한국산학기술학회논문지
Vol. 11, No. 1, pp. 130-140, 2010

공기 정보를 이용한 비정상 SIP 패킷 공격탐지 기법

김득용[1], 이형우[2*]
[1]한신대학교 컴퓨터공학부

Abnormal SIP Packet Detection Mechanism using Co-occurrence Information

Deuk-Young Kim[1] and Hyung-Woo Lee[2*]
[1]**School of Computer Engineering, Hanshin University**

요 약 SIP(Session Initiation Protocol)는 IP 기반의 VoIP(Voice over IP) 서비스를 실현하기 위한 시그널링 프로토콜이다. 그러나 SIP 프로토콜은 기존의 IP 망을 활용하기 때문에 많은 보안 취약점이 존재한다. 특히 SIP 헤더의 정보를 변경하여 전송하는 SIP Malformed 메시지 공격 같은 경우 VoIP 서비스의 오작동을 유발하거나, 악성코드를 삽입하여 SIP 클라이언트 시스템내 개인정보를 유출하는 등 심각한 문제점을 보이고 있어 이에 대한 대체 방안이 제시되어야 한다. 이에 본 논문에서는 SIP Malformed 메시지 공격탐지에 대한 기존의 연구를 분석하고, 언어 처리에서 단어의 연관성을 분석하는 기법으로 사용되는 공기 정보(Co-occurrence Information)와 네트워크에서 발생하는 실제 SIP 세션 상태 정보를 반영하여 SIP 연관규칙 패턴을 생성하는 기법을 제안하였다. 본 논문에서 제안한 공기정보 기반 SIP 연관규칙 패턴을 이용하여 SIP 비정상메시지 공격을 탐지한 결과 평균 87%의 탐지율을 보였다.

Abstract SIP (Session Initiation Protocol) is a signaling protocol to provide IP-based VoIP (Voice over IP) service. However, many security vulnerabilities exist as the SIP protocol utilizes the existing IP based network. The SIP Malformed message attacks may cause malfunction on VoIP services by changing the transmitted SIP header information. Additionally, there are several threats such that an attacker can extract personal information on SIP client system by inserting malicious code into SIP header. Therefore, the alternative measures should be required. In this study, we analyzed the existing research on the SIP anomaly message detection mechanism against SIP attack. And then, we proposed a Co-occurrence based SIP packet analysis mechanism, which has been used on language processing techniques. We proposed a association rule generation and an attack detection technique by using the actual SIP session state. Experimental results showed that the average detection rate was 87% on SIP attacks in case of using the proposed technique.

Key Words : SIP, Attack Detection, Co-Occurrence, Association Rule, Malformed Message

1. 서론

SIP 프로토콜(Session Initiation Protocol)[1]은 초고속 통신망과 인터넷 응용기술의 발전으로 일반화 되어가고 있는 IP 기반의 Voice over IP(VoIP) 서비스를 실현하는 프로토콜 기술이며, 상용 전화 서비스를 위해 제시된 H.323 표준기술을 대체할 목적으로 IETF(Internet Engineering Task Force)에서 개발된 시그널링 프로토콜이다.

그러나 VoIP 서비스를 실현하기 위한 통신기술인 SIP 프로토콜은 기존의 IP망을 그대로 활용하기 때문에 개방형 인터넷에서 발생할 수 있는 보안 취약성뿐만 아니라 세션설정을 위한 시그널링으로 인하여 SIP 프로토콜 작동 단계에서 다양한 형태의 공격이 가능하다. SIP 프로토

본 논문은 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음
(NIPA-2009-(C1090-0902-0016)
*교신저자 : 이형우(hwlee@hs.ac.kr)
접수일 09년 11월 11일 수정일 (1차 09년 12월 14일, 2차 10년 01월 07일) 게재확정일 10년 01월 20일

콜에서 발생하는 공격 형태는 크게 Malformed 메시지 전송 공격, SIP Flooding 공격 같은 서비스 거부 공격(Denial of Service)과 세션 Hijacking, 통화방해 공격 및 Spam 전송과 같은 서비스 오용공격 등으로 나눌 수 있어 이에 대한 대응 기술이 요구된다.

현재 SIP 서비스 거부 공격에 대한 대응 기법으로는 SIP 프로토콜 자체에 암호화 방식을 접목한 연구[2,3]가 진행되었으며, SIP Flooding 공격의 경우 상태전이모델(State Transition Model)[4]를 이용하거나, 발생메시지의 상한 값을 고려한 SIP INVITE 기반의 SIP Flooding 공격 탐지 방법[5] 등의 연구가 수행되었다.

하지만 SIP는 텍스트 기반의 시그널링 프로토콜이기 때문에 악의적 공격자에 의해 SIP 메시지 헤더 부분에 다른 문자들을 삽입하거나 변조 및 삭제 등과 같은 SIP 헤더 정보를 변경하여 전송하는 SIP Malformed 메시지 공격에 취약하다. 이 경우 SIP 프락시 서버는 수신된 SIP 패킷에서 삭제, 삽입, 변조된 SIP 헤더 부분을 식별 및 판단하기 어려워 이에 대한 연구가 필요하다.

이를 해결하기 위한 방법으로 RFC 3261에서 규정한 250여개의 ABNF(Augmented Backus-Naur Form) 규칙을 이용하여 송·수신되는 SIP 패킷에 대하여 정규표현식을 체크한 후 이를 바탕으로 SIP Malformed 메시지 공격 유·무를 판단하는 방법[6]만이 제안되었다.

하지만, 이러한 방식은 네트워크에서 발생하는 실제 SIP 트래픽 데이터의 상태를 반영하지 않았을 뿐만 아니라 SIP 메시지에서 나타나는 토큰들의 형식만을 정규표현식으로 나타내었기 때문에 SIP 헤더의 정보를 변경하여 전송하는 SIP Malformed 메시지 공격에 능동적으로 대응할 수 없다는 문제점이 있다.

언어 정보처리 분야에서 공기 정보(Co-occurrence Information)를 이용하여 문서내 핵심어를 추출하거나, 유사한 단어를 추출하는데 사용하는 기법[7,8,9]이 제시되었다. 이 기법을 사용할 경우 효율적으로 문서 정보내 핵심정보를 추출할 수 있으며, 문서내에 포함된 단어 간 연관규칙 정보를 획득할 수 있다. 따라서 이와 같은 단어의 연관성을 분석하는 공기정보 기반 분석 기법을 SIP 패킷에 적용할 경우 비정상행위 및 공격 판단에 적용 가능하다.

본 논문에서는 SIP 프락시에 송·수신되는 SIP 패킷 중에서 Malformed 메시지를 보다 효율적이면서도 정확하게 탐지하기 위해 공기정보를 이용하였다. 현재의 네트워크에서 발생하는 SIP 헤더 메시지에 있는 토큰들 사이의 연관성을 분석하고, 이를 기반으로 SIP 연관규칙 패턴을 생성하여 SIP Malformed 패킷을 분류 및 공격을 탐지하는 방법을 제안하였다.

본 논문의 구성은 다음과 같다. 2장에서는 SIP 프로토콜의 취약점과 공기정보 기반 분석 기법을 제시하고, 3장에서는 공기정보를 이용하여 SIP 연관규칙 패턴을 생성하는 기법과 이를 이용하여 공격을 탐지하는 기법을 제시한다. 그리고 4장에서는 제안한 탐지 기법에 대한 실험 및 성능평가를 하였으며 마지막으로 결론 및 향후 연구를 제시하였다.

2. 관련연구

2.1 SIP 프로토콜 분석

SIP[1]는 텍스트 기반의 응용 프로그램 계층 신호 및 호출 제어를 하는 시그널링 프로토콜로서, 구현이 용이하며 인터넷에서 사용되는 다른 많은 프로토콜과 결합하여 다양한 서비스들을 제공할 수 있는 유연성과 확장성을 가진 프로토콜이다. SIP는 세션의 생성, 수정, 종료를 제어하는 요청/응답의 클라이언트/서버 구조로서 TCP(Transmission Control Protocol)와 UDP(User Datagram Protocol)에 모두 사용할 수 있는 프로토콜이다[16]. SIP 포맷은 헤더와 바디로 구성되며, 헤더와 바디는 CRLF(Carriage Return Line Feed)로 구별된다. 아래의 그림 1은 SIP 메시지의 형식을 나타낸다.

INVITE sip:userB@aaa.ac.kr;transport=udp SIP/2.0	Request-Line
Via: SIP/2.0/UDP test.aaa.ac.kr:5060; branch=8b71236071-0 From: sip:userA@aaa.ac.kr To: sip:userB@aaa.ac.kr CSeq: 1 INVITE Call-ID: 15011089111@aaa.ac.kr Contact: <sip:userA@test.aaa.ac.kr:5060> Accept: application/sdp Content-Type: application/sdp Content-Length: 172	SIP Header
	Blank-Line
v=0 o=test.aaa.ac.kr 846930886 1804289383 IN IP4 211.112.217.32 s=SIP Library call c=IN IP4 211.112.217.32 t=3244893409 0 m=audio 32810 RTP/AVP 0 a=rtpmap:0 pcmu/8000	Body

[그림 1] SIP 메시지 예시

SIP 프로토콜은 INVITE, ACK, CANCEL, BYE 등의 메소드(Method)를 사용하여 세션 제어를 하며, 요청/응답 메소드의 종류는 각각 기본적으로 6가지의 유형이 존재한다. 아래의 표 1은 요청/응답 메소드 종류와 그 의미를 나타낸다.

[표 1] 요청/응답 메소드

Request Method	의 미	Response Method	의 미
INVITE	콜 요청	1xx	Informational
ACK	INVITE에 대한 최종 응답	2xx	Success
BYE	콜 종료	3xx	Redirection
CANCEL	미결정 콜 해지	4xx	Client Error
OPTION	Capability 정보 요청	5xx	Server Error
REGISTER	위치정보 등록 및 삭제 수정	6xx	Global Failure

2.2 SIP 프로토콜의 취약점 분석

최근까지 알려진 SIP 보안 취약점은 표 2와 같이 요약할 수 있다[15].

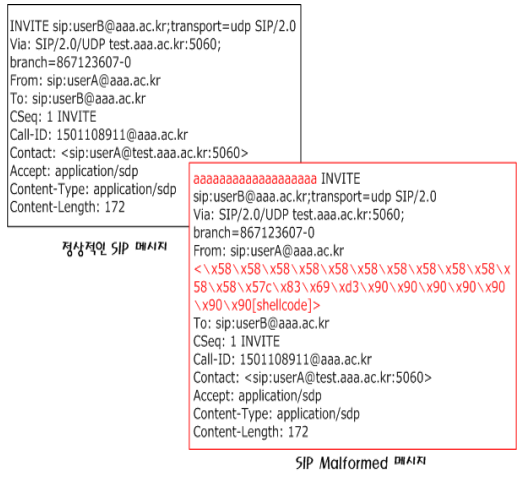
표 2와 같은 SIP 보안취약점 중 VoIP 서비스를 제공하는 사업자에게 가장 치명적인 공격은 서비스 거부 공격이다. 서비스 거부 공격은 VoIP 시스템을 악의적으로 공격하여 해당 시스템의 리소스를 독점하거나, 시스템의 자원을 고갈시켜 VoIP 사업자로 하여금 정상적인 서비스를 제공하지 못하게 한다. 이러한 서비스 거부 공격으로는 SIP Flooding 공격, Malformed 공격들이 존재한다.

SIP Malformed 메시지 공격은 SIP의 헤더와 바디 내용이 텍스트 기반으로 되어있다는 점을 이용하여 SIP 헤더내에 임의적으로 문자들을 삽입, 변조 혹은 삭제하는 것이다. 예를 들면 엄청난 수의 공백 문자를 넣어 오버플로우 예외를 발생시킨다거나 특수문자(한자어나 non-ASCII)를 넣어 이에 대응하지 못하게 하여 VoIP 서비스의 오동작을 유발한다.

[표 2] SIP 프로토콜의 취약점

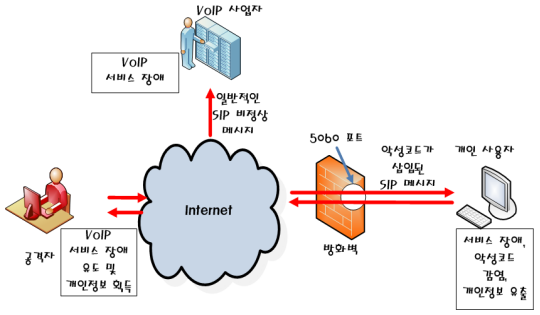
최근까지 알려진 SIP 프로토콜 취약점	
스니핑 (Sniffing)	음성 트래픽을 불법으로 스니핑하여 미디어로 재생, 정보를 수집하려는 시도
스푸핑 (Spoofing)	TCP/IP 프로토콜의 약점을 악용하여 발신주소를 조작, 정상적인 사용자로 위장
재사용 공격 (Replay Protection)	전자서명과 같은 암호화된 데이터를 주고받을 때 권한 없는 공격자가 이를 복사해 두었다가 나중에 그대로 사용하여 합법적 이용자로 가장하려는 시도
중간자 공격	불법적인 제 3자가 양단간 통신에 개입할 수 있는 권한을 획득하여 정당한 통신주체로 참여하려는 시도
Session Hijacking	공격자가 세션에 직접 개입하여 불법 정보를 발생시킬 수 있는 능동적 공격 시도
VoIP 스팸 및 음성메일 폭탄공격	불특정 다수에게 보내지는 음성광고 메시지로 인해 음성사서함이 무용화 되는 시도나 공격
악의적인 호 발생 공격	양단간 전화통화에 개입하여 악의적인 패킷을 통화 중에 삽입하여 통신을 방해하는 행위
비인가 장치	인증받지 않은 불법 VoIP 단말이나 시스템이 망에 접속하여 정상적인 시스템으로 위장
서비스 거부공격 (DOS 공격)	IP Server 같은 주요 시스템에 대한 자원을 고갈시키거나 독점 및 파괴하여 해당시스템이 서비스를 제공하지 못하도록 무력화하는 공격

그림 2는 SIP 정상메시지와 Malformed 메시지를 보여주며, 정상적인 SIP 메시지 헤더 내에서 INVITE 메소드 앞에 임의적으로 일반문자(aaaaaaaaaaaa)와 From 헤더와 To 헤더사이에 악성코드(<\x58\x58\x58\x58 … >)를 삽입한 SIP Malformed 메시지 전송 형태이다.



[그림 2] SIP 헤더 메시지 변조

이와 같은 패킷이 SIP 프락시 서버에 전송될 경우 VoIP 서비스의 오동작을 유발하여 사용자로 하여금 정상적인 서비스를 제공받지 못하게 한다. 또한 SIP 메시지 내에 악성코드를 삽입하여 SIP 패킷을 전송할 경우 악성코드로 인해 개인정보의 유출뿐만 아니라 침해당한 PC의 다운 등 2차, 3차의 위협이 발생한다[7].



[그림 3] SIP Malformed 메시지 공격

결국 이러한 SIP 보안 취약성들로부터 안정적인 VoIP 서비스 제공을 위해서 이에 대응 할 수 있는 메커니즘이 제시되어야 하며, 특히 SIP 헤더 정보를 변경하여 전송하는 SIP Malformed 메시지 공격인 경우 이를 즉각적으로 탐지하고, 능동적으로 대처할 수 있는 기법이 제시되어야 한다.

2.3 단어의 공기정보 기반 분석 기법

언어의 기본적인 통계적 성질 중 단어 간의 연관성을 이용하여 텍스트 문서를 표현하기 위해 단어의 공기정보(Term Co-occurrence)를 이용하는 방법[8-10]이 제시되었다.

공기정보란 두 단어가 동일 문서, 문장, 구 등에 같이 발생하는 현상을 말하며, 더 자주 발생할수록 밀접한 관계를 가지고 있다는 전제에 기반하고 있다.

표 3은 단어 간의 공기정보를 나타낸 테이블이다.

• 연관성 규칙 : 어떤 단어의 존재가 다른 단어의 존재를 암시하는 것을 의미

(단어 A) → (단어 B)

(if A then B : 만일 A가 일어난다면 B가 일어난다.)

[표 3] 단어 간 공기정보

단어 / 단어	T_1	T_2	…	T_m
T_1	-	cf_{12}	…	cf_{1m}
T_2	cf_{21}	-	…	cf_{2m}
⋮	⋮	⋮		⋮
T_m	cf_{m1}	cf_{m2}	…	-

• m : 단어의 개수

• $T_j(j=1,2..m)$: j번째 단어

• $cf_{ij}(i,j=1,2..m)$: i번째 단어와 j번째 단어가 동시에 나타난 빈도수

일반적으로 공기정보는 언어처리 분야에서 문서내의 핵심어를 추출하거나, 명사의 의미구분, 유해어의 필터링, 문서의 요약, 단어의 유사성, 연관성 및 의미관계를 나타내기 위하여 다양한 연구에서 사용되고 있는 통계적인 기법이다. 또한 데이터 마이닝(Data Mining) 분야[11,12]에서 사건 속에 포함된 항목간의 연관관계를 발견하고자 할 때 사용된다.

따라서 본 논문에서는 이와 같은 공기정보의 특성을 이용하여 SIP 패킷내의 토큰들에 대한 연관성을 분석하고, 이를 이용하여 SIP Malformed 메시지를 탐지하고자 한다.

2.4 기존 SIP Malformed 공격탐지 기법의 문제점 및 해결방안

기존 SIP Malformed 메시지 공격탐지 기법인 Secure SIP[6]은 RFC 3261에서 규정한 250여 가지의 ABNF 규칙을 이용하여 정규표현식을 안전성 있게 구성하고 이를 바탕으로 SIP 메시지의 형태를 체크한 후 SIP Malformed 메시지 공격 유·무를 결정한다.

예를 들면 RFC 3261을 보면 포트번호를 규정하는 port=1*DIGIT라는 SIP 규칙이 존재한다. 이는 포트번호가 1자리 이상의 숫자로 구성되어야 함을 의미하여, 다르게 정의하면 9999999같은 1자리이상의 모든 숫자는 포트번호에 적합하다는 것을 나타낸다. 그러나 포트번호는 0~65535 범위 내에서 존재해야하며 이를 해결하기 위하여 Secure SIP 에서는 port=1*DIGIT라는 SIP 규칙을 port=/d{1,5}와 같이 변경하여 포트번호는 1~5자리 숫자 사이에 있어야한다는 정규표현식을 생성하여 SIP 규칙을 체크하게 된다.

하지만 SIP Malformed 메시지 탐지를 위한 Secure SIP의 경우 RFC 3261에 존재하는 ABNF 규칙들을 정규표현식으로 안정성 있게 구성한다고 해도 SIP 메시지의 형식만을 체크하기 때문에 port=99999도 정상적인 포트번호로 판단하게 되며, 네트워크에서 발생하는 실제 SIP 메시지내의 고유 토큰에 대한 상태를 반영하지 않아서 SIP Malformed 메시지 공격에 대한 탐지율이 높지 않다.

[표 4] Secure SIP 규칙 예

Secure RFC 3261 regular expressions	
user:	(#alphanum#|₩_|₩-){1,12}
callid:	(#ASCII|#{1,50}(₩@(₩w₩.*){1,32})?)
SIP_Version:	((SIP₩/₩d₩.₩d){7,9})
extension_method:	(#ASCII_NAME#{1,20})
protocol_version:	(₩d{1,2}₩.₩d{1,2})

본 논문에서는 이러한 문제점을 해결하기 위하여 언어의 통계적 성질을 나타내는 공기정보를 이용하였다. 언어의 특징으로 보면 문서는 하나의 긴 문자열로 볼 수 있으며 SIP 메시지 또한 하나의 긴 문자열로 취급할 수 있다.

만일 SIP 패킷내 후보 토큰과 그 위치정보를 획득할 수 있다면 SIP 메시지내의 토큰들 간의 구조를 정형화 할 수 있으며, 또한 고유 토큰들 간의 순차 패턴을 생성할 수 있다.

공기 정보를 이용하면 SIP 메시지 내에 임의의 고유 토큰이 있을 경우, 그 토큰 이후에 나타날 수 있는 후보 토큰의 연관성 정보와 적합도를 판단하는 과정에 적용할 수 있다.

따라서 본 논문에서는 유무선 네트워크상에서의 정상적인 SIP 메시지를 이용해 SIP 고유 토큰의 공기 정보와 고유 토큰이 나타난 위치 정보를 이용해 연관성 정보를 분석하여 SIP 패킷내 메시지의 연관규칙 패턴을 생성하고 이를 기반으로 SIP Malformed 메시지 공격을 탐지하는 기법을 제안하였다.

3. 제안하는 기법

3.1 SIP Malformed 메시지 공격 탐지 시스템 구조

본 논문에서 개발하는 공기정보 기반 SIP Malformed 메시지 공격 탐지 시스템은 다음과 같이 설계하였다.

첫째, SIP 메시지를 구성하는 고유 토큰을 생성하기 위하여 RFC 3261 규약에 의존하여 SIP 메시지를 파싱하는 SIP Parser를 구현하였다.

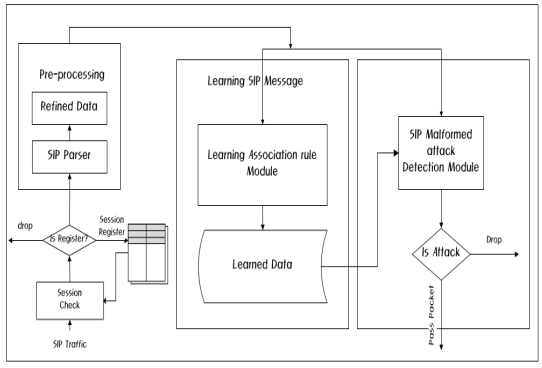
둘째, 파싱된 SIP 메시지를 구성하는 고유 토큰의 위치정보를 이용하여 SIP 메시지 고유 토큰들 사이의 연관성을 나타내어 순차 패턴을 생성하였으며, 마지막으로 SIP 메시지 내에서 선행 토큰이 존재할 때 반드시 존재해야하는 후행 토큰을 구하기 위하여 언어의 대표적인 통계 정보 중 하나인 SIP 토큰 기반 공기 정보를 이용하였다.

제안하는 SIP Malformed 메시지 공격 탐지 기법은 세션정보를 관리하는 세션테이블, SIP 메시지를 파싱하고, 데이터를 가공하는 전처리 모듈, SIP 메시지에 존재하는 연관정보와 공기정보를 이용하여 SIP 메시지의 연관규칙 패턴정보를 찾는 학습 모듈과 SIP Malformed 메시지 공격을 탐지하는 부분으로 구성이 된다.

본 논문에서 제안하는 기법은 아래와 같은 단계를 수행한다.

- 1단계 : SIP 패킷이 유입되면 세션 테이블을 구성한다.
- 2단계 : 유입된 패킷이 세션 테이블에 등록이 되어 있지 않은 상태로 수신된 등록 요청 메시지라면 SIP 패킷을 세션테이블에 등록하고, 그렇지 않다면 SIP 메시지를 차단한다.
- 3단계 : 2단계를 거친 패킷은 전처리 단계에서SIP 메시지를 고유 토큰으로 변환한다.
- 4단계 : 3단계를 거친 패킷은 SIP Malformed 메시지 공격 탐지 모듈에서 SIP 패킷에 대한 공격 여부를 결정한다.

아래 그림 4는 SIP 메시지내의 공기정보를 이용하여 Malformed 메시지 공격을 탐지하는 시스템의 전체 구성도이다.



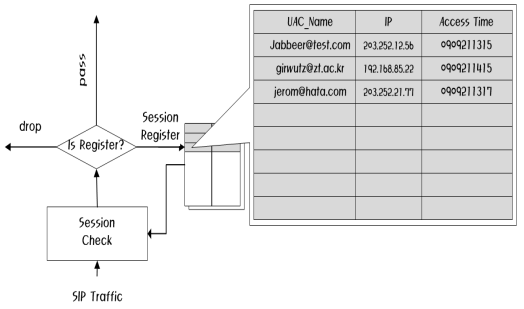
[그림 4] 제안하는 시스템 전체 구성도

본 논문에서는 위와 같은 흐름을 통하여 SIP Malformed 메시지 공격에 대한 탐지를 수행한다.

3.2 세션 테이블 구성 단계

세션테이블은 SIP 클라이언트의 등록현황을 파악하고 새로운 클라이언트에 대해 세션등록 과정을 수행한다. 또한 SIP 요청 메시지가 아니면서 세션테이블에 등록이 되어 있지 않을 경우 현재의 메시지를 공격으로 판단하게 된다.

세션테이블의 식별자로는 이메일 주소를 식별자로 사용하였으며 아래 그림 5는 세션 테이블구성도이다.

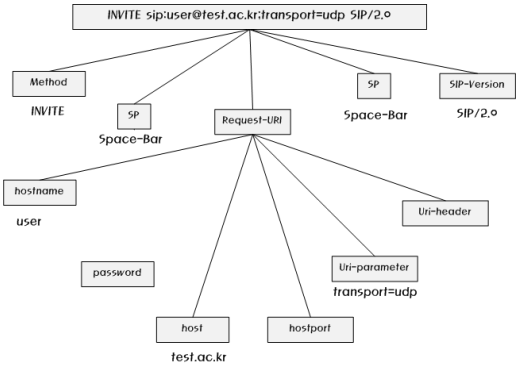


[그림 5] 세션 테이블 구성도

위와 같은 과정을 거친 SIP 패킷은 Malformed 메시지 여부를 판단하기 위하여 아래와 같은 전처리 과정을 거치게 된다.

3.3 전처리 단계

전처리 과정에서는 SIP 메시지를 고유 토큰으로 변환하기 위한 데이터 가공을 수행한다. SIP 메시지를 고유 토큰으로 변환하기 위해서는 우선 SIP 메시지를 파싱해야 되는데, 메시지 파싱시 RFC 3261에서 규정한 250여 가지가 넘는 ABNF 규칙들을 적용하여 SIP 프로토콜을 구성하는 각각의 필드를 기준으로 메시지를 파싱한다. 본 논문에서는 인터넷에 공개된 OpenSIPPaser 라이브러리를 이용하여 SIP 메시지를 파싱하였다. SIP 파서 수행 시 SIP 메시지를 파싱하지 못하면, ABNF의 형식에 일치하지 않는 것이므로 현재 파싱을 수행하는 SIP 메시지에 대해 Malformed 메시지로 1차 판정한다. 그림 6은 SIP 메시지에서 Request-Line에 속하는 문자열 INVITE sip:user@test.ac.kr;transport=udp SIP/2.0을 파싱한 결과를 보여준다. 그림에서 Method, SP, hostname, SIP-Version등은 Request-Line을 구성하는 필드를 나타내며, INVITE, user, test.ac.kr등은 각 필드에서 나타난 필드 값을 의미한다.



[그림 6] SIP 메시지 파싱 결과

위의 과정을 거쳐 파싱된 데이터 중 통계적인 정보를 가지지 않는 필드 값이 존재하는데 이런 값들을 가지는 hostname, password, host, branch-tag 필드의 통계정보를 얻기 위하여 필드의 이름을 심벌 값으로 변환하는 데이터 가공 과정을 수행하여 SIP 메시지 고유 토큰을 생성하였다. 또한 SIP 프로토콜을 구성하는 필드 중 SP 필드는 공백을 나타내는데, 하나의 공백이나 다수의 공백을 모두 동일한 값으로 인식하지만 본 논문에서는 SP 필드 값의 공백 수를 계산한 후 숫자로 할당하여 SP1과 같은 고유 토큰으로 생성하였다.

3.4 SIP 연관규칙 패턴 모델링 단계

SIP 연관규칙 패턴 모델링에서는 SIP Malformed 메시지를 탐지하기 위하여 정상적인 SIP 메시지의 연관규칙 패턴을 생성하여 모델링한다. SIP 연관규칙 패턴을 생성하기 위하여 본 논문에서는 공기정보를 이용하였다. 공기정보는 단어 간 동시에 발생할 확률을 나타낸다.

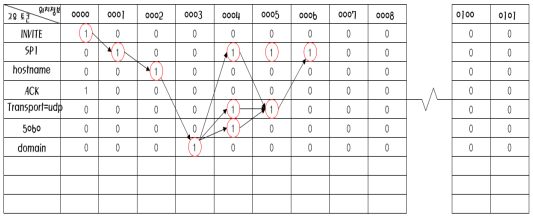
공기정보의 평가척도로는 신뢰도를 사용하는데, 공기정보가 얼마나 믿을 할 만한지를 나타낸다. 특히 신뢰도가 100%일 경우 두 단어는 반드시 같이 발생한다는 것을 의미한다. 이를 이용하면 정상적인 SIP 메시지의 경우 메시지에서 발생하는 고유 토큰들 사이에서 동시에 발생하는 고유 토큰들을 구 할 수 있으며, 이때 신뢰도가 100%일 경우 두 토큰은 반드시 동시에 발생하게 된다. 또한 SIP 메시지를 2차원 배열로 보고 각 위치에 따라 발생하는 고유 토큰을 구하면 SIP 메시지의 순서 규칙을 얻을 수 있는데 연관성 규칙인 “If A, then B"의 신뢰도는 아래와 같이 나타낸다.

· 신뢰도

$$Confidence = \frac{P(A \cap B)}{P(A)}$$

$$= \frac{A와 B가\ 동시에\ 발생한\ 빈도수}{A가\ 발생한\ 빈도수}$$

SIP 메시지의 순서 규칙을 생성하기 위하여 고유 토큰이 발생한 위치와 고유 토큰간의 매핑 테이블을 구성한다. 위치 정보는 4자리의 숫자로 구성이 되며, 앞의 두 자리 숫자는 고유 토큰이 나타난 행의 위치를 나타내며, 뒤의 2자리 숫자는 열의 위치를 나타나게 된다. 아래의 그림은 위치정보와 고유 토큰의 상관관계를 나타낸 테이블이며, SIP 메시지의 고유 토큰이 특정 위치에서 발생하였을 경우 1로 표기하고, 발생하지 않았을 경우 0으로 표기하였다.

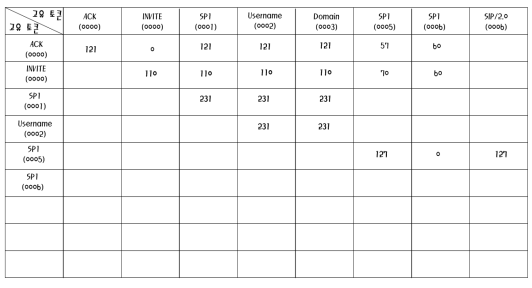


[그림 7] 위치정보-고유 토큰의 상관관계 테이블

위의 과정을 거쳐 생성된 위치정보와 고유 토큰의 상관관계 테이블을 보면 위치정보에 따른 고유 토큰의 연관성을 아래와 같이 볼 수 있다.

- Request-Line 첫 번째의 위치에서는 ACK, INVITE 등의 SIP 고유 토큰만이 올 수 있다.
- Request-Line 두 번째의 위치에서는 SP1 토큰만이 올 수 있다.
- Request-Line 세 번째 위치에서는 hostname 토큰만이 올 수 있다.
- Request-Line 네 번째 위치에서는 domain 토큰만이 올 수 있다.
- Request-Line의 다섯 번째에 올 수 있는 토큰은 SP1, Transport=udp 그리고 포트번호를 나타내는 5060이 나타날 수 있는 것을 알 수 있다. 이를 이용하여 SIP 메시지의 순서 규칙을 나타내면, INVITE 토큰이 발생한 후 SP1 토큰이 발생하고, hostname, domain 고유 토큰 순으로 발생하며, 그 다음으로 SP1, Transport=udp, 5060 중 하나가 발생하는 패턴이 나타나는 것을 알 수 있다.

그리고 반드시 동시에 발생하는 SIP 메시지의 고유 토큰을 구하기 위해 위치정보-고유 토큰의 상관관계 테이블을 이용하여 고유 토큰에 대해서 위치정보를 부여하고 이를 이용하여 위치정보가 부착된 고유 토큰들 사이의 공기정보를 구한다. 그림 8은 위치정보가 부착된 고유 토큰들 사이의 공기정보를 나타낸다.

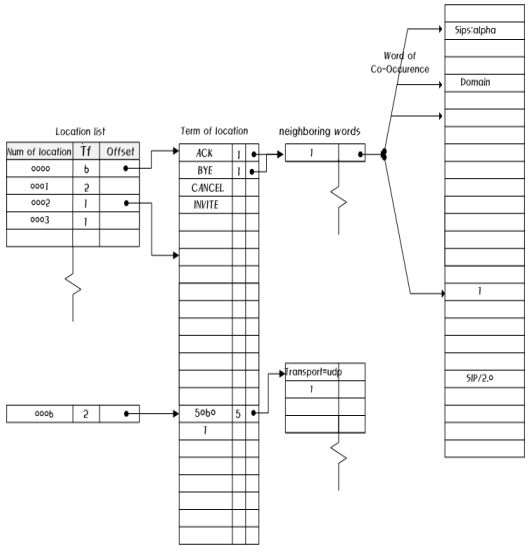


[그림 8] 위치정보가 부착된 고유 토큰들 사이의 공기정보 테이블

위의 위치정보가 부착된 고유 토큰들 사이의 공기정보 테이블을 보면 Request-Line 첫 번째 위치에서 ACK 토큰이 나타났을 때 두 번째의 위치에서 SP1 토큰 모두 121의 빈도수를 가지는 것을 볼 수 있다. 이 두 개 토큰의 신뢰도를 구하면 100%인 것을 알 수 있으며 이는 ACK 토큰이 나타났을 때 반드시 후행하는 토큰은 SP1인 것을 나타낸다. 위의 과정을 거쳐 생성된 토큰들 간의 공기정보의 특징을 살펴보면 아래와 같다.

- Request-Line 첫 번째 위치에서 ACK 토큰이 나타나면 두 번째에는 SP1 토큰 반드시 나타나야함.
- Request-Line 두 번째 위치에서 hostname 토큰이 나타나면 세 번째 위치에는 domain 토큰이 반드시 동시에 발생해야함.
- Request-Line 다섯 번째 위치에서 SP1 토큰이 발생하면 여섯 번째 위치에는 SIP/2.0 토큰이 반드시 나타나야함.

위치정보-고유 토큰의 상관관계 테이블과 위치정보가 부착된 고유 토큰들 사이의 공기정보 테이블을 이용하여 정상적인 SIP 메시지의 연관규칙 패턴을 생성한다. 아래의 그림 9는 SIP 연관규칙 패턴 모델링을 도식화 한 그림이다.



[그림 9] SIP 연관규칙 패턴 모델링

SIP 정상메시지를 가지고 생성된 SIP 연관규칙 패턴을 가지고 Malformed 메시지를 판단하는 근거로 사용한다.

3.5 SIP Malformed 메시지 공격탐지 단계

SIP Malformed 메시지 공격탐지는 3.4절에서 생성된 SIP 연관규칙 패턴을 이용하여 SIP 메시지에 대한 공격 여부를 판단한다. SIP 메시지에 대해 판단하는 과정은 아래와 같다.

-1단계 : 유입된 SIP 패킷을 위치정보가 부착된 고유 토큰으로 변환한다.

-2단계 : SIP 연관규칙 패턴에서 1단계를 거쳐 생성된 Request-Line 첫 번째 위치의 토큰에 대해 패턴의 발생 여부와 첫 번째 토큰이 나타났을 때 항시 같이 나타나야 하는 후행 토큰들이 현재 생성된 고유 토큰에 대해 위치정보와 토큰의 존재여부를 확인한다.

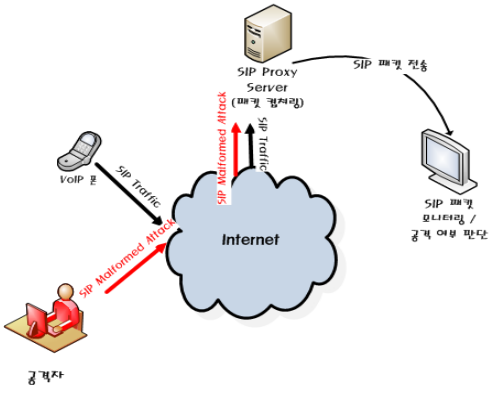
-3단계 : 모든 토큰에 대해 순서적으로 2단계를 실행하여, 중간 결과들을 조인한다.

-4단계 : 최종 조인 결과를 기반으로 현재 SIP 패킷에 대한 패턴이 연관규칙 패턴에 존재하는 지의 여부에 따라 공격을 판정한다.

4. 실험 및 성능평가

4.1 실험환경

본 논문에서 제안한 시스템은 소규모 네트워크 환경에서 Ubuntu Linux와 Windows 운영체제 시스템 상에서 개발하였다. Ubuntu Linux 시스템에서 공개 SIP 프락시 서버인 Openser를 이용하여 SIP 프락시 서버를 구축하였고, libpcap을 이용하여 SIP 패킷을 캡쳐 하였다. 또한 전처리 과정에서 SIP 메시지를 파싱하기 위해 인터넷에 공개된 OpenSIPParser를 이용하였으며, SIP 패킷에 대한 모니터링과 SIP 연관규칙 패턴을 생성하기 위하여 Windows 시스템에서 VC++를 이용하여 구현하였다.



[그림 10] 실험환경

그림 10과 같은 실험환경을 구축한 후 UDP 프로토콜 상에서 송·수신되는 SIP 패킷을 수집하고, 그 중 1000개의 SIP 요청 메시지만을 학습데이터로 사용하여 SIP 연관규칙 패턴을 생성하였다. 또한 테스트 데이터로는 인터넷의 공개 자료인 test-suit:007-sip를 사용하였다. test-suit:007-sip는 SIP Malformed 메시지 4526개 정도를 가지고 있으며 그 중 SIP Malformed 메시지 200개와 UDP 프로토콜 상에서 생성된 패킷 200개를 Malformed 메시지로 변경해서 테스트 데이터로 사용하여 공격 탐지 성능을 평가하였다.

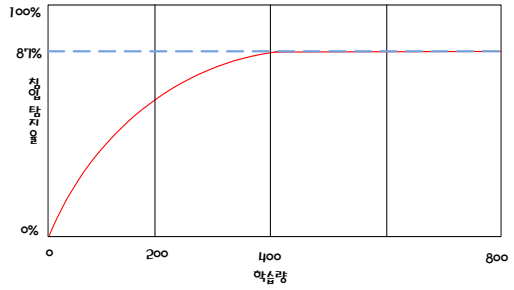
```
INVITE sip:userB@aaa.ac.kr;transport=udp SIP/2.0
Via: aaaaaaaaaaaaaaaaaaa branch=867123607-0
From: sip:userA@aaa.ac.kr
To: sip:userB@aaa.ac.kr
CSeq: 1 INVITE
Call-ID: 1501108911@aaa.ac.kr
Contact: <sip:userA@test.aaa.ac.kr:5060>
Accept: application/sdp
Content-Type: application/sdp
Content-Length: 172
```

[그림 11] SIP Malformed 메시지

4.2 성능평가 결과

본 논문에서 제시한 SIP Malformed 메시지 공격탐지 기법에 대한 실험 결과는 다음과 같다. 네트워크에서 발생하는 실제 SIP 트래픽 상태를 반영하여 SIP 헤더에서 고유토큰들을 대상으로 SIP 패킷 구조를 정형화하고, 고유토큰 사이의 연관성을 분석하는 공기정보 기반 분석 기법을 SIP 패킷에 적용하여 연관규칙 패턴을 생성하였다. 이를 기반으로 후보 토큰을 생성하고 SIP 패킷과 비교하여 SIP 공격 유무를 판단하였다.

아래의 그림 12는 제안한 기법에서 학습량에 따른 탐지율을 보여준다.

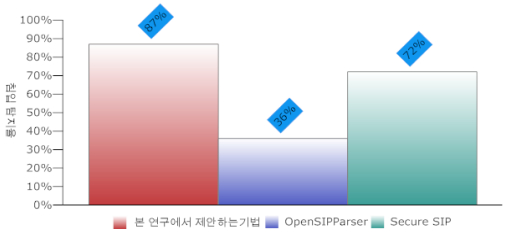


[그림 12] SIP 패킷 학습량에 따른 Malformed 메시지 탐지율

SIP Malformed 메시지 공격에 대한 실험결과는 정상 메시지의 학습량이 400개를 넘어가면서 평균적으로 87%

의 탐지율을 보이며 더 이상의 탐지율의 증가가 없는 것을 볼 수 있는데, 이는 학습데이터에서 나타나는 모든 고유토큰에 대한 연관규칙 패턴을 학습했다고 볼 수 있다.

기존 SIP Malformed 메시지 탐지 기법인 Secure SIP는 Malformed 메시지 공격 탐지율에 대해 언급하지 않고 26%의 성능향상만이 언급되어있어[14] 정량적인 비교는 할 수 없었지만 본 연구에서 SIP 메시지 파싱을 위해 사용한 공개 라이브러리 OpenserSIPParser와 본 논문에서 제안하는 공격탐지 기법 그리고 예상되는 Secure SIP 간의 비교 결과는 다음과 같다.

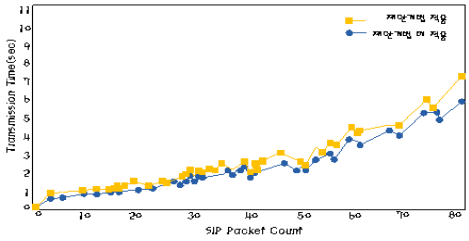


[그림 13] 기법에 따른 침입 탐지율

그림 13을 보면 본 연구에서 제안한 기법의 경우 SIP Malformed 메시지 공격 탐지율이 87%을 보였으며, OpenSIPPaser만을 사용한 경우 36%의 탐지율을 보였다. 또한 Secure SIP에서는 기존 ABNF 보다 26%의 성능향상이 나타났다고 언급하였기에 OpenSIPParser의 탐지율 36% 보다 26% 정도 향상된 약 62%의 Malformed 메시지 공격 탐지율을 보여 본 연구에서 제안한 SIP Malformed 메시지 공격탐지 기법이 Secure SIP 보다 효과적으로 Malformed 메시지 공격을 탐지하는 것을 알 수 있었다.

본 연구에서 제안한 SIP Malformed 메시지 공격 탐지율이 Secure SIP 보다 좋은 성능을 보인다고 이야기 할 수 있는 근거로는 Secure SIP의 경우 포트번호를 체크할 때 port=/d{1,5}의 정규표현식을 가지고 정상여부를 판단하는데 반하여 본 연구에서 제시한 기법은 실제로 SIP 헤더에서 생성되는 토큰을 대상으로 학습하기 때문에 실험환경에서 나타난 5060포트만을 정상 포트번호로 판단하기 때문이다.

추가적으로 만약 제안하는 시스템이 SIP 패킷차단을 위하여 SIP 프락시 서버내에 위치하고 제안하는 시스템은 유입된 SIP 패킷을 잡고 있는 상태에서 SIP Malformed 메시지 공격 여부를 판단한 후 판단 여부에 따라 패킷을 SIP 프락시 서버로 전송한다고 가정하였을 때 VoIP 서비스에 미치는 영향을 알아보려고 다음과 같은 실험을 하였다. 실험방법은 제안하는 시스템을 적용하지 않고 SIP 클라이언트에서 SIP 프락시 서버로 패킷을 전송하였을 때 패킷의 도착시간과 제안하는 시스템으로 SIP 패킷을 전송하여 Malformed 메시지 공격의 판단 여부를 완료한 시간을 비교하였다.



[그림 14] 실험에 따른 SIP 패킷 지연시간

그림 14를 보면 제안하는 기법을 적용하였을 경우와 그렇지 않았을 경우 패킷의 지연시간은 거의 차이가 없었다. 패킷 지연시간이 거의 차이가 나지 않는 이유는 본 연구에서 제안한 기법이 기계학습[13] 같은 추론하는 계산 과정이 없어 SIP Malformed 메시지를 판단하는 속도가 빠르기 때문이다.

따라서 제안하는 기법은 VoIP 서비스를 방해하지 않으면서 효과적으로 SIP Malformed 메시지 공격 탐지가 가능하다는 것을 알 수 있었다.

그러나 본 논문에서 제시한 기법의 탐지율이 100%를 보이지 못하였는데, 이러한 가장 큰 이유는 SIP 헤더 필드의 고유토큰 중 통계적인 데이터를 가지지 못한 필드에 대해 심벌 값으로 변환하는 전처리 과정을 수행하였기 때문이다. 또한 정상적인 SIP 메시지에서 나타나는 모든 고유토큰을 학습 할 수 없기 때문에 정상 메시지를 비정상 메시지로 판단하는 경우가 일부 발생하기도 하였으며, UDP 프로토콜 상에서 발생하는 SIP 패킷만을 가지고 연관규칙 패턴을 생성하였기 때문에 정상적인 SIP 패킷이라도 TCP 프로토콜 상에서 생성된 SIP 패킷의 경우 패킷의 시그니처가 달라 이를 공격으로 탐지하는 결과를 보였다.

하지만 이것은 네트워크에서 발생하는 실제 SIP 트래픽 상태가 다름을 의미하며, 본 논문에서 제안한 기법이 네트워크에서 발생되는 SIP 트래픽의 상태를 효과적으로 반영하는 것을 나타낸다.

마지막으로 본 논문에서 제안한 SIP Malformed 메시지 공격탐지 기법과 기존 Secure SIP에 적용된 기법을 비교하여 표 5에 ○, X로 표시하였다.

[표 5] 기존 Secure SIP 와 제안하는 기법의 비교

	ABNF 룰 매칭	세션분리	연관성 분석
기존 Secure SIP	○	○	X
제안하는 기법	○	○	○
	실제 SIP 트래픽 상태 반영	SIP Malformed 메시지 공격 탐지	
기존 Secure SIP	X	○	
제안하는 기법	○	○	

5. 결론

본 논문에서는 SIP Malformed 메시지를 탐지하기 위하여 공기정보를 사용하는 방법을 제안하였다. UDP 프로토콜을 기반으로 네트워크에서 발생하는 SIP 트래픽의 상태를 반영하여 SIP 헤더 내에 존재하는 고유 토큰들의 연관성을 분석하여 SIP 연관규칙 패턴을 생성 할 수 있었으며, 이를 기반으로 SIP Malformed 메시지 공격을 탐지할 수 있었다. 또한 기존의 ABNF만을 이용하는 것보다 효과적으로 SIP Malformed 메시지 공격을 탐지 할 수 있었다.또한 본 연구에서 제안한 기법은 공격 판정시 추론과정이 없어 Malformed 메시지 공격을 판단하는 속도가 빨랐다. 이로 인해 제안하는 기법이 VoIP 서비스를 방해하지 않으면서 효과적으로 SIP Malformed 메시지 공격 탐지가 가능하다는 것을 알 수 있었다.

본 논문에서 제안한 기법은 네트워크에서 발생하는 SIP 트래픽의 상태를 반영하여 비교적 높은 탐지율을 얻었지만, SIP 헤더의 고유 토큰들의 연관성을 분석할 때 전처리 과정에서 수행하는 데이터 가공으로 인해 SIP Malformed 메시지의 탐지율이 100%에 미치지 못한 87%의 탐지율을 보였다.

하지만 본 논문에서 제시한 기법은 Malformed 메시지 공격 탐지시 추론과정을 거치지 않아 SIP 헤더 내에서 발생하는 정상적인 토큰이라도 연관규칙 패턴에 학습되어 있지 않다면, Malformed 메시지로 판정하는 경우가 일부 발생하였다.

향후 연구에서는 본 논문에서 제안한 연관규칙 패턴을 개선하여 SIP Malformed 메시지 공격 판정시 SIP 패킷에 대해 추론을 할 수 있는 메커니즘을 제시하고 이를 추가적으로 보완할 예정이다.

참고문헌

[1] M. Handley, H. Schulzrine, E. Schooler, J. Rosenberg, “SIP : Session Initiation Protocol”, RFC 3261, IETF, 2002.

[2] Fengjiao Wang et al., “A New Provably Secure Authentication and Key Agreement Mechnism for SIP Using Certificateless Pubilic-Key”, 한국통신학회 논문지, Vol. 34, No. 8804, ICCIS 2007.

[3] Geneiatakis D. et al., “A lightweight protection mechanism against signaling attacks in a SIP based VoIP environment”, Telecommunication system, pp. 1018-4864, 2007.

[4] 이형우, “SIP 프로토콜 상태정보 기반 공격 탐지 기능을 제공하는 가상 프록시 서버 설계 및 구현”, 한국인터넷정보학회 논문지, Vol.9, No.6, 2008.

[5] 류제택, 류기열, 노병희, “발생메시지의 상한값을 고려한 SIP INVITE 플러딩 공격탐지 기법 연구”, 한국통신학회 논문지, Vol. 34 NO. 8, 2009.

[6] 국정원, 정보통신부, “2006 국가정보보호백서”, 2006.

[7] 원유재, “Security Issues for SIP Aware Services”, 한국정보보호진흥원, 2009.

[8] 안형근, 이원희, “유해어의 공기정보를 활용한 유해 웹문서 필터링”, 한국정보과학회 논문지, Vol.33, No. 2, 2006.

[9] 송원문, 김영진, 김은주, 김명원, “단어 빈도수와 공기 정보를 이용한 효율적인 핵심어 추출 기법 개발”, Preceedings of KIIS Fall Conference 2008, Vol. 18, No. 2, 2008.

[10] 이승우, 이근배, “국소 문맥과 공기 정보를 이용한 비교사 학습 방식의 명사 의미 중의성 해소”, 한국정보과학회 논문지 소프트웨어 및 응용, Vol. 27, No. 7, 2000.

[11] 김승우, 박상현, 원정임, “사이트의 접속 정보 유출이 없는 네트워크 트래픽 데이터에 대한 순차 패턴 마이닝”, 한국정보과학회 논문지 데이터베이스, Vol. 33, No. 7, 2006.

[12] 정경용, 김종훈, 강운구, 임기욱, 이정현, “스마트 홈에서 마이닝을 이용한 행동 순차 패턴 발견”, 한국콘텐츠학회 논문지, Vol.8, No.9, 2008.

[13] Huang. Y, Huang. S, Lin. T, Tasi. C, “Web application security assessment by fault injection and behavior monitoring”, In Proceedings of the 12th international Conference on World Wide Web, pp. 148-159, 2003.

[14] http://www.boannews.com

[15] 한국정보보호진흥원, “VoIP 정보보호가이드”, 2005.

[16] 이영민, 노영섭, 조용갑, 오삼권, 황희융, “SIP 프록시 서버의 부하 최소화를 위한 분산 처리,” 한국산학기술학회 논문지, Vol. 9, No.4, pp. 929-935, 2008.

[17] 김태욱, 성경상, 오해석, “효율적 키 관리 방식 적용

을 통한 전자문서 암호화에 관한 연구," 한국산학기술학회논문지, Vol.10, No.5, pp.1000-1008, 2009. 5.
[18] 정민경; 신승수; 한군희; 오상영, "스마트카드를 이용한 원격 시스템 사용자 인증 프로토콜," 한국산학기술학회논문지, Vol.10, No.3, pp.572-578, 2009. 3.

김 득 용(Deuk-Young Kim) **[정회원]**

- 2008년 2월 : 백석대학교 정보통신학부 (학사)
- 2010년 2월 : 한신대학교 일반대학원 컴퓨터학과 (공학석사)

<관심분야>
네트워크 보안, 정보보호, SIP 보안, 신경망, AI

이 형 우(Hyung-Woo Lee) **[정회원]**

- 1994년 2월 : 고려대학교 전산과학과 (전산학 학사)
- 1996년 2월 : 고려대학교 일반대학원 전산과학과 (전산학석사)
- 1999년 2월 : 고려대학교 일반대학원 전산과학과 (전산학박사)
- 1999년 3월 ~ 2003년 2월 : 백석대학교 정보통신학부 조교수
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터공학부 교수

<관심분야>
네트워크 보안, 정보보호, 무선네트워크, SIP 보안