로부터 레지스터 요청을 수신하여 사용자의 위치 정보를 알려준다[4].

③ Redirect Server : SIP의 요청을 받아들여 Address를 매핑 관리하고, Client에게 Address를 알려주는 역할을 수행한다[4].

④ Location Server : Redirect 서버 및 Proxy 서버에게 발신자의 위치를 제공하고 Redirect Server로부터 SIP 목적지 SIP 콜 주소를 요청하면 Resolution 해주는 역할을 수행한다[4].

2.4 SIP 프로토콜 스택(Stack)

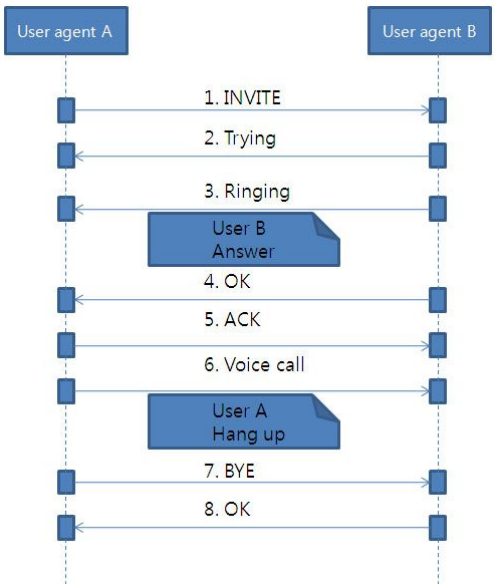
본 논문에서 구현한 VoIP 시스템의 경우 시그널링 프로토콜로 SIP를 사용하고 있으며 RTP(Real Time Protocol)을 통해 음성을 전송하고 있다. 이로 인해 VoIP 시스템이 운용되기 위해서는 SIP를 통해 호 설정이 수행되는 시그널링 채널과 음성이 전송되는 미디어 보안이 필수적이다[8]. 아래 <표 2>는 VoIP 시스템의 가장 기본적인 프로토콜 스택이다.

<표 1> VoIP Layer

User Agent	SIP Server
Application	Application
RTP/RTCP	
UDP	
IP	

2.5 Typical Call Flow

아래 <그림 2> SIP Call Flow는 먼저 UAC(User Agent Client)가 UAS(User Agent Server)에게 전화를 요청(INVITE)하면. UAS가 INVITE 메시지를 받게 된다. 이때 Ringing 메시지를 전송함으로써 INVITE 메시지의 수



<그림 2> SIP Call Flow

신을 알리게 된다. 그러면 UAS가 제대로 수신했으면 ACK Request Sign을 보내서 알리게 되고, ACK를 받은 UAC는 VoIP 연결이 성공적으로 성립됨을 확인하고 쌍방간에 통화를 한 후 통화를 종료하게 된다[9].

RTP(Real Time Transport Protocol)는 미디어 데이터(오디오, 비디오)를 실시간으로 전송하기 위한 프로토콜로 통화 메시지 종료에 대한 부분을 맡아서 처리하는데 UAC와 UAS 둘 중 어느 한 쪽이 먼저 BYE 메시지를 전송하게 되면 세션 연결은 종료하게 된다.

Ⅲ. 위협요소 및 공격 방법

VoIP는 IP 기반의 인터넷 음성 서비스로 보안 취약성이 매우 취약한 요소에 노출되어 있어, 소프트 단말기와 같은 장비를 해킹하여 악성의 공격 패킷을 전송시켜 통화 장애를 유발하고, 대량의 패킷을 발송하여 음성 데이터가 전달되지 않도록 할 수 있다. 또한 가입된 등록정보

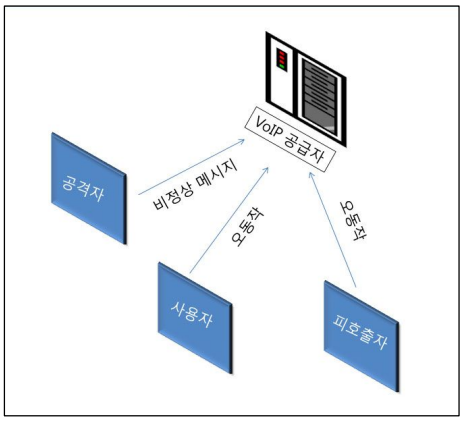
를 조작해 다른 사용자에게 통화요금을 지급하게 할 수 있는 등 VoIP를 타켓으로 SIP 기반과 RTP기반의 위협 요소가 있는데 특징은 다음과 같다[10].

3.1 SIP 기반 위협

SIP 기반 위협 요소는 크게 비정상 메시지 공격(Malformed Message Attack), SIP Flooding 공격(SIP Flooding Attack), IP 스푸핑 공격(Spoofing Attack) 등이 있는데 그 특징적 설명은 다음과 같다[11].

3.1.1 비정상 메시지 공격

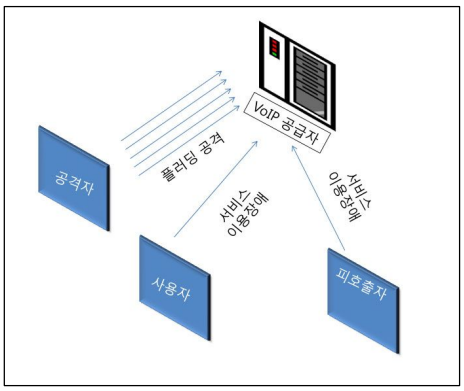
<그림 3> 비정상 메시지 공격은 SIP의 헤더 부분과 본문 내용이 텍스트로 되어있다는 점을 악용하여 본문에 이상한 문자들을 삽입하거나 내용을 삭제하여 변조시킨 후 고의적으로 사용할 수 없도록 오작동을 유발시킨다. 한 사례의 예를 들면 본문에 많은 Space의 공백을 삽입하여 Overflow를 발생시키거나 인식할 수 없는 이상한 Character(한자, 특수문자) 등을 삽입하여 대응할 수 없도록 VoIP 서비스의 과부하 및 오동작을 유발시키는 것이다[12].



<그림 3> 비정상 메시지 공격의 예

3.1.2 SIP Flooding 공격

<그림 4> SIP Flooding 공격은 SIP 메시지를 대량으로 보내어 VoIP 사용자가 정상적인 서비스를 이용할 수 없도록 하며, DDoS(Distributed Denial of Service) 공격과 비슷하게 대량의 불량 패킷을 다수의 IP 또는 특정 IP에 집중적으로 공격하여 네트워크를 마비시키는 개념이 유사하며 공격자의 위치 파악하기가 쉽지 않다[12].



<그림 4> SIP Flooding 공격의 예

3.1.3 IP 스푸핑 공격(Spoofing Attack)

IP 스푸핑 공격은 TCP/IP 프로토콜의 약점을 악용하여 IP를 속이고 조작하여 공격하는 기법으로 주로 공격자의 신분을 숨기고 정상적인 사용자로 위장하거나 발신자의 IP나 URI(Uniform Resource Identifiers) 등을 변조하여 공격한다. IP 스푸핑 공격은 주로 공격자가 불법으로 인터넷 전화요금 과금을 회피하는데 사용된다[7].

3.2 RTP 기반 위협

RTP 기반 위협 요소는 RTP 패킷을 대량으로 생성하여 사용자에게 임의의 소리를 재생하게 하거나 통화의 품질을 떨어뜨리고 통화 차단을 유발시키는 공격으로 공

격 기법에는 RTP 플러딩 공격, VoIP Spam, MITM 등이 있는데 그 특징적 설명은 다음과 같다[10].

3.2.1 RTP 플러딩 공격

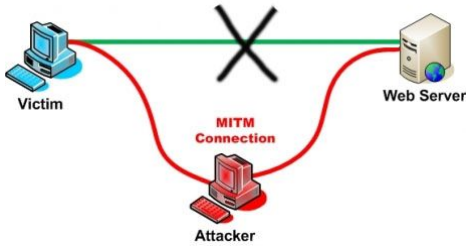
RTP 플러딩 공격은 미디어 스트림을 대량으로 수신자에게 전송시켜 정상적인 서비스를 할 수 없도록 방해하는 공격이다[10].

3.2.2 VoIP Spam

VoIP Spam 공격은 대량의 스팸 발송으로 최근에 가장 많이 알려진 공격 유형의 하나로 상업적인 목적으로 자동화 시스템을 이용하여 불특정 다수에게 다량의 전화 연결을 시도하는 공격이다.

3.2.3 MITM(Man-In-The-Middle)

MTM 공격 <그림 5>은 공격자가 서버와 사용자(Victim) 사이에 위치하여 송신자와 수신자의 통화 내용을 도청, 감청을 수행하며, 사용자(Victim)와 서버간의 연결된 통신라인에 X표시의 의미는 공격자의 방해로 서버로부터 원활한 통신 서비스가 이루어지고 있지 않고 있음을 표시하고 있다.



<그림 5> 송·수신 감청

IV. SIP기반 트래픽 탐지 실험

본 실험은 VoIP 트래픽 생성 및 탐지를 위한 실험으로 VoIP 공격자가 VoIP 이상 트래픽을 다량으로 생성하여 프록시 서버로 전송하도록 한다. 이 때 VoIP 트래픽을 탐지하여 서버에서 패킷들을 분석하여 트래픽 모니터링 결과를 판단하는 실험이다. 먼저 VoIP 공격자가 대량의 메시지를 보내게 되면 우선적으로 어느 세션에 속한 패킷인지를 판단하여 해당 IP 주소와 Port 번호 등을 분석하여 세션을 형성한다. 해당 SIP 패킷이 속한 세션에서 과도한 메시지 송수신이 있었는지를 State Transition Model과 Threshold 기준을 사용하여 검사하게 된다. 해당 SIP 패킷의 검사 자료를 기준으로 판단하여 VoIP 사용자에게 패킷 차단 실행 및 경고 메시지를 송출하게 된다.

4.1 시스템 구현 환경

본 논문에서는 <표 3>과 같이 고정 IP Port, 고정 및 동적 From 정보의 INVITE Flooding 공격에 대한 탐지 및 SIP 패킷 검사와 Module 검사에 대한 성능을 측정하기 위해 아래와 같은 시스템을 이용하였다.

<표 3> 실험 시스템 현황

SIP Proxy Server(2대)	User Agent (2대)
전화 소프트웨어 : SKYPE	S사 인터넷 전화
해킹 S/W : CAIN & ABEL	탐지 차단 S/W : 공개용 IDS (Securepoint Intrusion Detection)
O/S : Linux	O/S : Window 7
시스템 : Pentium(R) 4 CPU 3.00(GHz)	시스템 : Pentium(R) 4 CPU 3.00(GHz)
메모리 : 램 4GB	메모리 : 램 2GB

4.2 시험 절차

① 해킹 Application을 이용하여 IP를 Spoofing 한다<그림 6>.

② 고정 IP/Port 및 고정 From 정보로 Proxy Server에 INVITE 메시지를 요청하여, 1001번 전화기에 100개의 메시지를 2초에 한번 간격으로 계속 반복하여 전송한다<그림 7>.

③ 고정 IP/Port 및 동작 From 정보로 Proxy Server에 INVITE 메시지를 요청하여, 1003번 전화기에 666번의 대량의 INVITE 메시지를 전송한다<그림 8>.

④ 트래픽 패킷을 생성하여 수집된 정보를 전송한 후, 전송된 패킷을 다시 디코딩한 후 데이터베이스에 저장한다. 저장된 트래픽은 모니터링한 트래픽 결과를 분석하게 되며 탐지 여부를 판단한다<그림 9>.

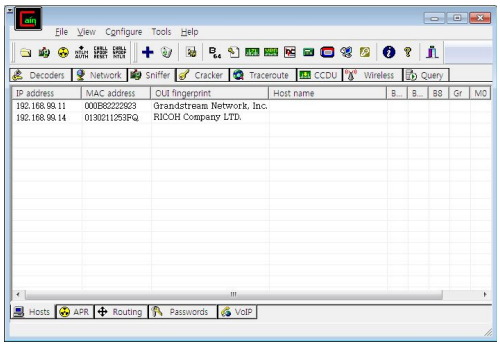
4.2.1 공격할 대상 IP 확보

<그림 6>과 같이 해킹 툴을 이용하여 공격 대상의 LAN IP를 확보하기 위해 공격자와 같은 동선상의 IP 주소 및 Port번호를 해킹하여 이상 트래픽 생성에 사용하기로 한다.

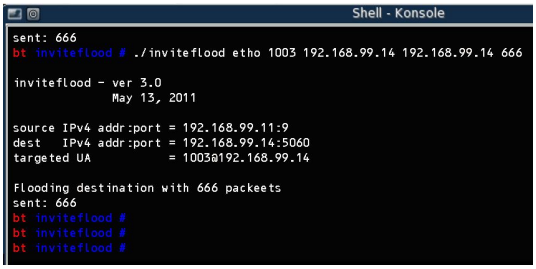
공격자는 생성된 이상 트래픽을 이용하여 사용자 간에 전화 통화 시도, 대량의 메시지 전송, 음성 품질 저하, 통화 강제 종료 등을 시도할 수 있으며 특히 대량의 메시지를 전송하여 전화 서비스를 방해할 수 있다. 본 논문에서는 <그림 7><그림 8> 실험을 통해 대량의 데이터를 전송함으로써 서비스를 방해하는 실험과 <그림 9>를 통해 VoIP 이상 트래픽 탐지에 대한 실험 결과를 보여주고 있다.

4.2.2 반복 INVITE Flooding

<그림 7>과 같이 공격자의 IP 주소를 임의로 192.168.99.1로 만든 후, 동선상의 LAN에 위치해있는 Proxy Server(192.168.99.14)를 공격 대상자로 선정한 후, 1001번 전화기로 INVITE 메시지를 계속해서 2초 간격으로 반복하여 100번 INVITE 메시지를 송출하였다.



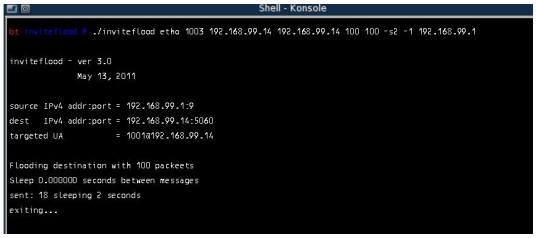
<그림 6> 해킹 툴을 이용하여 IP 확보



<그림 7> 1001번 전화기에 메시지 전송

4.2.3 대량의 INVITE Flooding

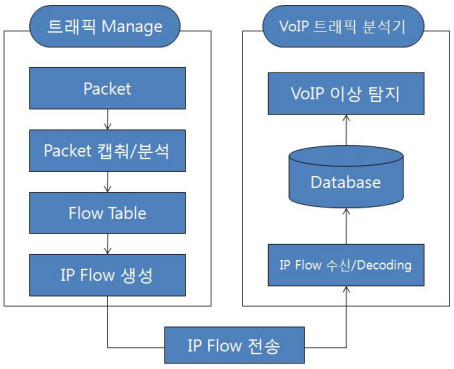
<그림 8>과 같이 공격자의 IP 주소를 임의로 192.168.99.11로 만든 후 동선상의 LAN에 위치해 있는 Proxy Server(192.168.99.14)를 공격 대상자로 선정한 후, 1003번 전화기에 666번의 대량의 INVITE 메시지를 보내게 하여 전화 서비스를 이용하지 못하도록 방해하였다.



<그림 8> 1003번 전화기에 INVITE 메시지 전송

4.2.4 트래픽 탐지

<그림 9>는 이상 트래픽을 탐지하는 구조로 패킷에 대한 트래픽을 캡처하여 이를 Flow 형태로 수집하여 관리한 후, Flow를 생성하여 전송한다. 이 때 VoIP 트래픽 분석기는 Flow를 통해 수신하여 이를 디코딩한 후 데이터를 데이터베이스에 저장시킨다. 저장된 트래픽은 모니터링 분석에 의한 결과에 따라 VoIP 이상 트래픽에 관한 탐지 정보를 생성한다.



<그림 9> 이상 트래픽 탐지

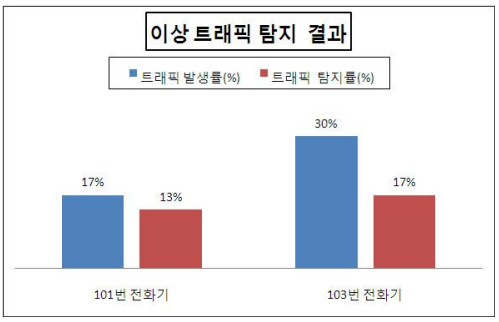
4.3 실험 탐지 분석 결과

<그림 10>은 이상 트래픽을 탐지한 분석 결과로 VoIP 단말 IP에 대해 SIP Application 계층의 메시지 헤더 필드 값의 고정 Record 루트를 통하여 특정 서버에서 고정적으로 초당 유입되는 비정상적인 트래픽 값을 탐지한 후 비정상적인 트래픽 발생에 의한 의심되는 정보를 파악하여 저장하게 된다. 또한 Unique한 Call-ID의 INVITE 메시지에 대해서도 IP가 동일한지에 대한 유무를 체크한 후, IP가 다른 경우와 계속되는 반복 Ring Signal의 경우에도 의심되는 정보로 인식하게 되면, 서버가 이를 침입으로 판단하여 IP를 차단하게 된다.

VoIP 단말 IP에 대한 비정상적인 트래픽 탐지 결과를 Output 하기 위해 트래픽 발생률(%)은 탐지된 이상 트래픽 중에서 실제로 이상 트래픽이 얼마나 발생하였는지에 대한 척도를 나타내었고, 트래픽 탐지률(%)은 전체 트래픽 중에서 이상 트래픽을 얼마나 잘 탐지하였는지에 대한 척도를 표시하였다.

$$\text{트래픽발생}(\%) = \frac{True\,Positive}{(True\,Positive + False\,Positive)}$$

$$\text{트래픽탐지}(\%) = \frac{True\,Positive}{True\,Positive + False\,\neg ative}$$



<그림 10 > 이상 트래픽 탐지 결과

V. 결론

본 논문에서는 VoIP의 SIP Flooding 위협 요소 중 인증 절차 없이 대량의 메시지를 전송하는 INVITE Flooding 공격을 시도하여 실험을 통해 어느 정도 탐지가 가능한지에 대한 성능 평가와 차단 방법으로 그 해결책을 제시하였다. 물론 UDP Flooding과 RTP Flooding과 같은 치명적인 공격을 유도하기 위해서는 훨씬 더 많은 호스트를 가지고 동시에 공격을 해야 하는 실험적인 요소가 필요하긴 했다.

본 논문에서 제안한 시 SIP 기반의 INVITE Flooding 공격들이 고정적인 IP에서는 효과성 있게 탐지하는 것이 가능하며 단말기에 치명적인 성능 감소를 초래할 수 있는 차단 기술을 제안하였다.

참고문헌

[1] 한국정보보호진흥원, "VoIP 정보보호기술 개발," 지식경제부, 2009.

[2] Thomas Porter · Michael Gough, "How to cheat at VoIp security," 2007. p. 8.

[3] 최관식, "SIP 기반의 VoIP 스팸 대응 기술 분석에 관한 연구," 숭실대학교 정보과학대학원, 2008. p. 5.

[4] 장종환, "H. 323 프로토콜을 이용한 VoIP 서비스 구현 연구," 배재대학교 정보통신대학원, 2002. p. 3.

[5] 김기영 · 서유화, "모바일 VoIP 서비스를 위한 핸드오프 알고리즘," 디지털산업정보학회논문지, 제3권, 제4호, 2007.

[6] Rosenberg, J., "A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)," RFC 3857, 2004.

[7] 이홍구, "SIP 기반의 VoIP 취약성 분석," 숭실대학교 정보과학대학원, 2007. p. 15.

[8] 신영찬 · 김규영 · 김민영 · 김중만 · 원유재 · 류재철, "VoIP를 위한 보안 프로토콜 성능 평가," 정보보호학회논문지, 제18권, 제3호, 2008.

[9] Endler & Coller, "Hacking Exposed VoIP : Voice Over IP Security Secrets & Solutions," 2006. p. 60.

[10] 손현구 · 이영석, "VoIP 이상 트래픽의 플로우 기반 탐지 방법," 정보과학회논문지, 제37권 제4호, 2010. p. 267.

[11] 이영구 · 김정재 · 박찬길, "VoIP 시스템에서 SIP를 이용한 보안 인증기법에 관한 연구," 디지털산업정보학회논문지, 제7권, 제1호, 2011.

[12] 류제택 · 류기열 · 노병희, "발생 메시지의 상한값을 고려한 SIP INVITE 플러딩 공격 탐지 기법연구," 한국통신학회논문지, 제34권, 제8호, 2009.

■ 저자소개 ■

최 희 식
Choi, Hee Sik

2011년 5월~현재 숭실대학교 대학원 컴퓨터학과 박사과정
2006년 2월 숭실대학교 컴퓨터공학(공학석사)
2007년 3월 숭실대학교 전자계산원 출강
2007년 3월 삼육대학교 출강
2008년 3월 경원대학교 출강

관심분야 : DRM, 유비쿼터스, RFID, VoIP, SNS 보안, 인터넷보안
E-mail : dali3054@ssu.ac.kr

박 재 표
Park, Jae Pyo

2010년 3월~현재 숭실대학교 정보과학대학원 교수
2008년 9월~2009년 8월 숭실대학교 정보미디어기술연구소 전임연구원
2004년 8월 숭실대학교컴퓨터과학과(공학박사)
1998년 8월 숭실대학교 컴퓨터학과(공학석사)
1996년 2월 숭실대학교 컴퓨터학부(공학사)

관심분야 : 컴퓨터보안, 유비쿼터스, 컴퓨터통신
E-mail : pjerry@ssu.ac.kr

전 문 석
Jun, Mun Seog

1991년 3월~현재 숭실대학교 컴퓨터학과 교수
1989년 University of Maryland Computer Science(공학박사)
1986년 University of Maryland Computer Science(공학석사)
1989년 Morgan State University 조교수

관심분야 : 정보보안, 전자상거래보안, 인터넷보안, 멀티미디어보안
E-mail : mjun@ssu.ac.kr

논문접수일 : 2011년 5 월 3 일
수 정 일 : 2011년 5 월 26 일
게재확정일 : 2011년 5 월 31 일