SIP 공격 대응을 위한 보안성이 강화된 Stateful SIP 프로토콜

Stateful SIP Protocol with Enhanced Security for Proactive Response on SIP Attack

윤하나, 이형우
한신대학교 컴퓨터공학부

Ha-Na Yun(ha1na11@nate.com), Hyung-Woo Lee(hwlee@hs.ac.kr)

요약

SIP 프로토콜 기반 VoIP 서비스는 편리함과 저렴한 통신비용으로 사용자 수가 급증하고 있다. 하지만 SIP 프로토콜은 텍스트 형태의 SIP 헤더 정보를 UDP 방식으로 전송하기 때문에 손쉽게 위변조 할 수 있으며, 송신자에 대한 인증 기능을 제공하고 있지 않기 때문에 악의적 공격자에 의해 SIP 패킷 폭주 공격 등에 매우 취약하다. 따라서 본 논문에서는 이러한 SIP 취약성을 해결하기 위해 SIP 상태코드를 모니터링 하여 SIP 폭주 공격을 탐지하고 SIP 패킷에 대해 인증 및 보안 기능이 강화된 프로토콜을 제시하였다. SIP 공격탐지 시스템을 구축하여 SIP 세션을 능동적으로 관리하였으며 보안 기능을 강화하기 위해 사용자 인증을 적용하여 SIP 프로토콜의 취약점을 해결할 수 있었다. 본 논문에서 제시한 기법은 기존 SIP 프로토콜에서의 보안 취약성을 해결하고 최소한의 트래픽 전송 지연만으로도 안전하게 패킷을 송수신할 수 있도록 하였으며 SIP 프록시 서버에서의 서비스 지연, 서버의 과부하 등의 문제를 최소화할 수 있도록 설계되었다.

■ 중심어 : | SIP | 공격 탐지 | 상태정보 | 보안 및 인증 |

Abstract

The user valence of VoIP services with SIP protocol is increasing rapidly because of cheap communication cost and its conveniency. But attacker can easily modify the packet contents of SIP protocol as SIP header is transmitted by using UDP methods in text form. The reason is that SIP protocols does not provide an authentication function on the transmission session. Therefore, existing SIP protocol is very weak on SIP Packet Flooding attack etc. In order to solve like this kinds of SIP vulnerabilities, we used SIP status codes under the monitoring module for detecting SIP Flooding attacks and additionally proposed an advanced protocol where the authentication and security function is strengthened about SIP packet. We managed SIP session spontaneously in order to strengthen security with SIP authentication function and to solve the vulnerability of SIP protocol. The proposed mechanism can securely send SIP packet to solves the security vulnerability with minimum traffic transmission. Also service delay in SIP proxy servers will be minimized to solve the overload problem on SIP proxy server.

■ keyword : | SIP | Attack Detection | Status Code | Security and Authentication |

* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음" (NIPA-2009-(C1090-0902-0016))

접수번호 : #091008-007
접수일자 : 2009년 10월 08일
심사완료일 : 2010년 01월 05일
교신저자 : 이형우, e-mail : hwlee@hs.ac.kr

Ⅰ. 서 론

현재 인터넷 전화 서비스라고 불리는 VoIP (Voice Over Internet Protocol)[1]서비스는 IP망을 이용해 음성 데이터를 전송하는 기술이다. 이 기술은 저렴한 통신비용과, 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 다양한 편리함을 갖고 있어 여러 사용자들을 통해 빠르게 확산되어가고 있는 추세이다. 기존의 여러 상용화된 VoIP 시스템은 대부분 ITU-T (International Telecommunication Union Telecommunication Standardization Sector)의 H.323이라는 시그널링 프로토콜을 사용하여 초창기에 VoIP 서비스를 시작하였다. 하지만 H.323 프로토콜[2]은 LAN 환경에서 멀티미디어 통신을 지원하기 위해 개발된 프로토콜로 확장 네트워크 구성과 대규모 사용자를 지원하는데 한계가 있었다. 또한 H.323 프로토콜은 서비스 구현이 복잡하고 호환성을 보장하지 못한다는 단점을 가지고 있다. 따라서.최근에는 이러한 단점을 보완하기 위해 SIP(Session Initiation Protocol)[3]이 등장하였다. SIP는 H.323에 비해 개방형 네트워크를 기준으로 개발되고 다양한 멀티미디어서비스를 쉽게 수용할 수 있고 간단한 프로토콜 구조를 가지고 있기 때문에 개발이 쉬워 확장성이 뛰어나다. 하지만 이러한 여러 장점들 때문에 새로운 문제가 발생하고 있다. SIP 프로토콜 역시 기존의 IP 프로토콜을 이용하기 때문에 IP 기반 공격에 그대로 노출된다는 한계를 가지고 있다. 대표적인 SIP 공격기법으로는 비정상 메시지 공격(Malformed Message Attack), SIP 메시지 폭주 공격(SIP Message Flooding Attack), SIP 스푸핑 공격(Spoofing Attack), 도청, DoS 등의 다양한 공격이 존재한다.이러한 공격기법의 근본적인 문제는 공격자가 정상적인 SIP 통신 패킷을 수정 및 삭제하고 이를 변경하는데 문제가 없기 때문에 발생하는 공격들이다. SIP 메시지 폭주 공격을 탐지[5]하기위해 CUSUM (Cumulative Sum), 헬링 거리 (Hellinger distance), 가변 임계치(Adaptive threshold) 등의 다양한 방법과 HTTP 인증, TLS, DTLS 기법, S/MIME(Secure/ Multipurpose Internet Mail)기법[6] 등 다양한 연구가 수행되어져 왔다. 하지만 이러한 기법들 또한 실질적으로 근본적인 문제를 해결하지 못하는 못하고 있고 서비스의 지연 문제로 인해 정상적인 SIP 통신을 하는데 큰 문제가 있다.

따라서 이러한 SIP 프로토콜 취약성을 이용한 공격에 대한 능동적 해결방안의 근본적인 연구가 절실히 필요한 실정이다. 현재 SIP 서비스는 사용자 등록 과정을 수행하는 프록시 서버(Proxy Server)와 각각의 사용자(Client)들로 구성되며, SIP 호 연결 과정을 통해 사용자들이 RTP/RTCP 프로토콜을 이용해 통화를 통해 서비스를 받을 수 있는 구조를 가지고 있다. 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.

본 논문에서는 기존의 공격탐지 기법의 문제점을 해결하기 위해 기존 SIP프로토콜을 최대한 현 상태로 유지하고 SIP 프로토콜의 근본적인 취약점을 해결할 수 있는 메커니즘을 제시하고 기존 SIP서비스의 취약점을 근본적으로 해결하기 위해 SIP 프록시 서버와 사용자간의 전송되는 패킷에 대한 명확한 분류와 상태정보 분석 과정(SIP Stateful Inspection)이 선행하고, 정확한 사용자 인증을 통해 사용자들로 하여금 정상적인 서비스를 보장하기 위한 인증기법을 제안 하다. 또한 SIP 프로토콜의 근본적인 취약점 즉, SIP 패킷에 대한 변/복조를 대응하고 기존 공격기법을 예방하기 위해 SIP Firewall 개념과 SecureSIP 프로토콜을 제시하였다.

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

II. 관련연구

2.1 SIP 프로토콜 분석

SIP(Session Initiation Protocol)[2]는 음성을 포함한 화상, 텍스트 등 멀티미디어 통신 세션을 생성, 삭제, 변경할 수 있는 프로토콜로서 국제 표준화 기구인 IETF(Internet Engineering Task Force) 표준이다. SIP는 H.323 프로토콜[2]에 비해 앞서 설명되었던 바와 같이 다양한 멀티미디어서비스를 쉽게 수용할 수 있고, 간단한 프로토콜 구조, 개발이 쉬워 확장성이 뛰어나다는 장점을 갖고 있다. 이를 바탕으로 빠른 속도로 확산되고 있다. SIP 세션 설정 및 통신 과정은 사용자가 프록시 서버에 등록하는 과정부터 시작된다. SIP 프록시 서버는 사용자로부터 호 연결 및 해제 요청을 대행해 주는 서버이다. [그림 1]은 SIP 통신과정의 패킷 흐름에 대한 전반적인 그림이다.

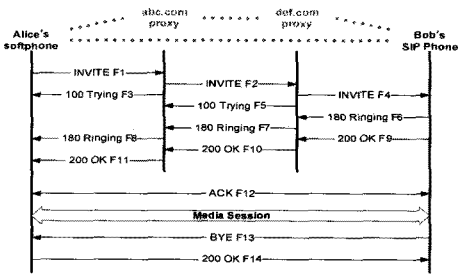


그림 1. SIP프로토콜 등록 과정

SIP 메시지는 TEXT 기반 메시지 형태로 구성되어 있다. 구체적인 내용을 보면 기존의 HTTP 언어 형태의 메시지 구조를 사용한다. 메시지의 구분과 형태는 [표 1]과 같다.

표 1. SIP Request/Response 메시지

종류	세부메시지	내 용
Request 메 시 지	Invite	SIP 세션을 시작할 때 즉, 콜을 만들 때 클라이언트가 서버 쪽으로 전송하는 메시지
	ACK	다른 메시지의 응답메시지
	BYE	클라이언트가 콜을 종료할 때 서버에서 해당 콜이 종료되었음을 알릴 때 사용하는 메시지
	Cancel	앞서 요청된 하지만 아직 완료되지 않은 요청을 취소 할 때 사용하는 메시지
	Option	콜 셋업과 관계없이 서버에 대한 정보를 요구할 때 사용되는 요청 메시지
	Register	자신의 SIP 주소와 IP 어드레스 정보 등을 등록할 때 사용하는 메시지
Response 메 시 지	1XX	요청에대한 응답 메시지. 클라이언트가 요청한 정보에 대한 응답으로 사용.
	2XX	성공 메시지
	3XX	Redirect 메시지. SIP Redirect 서버를 사용 시 발생
	4XX	클라이언트의 요청 메시지에 문제가 있음을 표시
	5XX	500번대 메시지는 서버의 문제를 나타낸다.
	6XX	그 외 나머지 일반적인 에러를 표현

이러한 메시지들의 흐름을 다이어그램을 이용하여 순서대로 표현하게 되면 [그림 2]와 같이 상태의 흐름을 나타낼 수 있다.

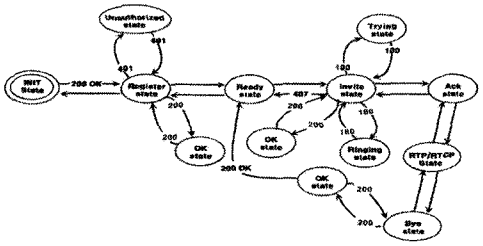


그림 2. 기존의 SIP State Diagram

2.2 SIP 취약점 분석

SIP 프로토콜은 많은 장점들을 가지고 있다. 하지만 동시에 현재의 SIP 서비스는 심각할 정도로 많은 취약성[4][7]을 가지고 있다. 서론에서 언급된 바와 같이 SIP프로토콜의 가장 취약점은 텍스트 기반의 패킷을 사용하고 있어 공격자가 패킷을 자유자재로 수정/삭제하여 생기는 공격들이 발생한다는 것이다. [그림 3]은 가장 대표적으로 SIP 서버와 클라이언트를 스캐닝하고 이에 맞는 패킷을 수정/삭제하여 공격을 할 수 있는 도구[8]이다.

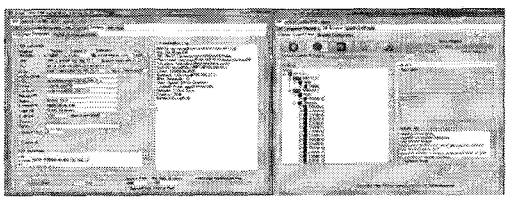


그림 3. SiVus 도구

[그림 4]는 대상 사용자와 프록시 서버의 취약점을 테스팅 하는 도구이다. 이 도구 또한 [그림 3]의 SiVus와 비슷하지만 다양한 메시지를 수천 혹은 수만 개를 생성하여 보냄으로서 어떤 공격에 취약한지를 테스트함과 동시에 취약점에 대한 공격도 할 수 있다.

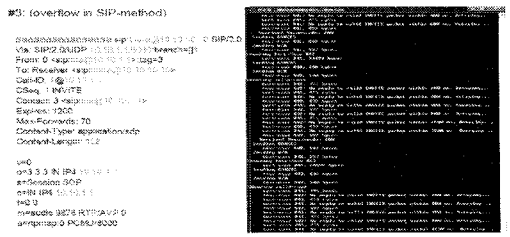


그림 4. Protos Test-Suit(c07-sip)

이외에도 공격자는 와이어샤크 등과 같은 수십 가지의 공격/테스팅 툴을 간단히 이용하여 SIP 프로토콜을 공격하고 자신이 원하는 정보를 얻을 수 있고 또한 이를 이용하여 정상적인 서비스를 방해하기 위해 손쉽게 패킷을 수정/삭제 할 수 있다. 또한, 공격자가 공개되어 있는 툴들을 이용하여 스팸, SIP 메시지 변조(Parser), 폭주(Flooding), DoS 등의 공격들을 하기 때문에 다양한 문제가 발생한다. 따라서 단순히 다른 기존의 연구들처럼 공격탐지의 수준이 아닌 인증과 안전한 SIP 통신을 보장하고 서비스의 QoS를 보장하고 지연이 없이 근본적인 문제 해결책이 절실히 필요한 실정이다.

2.3 기존의 해결방안

Kerberos는 MIT의 Athena프로젝트의 일부로 개발된 인증 서비스로 워크스테이션을 이용할 때 분산된 네트워크 환경에서 사용자 인증을 목적으로 쓰였다. 이는 대칭키 알고리즘 같이 이전부터 많이 사용된 알고리즘을 사용하고 스푸핑(Spoofing), 도청(Eavesdrop), 재전송 공격을 대응하기 위한 기법이다. Kerberos는 티켓이라는 인증매체를 이용하고, 모든 종류의 암호화 기법을 지원한다. Kerberos 프로토콜[9][10]은 [그림 5]와 같이 제 3자 인증 서비스로서 인증을 수행한다. Kerberos는 호스트 오퍼레이팅 시스템의 인증에 의존하지 않고, 호스트 주소에 대한 신뢰를 기초로 하지 않으며, 네트워크상의 모든 호스트의 실제 보안을 요구하지 않고, 네트워크에 돌아다니는 패킷을 언제든지 읽고 수정하고 삽입할 수 있다는 가정 하에서 ID를 검증할 수 있는 수단을 제공한다.

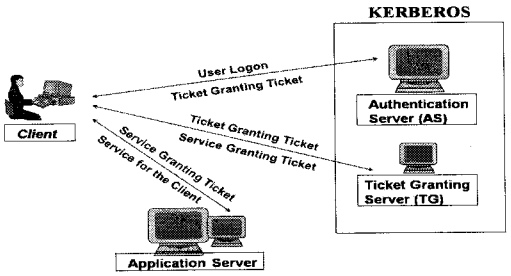


그림 5. Kerberos 프로토콜

현재 SIP 프로토콜을 위한 다양한 보안 메커니즘이 제시되었지만 아직까지 새로운 공격에 즉각 대응하지 못하기에 많이 부족한 실정이다. 또한 지연시간의 문제와 시스템의 과부하 문제를 해결하지 못한다는 문제점이 있다. 앞서 2.2절에서 언급했던 SIP 프로토콜의 취약점을 해결하기 위한 근본적인 해결책이 절실히 필요하다.

따라서 본 논문에서는 이러한 기존의 문제점을 해결하기 위해 상태정보를 분석하고, 안전한 SIP 프로토콜의 통신을 보장하기 위해 각 사용자들의 개별적인 인증과 데이터의 무결성을 보장할 수 있는 안전한 세션을 보장하기 위한 연구를 하였다.

III. 제안하는 프로토콜

본 논문에서는 상태정보를 분석함으로 보안침해사고를 일으키는 공격을 빠르게 분류하여 비정상적 행위를 효율적으로 탐지하는 기술을 수행하는 상태정보(stateful)기법과 각각의 사용자와 프록시 서버 사이의 인증을 통한 안전한 SIP 통신(Secure SIP)환경을 제시하고자 한다.

3.1 전체 프로토콜 구조

본 논문에서 제안하는 시스템 구조는 [그림 6]과 같이 기존의 SIP 통신환경에 SIP Firewall을 추가 하고, 상태정보를 실시간으로 체크 할 수 있고 안전한 SIP 통신을 제공하기 위해 인증 모듈과 암/복호 알고리즘을 협상하는 단계를 적용하여 안전한 SIP 프로토콜을 설계하였다.

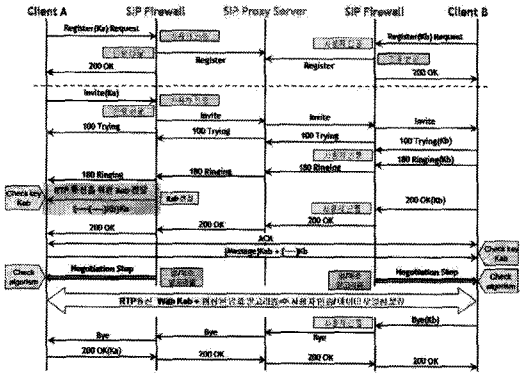


그림 6. 제안한 SIP프로토콜의 흐름

그 결과 기존 SIP에 없었던 실시간 상태정보, 인증정보 확인 그리고 암호화 알고리즘의 협상단계를 통해 데이터의 무결성을 보장하면서 통신가능한 안전한 SIP 프로토콜을 제안하고, 또한 기존 SIP 프로토콜에 최소한의 변화와 SIP Firewall을 통해 작업을 분산 처리 하면서 서비스의 지연 문제를 해결한다. 본 논문에서 제안하는 Stateful/Secure SIP 프로토콜은 앞서 설명되었듯이 SIP 프로토콜의 근본적인 문제를 해결하기 위해 각 단계별로 세부적으로 준비 단계와 인증확인, 협상단계가 순차적으로 필요하다. 따라서 이해를 위해 3.2에서 부터는 간단한 용어 설명이 되어있고, 3.3에서 부터는 SIP 통신 순서를 기반으로 순서대로 각 단계에서 수행되어지는 행위와 인증단계를 위한 준비 과정에 대해 세부적으로 서술 하였다.

3.2 용어 정의(Notation Definition)

본 논문에서 제안하는 프로토콜을 이해하기 위한 용어 설명을 [표 2]에서 보여주고 있다.

표 2. 용어 정의

Symbol	Definition
사용자 키	안전한 인증을 통한 호 설정을 위한 사용자 개개인의 키
Session Key	두 사용자의 RTP/RTCP 통신을 위한 SIP Firewall에서 생성된 임시 세션 키
SIP Client	IP 네트워크를 통해 서버와 다른 사용자들의 연결을 요청하는 사용자
SIP Proxy Server	SIP 사용자의 등록과 호 설정/연결을 도와주는 서버
SIP Firewall	사용자들의 개별 인증 및 세션키 생성, 암호화 알고리즘 협상 역할 수행
K_a	사용자 A의 키
K_b	사용자 B의 키
K_{ab}	사용자 A와 B가 RTP/RTCP 통신을 하기 위한 세션키
E	암호화
D	복호화
Et	Negotiation 단계를 통해 선택되어질 공개키 암호화 알고리즘의 집합
$Keylength$	Negotiation 단계를 통해 선택되어질 암호문의 길이
TS	현재시간
TD	생성된 세션 키의 유효시간
α	TS, TD, K_{ab}를 포함한 집합 표현

3.3 키 등록 및 SIP 레지스트리 단계

본 논문에서 제안한 기법은 Kerberos 프로토콜의 사용자의 인증 부분을 응용하고, 간소화 하여 SIP프로토콜에 적용한 기법이다. 빠르고 안전한 통신을 시작하기 위한 첫 번째 준비 과정으로 사용자 인증과 안전한 호 설정 과정을 위한 준비 과정이다. [그림 7]에서와 같이 오프라인 형식의 사용자들의 개인의 키를 등록 과정이다.

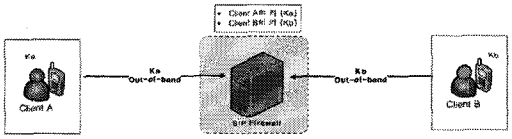


그림 7. 통신 전 사용자 키 등록

[그림 7]에서와 같이 각각의 사용자 Client A, B는 자신의 키를 오프라인 형태로 네트워크 환경을 거치지 않고 키 $\{K_a, K_b\}$를 사전에 SIP Firewall에 안전하게 등록하게 된다. 또한 이 과정을 통해 등록 되어진 키를 이용해 각각의 사용자는 자신과 서버사이의 각종 등록, 전화요청 등의 단계를 서버에 요청하기 전에 SIP

Firewall을 통해 사전 인증단계와 안전한 연결을 주고 받을 수 있도록 한다. 위의 단계를 거친 후 사용자는 실시간 인증과정을 통해 [그림 8]에서와 같이 안전한 호 설정과 Register 단계를 수행할 수 있게 된다. 또한, 각 사용자의 인증키가 일치 하지 않을 경우 SIP Firewall 단에서 실질적인 등록을 차단하여 SIP 프록시 서버의 과부하 문제 또한 해결할 수 있게 된다.

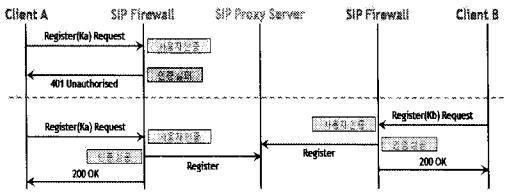


그림 8. 사용자 키를 이용한 등록의 흐름

본 논문에서는 위의 그림과 같이 사전의 교환된 키를 통해 아래 [그림 9]와 같이 각각의 사용자들은 자신들의 키를 통해 안전하게 호 설정 및 연결을 할 수 있도록 제안한다. 또한 SIP 통신 환경과 속도에 최대한 지장을 주지 않기 위해서 그림에서와 같이 패킷의 전체에 대한 암/복호화가 아닌 불필요한 부분을 제하고 인증을 위한 일부분의 필요한 정보에 대해서만 각 사용자의 키를 통해 암호화함으로써 복호화의 시간 또한 절약한다.

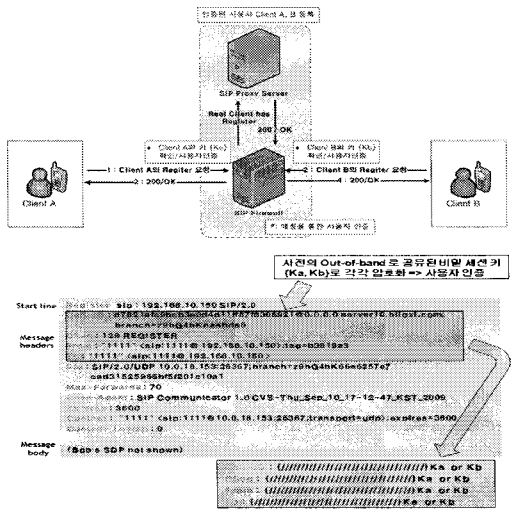


그림 9. 사용자 키를 이용한 사용자 인증 및 등록

3.4 SIP 호 설정 단계

SIP 통신과정 중 상대방 사용자와 통화(RTP/RTCP)를 하기위해 Invite 단계를 통해 요청하는 단계가 있다. 기존의 SIP 취약점 중 공격자가 메시지를 수정/삭제하기 위해 가장 많이 간섭하는 단계 중 하나이다. 따라서 본 논문에서는 이러한 공격들을 사전에 방지하기 위해 기존의 프로토콜에 전 단계에서 설명한 사용자별 키를 이용해 인증단계를 추가시켰다. [그림 10]은 본 논문에서 제안한 SIP 프로토콜 흐름으로 기존 프로토콜에 사용자 인증 단계를 추가시켜 SIP Firewall과 사용자가 서로 신뢰 할 수 있는 통신을 보장 받을 수 있는 환경을 표현한 그림이다.

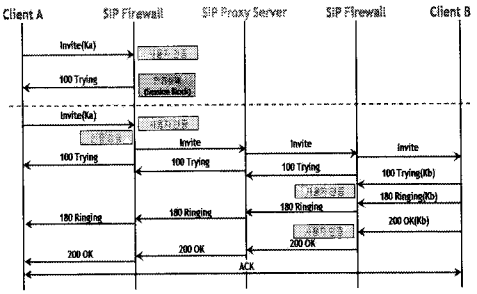
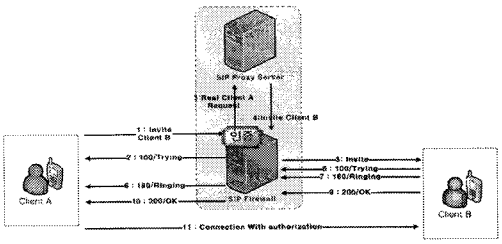


그림 10. 각 호 설정 요청시의 인증단계

3.3의 등록 단계와 위의 그림에서와 마찬가지로 Invite 호 설정 요청 시와 기타 호 설정 시 각 사용자와 SIP Firewall 사이에 안전한 연결을 위해 패킷의 일부분을 암호화하여 신뢰할 수 있는 SIP통신환경을 제안한다. 호 설정 또한 SIP 서비스의 지연을 최대한 줄이기 위해 패킷의 일부분만 암/복호화 함으로써 시간을 절약한다.



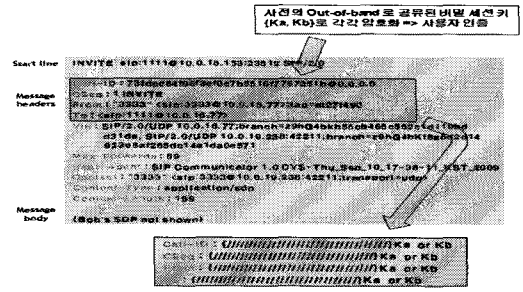


그림 11. 인증된 사용자의 호 설정

3.5 RTP/RTCP 통신 단계

본 논문에서는 안전한 RTP 통신을 위한 준비를 하기 위해 [그림 12]와 같이 RTP/RTCP 통신의 전전 단계(Ringing)에서 SIP Firewall을 통해 두 사용자만의 특별한 세션키를 전달할 수 있는 단계를 추가 시켰다. 이는 SIP 통신이 UDP 통신을 한다는 전제조건을 감안하여 혹시 있을 패킷지연에 대한 사전 대응방법이다. [그림 12]에서와 같이 각 호 설정 시 SIP Firewall 단에서의 각 사용자의 고유 세션키의 확인을 통한 사용자 인증단계를 반복하게 되고 호 연결을 요청한 두 사용자의 세션키를 조합한 새로운 세션키인 K_{ab}를 각 사용자에게 전달하게 된다.

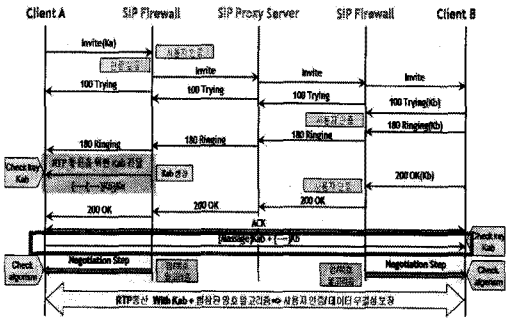


그림 12. 제안 키 전달 과정

각 사용자가 통신을 위한 키를 체크하게 되면 두 사용자는 [그림 12]에서와 같이 패킷의 일부분을 암호화해서 보낼 수 있고 각각 복호화 단계를 통해 비정상적인 사용자 혹은 정상적인 사용자에게서 전달된 패킷인지의 여부를 확인할 수 있다.

$$\alpha = TS + TD$$

$$E((\alpha, K_{ab}(E((\alpha, K_{ab}), K_b))), K_a)$$

$$C = E(\alpha, K_b)$$

$$Ct = \alpha + C$$

$$C' = E(Ct, K_a)$$

위의 수식은 각 사용자의 앞서 언급했던 Kerberos에서 사용하는 방법을 통해 두 사용자의 개인키 K_a, K_b를 조합하여 새로운 K_{ab}를 생성하여 SIP Firewall을 통해 서로 전달 받는 과정이다. α는 TS(현재시간), TD(키의 유효시간)을 포함한다.

$$D(Ct, K_a) = A + C \Rightarrow \text{Key for Client A}$$
$$D(C, K_b) = A + C \Rightarrow \text{Key for Client B}$$

SIP Firewall 은 각각의 사용자만이 공유키로 복호화하여 K_{ab}의 세션키를 확인 할 수 있도록 따로 암호화하여 인증된 사용자들이 공유 할 수 있도록 도와준다.

또한 더욱더 안전한 SIP 통신환경을 위해 키 교환이 안전하게 교환되었다는 확인이 되면 통화를 시작하기 전에 마지막 준비 단계인 협상단계(Negotiation)를 통해 미리 제안된 대칭키 알고리즘의 선택과 키 길이에 대한 협상 단계를 거쳐 이를 바탕으로 RTP 통신을 하게 된다. α에 현재포함하고 있는 두 가지 정보이외에 또한 추가적인 정보도 추가 가능하다.

$$Et = \{AES, DES, ARIA, Seed.....\}$$
$$Keylength = \{64, 128, 192, 256\}$$
$$Et_i = rand()$$
$$Keylength_i = rand()$$
$$Et' = EType(Et_i, Keylength_i)$$
$$C = Et'(msg, K_{ab})$$

위의 식은 세션키 K_{ab}를 교환 후에 SIP 프록시 서버의 앞단에 존재하는 SIP Firewall을 통해 호 설정 요청

을 하는 두 사용자에게 같은 협상단계를 수행하는 과정이다. 랜덤 값을 통해 암호화 알고리즘과 암/복호화 할 평문의 길이를 선정하는 단계이다. RTP/RTCP 통신단계에서 사용할 암호화 알고리즘과 길이가 정해지면 이를 이용하여 통신을 하게 된다.

3.6 세션키 교환기반의 사용자 인증 및 데이터 무결성 보장

본 논문에서 사용하는 키는 크게 사용자별로 각자 가지고 있는 키와 두 사용자가 호 연결 신청을 했을 때 통신을 위해 생성되어지는 세션키가 있다. 이 두개의 키를 사용하여 3.3절과 3.4절에서 언급한 것과 같이 패킷의 일부분을 암호화 하고 비교 분석하여 이를 통해 정상적인 사용자의 인증과 데이터의 무결성을 동시에 보장하는 기법을 제시한다. [그림 13]은 본 논문에서 제안한 인증 패킷 구조이다. 설명에서와 같이 SIP Header, SDP 패킷의 일부분을 복사하여 사용자별 키로 암호화하여 패킷의 뒷부분에 첨가하여 SIP Firewall에서 정확한 사용자인지의 여부를 검토하고 인증을 한다. 또한 생성된 세션키와 협상단계(Negotiation Step) 단계에서 결정된 암호화 알고리즘을 통해 RTP/RTCP 통신 패킷도 일부분 암호화하여 인증단계와 데이터의 무결성을 확인하게 된다.

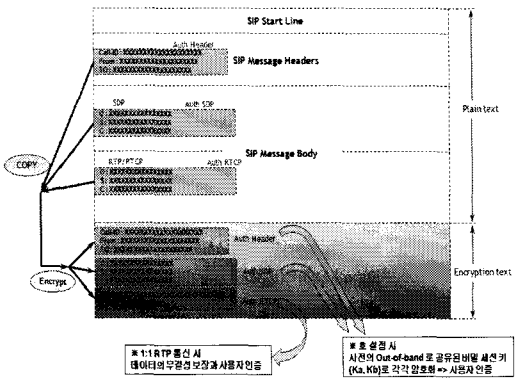


그림 13. 제안 인증 패킷 구조

앞서 지속적으로 언급했던 부분 또한 [그림 13]에 나타나 있다. 기존의 SIP 암/복호화 프로토콜들과는 다른 방법인 패킷의 일부분만 암호화 하여 전송하고, 받은 패킷을 복호화하여 비교/분석함으로써 패킷의 변조 여부와 정상적인 사용자에 대한 인증과정을 통해 보다 안전한 통신을 보장 할 수 있다.

Ⅳ. 공격 탐지 및 대응 메커니즘

본 논문에서 제안하는 시스템 구조는 [그림 14]와 같이 기존의 SIP 통신환경에 변화를 최소화하고 가급적 기존의 방식을 유지하는 방식이다. (1) 기존의 SIP 통신장비와 SIP 통신패킷의 인증모듈을 적용시킨 SIP 사용자 (2) 사용자 키를 관리 및 확인, 전달하는 SIP Firewall로 크게 두 가지로 나눌 수 있다. 따라서 이 구조를 통해 각 사용자와 서버 사이의 상태정보를 수시로 체크하고, 사용자별 키를 체크하여 정상적인 사용자가 호 연결을 요청 했는지의 인증과정과, 각 메시지의 무결성을 체크할 수 있다.

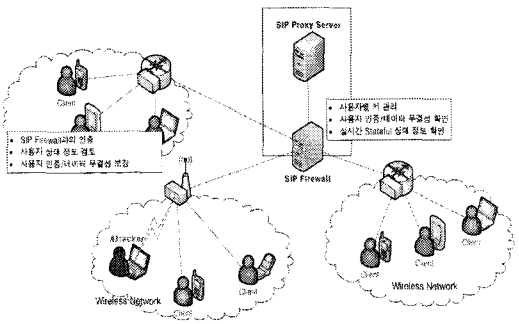


그림 14. 전체 시스템 구조

본 논문에서 제시한 모듈에서는 보다 안전하고 효율적인 공격의 탐지를 하기 위해 클라이언트와 서버 간의 SIP 프로토콜 상태정보를 저장하고 관리한다. 사용자 인증과정을 수행한 후에 [그림 15]에서와 같이 본 논문에서 추가한 사용자 인증단계를 고려하여 작성된 SIP Formal State를 비교/분석하고 실시간 정상적인 상태정보를 유지하고 분석한다.

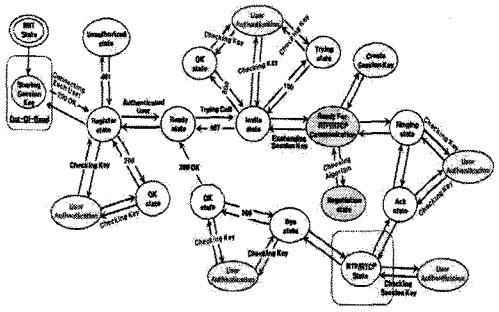


그림 15. SIP Formal State Model

또한 [그림 15]에서와 같이 기존에 없던 각 단계별 인증단계를 추가로 삽입하여 보다 안정적으로 보장된 SIP 통신이 가능해 졌다.

[그림 16]은 본 논문에서 제안한 SeureSIP 기반의 SIP Firewall의 전체 모듈 구성도이다. 앞서 설명한 각 사용자별 인증과, 정상적인 상태정보 패킷에 대한 검사, RTP 통신을 위한 암/복호화 알고리즘 테이블을 참조하는 단계를 수행한다.

- 1단계 : 필터링(Filtering) 단계를 거쳐 SIP 패킷의 여부를 확인하고 블랙리스트(Black List)와 각 사용자별 세션키를 이용한 사용자 인증을 하는 단계.
- 2단계 : 각 사용자들의 Session Classification단계 수행 후, 실제 SIP 패킷과 사용자의 키를 분리하여 Key table과의 Verification 단계를 통해 사용자 인증을 한다. 또한 동시에 SIP Analysis 단계를 거쳐 SIP State Table에 현재 상태정보를 최신화하는 단계.
- 3단계 : SIP Formal Model 기반의 실시간 상태정보를 비교/분석하여 정상적인 상태정보 여부가 오는지의 여부를 체크하는 단계와 패킷의 통과여부를 검증.
- 4단계 : 협상단계(Negotiation state) 단계를 체크하고 해당될 시 SIP Firewall에 있는 공개 알고리즘 테이블을 참조하여 필요한 알고리즘을 협상하는 단계를 수행.

위와 같은 모듈을 통해 정상적으로 인증된 사용자의 여부와 정상적인 상태정보를 포함한 패킷인지의 여부를 검토를 하여 기존의 공격을 사전 방어/대응을 하게 된다.

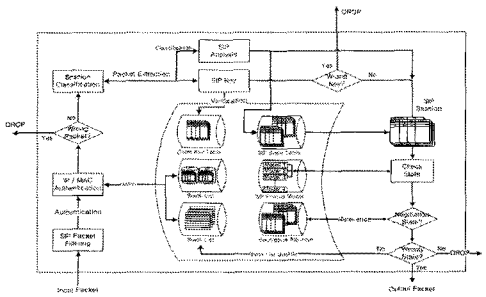


그림 16. SIP Firewall 전체 모듈 구성도

또한, 이러한 흐름에 방해가 되거나 일치 하지 않는 패킷은 공격이라 판단하며, 실시간 BlackList에 등록과정을 통해 다음번의 경우에 이를 사전에 빠르게 차단할 수 있도록 정보를 갱신 한다.

V. 안정성 분석

본 논문를 통해 제안된 Stateful/Secure SIP 프로토콜은 기존의 문제점을 해결하고 SIP 인증 취약점을 보완하기 위해 제안한 대응 메커니즘이다. 본 장의 안정성 분석은 기존 SIP 보안 메커니즘과 제안된 몇 가지 기법들을 비교/분석하였다.

5.1 SIP 메시지의 변조 공격에 대한 탐지 및 대응

앞서 설명 되었듯이 기존 SIP 프로토콜의 패킷은 텍스트 형식이다. 이는 가장 큰 장점인 동시에 단점이 되어 공격에 쉽게 수정 및 삭제가 된다는 문제점을 안고 있다. 따라서 본 논문에서는 근본적인 SIP 메시지의 변조 공격에 대한 탐지 및 대응을 하기 위한 기법을 제시하였다. SIP 메시지의 변조에는 크게 몇 가지가 있다. 공격자가 자신의 IP로 패킷을 돌리기 위해 필요한 정보를 수정하거나, 통신 중간에 통신을 끊는 상태정보를 (Cancel, Bye) 수정 및 삽입하여 정상적인 서비스를 방해한다. 본 논문에서는 [그림 17]에서와 같이 SIP 통신

패킷에 대한 일부를 암호화 하고 SIP Firewall에서 비교/분석하여 패킷의 변조 여부에 대해 확인을 하게 된다. 따라서 중요한 일부분의 대조한 결과 비정상적인 사용자로 하여금 수정/변조 여부를 확인 하여 공격을 탐지하고 이를 BlackList에 Update 하여 다음 공격에 대한 사전 대응을 한다.

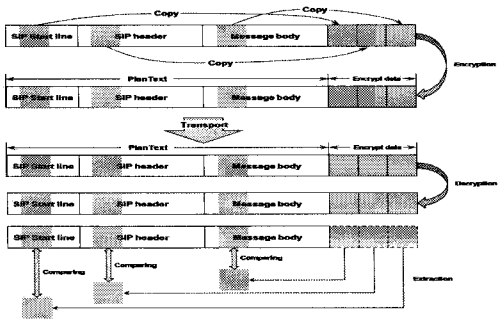


그림 17. SIP 패킷 암/복호화와 비교 분석

또한 SIP Message Flooding공격과 같이 다량의 메시지를 보내 정상적인 서비스를 방해 하는 경우에도 위의 [그림 17]과 [그림 15]의 정상적인 상태 정보 패턴과 맵핑하여 공격의 여부를 판단하고 또한 이를 대응한다. 예전에 힘들었던 SIP Register Message Flooding 공격에 대한 문제 또한 각 사용자와 세션에 대한 보장을 통해 이를 간단하게 해결할 수 있었다.

5.2 메시지 및 사용자 인증

5.1절 메시지의 변조의 여부 분석을 위해 메시지, 사용자의 인증은 필수적인 요소이다. 본 논문에서는 이와 같은 문제 해결을 위해 빠른 속도와 안전한 키 전달을 위한 연구를 하였다. 그 결과 안전한 키 전달은 3.3절에서 설명 되었던 바와 같이 Out-of-band를 통해 offline에서의 키를 전달하였다. 또한 SIP 서비스의 지연문제 해결과 정상적인 속도의 보장을 위해 패킷의 필요한 일부분만을 복사하여 암호화 하고 이를 SIP Firewall에서 비교 및 분석하였다.

메시지 및 사용자 인증에서 msg는 SIP 원본 메시지를 나타내고, $Pmsg$는 암호화할 SIP 메시지의 일부분을 나타낸다. 또한 K_a는 키 집합 사용자의 본인의 개인키이다. 사용자 인증시 msg 패킷의 중요 일부를 선택해서 $Pmsg$를 생성하여 $Pmsg$를 키 K_a로 암호화한 후 다른 사용자에게 전달하기 이전에 SIP Firewall을 거쳐 사용자와 메시지 인증을 받게 된다. 이는 암호화된 $Pmsg$를 복호화 하여 실제 $Pmsg$와 비교/대조하여 일치하는지의 여부를 통해 각 사용자들의 키와 메시지의 변조 유무를 확인하는 단계이다.

$msg + E(Pmsg, K_a) = msg'$
send(msg') to *SIP Firewall*
$msg + D(E(Pmsg, K_a), K_a)$
if $D(Pmsg, K_a)$ == "Original $Pmsg$" is true
else false {Not Authenticate}

따라서 이러한 과정을 통해 정상적인 사용자와 정상적인 키의 여부 확인과 메시지의 변조 여부를 검토하여 메시지의 인증과정을 동시에 확인하여 이를 효율적으로 인증하게 된다.

본 논문에서 제안한 SIP Firewall을 통해 기존 SIP 서버의 과부하 문제 또한 해결하고 커버로스를 응용하여 각 사용자별 키 관리를 하여 빠르게 메시지와 사용자 인증 문제도 해결할 수 있다.

5.3 제안한 프로토콜의 안정성 분석

정보에 대한 위협이란 허락되지 않은 접근, 수정, 노출, 훼손, 파괴 등이다. 본 논문에서는 SIP 프로토콜의 보안을 보장하기 위한 방법을 제안하였다. 또한 정보보안의 기본적인 요소들을 보장함으로써 안전한 SIP 프로토콜 기법을 제안하였다.

1) 기밀성 보장

기밀성이란 허락 되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것이다. 원치 않는 정보의 공개를 막는다는 의미에서 프라이버시 보호와 밀접한 관계가 있다. 본 논문에서는 필요한 중요 일부 정보를 암/복호화 과정을 통해 SIP 통신과정중 사전의 인증된 사용자만을 보호하고 불규칙한 협상단계를 통해 $Pmsg$를 비교 분석 하였다. 또한 이를 통해 메시지의

변조 유무를 검토하여, 기밀성 보장을 하고 보다 안전한 SIP 통신환경을 보장하였다.

2) 무결성 보장

허락 되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는 것이다. 따라서 공격자로 하여금 SIP 통신 패킷 즉, 메시지를 임의로 수정/삭제할 수 없도록 보장해야 된다. 본 논문에서는 SIP 통신의 무결성을 보장하기 위해 패킷의 일부를 복사하고 암호화 과정을 통해 원본 패킷의 변조가 이루어졌는지의 여부를 검토함으로써 공격의 여부를 판단하게 된다. 따라서 SIP 통신상의 무결성 또한 보장할 수 있다.

3) 가용성 보장

허락된 사용자 또는 객체가 정보에 접근하려 하고자 할 때 이것이 방해받지 않도록 하는 것이다. SIP 환경에서의 가용성을 해치는 대표적인 공격은 SIP Message Flooding, Parser 공격이 있다. 이는 본 논문에서 제안한 Formal State Diagram을 통해 정상적인 형태의 패킷이 아닐 경우 이를 탐지하고 이를 대응함으로써 가용성을 보장하게 된다.

4) 인증

본 논문에서 제안한 사용자 개인의 키와 RTP/RTCP 통신 하에 사용하는 두 사용자만의 세션키를 통해 인증 과정을 수행하게 된다. 사용자별 개인의 키는 호 설정 과정에서의 SIP Firewall에서의 검증을 통해 정상적인 사용자의 패킷 여부를 검토 하게 되고 RTP/RTCP 통신이전에는 SIP Firewall에서 두 사용자의 새롭게 조합된 세션키를 전달하고 또한 랜덤하게 선택된 대칭키 알고리즘과 암호문의 길이를 협상하여 보다 안전한 통신을 제공한다.

따라서 본 논문에서는 위의 네 가지 보안 요소를 모두 제공한다. 또한, 기존의 문제였던 서버의 과부하 문제와 서비스의 지연문제 또한 빠르게 해결할 수 있도록 필요한 기능을 제공하여 안전하고 빠른 SIP 통신을 보장할 수 있다.

5.4 기존 시스템과의 비교

본 논문에서 제안한 Stateful/SecureSIP 프로토콜은 5장에 설명되었듯이 [표 3]에서와 같은 다양한 기능을 제공하여 기존의 기법들보다 뛰어난 성능을 가지고 있다.

표 3. Stateful/SecureSIP 프로토콜 기능

	메시지 변조 탐지	상태정보 패턴 매칭	사용자 인증	데이터 무결성 보장	안전한 호 설정 보장	RTP 통신 환경 보장
결과	O	O	O	O	O	O

본 논문에서 제안한 기법은 SIP 통신의 근본적인 문제를 해결하고 또한 호 설정 단계와 RTP/RTCP 통신에서 공용으로 대응할 수 있는 해결책을 주목적으로 하였다. 따라서 SIP 통신상의 실시간 상태정보 관리와 Kerberos 시스템을 응용한 SIP Firewall을 제안함으로써 효율적인 암/복호화와 이를 통한 사용자, 메시지의 인증을 할 수 있었다. 또한 이를 통해 기존 시스템의 기본적인 문제점인 서비스 지연, 서버의 과부하 문제를 해결하고, 또한 호 설정단계와 SIP 통신 상태를 동시에 관리/인증할 수 있는 환경을 제안 하였다. 본 논문에서 제안한 프로토콜을 기존의 시스템들과 비교하여 [표 4]로 비교/분석하였다.

비교/분석 결과 본 논문에서 제시한 기법은 기존의 시스템에서 제공하지 못했던 여러 부분을 제공하고 기존의 문제점을 해결할 수 있다는 것을 확인할 수 있었다.

표 4. 기존 기법들과의 성능 분석

기법 / 기능	제안한 Stateful/ Secure SIP 프로토콜	vIDS [11]	SRTP [12]	DTLS [13]
사용자 인증 여부	O	X	X	O
데이터 무결성 보장	O	X	O	O
RTP 통신 보장	O	X	O	O
Spoofing 공격탐지	O	O	X	X
Flooding 공격탐지	O	O	X	X
Parser 공격탐지	O	X	X	X

VI. 결 론

현재 SIP를 응용한 IP Phone을 포함한 많은 장비들과 이를 사용한 사용자 또한 급속도로 증가 하고 있는 추세이다. 이는 VoIP를 이용한 SIP 서비스가 IP망을 이용하기 때문에 통신비용이 저렴하고, 다양한 부가서비스를 제공하며, 기존 IP 기반 네트워크 자원의 가용성과 효율성을 극대화 할 수 있기 때문이다.

본 논문에서는 기존의 공격탐지 기법의 문제점을 해결하기 위해 기존 SIP프로토콜을 최대한 현 상태로 유지하고 SIP 프로토콜의 근본적인 취약점을 해결할 수 있는 메커니즘을 제시하였다. 이는 기존 SIP서비스의 취약점을 근본적으로 해결하기 위해 SIP 프록시 서버와 사용자간의 전송되는 패킷에 대한 명확한 분류 및 분석 과정을 선행하고, 정확한 사용자 인증을 통해 사용자들로 하여금 정상적인 서비스에 보장하기 위한 인증기법을 제안하였다. 또한, SIP 프로토콜의 근본적인 취약점 즉, 패킷에 대한 변/복조를 대응하고 기존 공격기법을 예방하기 위해 SIP Firewall 개념과 SecureSIP 프로토콜을 제시하였다. SIP Firewall의 기능을 강화하여 사용자 인증을 위한 키 관리, RTP 통신을 위한 세션 키 제작, 안전한 SIP통신을 위한 암호화 알고리즘과 암/복호문의 길이를 결정하기 위한 협상단계, 각 호 설정별 상태정보 관리의 기능을 추가 하였다. 따라서 기존 SIP 서버/클라이언트 통신의 과부하 문제를 해결함과 동시에 SIP 통신의 근본적인 취약점을 해결하기 위한 해결책을 제시 할 수 있었다.

참 고 문 헌

[1] 한국전자통신연구원(ETRI) 기술평가팀, "VoIP 기술 및 시장 동향", 한국전자통신연구원(ETRI) 2006.

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

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

[4] 구자현, "VoIP 서비스 보안 취약성 분석", 한국 정보보호학회지, Vol.16, No.1, pp.60-63, 2006.

[5] 원용근, "SIP프로토콜 기반 VoIP 서비스에서 DoS 공격 대응 방안 연구", 한국정보보호학회 동계학술대회, 2007.

[6] 박진범, "VoIP 보안 취약점 공격에 대한 기존 보안장비의 대응 분석 연구", 한국정보보호학회지, Vol.17, No.5, 2007.

[7] C. Mark, "VoIP Vulnerabilities Registration Hijacking," SecureLogix Corporation, pp.1-4, 2005.

[8] http://www.vopsecurity.org, SiVuS(Sip Vulnera-bility Scanner), "User Guide Vol.07," 2004.

[9] J. Y. Migeon, "The MIT Kerberos Admi-nistrator's How-to Guide," Kerveros constortium, 2008,

[10] C. Neuman, J. Kohl, and T. Ts'o, "The Kerberos Network Authentication Service (V5)," Internet draft (work in progress), draft-ietf-cat-kerberos -revisions-06.txt, 2000.

[11] S. Hemant, "VoIP Intrusion Detection Through Interacting Protocol State Machines," 2006.

[12] 최재덕, "SIP 기반의 VoIP 보안 시스템 구현", 한국통신학회 논문지, Vol.29, No.9B, 2004.

[13] 신영찬, "VoIP를 위한 보안 프로토콜 성능 평가", 한국 정보보안학회 논문지, Vol.18, No.3, 2008(6).

저 자 소 개

윤 하 나(Ha-Na Yun) 준회원

- 2008년 2월 : 한신대학교 컴퓨터학부(공학사)
- 2010년 2월 : 한신대학교 컴퓨터학부(공학석사)
- 2008년 3월 ~ 현재 : 한신대학교 대학원 석사과정

<관심분야> : 정보보호, 네트워크보안, VoIP 보안, 홈네트워크보안, 인터넷보안

이 형 우(Hyung-Woo Lee) **정회원**

- 1994년 2월 : 고려대학교 컴퓨터학과(이학사)
- 1996년 2월 : 고려대학교 컴퓨터학과(이학석사)
- 1999년 2월 : 고려대학교 컴퓨터학과(이학박사)
- 1999년 3월 ~ 2003년 2월 : 백석대학교 정보통신학부 교수
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터공학부 교수

<관심분야> : 정보보호, 네트워크보안, 무선랜, 침입탐지/차단, 웹 보안 기술, 컨텐츠 보호