SIP 프로토콜 상태정보 기반 공격 탐지 기능을 제공하는 가상 프록시 서버 설계 및 구현☆

Stateful Virtual Proxy Server for Attack Detection based on SIP Protocol State Monitoring Mechanism

이 형 우*
Lee, Hyung-Woo

요 약

VoIP 서비스는 IP망에서 SIP 프로토콜을 이용하여 음성 데이터를 전송하는 기술이다. SIP 프로토콜은 IP망을 이용하여 다양한 음성과 멀티미디어 서비스를 제공하고 저렴한 통신 비용에 대한 장점 때문에 빠르게 보급되고 있다. 하지만 SIP 프로토콜은 IP기반 위협에 그대로 노출된다는 한계를 가지기 때문에 이에 대한 대처방안이 제시되어야 한다. 기존의 여러 보안 메커니즘이 존재하지만 새로운 방식의 SIP 공격에 즉각 대응하지 못하고, 프로토콜 서비스 지연시간의 문제와 시스템의 과부화의 단점을 해결하지 못하고 있다. 이에 본 연구에서는 기존의 프록시 서버 앞단에 새로운 가상 프록시 서버를 두어 SIP 세션에 대한 상태정보를 분석하고 비정상적인 행위를 효율적으로 탐지하는 방법을 제시하였다. 본 연구에서 제시한 상태정보 기반 가상 프록시 서버(Stateful Virtual Proxy Server) 시스템의 성능평가 결과 최소한의 트래픽 전송지연만으로도 SIP 메시지 폭주(Message Flooding) 공격을 탐지할 수 있었다.

Abstract

VoIP service is a transmission of voice data using SIP protocol on IP based network. The SIP protocol has many advantages such as providing IP based voice communication and multimedia service with cheap communication cost and so on. Therefore the SIP protocol spread out very quickly. But, SIP protocol exposes new forms of vulnerabilities on malicious attacks such as Message Flooding attack and protocol parsing attack. And it also suffers threats from many existing vulnerabilities like on IP based protocol. In this paper, we propose a new Virtual Proxy Server system in front of the existed Proxy Server for anomaly detection of SIP attack and stateful management of SIP session with enhanced security. Based on stateful virtual proxy server, out solution shows promising SIP Message Flooding attack verification and detection performance with minimized latency on SIP packet transmission.

☞ Keyword : SIP, VoIP, 공격탐지, 가상 프록시, 상태 전이도, 메시지 폭주 공격

1. 서 론

VoIP(Voice Over Internet Protocol)[1] 서비스는 IP망을 이용해 음성 데이터를 전송하는 기술이다. 이는 통신비용이 저렴하고, 다양한 부가서비스를 제공하며, 기존 IP 기반 네트워크 자원의 가용성과 효율성을 극대화 할 수 있다. 또한 물리적 위치에 구애받지 않고 인터넷망에 접속할 수 있다면 언제 어디서나 음성 전화 서비스를 이용할 수 있다는 편리함을 갖고 있다.

VoIP는 이러한 서비스를 제공하기 위해 초기에 H.323[2] 프로토콜을 사용하였다. 하지만 H.323 프로토콜은 LAN 환경에서 멀티미디어 통신을 지원하기 위해 개발된 프로토콜로 확장 네트워크의 구성

* 종신회원 : 한신대학교 컴퓨터공학부 부교수
hwlee@hs.ac.kr (제 1저자, 교신저자)
[2008/05/21 투고 - 2008/05/22 심사 - 2008/07/21 심사완료]
☆ 본 연구는 지식경제부 및 정보통신연구진흥원의 IT성장동력기술개발사업[2007-S-022-02, All-IP 환경의 지능형 사이버공격 감시 및 추적 시스템] 및 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음 "(IITA-2008-C1090- 0801-0016)"

과 대규모 사용자를 지원하는데 한계가 있었다. 또한 H.323 프로토콜은 서비스 구현이 복잡하고 호환성을 보장하지 못한다는 것이 치명적인 약점으로 인해 최근에는 이러한 단점을 보완하기 위해 SIP(Session Initiation Protocol)[1,2]가 등장하였다. 따라서 SIP는 H.323을 대체할 표준으로 급성장하고 있다.

하지만 SIP 프로토콜 역시 기존의 IP 프로토콜을 이용하기 때문에 IP 기반 공격 방법 및 위협에 그대로 노출된다는 한계를 갖고 있다. 현재 나타나고 있는 SIP 서비스의 사이버 위협 요소[3]로는 기존의 IP 기반 네트워크에서 적용 가능한 공격인 도청과 서비스 거부공격, 서비스 오용공격 등이 있다. 이러한 공격들은 SIP 프로토콜에도 적용이 가능하며 지속적으로 문제가 되고 있는 실정이다. 최근 SIP 프로토콜의 위협요소로 다양한 공격 형태가 제시되고 있지만 대부분의 방식은 SIP 프로토콜을 통해 송수신되는 메시지에 대한 변형/대체하는 공격 방식과 또는 호 설정을 차단하는 방식이 있다.

구체적으로 SIP의 헤더와 메시지 본문 내용이 일반 텍스트 문자 형태로 송수신 된다는 점을 이용하여 공격자에 의해 다른 문자들로 삽입, 변조 혹은 삭제하는 방식을 이용한 비정상 메시지 공격(Malformed Message Attack)이 가능하다. 또한 SIP 사용자나 사업자가 정상적인 서비스를 제공하는 과정에서 비정상적인 SIP 세션 패킷을 지속적으로 보내는 SIP 메시지 폭주 공격(SIP Message Flooding Attack)이 있다. 이와 같은 SIP 공격을 시도할 경우 SIP 서비스 자체의 중지 또는 오작동을 일으키게 되고 SIP 서비스에 대한 품질 저하를 가져오게 된다. 따라서 이러한 SIP 프로토콜 취약성을 이용한 공격에 대한 능동적 해결방안에 대한 연구가 절실히 필요한 실정이다.

SIP 프로토콜의 공격에 대처하기 위해 기존에 제시된 연구[4,5]를 살펴보면 (1) HTTP 인증과 같이 메시지 인증 기능을 사용하며, 재사용 공격방지와 사용자 인증 기능을 제공하는 기법, (2) SIP 메시지에 대한 암/복호화를 통한 홉 간의 신뢰구간을 형성하며 SIP 메시지의 기밀성과 무결성을 제공하는 TLS 기법 및 (3) 종단 간 SIP 사용자에게 보안기능을 제공하고, 메시지에 대한 기밀성, 무결성과 상호 인증기능을 제공하는 S/MIME (Secure/Multipurpose Internet Mail)기법 등 다양한 연구가 수행되어져 왔다.

하지만 기존의 연구들은 아직까지 새로운 공격에 대해 즉각적으로 대응하지 못하며, 지연시간과, 시스템 부하가 커진다는 단점을 가지고 있다. 또한 공격자가 다양한 공격툴(Sivus, spitter, redirectpoison 등)을 이용해 공격을 수행할 경우 이를 능동적으로 판별하거나 대처하지 못한다는 문제점이 있다.

현재 SIP 서비스를 제공하기 위해서는 프록시 서버(Proxy Server)에 사용자 등록 과정을 수행하고, 각각의 사용자(Client)는 프록시 서버를 통해 SIP 호 연결 과정을 수행한다. 이러한 과정은 실시간 데이터를 전송을 지원하기 위해 사용자간 전송서비스인 RTP(Real-time Transport Protocol) 프로토콜을 이용하기 위한 준비단계이다. 사용자는 RTP 프로토콜을 이용하여 실시간 데이터를 주고 받을 수 있게 된다. 앞의 여러 과정을 통해 SIP 서비스가 제공되며 최종 호 해제 과정에서는 다시 프록시 서버와 세션 정보를 송수신하여 호를 해제하게 된다.

따라서 SIP 프로토콜에 대한 공격은 결국 SIP 프록시 서버와 사용자간의 송수신되는 메시지에 대한 공격을 통해 이루어지게 된다. 공격자는 SIP 프록시 서버에 송수신되는 SIP 세션 정보에 대한 스니핑과 스캐닝 공격, 그리고 MITM(Man In The Middle attack) 등을 수행 할 수 있기 때문에 이에 대한 대응 방안이 제시되어야 한다.

프록시 서버와 사용자간 송수신되는 SIP 세션 정보를 암복호화할 수도 있지만 이 경우 프록시 서버의 과부하와 송수신 지연이 또다른 오버헤드가 되고 있다. 따라서 기존 SIP 기반 VoIP 서비스의 취약점을 근본적으로 해결하기 위해서는 SIP 프록시 서버와 사용자간의 전송되는 패킷에 대한 명확한 분류 및 분석 과정(SIP Stateful Inspection)이 선행되어야 하고, 이를 통해 SIP 공격을 사전에 탐지/차단할 수 있어야 한다.

따라서 본 연구에서는 SIP 서비스에 대한 보안 위협 및 취약점을 보완하기 위해 기존의 SIP 프록시 서버에 가상화된 프록시 서버(Virtual Proxy Server) 모듈을 추가하여 상태정보 기반 SIP 세션 분석 기능을 제공하고 이를 실시간으로 분석하여 공격을 탐지/차단하는 방식을 제시하였다.

본 연구의 2장에서는 SIP 기본 프로토콜과 취약점 현황을 분석하여 관련 연구의 문제점을 제시하며, 이를 해결하기 위해 본 연구에서 설계한 모델을 3장에 제시하였다. 또한 SIP 공격탐지 기법을 4장에서 제시하였다. 그리고 5장에서는 본 연구를 통하여 나온 결과를 분석하였으며 결론을 제시 하였다.

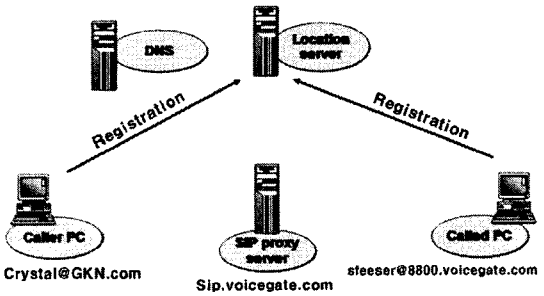
2. 관련연구

2.1 SIP 프로토콜

SIP 프로토콜[6]은 음성 및 멀티미디어 통신 세션을 생성하거나 삭제 변경하기 위한 절차를 명시한 응용 계층의 시그널링 프로토콜이다. 이는 사용자/서버 방식으로 TCP와 UDP프로토콜 모두 사용 가능하고 구현이 용이하다는 장점을 가지고 있다. SIP는 음성 통신 서비스에서의 유연성과 확장성을 제공하며 H.323에 비해 간편한 프로토콜 작동 구조로 구성되어 있다.

SIP 세션 설정 및 통신 과정은 사용자가 프록시 서버에 등록하는 과정부터 시작된다. SIP 프록시 서버는 사용자로부터 호 연결 및 해제 요청을 대행해 주는 역할을 한다.

[그림 1]에서 Location Server와 Proxy Server는 물리적으로 동일한 서버에 동작을 한다. 소규모 LAB 환경에서는 프락시 서버, Location Server, Registrar Server가 하나의 서버로 운영된다. [그림 1]에서는 각 사용자가 콜을 하기 이전에 자신의 위치정보를 Location 서버에 제공하는 그림이다. 이들 정보에는 자신의 SIP 어드레스와 IP 어드레스 정보 등이 포함된다.

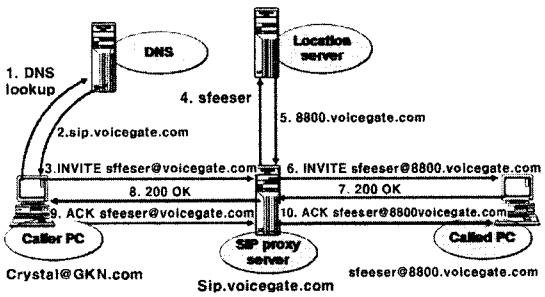


[그림 1] SIP 프로토콜 등록과정

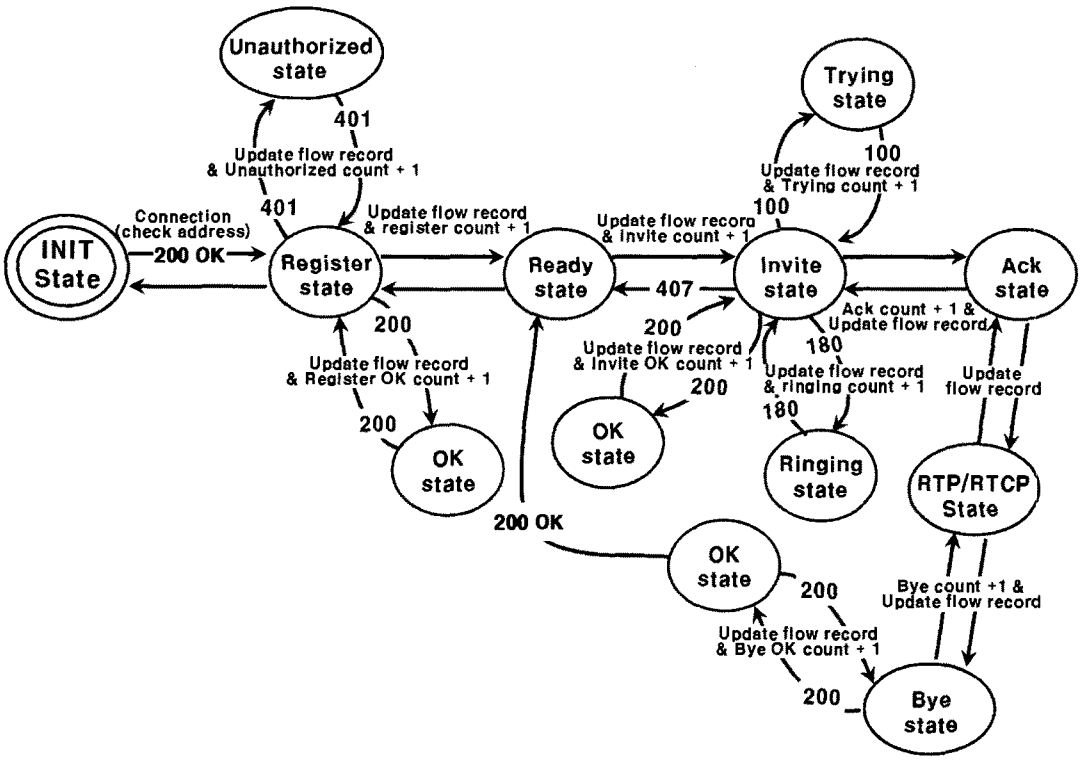
각 사용자와 서버들은 서로의 위치를 알아내기 위해 DNS와 Location Server를 통해 서로의 정확한 위치 정보를 받게 된다. 이를 이용하여 각 사용자들은 처음 Invite를 하는 경우 Location Server를 통해 필요한 상대방의 위치정보를 획득하여 사용자들이 서로 호 설정을 할 수 있도록 도움을 준다.

SIP 메시지는 TEXT 기반 메시지 형태로 구성되어있다. 구체적인 내용을 보면 기존의 HTTP 언어 형태의 메시지 구조를 사용한다. 메시지의 구분과 형태는 다음과 같다.

- Register : SIP 클라이언트들은 반드시 Registrar 서버에 자신의 위치 정보를 제공해야 한다. 즉, 자신의 SIP 어드레스와 IP 어드레스 정보 등을 등록해야 한다.
- Invite : SIP 세션을 시작할 때 즉, 콜을 만들 때 사용자(UAC)가 서버 쪽으로 전송하는 메시지이다. 경우에 따라서는 상대 사용자(UAS) 쪽으로 바로 전송 할 수도 있다.



[그림 2] SIP 프로토콜 동작



〔그림 3〕 SIP State Diagram

- ACK : 사용자는 Invite 메시지에 대한 최종 Response 메시지를 받고 그 Response에 대해 ACK를 회신한다. Response가 Success 또는 Fail 이라도 자신의 Invite에 대한 최종 Response 에 대해 ACK로 회신한다.
- BYE : 클라이언트가 콜을 종료할 때 서버에서 해당 콜이 종료되었음을 알릴 때 사용한다.

위에서 설명한 4가지 메시지 이외에도 여러 메시지를 통해 SIP 통신 과정을 지원하게 된다. 이는 대략 10단계의 호 설정 과정을 수행하며 이때 발생하는 상태코드의 순서는 정해져 있다. 이러한 메시지들의 흐름을 Diagram을 이용하여 순서대로 표현하게 되면 [그림 3]과 같이 state의 흐름을 나타낼 수 있다. [그림 3]의 경우 사용자 등록부터 통신하고 해지하는 모든 과정을 Diagram을 이용해 표현한 것이다. 이러한 과정을 다시 종류별로 4단계로 표현하게 되면 다음과 같이 표현할 수 있다.

1단계 : 자신을 등록 하는 Register 단계.

2단계 : 다른 사용자와 통화를 하기 위해 Invite를 요청하는 단계와 부가적인 Ringing, Trying, OK, ACK 단계를 통해 호 설정을 하려고 하는 단계.

3단계 : 호 설정 단계들이 마무리가 되면 RTP/RTCP 단계를 통해 사용자간 쌍방향 통신을 하는 단계.

4단계 : RTP통신 단계를 종료시키고 다시 대기상태로 들어가는 Bye, OK 단계를 거쳐 사용자는 다시 대기 상태로 유지되는 단계.

2.2 SIP 취약점

SIP 서비스에 대한 정보보호 위협[7]은 IP 기술에서 나타났었던 위협들을 그대로 상속한다. 따라서 대부분의 공격은 IP기반의 공격을 기반으로 SIP 서비스를 방해하는 형태의 공격으로 발전되고 있다.

- 도청 : 사용자의 통화 내용을 공격자가 청취할 수 있다.
- 서비스 거부공격 : 중요 SIP 서비스 관련 시스템 또는 단말에 대한 공격을 통해 SIP 서비스가 정상적으로 제공되지 않도록 한다.
- 세션 하이제킹 : SIP 프로토콜의 사용으로, 기존과 달리 새로이 대두된 위협으로써, 호 설정 과정에 개입하여 도청 또는 서비스 오용 등 2차 공격을 유발 할 수 있음.

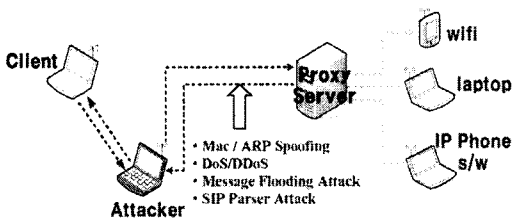
이와같은 공격들과 그 외의 공격들은 기본적으로 MITM의 중간자 공격을 기본으로 SIP 서버와 사용자들을 공격한다. 하지만 이러한 공격에 대한 대처 방안이 없다는 문제점이 대두되고 있다. 이를 대처하지 못하는 기존의 해결책은 아무 의미가 없다. 따라서 이러한 문제점을 해결 할 방안이 필요하다. 또한 공격인지 정당한 사용자의 요청인지의 여부를 분석하고, 판별할 수 있는 기법에 관한 연구가 필요하다[8].

따라서 본 연구에서는 상태정보 기반의 상태 정보 분석을 통해 MITM 공격에 확실히 대처할 수 있는 방안을 연구하였다.

2.3 SIP 공격기법

현재 SIP 공격 기법[5]은 크게 두 가지가 있다. 첫 번째로 SIP 메시지를 대량으로 보내어 SIP 사용자나 사업자가 정상적인 서비스 이용 혹은 제공하지 못하게 하는 것으로, 일반 네트워크에서 DoS(Denial of Service)와 비슷한 개념이 비슷한 Message Flooding 공격이 있다. 이 공격은 공격자가 INVITE, Register 등의 메시지들을 다량으로 보내어 정상적인 사용자 혹은 서버의 서비스 오작동이나 오류를 발생시켜 실질적인 사용자가 서비스를 사용 할 수 없게 한다. 대표적인 Message Flooding 공격은 다음과 같다[3].

- Register Flooding 공격 : 공격자의 반복적인 register를 통해 다른 사용자가 서버를 사용하지 못하게끔 과부하를 거는 공격의 형태이다. 대표적으로 서버 flooding 공격이 있다.
- Invite, RTP Flooding : 공격 대상은 SIP 서버(Register, Redirect, Proxy), Software Switch, 사용자 단말 및 PC(소프트 폰)이며 공격자는 많은 수의 유효한 요청 메시지(SIP INVITE) 또는 음성 메시지를 보내어 시스템이 이에 대하여 응답 메시지를 준비하게 함으로써 해당 시스템의 CPU 및 메모리 자원을 고갈시킨다. 피해내용은 시스템 자원의 고갈로 인하여 서비스의 이용 및 사용하고 있는 모든 사용자의 서비스지연 또는 마비가 된다.
- Cancel 공격 : 공격자가 SIP 사용자 단말의 호 설정을 방해하기 위한 공격이다. 주로 연결되어 있는 호 설정을 끊기 위해서 사용된다.
- Bye 공격 : 이 공격은 Cancel 공격과 유사한 공격이다. Cancel 공격이 호 설정단계에서 수락메시지가 오기 전에 Cancel 메시지를 보내야 하기 때문에 공격하는 시점이 매우 중요하지만 Bye 공격은 SIP 단말들이 통화 하고 있는 어느 시점에서도 공격이 가능하다는 특징이 있다.



〔그림 4〕 SIP 공격기법

두 번째 공격 기법으로는 SIP Parser공격으로 Malformed Message공격(비정상 메시지 공격)이 있다. 이는 SIP의 헤더와 바디 내용이 일반 문자로 되어있다는 점을 이용하여 다른 문자들로 삽입, 변조 혹은 삭제하는 것이다.

2.4 기존 프록시 서버의 문제점 및 해결 방안

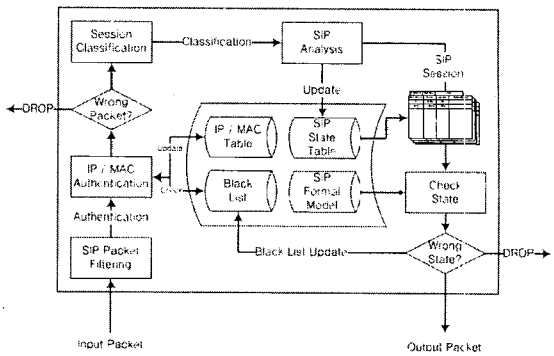
기존 SIP 공격에 대한 문제점을 해결책에 대한 문제[8] 중 하나는 SIP 프록시 서버이다. 가장 큰 문제는 서버의 과부화로 인한 서비스적인 지연문제이다. 하지만 이를 해결하기 위해 프록시 서버를 수정하게 될 경우 서버의 과부하 문제를 해결하지 못한다는 단점이 있다. 또한 기존의 SIP 프로토콜의 장점이 사라지고 너무 복잡해진다는 문제점과 호환성의 문제가 여전히 존재하고 이러한 단점들을 확실하게 해결하지 못한다는 문제점[11,12]들이 있다.

따라서 이러한 SIP 프록시 서버의 문제점을 해결하기 위해 본 연구에서는 기존의 서버에 상태정보를 분석하고 과부하를 줄여주기 위해 프록시 서버의 이전 단계에 추가적으로 SIP 가상 프록시 서버를 구현하여 상태정보 분석 기법을 이용하여 각 사용자의 상태정보를 유지하고 이를 기반으로 공격 탐지/차단 기법에 대해 연구를 하였다.

기존의 연구들은 앞에서 제시된 SIP의 문제점을 이용한 공격을 정확하게 탐지/차단 기능이 제공되어 있지 않는다. 따라서 본 연구에서는 SIP공격을 탐지/차단하기 위한 알고리즘과 구체적 모듈 설계 및 구현결과를 제시하였다.

3. 제안하는 SIP 가상 프록시 서버

본 연구에서는 상태정보를 분석함으로 보안침해 사고를 일으키는 공격을 빠르게 분류하여 비정상적 행위를 효율적으로 탐지하는 기술을 수행하고, 이를 통한 안전한 SIP 통신 환경 구축 및 관리하는 상태정보(stateful) 기법을 제시하고자 한다.



〔그림 5〕 가상 프록시 서버 전체 시스템 모듈 구성도

3.1 전체 시스템 구조

본 연구에서 제안하는 시스템 구조는 크게 세가지 모듈로 구성 된다. (1) 기존의 SIP 통신장비를 이용하여 통신을 제공하는 모듈, (2) SIP 가상 프록시 서버를 추가하여 IP/MAC 인증 하는 모듈, (3) 상태정보를 분석하고 이를 기반으로한 공격탐지/차단하는 모듈로 구성된다. 따라서 본 연구에서는 상태정보 기반의 가상 프록시 서버를 구현하고 사용자의 IP/MAC 기능을 추가하였고, 상태정보를 수집하여 분석하고, 이를 기반으로 공격 탐지/차단 여부를 판단한다.

사용자가 프록시 서버에 접속하여 SIP 통신을 시도하는 경우 [그림 5]와 같이 가상 프록시 서버에서는 실제 프록시 서버 이전 단계에서 미리 패킷을 받아 아래와 같은 단계를 수행할 수 있다.

- 1단계 : 사용자가 접속을 시도할 경우 처음 단계인 SIP Packet Filtering 단계를 거치면서 SIP 패킷인지의 여부를 판별한다.
- 2단계 : SIP 패킷이라 판별된 패킷은 다음단계인 IP/MAC 테이블과 Black List 테이블을 이용하여 IP와 MAC 주소값에 대한 인증을 받는다.
- 3단계 : 2단계에서 인증된 패킷은 Session Classification 단계에서 나누어 지게 된다.
- 4단계 : Classification 된 패킷들은 SIP Analysis 단

계에서 현재 상태정보를 SIP State Table에 추가하고 이를 저장 한다.

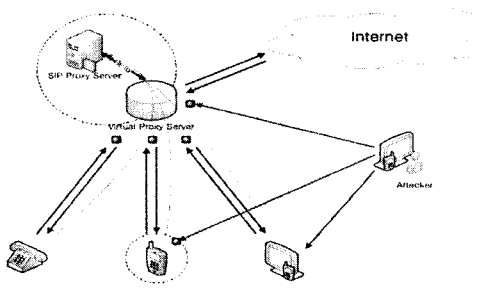
- 5단계 : Check State 단계에서는 현재 상태정보와 SIP Formal Model을 바탕으로 상태정보를 비교/분석하여 공격 탐지를 하고 그에 대한 패킷의 통과 여부를 결정해주는 단계이다.
- 6단계 : 모든 단계를 거친 패킷은 버려지고 Black List에 저장되거나 혹은 통과 하고 정상적인 통신을 하게 된다.

본 연구에서는 위와 같은 흐름을 통하여 공격에 대한 차단여부를 결정하게 되고 탐지된 공격에 대해서는 Black List를 통하여 최신화를 하였다. 또한 사용자들의 현재 상태정보를 최신화하면서 지속적인 실시간 공격 탐지를 할 수 있다.

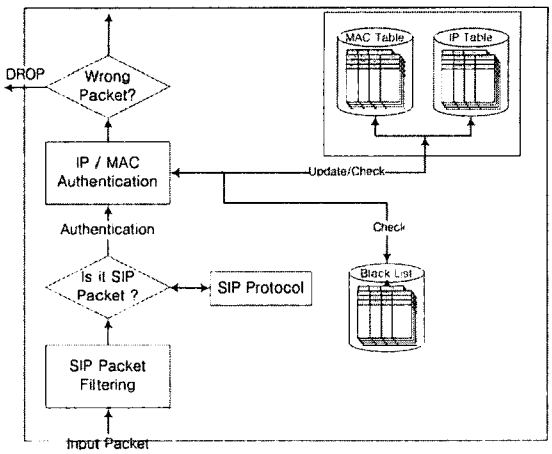
3.2 IP/MAC 상호인증

본 연구에서는 IP/MAC Spoofing 공격을 해결하기 위해 사용자와 가상 프록시 서버간의 IP/ MAC 인증 기법을 사용하였다. [그림 7]에서 IP/MAC 인증 기법은 SIP Packet Filtering을 거친 패킷에 대해 인증을 한다. IP/MAC인증은 IP/MAC Table과 Black List에 있는 데이터를 이용하여 비교를 하고 인증의 여부를 결정한다.

IP/MAC Table과 Black List를 비교하여 인증 여부를 결정하여 이를 통해 IP/MAC 인증을 할 수 있다. 또한 이를 통해 Spoofing 공격을 탐지/차단 하



〔그림 6〕 제안한 시스템 모델의 전체 시스템 구조



〔그림 7〕 IP/MAC 상호인증

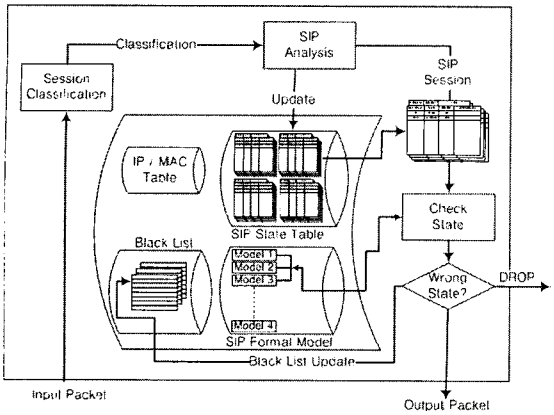
고 허용된 패킷은 다음 단계인 Session Classification 단계로 넘겨주게 된다. 이는 IP와 MAC Address를 lookuptable List로 비교 하여 허용이 되지 않거나 등록이 되어있지 않은 IP address와 MAC address를 가진 사용자는 접속하지 못하게 차단하는 단계이다.

위 단계에서는 프록시 서버로 접속한 사용자에 대한 인증 과정을 수행하는 단계이다. IP 정보 및 MAC 주소 정보를 이용하여 적법한 클라이언트에 대한 판별 과정을 수행하게 되고 공격자에 대한 사전 차단 기능을 수행하게 된다.

3.3 SIP 상태정보 저장 및 관리

IP 및 MAC 정보에 대한 인증 과정을 수행한 후에 가상 프록시 서버에서는 SIP 상태정보를 저장 관리하는 과정을 수행한다. 본 연구에서 제시한 모듈에서는 보다 안전하고 공격의 탐지를 하기 위해 클라이언트들 간의 SIP 프로토콜 상태정보를 저장하고 관리한다. 이와 같은 과정을 수행하면 SIP 서버의 과부하를 최소화 할 수 있고 비정상행위에 대한 판단 및 공격 탐지/차단 과정을 수행하게 된다.

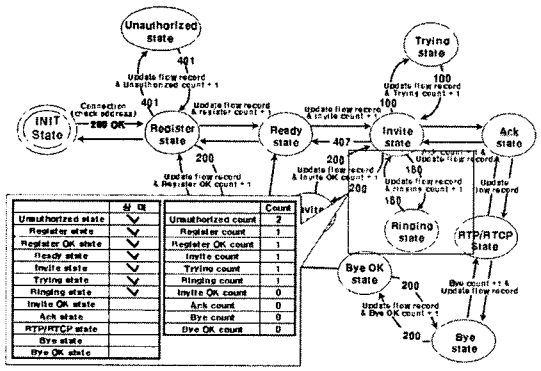
[그림 8]에서 분류된 세션들이 SIP Analysis 과정을 거치면서 SIP State Table에 업데이트 한다. 또한 Rule 기반의 모델인 SIP Formal Model을 참조하여



〔그림 8〕 상태정보 저장 / 관리

Check State과정을 거치면서 비정상적인 SIP 공격여부를 결정하게 된다.

[그림 9]는 [그림 3]의 SIP State Diagram을 바탕으로 본 연구에서 중점을 두고자 하는 상태정보 기반의 공격탐지 위한 그림이다. 본 연구의 가상 프록시 서버의 가장 큰 핵심은 상태정보를 저장하여 체크 리스트를 만들어 상태정보를 비교/분석하고, 이에 대한 상태정보와 공격탐지를 위한 중요 상태코드에 대한 count값도 같이 최신화 한다. 이는 상태정보 기반의 다이어그램을 이용해 현재 상태정보를 항상 확인/모니터링 하고, 각 단계에 Message Flooding 공격에 대처하기 위해 각 메시지에 대한 Count를 세는 과정이다. 이는 비정상적인 상태정보 혹은 각 단계의 기준 이상의 Count가 발생할 경우 공격을 탐지하기 위한 방법이다.

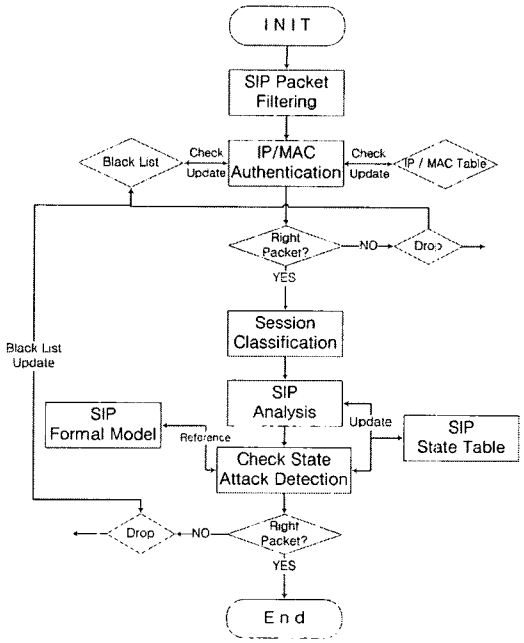


〔그림 9〕 상태정보 기반 가상 프록시 서버 다이어그램

본 연구에서는 가상 프록시 서버를 통해 상태정보 기반의 분석으로 MITM 공격과 Message Flooding 공격에 보다 확실히 대응하고 또한 인증과 암호화로 인한 실제 프록시 서버에 과부화를 줄여주고 더욱 더 안전한 SIP 통신을 할 수 있도록 초점을 두었다.

4. 가상 프록시 서버기반 SIP 공격 탐지 방법(Message Flooding 공격탐지)

SIP 프로토콜 통신에 대한 상태정보 기반의 가상 프록시 서버는 각 세션별로 상태정보를 저장하고 이에 대한 in/out정보와 일부 중요 Count정보를 제시한 SIP State Table에 저장한다. SIP State Table에 저장된 상태정보들과 SIP Formal Model의 규칙과 예외 경우를 비교하여 이를 기반으로 공격을 판별하고 이를 Drop시킨다. [그림 10]는 상태정보 기반의 가상 프록시 서버의 전체 순서도를 표현한 그림이다.



〔그림 10〕 제안한 SIP 공격 탐지 순서도

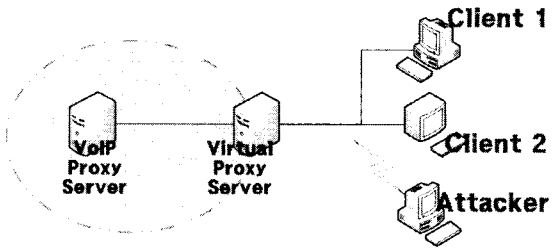
[그림 10] 상태정보 기반 가상 프록시 서버의 순서도 가상 프록시 서버 기반 SIP 공격 탐지는 Register, Reinvite, RTP, Cancel, bye Message Flooding 공격에 대해 탐지하고 이를 차단하는 기능을 수행한다.

[그림 10]의 순서도에는 공격에 대한 탐지/차단부분도 포함되어있다. SIP의 Session classification 단계에서는 패킷을 발신자 기준으로 분류를 하고 나눠지게 된다. Session classification 모듈을 의사코드로 표현하면 다음과 같다.

```
V_s : Sender of VoIP packet
V_p : Packet string of VoIP
For 0 to ( V_p's length) step 1 {
    If V_p = V_s then
        Make a Session Classification
    End if
}
```

패킷들을 SIP analysis 단계에서 패킷에 대한 분석 하여 필요한 부분을 상태정보를 저장해놓은 SIP State Table과 규칙기반의 SIP Formal Model에 의해 공격탐지 단계를 거친다. 이 단계를 통해 가상 프록시 서버는 SIP 통신상의 공격에 대해 탐지를 하고 이를 차단하는 Drop 단계를 거쳐 SIP 통신의 안전한 통신 상태를 제공한다. 공격탐지 모듈을 의사코드로 표현하면 다음과 같다.

```
S_d : State diagram
S_n : now State
S_b : before State
State_compare( ) {
    For 0 to (S_d len) step 1
        If S_b = S_d[i] && S_n = S_d[i] then
            Print "Not Attack"
        else S_b != S_d[i] || S_n != S_d[i]
            Alert "VoIP Attack"
}
```



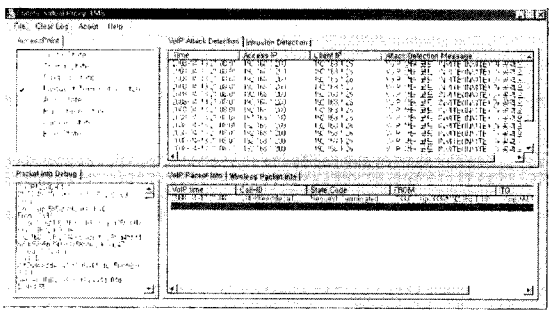
[그림 11] 가상 프록시 서버 시스템 구성도

본 연구에서는 공격탐지부분에서 SIP State Table, SIP Formal Model, Black List 3가지 경우와 조건을 통해 정확한 탐지를 하고, 실시간의 SIP State Table, Black List의 최신화로 새로운 공격에 대해 신속하게 탐지/차단을 한다. 이러한 공격탐지의 단계를 거쳐 보다 안전한 SIP 통신을 보장하며 이전에 탐지하지 못했던 부분까지 관리/분석을 할 수 있다는 장점이 있다.

5. 구현 결과 및 성능평가

본 연구를 통해 개발된 시스템에 대한 성능평가를 위해 [그림 11]과 같이 시스템을 구성하였다. SIP 프록시 서버 앞 단계에 이를 보호 할 가상 프록시 서버를 설치하였다. 가상 프록시 서버에서는 패킷정보 수집, 분석/비교를 하고 공격에 대한 탐지/차단할 수 있는 시스템을 구성한다. 또한 SIP의 모든 패킷을 모니터링/제어를 하였다.

이를 통해 공격에 대해 탐지하고 차단하는 시간을 비교 평가하였다. 패킷의 통계는 일반적으로 많



[그림 12] SIP 공격 탐지

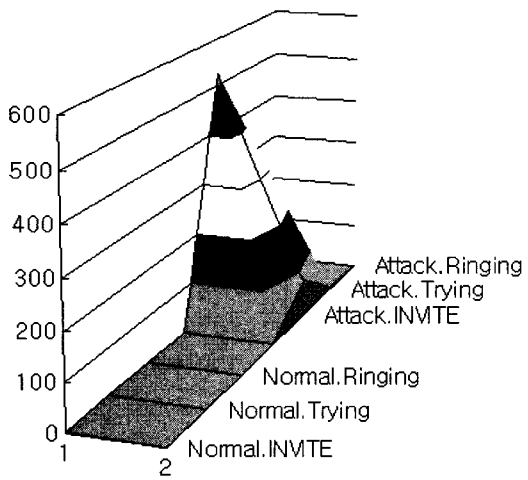
이 이용하고 있는 Ethereal과 WireShark를 이용하였다.

5.1 SIP 공격 탐지 시스템

가상 프록시 서버는 SIP에서의 인증 프로토콜에 대한 정보를 수신한다. 수신된 SIP 인증 정보는 가상 프록시 서버에 설정된 Possible State Diagram에 따라서 공격 여부를 판단하게 되며 공격일 경우 차단 신호를 보내어 차단을 수행하게 된다.

5.2 SIP 공격 탐지 및 대응 분석

SIP를 사용하는 클라이언트 프로그램은 "REGISTER" 패킷을 계속적으로 송신한다. 이에 따라 PROXY 서버는 "200 OK" 패킷을 지속적으로 전송하게 된다. 그러므로 가상 프록시 서버에서는 "REGISTER" 와 "200 OK"를 독립적으로 처리하지만 "INVITE" 패킷의 경우 자주 있는 패킷이 아니며 "INVITE", "Trying", "Ringing" 순서로 흐르게 된다. 따라서 SIP 공격과 같이 동일한 패킷을 지속적으로 전송하게 되는 경우 프로토콜의 순서를 무시하게 된다. 따라서 본 연구의 구현결과 SIP Possible State Diagram을 통하여 공격탐지가 가능하다는 것을 알 수 있다.

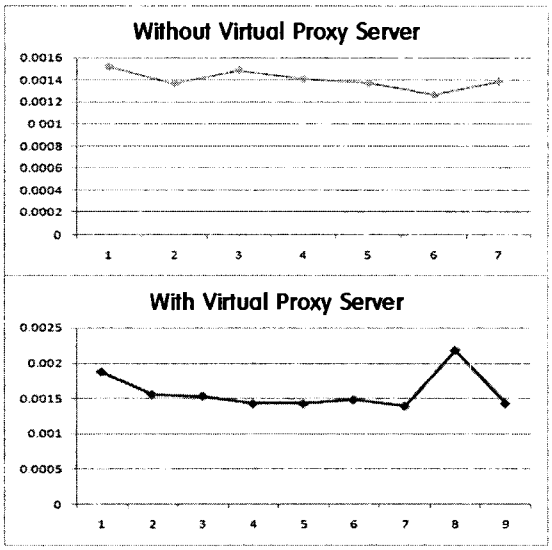


〔그림 13〕 SIP 상태 코드를 이용한 공격 패킷 통계

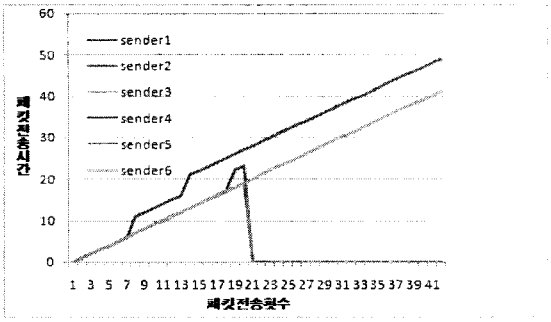
위 [그림 13]을 보면 알 수 있듯이 SIP 공격을 하게 되면 동일한 패킷이 계속 생성이 되며 이를 처리할 수 있는 SIP 프록시 서버의 속도를 넘기 때문에 프로토콜의 순서를 무시하게 된다. 이러한 분석을 통하여 본 연구의 가상 프록시 서버는 SIP 공격을 탐지하고 이에 대응할 수 있다.

SIP 환경에서는 실시간으로 패킷을 전송하고 모니터링을 해야 하기 때문에 패킷의 수정과정을 거치지 않고 패킷 헤더를 추출하여 바로 전송과정을 거친다. 하지만 공격을 탐지하고 대응을 하기 위해서는 IP 주소와 MAC 주소를 이용하여 차단할 패킷을 판단하는 과정을 거쳐야 한다. 본 연구에서는 차단 IP주소와 MAC주소 비교과정을 거치게 되며 이러한 비교과정으로 인한 SIP 통신에 영향을 끼쳐서는 안된다. 따라서 본 연구에서는 SIP 패킷의 정보 추출을 할 뿐 앞서 설명한 패킷 마킹과정과 겹쳐서 작동하지는 않는다.

[그림 14]의 패킷 전송시간을 보면 모듈을 구동하지 않았을 경우(without)의 전송간격과 모듈을 구동하였을 경우(Module1, Module2)의 전송간격에는 거의 차이가 없다.



〔그림 14〕 제안 모델을 이용했을 경우의 INVITE-Trying의 간격



〔그림 15〕 SIP 이상 트래픽 공격 탐지 및 대응

실험결과를 살펴보면 알 수 있듯이 본 연구의 SIP 공격탐지 및 대응 모듈은 실제 SIP 통신에는 영향을 미치지 않는다. 따라서 본 연구의 SIP 공격 탐지 및 대응 모듈은 사용자에게 영향을 미치지 않으면서 관리자는 실시간 모니터링을 할 수 있다는 것을 알 수 있다.

또한 아래 그림과 같이 본 연구에서 제안한 기법을 이용하였을 경우 6개의 SIP 클라이언트가 접속하여 송수신하는 SIP 패킷을 모니터링하고 있다가 공격을 시도하였을 경우 트래픽에 대한 모니터링 결과를 제시하고 있다. 실험 결과 본 연구에서 제시한 기법을 이용하였을 경우 패킷량이 증가할 경우에도 큰 지연 현상 없이 SIP 이상 트래픽에 대한 탐지 및 모니터링 기능을 제공한다는 것을 확인할 수 있었다.

본 연구는 최대한 다양한 SIP의 상태코드를 고려하고자 하였다. 따라서 본 연구의 SIP 공격 탐지와 유사한 vIDS와 본 연구에서 제안한 VPS(Virtual Proxy Server)를 비교하면 [표 1]과 같다.

	INVITE	Busy here	Trying	Ringing	200 OK
vIDS	O	X	O	O	O
VPS	O	O	O	O	O
	ACK	BYE	CANCEL	Request Terminated	
vIDS	O	O	X	X	
VPS	O	O	O	O	
	SIP 패킷분석	SIP 세션분류	무선 SIP 모니터링	SIP 프록시 서버 연계 가능	
vIDS	O	O	X	X	
VPS	O	O	O	O	

〔표 1〕 가상 프록시 서버와 vIDS의 처리 상태 코드 비교

기존의 vIDS는[13] 다양한 상태를 고려하고 있지만 Busy here, CANCEL, Request Terminated와 같은 자주 나올 수 있는 상태를 고려하지 않고 있다. 대체적인 Message Flooding 공격은 SIP 통신상에서 호 설정 및 해지에 대한 공격이 대부분이다. 대표적인 예로 Invite, Busy here 메시지에 대한 공격은 호 설정을 방해하고, Cancel, Request Terminated 메시지에 대한 공격은 연결이 되어있는 통신을 중간에 임의대로 종료시키기 위해 사용된다. 따라서 이러한 공격에 대한 탐지 및 대응이 필요한 실정이다.

본 연구에서 제시한 기법은 기존의 vIDS 시스템과 마찬가지로 SIP 패킷분석 기능을 제공하며 해당 SIP 세션에 대한 분류 기능을 포함하고 있다. 하지만 본 연구에서 제시한 기법은 추가적으로 유무선 SIP 트래픽에 대한 이상탐지 기능을 제공할 수 있으며, SIP 프록시 서버와 연계되어 프록시 서버의 성능을 높이고 SIP 프로토콜 구조의 안전성을 높일 수 있었다. 또한 본 연구에서 제시한 기법은 실제 SIP 통신을 사용함으로써 vIDS에서 고려되지 않은 상태를 찾아내어 기존의 SIP 공격 탐지보다 더 많은 공격을 탐지 할 수 있는 방안을 제시하였다.

6. 결 론

SIP 기술은 다양한 부가서비스와 저렴한 통신비용으로 나날이 발전하고 있으며 사용자 수도 급증하고 있다. 하지만 이와 같은 SIP 서비스 이용의 장점에 비해 프록시 기반 SIP 프로토콜 자체의 문제점을 이용한 SIP Message Flooding 공격에 취약하는 단점이 있다. 따라서 본 연구에서는 기존 SIP 프로토콜의 공격 취약성을 해결하기 위해 기존의 vIDS 시스템에서 사용한 접근방법과 다르게 SIP 상태코드와 Formal Model을 비교/분석하여 SIP Message Flooding 공격을 탐지/차단하는 방법을 제시하였다.

본 연구에서는 우선 현재의 SIP 프로토콜에 대한 상태정보 다이어그램을 구성/제시하였으며 이를 토대로 가상 프록시 서버에서 SIP 패킷을 분석/모니

터링하고 공격을 탐지하기 위한 방법을 제시하였다.

본 연구에서 제시한 기법은 가상 프록시 서버를 구축하여 기존의 SIP 프록시 서버로 송수신되는 SIP 패킷에 대해 필터링 및 IP/MAC 인증 과정을 수행하고 패킷에 대한 세션 분석을 통해 프록시 기반 SIP 세션을 능동적으로 모니터링 하였으며, SIP Formal Model에 기초하여 SIP 패킷에 대한 이상 현상을 분석하도록 하였다. 그 결과 가상 프록시 서버를 중심으로 SIP 비정상 메시지 공격과 INVITE 메시지 폭주 공격 등과 같은 비정상적인 공격 행위를 효율적으로 탐지/차단할 수 있었다.

성능 평가 결과 본 연구에서 제시한 기법은 기존의 보안기법의 문제를 해결하고 가상 프록시를 중심으로 패킷 모니터링 과정에 의한 부하와 트래픽 전송 지연을 최소화하면서도 효율적으로 SIP 공격을 탐지하는 것을 확인할 수 있었다. 본 연구에서 제시된 기술을 토대로 최근 이슈가 되고 있는 무선 네트워크 환경에서 SIP 공격을 능동적으로 탐지 차단할 수 있는 기술에 대한 연구를 수행하고자 한다.

참 고 문 헌

[1] 한국전자통신연구원(ETRI), "VoIP 기술 및 시장 동향", 기술평가팀 P.4~13, P.19~45, 2006

[2] http://www.voip-forum.or.kr, VoIP 국내표준, "H.323 기반 인터넷 텔레포니 단말", "SIP 기반 인터넷 텔레포니 단말", 2005.

[3] 한국정보보호진흥원. "VoIP 정보보호 가이드" 2005.

[4] 구자현, "VoIP서비스 보안 취약성 분석", 한국정보보호학회지, 제 16권 1호, P.60~63, 2006.

[5] 박진범, 백형구, 원용근, "VoIP 보안 취약점 공격에 대한 기존 보안장비의 대응 분석 연구", 한국정보보호학회, 한국정보보호 학회지 제17권 제 5호, P.57~65, 2007.

[6] D.Malas. SIP performance metrics. Internet draft draft-malas-performance-metrics-06.txt (work in progress), IETF, 2007.

[7] M.Collier, "VoIP Vulnerabilities Registration Hijacking", SecureLogix Corporation, P.1~4, 2005.

[8] D.Richard Kuhn, Thomas J.Walsh, Strffen Fries, "Security Consideration for Voice over IP Systems", NIST, P.10~13, P.19~44, P.52~ 73, 2005.

[9] D.Powell, "Enterprise Security Management (ESM) : Centralizing Management of Your Security Policy", SANS Info, 2002.

[10] Jay Beale, James C.Foster, Jeffrey Posluns, Brian Caswell, "Snort 2.0 Intrusion Detection", Syngress Publishing, 2003.

[11] H.Sengar, D.Wijesekera, H.Wang, S.Jajodia, "VoIP Intrusion Detection Through Inter- acting Protocol State Machines", Proceedings of IEEE DSN'2006 , Philadelphia, PA, 2006.

◐ 저 자 소 개 ◑

이 형 우(Hyung-Woo Lee)

1994년 고려대학교 전산과학과 졸업(학사)
1996년 고려대학교 대학원 전산과학과 졸업(석사)
1999년 고려대학교 대학원 전산과학과 졸업(박사)
1999년~2003년 2월 천안대학교 정보통신학부 조교수
2003년~현재 한신대학교 컴퓨터공학부 부교수
관심분야 : 정보보호, 유무선 네트워크 보안, 웹 보안기술
E-mail : hwlee@hs.ac.kr