논문 2008-45TC-10-12

VoIP 환경에서 스팸 유형 분석 및 Spamtester 구현

(Spamtester using Spam Categorization in SIP-based VoIP Networks)

최 재 식*, 최 재 덕**, 정 수 환***

(Jaesic Choi, Jaeduck Choi, and Souhwan Jung)

요 약

본 논문에서는 SIP 기반의 VoIP상에서 스팸 공격의 위협에 대해 분석하고 이와 같은 공격을 확인 할 수 있는 Spamtester를 구현하였다. VoIP에서 스팸 공격은 여러 유형들이 존재하지만 구체적인 공격 과정과 위협 결과를 확인 할 수 있는 정보가 부족하다. 특히 정상적인 경로를 통한 스팸 공격 외에 비정상적인 경로를 통한 스팸 공격은 구체적인 정보가 부족하여 발신자 추적은 물론 법적 제재를 가하기 어렵다. 따라서 VoIP에서 실제로 스팸 공격이 가능한 유형들과 공격 과정을 확인할 필요가 있다. 본 논문에서는 이와 같은 스팸 공격들 중 비정상적인 스팸 공격을 분석하고 공격 과정을 설계하였다. 또한 Spamtester를 통해서 스팸을 발송함으로써 구체적인 스팸 공격 과정을 확인할 수 있다. 이는 VoIP에서 스팸 위협을 확인하고 그 스팸 대응 방안을 찾는데 유용할 것이다.

Abstract

In this paper, we analyse the vulnerability of spam attacks and develop the Spamtester to confirm these spam attacks in SIP-based VoIP networks. Although there are several spam attacks on VoIP networks, the detail information for the SPIT is not enough to confirm the procedure and the result of spam attacks on VoIP networks. Specially, the spam attacks through abnormal process are difficult to trace the sender of spam. Also, it is not easy to impose the legal restriction to the spammer because of lack of information for the spam attack. Therefore, on VoIP networks, the possible scenario and detail procedure for VoIP spam is needed to be confirmed. This paper designes and implementes the spamtester, which is helpful to protect VoIP networks from the spam attacks.

Keywords: VoIP, Spam attacks, Spamtester, Vulnerability, Abnormal process

I. 서 론

SIP를 기반으로 한 VoIP 서비스는 현재 상용화 되어 활발히 진행되고 있다. 하지만 SIP[1] 프로토콜을 기반으로 한 VoIP는 스팸 공격에 쉽게 노출되어 VoIP 서비스 추진에 걸림돌이 되고 있다. 이는 다음과 같은 VoIP의 특징 때문이다. 우선 VoIP 시그널링을 위한 SIP 메시지는 이메일과 마찬가지로 텍스트를 기반으로 하고 있어서 스패머가 메시지를 스니핑하거나 변조하기 쉽다. 또한 VoIP는 PSTN 환경보다도 상대적으로 비용 부담이 적기 때문에 스패머가 대량 스팸 발송을 하는데 이용될 수 있다. 하지만 현재 VoIP 스팸 대응 방안은 스팸 공격의 구체적인 정보가 부족하여 해결 방안을 찾는데 어려움이 있다. 특히 정상적인 시그널링에 의한 스팸 공격의 정보가 부족하여 스패머에 대한 발신자 추적이 어렵기 때문에 이에 대한 연구가 필요하다.

본 논문에서는 VoIP 환경에서 스팸 공격의 위협과 취약성을 바탕으로 실제 스팸 공격이 가능한 유형들을 확인하기 위해 비정상적인 스팸 공격 유형들을 분석하고 VoIP 망에 다양한 스팸 공격들을 실험 하였다. 또한 본 논문에서 분석된 스팸 유형들은 Spamtester를 통해 VoIP 망에 스팸 발송을 할 수 있도록 구현하여,

* 학생회원, ** 정회원, *** 평생회원-교신저자
숭실대학교 정보통신전자공학부
(School of Electronic Engineering, Soongsil University)

※ 본 연구는 숭실대학교 교내연구비 지원으로 이루어 졌음.
접수일자: 2008년6월10일, 수정완료일: 2008년10월16일

VoIP스팸 공격 과정을 구체적으로 확인 할 수 있도록 하였다.

본 논문은 다음과 같이 구성되어 있다. Ⅱ장에서는 VoIP 스팸 유형 및 관련 도구에 대해 살펴보고, Ⅲ장에서는 VoIP 환경에서의 SPIT (SPam over Internet Telephony) 시나리오를 설계하며, Ⅳ장에서는 SPIT 시나리오를 바탕으로 실제 스팸을 발생 시킬 수 있는 Spamtester의 구현을 살펴본다. 또한 Ⅴ장에서는 구축된 VoIP 망에서 스팸 발송 실험을 통해 스팸 공격의 위협 결과를 확인하며, Ⅵ장에서는 구현한 Spamtester와 관련도구를 비교하고, Ⅶ장에서는 본 논문의 연구에 대해 결론을 맺는다.

Ⅱ. VOIP 스팸 유형 및 관련 도구

VoIP에서는 스팸 공격이 가능한 다양한 유형들이 존재한다. VoIP 망에서 발생할 수 있는 스팸 공격들은 크게 IM (Instant Messaging) 스팸, 프리젠스 스팸, 콜 스팸 등이 있으며 등록 과정, SIP 세션 과정, 미디어 과정에서의 조작을 통해 다양한 스팸을 발송할 수 있다. 그 중에서 콜 스팸은 실시간으로 음성 파일을 다수의 VoIP 가입자에게 전송함으로써 심각한 피해를 줄 수 있으며 시스템 관리상의 오류나 해킹 등을 통해서도 스팸 발송이 가능하다. 본 장에서는 이와 같은 스팸 공격의 유형들과 SIP 메시지를 생성하거나 스니핑 및 분석할 수 있는 관련 도구들에 대해 살펴본다.

1. VoIP 스팸 유형

첫 번째로 대표적인 VoIP 환경에서의 콜 스팸 공격은 P2P (Peer-to-Peer) 스팸 공격이다[4]. P2P 스팸 공격은 프락시를 우회하여 UAS (User Agent Server)에게 직접 스팸 공격을 할 수 있다. 따라서 발신자 추적은 물론 법적인 제재를 가하기 어렵고 대량 전송에 의해서 다수의 정상 가입자에게 스팸을 전송함으로써 피해가 가장 클 수 있는 스팸 공격이다. 두 번째로 RTP 조작에 의한 스팸 공격이다[5]. 이 공격은 정상 사용자들 간의 호 설정이 형성된 후 스패머가 RTP 패킷 헤더의 sequence number를 무작위로 생성하여 공격 대상자에게 스팸을 전송한다. 따라서 간헐적으로 정상 사용자들의 통화에 스팸이 합성된 공격이 가능할 수 있다. 세 번째로 세션 가로채기 스팸 공격이다[5~6]. 세션 가로채기 스팸 공격은 RTP 세션이 성립이 되기 전 혹은 후에 정상 사용자들 간의 호를 끊고 스패머와 정상 사용자간의 호 성립을 만들 수 있는 공격이다. 네 번째로 데이터베이스 조작을 통한 SQL 삽입 스팸 공격이다[7]. SQL 삽입 스팸 공격은 등록되어진 정상 사용자의 초기 아이디나 비밀번호를 변경하여 정상 사용자의 권한을 불법으로 획득하고 이를 이용하여 공격대상자에게 스팸을 공격하는 방법으로 SIP 메시지에 SQL문을 삽입하여 정상적인 사용자인 것처럼 데이터베이스 테이블을 조작하고 인증되어질 수 있는 공격이다. 다섯 번째로 IM 스팸 공격이다[5]. 이 공격은 콜 스팸은 아니지만 사용자들에게 피해를 줄 수 있는 스팸 공격 중 하나이다. 콜 스팸은 스패머와 공격 대상자 간의 RTP 세션을 연결하여 미리 녹음된 광고성 스팸을 발송하는 공격이지만 IM 스팸은 콜 스팸의 호 설정과는 상관없이 링이 울리는 순간에 공격 대상자의 단말에 광고성 메시지를 보여주는 스팸 공격이다. 이와 같은 스팸 공격은 SIP 메시지 중 INVITE 메시지 일부에 광고성 문구를 삽입하여 스팸 공격을 하며 SIP INVITE 메시지가 공격 대상자에게 도달하는 단계만으로 공격이 가능할 수 있다.

2. SIP 메시지 생성 및 관련 도구

스팸 공격을 하기 위해서 스패머는 본 논문에서 구현된 Spamtester와 같은 관련 도구를 이용할 수 있다. 특히 이메일 상에서 대량 스팸을 발송하는 소프트웨어 프로그램과 같은 툴을 사용하는 스패머는 사용자들에게 더 큰 피해를 끼칠 수 있다. 하지만 VoIP에서 스팸 공격을 실험해 보기위해 만들어진 특정 도구는 거의 존재하지 않는다. 따라서 본 장에서는 스팸 전송에 이용될 수 있는 관련 도구나 툴을 살펴본다. 먼저 SiVus에의한 메시지 스니핑 툴이다[8]. SiVus는 세 가지의 중요 모듈로 구성되며 주로 취약성이 있는 공격 대상자의 ID나 IP를 찾는 스니핑의 목적으로 이용된다. SiVus의 세 가지의 중요 모듈로는 SIP 메시지 생성기 모듈 (SIP Message generator), 공격 대상자를 찾는 모듈 (SIP component discovery), SIP 취약성 분석 모듈 (SIP vulnerability scanner) 이다. 각 모듈의 기능은 SIP 취약성 분석 모듈과 공격 대상자를 찾는 모듈을 통해서 취약성이 있는 공격 대상자를 조사하고 SIP 메시지 생성기를 이용하여 공격자에게 발송할 SIP 메시지를 생성한다. 다음으로 PROTOS c07-SIP 테스트 툴이다[8]. PROTOS c07-SIP은 초기에는 UA (User Agent)나 프락시와 같이 VoIP 망을 구성하고 있는 각 컴포넌트의 동작과정을 테스트하는 툴이였다. 하지만 최근에는 스패머가 이 툴에서 제공하는 비정상적인 INVITE 메시

지를 VoIP 망에 전송하여 취약성이 있는 UA나 프락시를 찾는 도구로 사용된다. 이밖에 오픈 소스 기반의 SIP Forum Test Framework, SipSak, Ohrwurm, Smap, SipBomber 등의 관련 툴이 있다.

이처럼 스팸 공격의 위협과 취약성을 보여줄 수 있는 다양한 스팸 유형과 관련 도구들이 존재한다. 하지만 스팸 공격 유형 중 실제 스팸 공격이 가능한 것과 구체적인 공격 과정에 대한 정보는 부족하다. 따라서 본 논문에서는 VoIP 환경에서의 위협이 되고 있는 스팸 공격의 심각성을 인식하고 이와 같은 스팸 공격 유형들이 VoIP 망에서 어떤 과정을 거쳐 공격될 수 있는지를 실험 해본다. 그래서 본 논문에서는 스팸 공격 유형을 분석 및 설계하고 VoIP 실험 망을 구축 하였으며 Spamtester를 구현하여 실제 스팸을 발송 해 보았다.

III. SPIT 시나리오

본 장에서는 VoIP 상의 취약성을 분석하고 실제 스팸 공격이 가능한 스팸 유형을 설계하였다. 본 장에서는 정상적인 경로를 통한 스팸 공격 외에 비정상적인 경로를 통한 스팸 공격의 위협을 확인하기 위해 P2P 스팸 공격, 세션 가로 채기를 통한 스팸 공격, 재전송 공격을 통한 스팸 공격, 프락시 위장을 통한 스팸 공격, 사전공격을 통한 스팸 공격 등 총 다섯 가지의 스팸 유형을 설계하였다. 본 논문에서 언급한 비정상적인 경로를 통한 스팸 공격은 사용자가 정상적인 등록 절차를 거쳐 인증을 받고 공격 대상자에게 스팸을 발송하는 것이 아닌 등록 인증이 되지 않은 사용자가 정상 사용자의 권한을 획득하고 스팸을 전송하거나 또는 권한 획득 없이 VoIP 망에 스팸을 전송하는 경우를 뜻한다.

1. P2P 스팸 공격

표준 문서에서는 inbound 프락시 서버와 UAS 간에 TLS (Transport Layer Security)[3] 보안 정책을 선택적으로 적용하도록 하고 있다. 따라서 inbound 프락시와 UAS간에 TLS를 적용하지 않을 시 스패머는 정상적인 프락시 서버로 위장해 UAS로 스팸을 발송할 수 있다. 이와 같은 P2P 스팸 발송은 프락시 서버를 경유하지 않고 UAS로 직접 스팸을 발송하므로 발신자를 추적할 수 없고 별도의 프락시 서버 정보 없이 직접적으로 스니핑 한 샘플 메시지를 이용해 INVITE 메시지를 공격 대상자에게 발송할 수 있다.

P2P스팸 발송은 다음과 같다. 먼저 임의의 공격대상자의 정상적인 INVITE 메시지를 스니핑하고 저장한다. 그리고 저장되어진 INVITE 메시지를 발송한 후 200 OK 메시지 스니핑 모듈 및 BYE 메시지 스니핑 모듈과 연동해 스팸을 발송한다. 이 때, 스패머는 호 설정을 스패머와 공격대상자 간의 맺기 위해서 두 가지 작업을 시행한다. 첫 번째는 발송 INVITE 메시지의 Contact 필드를 스패머의 IP로 스푸핑한다. 두 번째로 SDP (Session Description Protocol) 정보의 주소와 포트번호를 스패머의 주소와 포트번호로 스푸핑하여 RTP 세션을 스패머와 공격 대상자 간에 맺을 수 있도록 한다. 공격 대상자는 스패머의 INVITE 메시지를 받고 응답으로 200 OK 메시지를 스패머에게 발송하게 된다. 그리고 스패머는 200 OK 메시지를 스니핑하고 ACK 메시지로 응답함으로써 스패머와 공격 대상자 간의 RTP 세션이 성립되어질 수 있도록 한다.

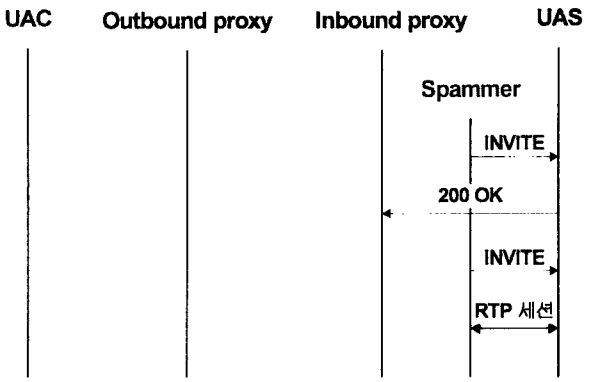

그림 1. P2P 스팸 공격 시나리오
Fig. 1. SPIT scenario using P2P.

2. 세션 가로채기를 통한 스팸 공격

세션 가로채기를 통한 스팸 발송은 정상 호가 성립되기 전 혹은 후에 스팸을 발송할 수 있다. 즉, 스패머는 임의로 전송되는 INVITE 메시지를 스니핑한 후 응답으로 200 OK 메시지를 생성해 UAC (User Agent Client)로 전송함으로써 스패머와 공격 대상자 간의 호가 성립될 수 있다. 또한 호가 성립되어진 후 RE-INVITE, UPDATE 메시지를 이용하여 연결되어진 호를 가로챌 수 있다. 본 논문에서 구현한 Spamtester는 200 OK를 이용해 UAC와 스패머 간 호 성립이 되는 것을 그림 2와 같은 절차로 구현하도록 하였다.

이 시나리오는 INVITE 메시지 스니핑 모듈, 200 OK 메시지 스니핑 모듈 그리고 BYE 메시지 스니핑 모듈과 연동해 설계하고 스팸을 발송한다. 먼저 스패머는 공격 대상자의 INVITE 메시지 발송을 스니핑한 후

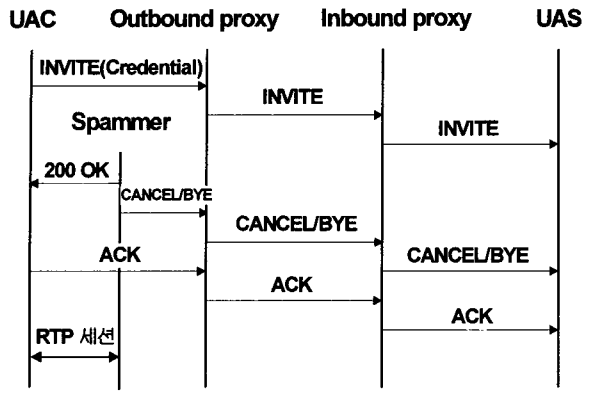

그림 2. 세션 가로채기를 통한 스팸 공격 시나리오
Fig. 2. SPIT scenario using session hijacking.

공격 대상자에게 200 OK 메시지를 발송해 정상 UAS보다 먼저 호를 성립한다. 그리고 기존의 UAS에게는 CANCEL/BYE 메시지를 발송하여 호를 끊는다. 그래서 오직 스패머와 UAC 간에 호가 성립될 수 있도록 한다.

3. 재전송 공격을 통한 스팸 공격

표준 문서에서는 프락시가 UA를 인증하기 위해서 HTTP 다이제스트 인증 보안 메커니즘을 반드시 적용하도록 하고 있다. 하지만 취약성이 있는 프락시는 407 메시지에 포함하는 인증 파라미터 중 nonce 값을 일정 시간동안 유지하는 특징이 있기 때문에 스패머는 공격 대상자의 정상적인 인증 값을 스니핑 후 프락시에게 재전송함으로써 일정 시간동안 인증이 될 수 있는 취약성이 존재한다.

재전송 공격을 통한 스팸 발송은 다음과 같다. 먼저 스패머는 공격 대상자의 인증 값이 포함된 INVITE 메시지를 스니핑하고 저장한다. 그리고 UAC와 UAS 간의 호가 연결되어 있을 수 있으므로 기존의 호를 끊기 위해 CANCEL/BYE 메시지를 UAS에게 전송한다. 다음으로 취약성이 있는 프락시에게 미리 저장된 인증 값이 포함된 INVITE 메시지를 발송하면 프락시는 그 메시지를 정상적인 사용자로 인증하고 공격 대상자에게 메시지를 전송한다. 공격 대상자는 200 OK 메시지로 응답함으로써 스패머와 UAS 간의 호가 성립될 수 있다.

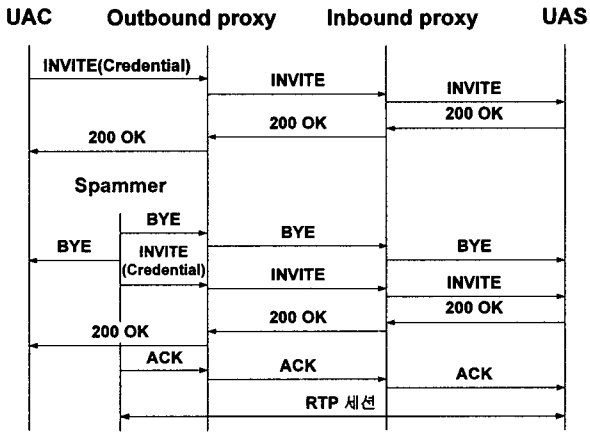

그림 3. 재전송 공격을 통한 스팸 공격 시나리오
Fig. 3. SPIT scenario using replay attack.

4. 프락시 위장을 통한 스팸 공격

표준 문서에서는 서로 다른 프락시 간의 TLS를 반드시 적용하도록 하고 있다. 하지만 프락시 간의 TLS 적용을 하지 않을 시 프락시 위장을 통한 스팸 발송이 가능 할 수 있다. 즉, 스패머는 임의의 outbound 프락시로 가장하고 공격 대상 inbound 프락시 서버를 선택하여 스팸 공격을 할 수 있다. 이 공격은 그림 4와 같이 공격 대상 inbound 프락시 서버에 INVITE 메시지를 스푸핑하여 발송하면 스패머와 공격 대상 UAS 간의 SIP 시그널링이 성립하여 스팸 공격이 가능하다.

먼저 스패머는 스니핑 한 샘플 메시지를 바탕으로 프락시 도메인을 위장한다. 그러기 위해서 INVITE 메시지의 Via 헤더를 임의의 outbound 프락시 도메인으로 위장하는 메시지 스푸핑 과정을 거친다. 그 후 inbound 프락시 서버에게 스푸핑된 INVITE 메시지를 발송한 후 200 OK 메시지 스니핑 모듈 및 BYE 메시지 스니핑 모듈과 연동해 그림 4와 같은 스팸 공격을 할 수 있다.

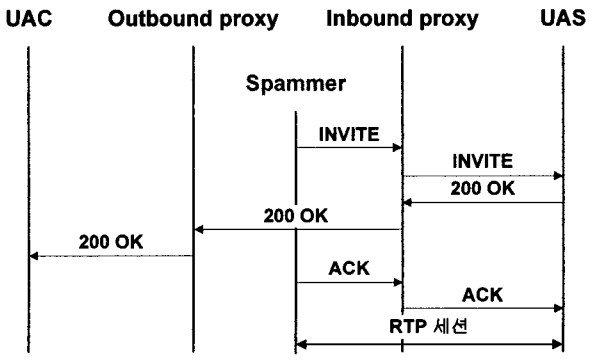

그림 4. 프락시 위장을 통한 스팸 공격 시나리오
Fig. 4. SPIT scenario using impersonation attack.

5. 사전공격을 통한 스팸 공격

사전공격을 통한 스팸 발송은 각 UA의 REGISTER 과정이나 INVITE 메시지를 전송하는 과정에서 HTTP

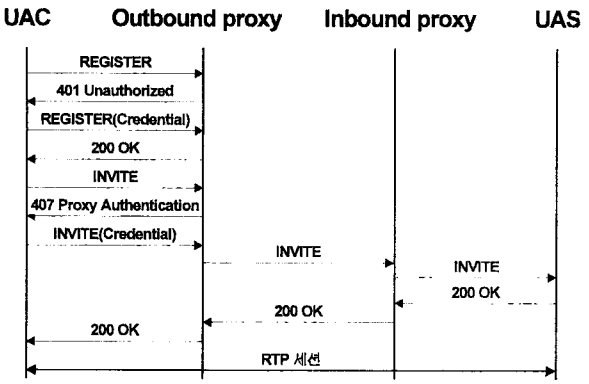

그림 5. 사전공격을 통한 스팸 공격 시나리오
Fig. 5. SPIT scenario using dictionary attack.

다이제스트 인증의 취약성을 보여주기 위해 설계되었다. HTTP 다이제스트 인증은 패스워드 기반으로 사전에 사용자가 프락시에게 인증 절차를 실행한다. 하지만 HTTP 다이제스트 인증은 패스워드 기반이기 때문에 사전 (Dictionary) 공격을 통해서 패스워드가 노출될 수 있다. 따라서 스패머는 정상 사용자의 REGISTER 또는 INVITE 메시지의 credential 값을 수집하고 사전공격을 이용해 비밀번호를 알아낸 후 그림 5와 같이 정상 등록 과정 및 호 설정 과정을 통해 공격 대상자에게 스팸을 발송한다.

이 공격은 INVITE 메시지나 REGISTER 메시지가 스니핑 되었을 때 Spamtester의 DB를 통해 등록되어진 단어 조합을 이용해 자동으로 패스워드를 추출하고 정상 등록하여 임의의 공격 대상자에게 스팸 공격을 시도하도록 설계하였다. 먼저 Spamtester를 이용하여 REGISTER 메시지를 스니핑한 후 사전공격을 이용하여 정상 사용자들의 비밀 번호를 추출한다. 그리고 정상 등록 절차를 시행하기 위해 401 메시지가 프락시에게 전달되는 즉시 스패머는 인증 값이 포함된 REGISTER 메시지를 프락시에게 전달하여 정상 등록 과정을 마친다. 그리고 이 공격은 그림 1과 같은 P2P 스팸 발송 시나리오와 유사한 절차에 따라 스팸 발송을 한다. 특히 사전공격을 통한 스팸 공격은 비밀 번호를 알아 낸 후 P2P 스팸 발송과 마찬가지로 대량 스팸 공격을 할 수 있기 때문에 다수의 사용자들에게 피해를 끼칠 수 있다.

IV. Spamtester 구현

본 논문에서는 스팸 생성 유형을 설계하고 UAC 혹은 UAS에게 스팸 공격을 실험해 보았다. 그러기 위해서 소프트 프로그램으로써 Spamtester를 구현 하였다. Spamtester는 본 논문의 III장에서 설계한 스팸 유형들을 기반으로 스팸 발송을 하도록 구현 하였다. Spamtester는 크게 메시지 스니핑, 메시지 생성, 스팸 발송, 사용자 정보 수집/저장 등의 모듈로 구성되어 있다.

본 논문에서는 Spamtester 구현을 위해 VC++ 프로그래밍 툴을 사용하며 SIP 메시지 스니핑을 위해 wincap 라이브러리를 사용하고 RTP 스팸 발송을 위해 JMF를 사용한다. 또한 OS로 Windows 2000 Professional을 이용하였으며 실험 망의 프락시 서버는 리눅스 기반의 IPTEL 프락시 서버를 이용한다. 그리고 UA는 소프트 폰인 X-Lite와 하드폰인 Linksys의 SPA942를 사용한다.

- OS : Windows 2000 Professional, Linux Fedora core 3
- Library : Winpcap library
- Programming tools : Microsoft VC++, JMF(Java Multimedia Framework)
- Proxy server : IPTEL(ser-0.9.6)
- UA : X-Lite, SPA942(Linksys)

1. Spamtester 동작 과정

Spamtester는 자동적으로 스팸을 발송할 수 있도록 스니핑 기능과 스팸 유형 결정, 스팸 발송 등의 주요 기능 절차를 수행한다. Spamtester의 스니핑 기능은 공격 대상자의 정보를 수집하기 위해서 모든 스니핑 대상자의 IP와 ID를 수집하여 DB에 저장하며 스팸 유형은 III장에서 설계한 각 스팸 발송 시나리오들의 절차를 따른다. 또한 Spamtester는 스팸 유형에 맞게 SIP 메시지를 스푸핑하여 공격 대상자에게 메시지를 발송한다. 그래서 스패머와 공격 대상자 간의 RTP 세션이 만들어지면 스팸을 발송한다.

1) Spamtester는 실행 초기에 스레드 모듈이 동작한다. 스레드 모듈은 세 가지의 기능을 수행한다. 첫 번째는 SIP 메시지 스니핑 모듈, 두 번째는 스니핑 모듈에 의해 캡처되어진 공격 대상자 수집 및 저장 모듈, 세 번째는 수집되어진 공격 대상자의 비밀 번호 획득을 위한 사전공격 모듈이다. 이와 같은 스레드 모듈은 자동적으로 SIP 메시지를 스니핑할 때마다 세 가지의 기능을 독립적으로 수행하게 된다.

2) 스팸 유형 및 공격 대상자 선택과 메시지 스푸핑은 공격 대상자 정보를 저장하고 있는 데이터베이스와

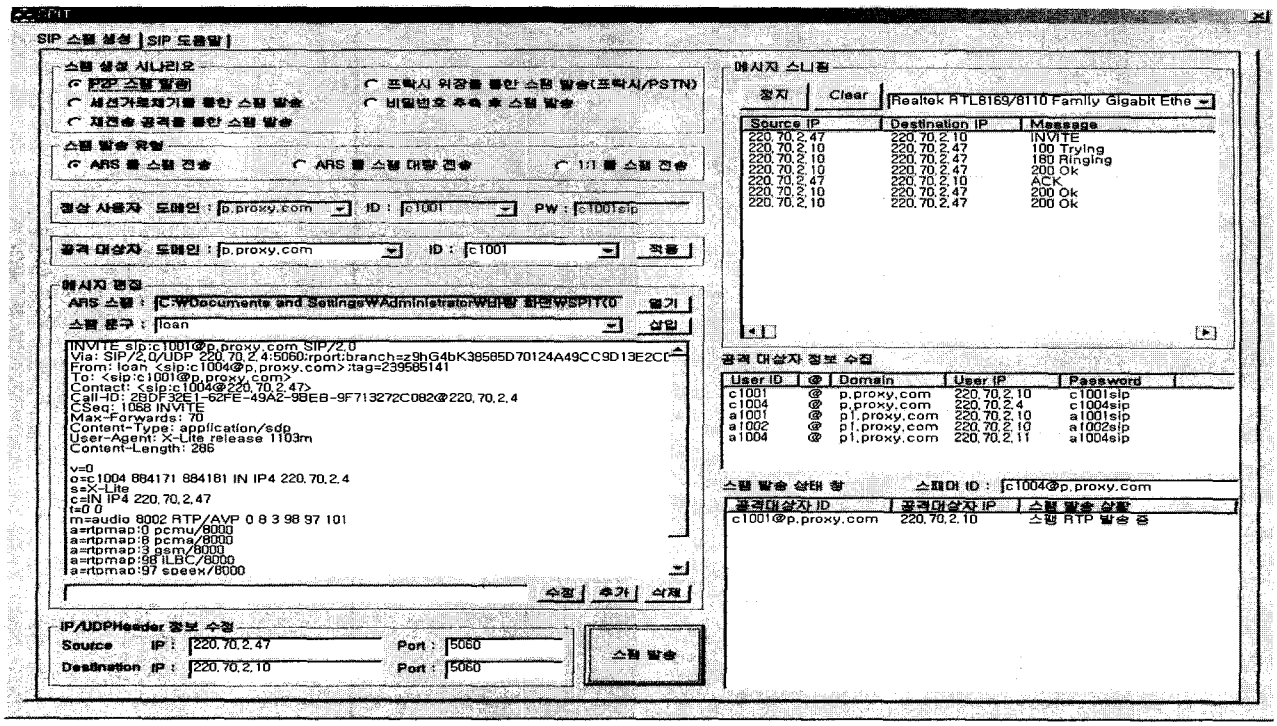

그림 6. Spamtester GUI
Fig. 6. Spamtester GUI.

연동하여 자동적으로 스팸을 발송할 수 있도록 구현하였다. 또한 사용자에 의해서 수기로 SIP 메시지의 스푸핑 및 공격 대상자 선택이 가능하도록 구현 하였다.

3) 스팸 발송 모듈은 최종적으로 선택되어진 공격 대상자에게 스팸을 발송한다. 그리고 Spamtester의 IP 스푸핑을 위해서 raw 소켓을 이용한다. raw 소켓은 IP뿐만이 아니라 포트 번호까지 스푸핑이 가능하도록 구현하였다.

2. Spamtester GUI

SIP Spamtester의 GUI는 각 스팸 생성 시나리오에 맞춰 SIP 메시지 생성 및 수정, 스팸 발송 뿐만 아니라 메시지 스니핑 및 저장, 공격 대상자 정보 수집 등 다양한 기능을 수행할 수 있도록 개발하였다. 그림 6은 SIP 스팸 생성 창에서 P2P 스팸 생성 시나리오를 선택한 경우의 동작 화면을 나타낸다. 그림 6에서 왼쪽 화면의 기능은 메시지의 스푸핑을 통해 스팸 메시지를 생성할 수 있고 오른쪽 화면의 기능은 메시지 스니핑 및 공격 대상자 정보를 수집할 수 있다. 또한 스팸 발송 유형으로는 녹음된 스팸을 발송하는 형태와 1:1로 공격 대상자와 접촉할 수 있는 형태, 대량 전송을 통한 수집된 공격 대상자 모두에게 스팸을 발송하는 형태가 있다.

V. 스팸 공격 실험

본 논문에서는 설계한 비정상적인 스팸 공격 유형을 실험해 보기 위해 VoIP 실험 망을 구축 하였다. VoIP 실험 망은 오픈 소스인 IPTEL 프락시와 UA로 소프트폰인 X-Lite와 하드폰인 Linksys SPA942로 구성된다. 첫 번째 실험은 UA를 X-Lite 폰만을 이용하였을 때와 두 번째로 Linksys 폰을 이용하였을 때, 마지막으로 X-Lite와 Linksys폰을 같이 이용했을 때로 구분하여 각 SPIT 설계 시나리오에 따라 스팸을 발송해 보았다. 또한 각 스팸 유형의 실험된 결과는 캡처 프로그램(ethereal)을 통해 캡처 하였다.

P2P 스팸 공격의 결과는 그림 7과 같이 공격이 가능한 것을 확인 하였다. P2P 스팸 결과 확인할 수 있는 것은 프락시를 거치지 않은 SIP 메시지는 단말에서 특별한 검증절차 없이 모든 메시지를 수신하기 때문에

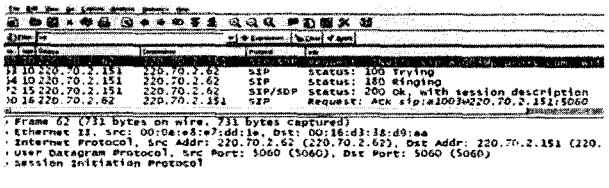

그림 7. P2P 스팸 공격 실험
Fig. 7. Experiment of the SPIT using P2P.

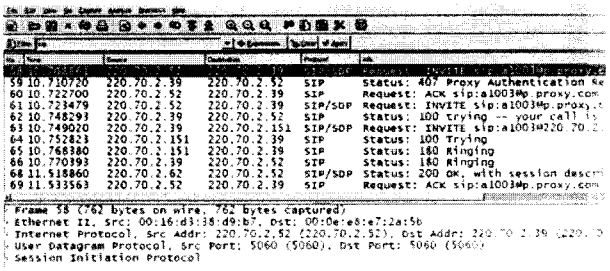

그림 8. 세션 가로채기를 통한 스팸 공격 실험
Fig. 8. Experiment of the SPIT using session hijacking.

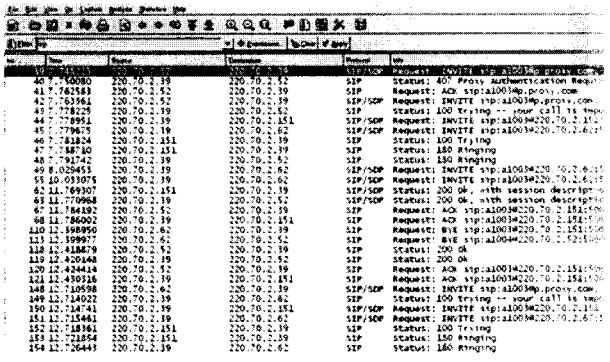

그림 9. 재전송 공격을 통한 스팸 공격 실험
Fig. 9. Experiment of the SPIT using replay attack.

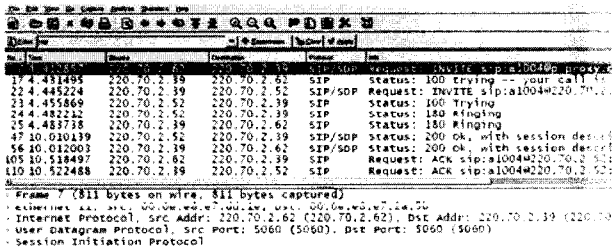

그림 10. 프락시 위장을 통한 스팸 공격 실험
Fig. 10. Experiment of the SPIT using impersonation attack.

P2P 스팸 공격이 가능함을 확인 하였다.

다음은 세션 가로채기를 통한 스팸 공격을 실험해 보았다. 그림 8과 같이 스팸 공격이 가능한 것을 볼 수 있다.

다음은 재전송 공격을 통한 스팸 공격을 실험해 보았다. 그림 9와 같이 스팸 공격이 가능한 것을 볼 수 있다.

하지만 실험에서 UA를 소프트폰인 X-Lite를 이용했을 때는 스팸 공격이 가능하였으나 하드폰인 SPA942에서는 스팸 공격의 SIP 시그널링 과정은 가능하나 Spamtester로부터 RTP 전송은 불가능 하였다.

다음은 프락시 위장을 통한 스팸 발송을 실험해 보았다. 그림 10과 같이 스팸 공격이 가능한 것을 볼 수 있다.

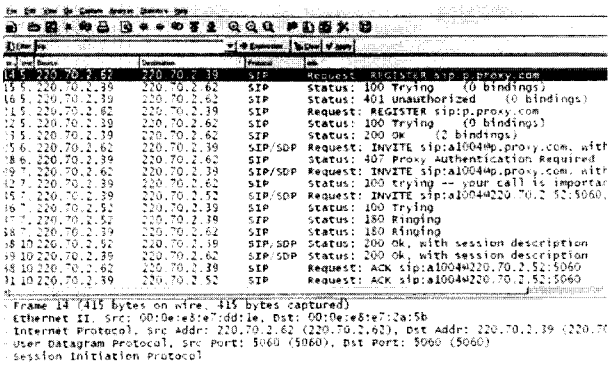

그림 11. 사전공격을 통한 스팸 공격 실험
Fig. 11. Experiment of the SPIT using dictionary attack.

표 1. 스팸 공격 시나리오 실험 결과
Table 1. Result of the SPIT.

UA / 스팸유형	X-Lite	Linksys (SPA942)	X-Lite Linksys
P2P 스팸 공격	가능	가능	가능
세션가로채기를 통한 스팸 공격	가능	가능	가능
재전송 공격을 통한 스팸 공격	가능	실패	실패
프락시 위장을 통한 스팸 공격	가능	가능	가능
사전공격을 통한 스팸 공격	가능	가능	가능

다음은 사전공격을 통한 스팸 발송을 실험해 보았다. 그림 11과 같이 Spamtester를 이용해 정상 사용자의 비밀번호를 알아낸 후 그 사용자의 정보를 이용해 인증 과정을 마치고 임의의 공격 대상자에게 스팸 공격이 가능한 것을 볼 수 있다.

실험된 전체 결과는 다음과 같다. 스팸 공격은 UA를 X-Lite폰으로만 테스트 했을 때 설계한 모든 스팸 유형들이 가능 하였으며 UA를 Linksys폰만을 이용하여 실험했을 때 재전송 공격을 통한 스팸 발송을 제외한 나머지 스팸 공격들이 가능 하였다. 또한 스팸 공격 실험을 X-Lite폰과 Linksys폰을 같이 이용하였을 때 재전송 공격을 통한 스팸 발송을 제외한 나머지 공격들이 가능 하였다. 전체적인 실험 결과는 표 1과 같다.

VI. 관련 도구 비교

본 장에서는 구현한 Spamtester와 관련 도구를 비교해 본다. 본 논문에서 구현한 Spamtester는 SIP 메시지 스니핑 및 스푸핑, RTP 세션을 이용한 다양한 스팸 공격을 실험해 보도록 구현 되었다. 하지만 VoIP에서는 본 논문에서 구현한 Spamtester처럼 스팸 발송을 할 수 있는 도구가 거의 존재하지 않아서 SIP 메시지 생성 도

표 2. Spamtester, SiVus, PROTOS c07-SIP 비교
Table 2. Comparison on Spamtester with SiVus and PROTOS c07-SIP.

	Spamtester	SiVus	PROTOS c07-SIP
기능	SIP 메시지 스니핑, 스푸핑, SIP 메시지 발송, VoIP 스팸 공격 실험	SIP 메시지 스니핑 및 스푸핑, 발송	제공된 INVITE 메시지만 발송
장점	SIP 메시지 발송을 통한 취약한 프락시나 UA 테스트, 스팸 발송을 통한 미디어 채널의 안정성 실험, SIP 시그널링 메시지 생성	SIP 메시지 발송을 통한 취약한 프락시나 UA 테스트, SIP 메시지 생성	비정상적인 다수의 INVITE 메시지를 제공, SIP 메시지 발송을 통한 취약한 프락시나 UA 테스트
단점	제공된 기능을 사용하기 위해 다수의 추가적인 라이브러리 설치가 필요함	순차적인 기능 실행 시 프로그램 재부팅이 필요함, 실험된 데이터의 부정확성	테스트를 위해 INVITE 메시지만 발송할 수 있음, 실험된 데이터의 부정확성

구 및 스니핑 그리고 VoIP 망 테스와 관련된 도구들을 비교해 본다.

SiVus는 SIP 메시지 스니핑 및 메시지 생성도구이며 PROTOS c07-SIP는 VoIP에서 취약성이 있는 프락시나 UA를 테스하기 위해 설계되어진 도구이다[8]. 한편 SiVus는 윈도우 GUI(graphical user interface) 방식을 사용자에게 제공하므로 사용자에게 익숙한 인터페이스를 이용하여 사용자가 사용하기 쉽도록 구성되어 있다. 하지만 사용자가 SiVus의 다양한 기능을 순차적으로 실행할 시 시스템의 설정이 불안정하여 초기 설정 상태로 돌아가기 위해 프로그램을 재부팅해야 하는 불편함이 있다. 또한 PROTOS c07-SIP는 제공되는 여러 종류의 비정상 INVITE 메시지를 이용하여 VoIP 망의 취약성을 실험해 볼 수 있으나 SIP 메시지 중 INVITE 메시지만을 발송할 수 있는 단점이 있다. 또한 실험해 본 결과 값은 정확한 분석이 부족하여 실험된 UA나 프락시의 실험 데이터를 완전히 신뢰할 수는 없는 단점이 존재한다. 하지만 본 논문에서 구현한 Spamtester는 SiVus와 PROTOS c07-SIP의 기능을 모두 포함하고 있다. 본 논문에서 구현한 Spamtester는 SiVus처럼 SIP 메시지 스니핑과 스푸핑이 가능하며 윈도우 기반의 GUI를 제공하여 쓰임에 어려움이 없으며 PROTOS c07-SIP처럼 VoIP 망을 테스트하기 위해 INVITE 메시지뿐만 아니라 200 OK와 ACK 메시지 전송도 가능하다. 또한 Spamtester는 미디어 경로로 스팸을 발송해 봄으로써 SIP 시그널링과 RTP 세션까지 모든 VoIP의 취약성 실험이 가능하다.

Ⅶ. 결 론

VoIP에서는 PSTN 망에서보다 더 저렴한 가격으로 음성 서비스 및 패킷 기반의 데이터를 이용한 다양한 서비스를 제공하는 것이 가능하다. 하지만 보안을 고려한 VoIP 환경이 잘 갖추어져 있지 않을 시 스팸 공격이 발생할 수 있다. 이와 같은 위협을 확인하고 근본적인 보안 방안을 강구하기 위해서는 우선 VoIP에서의 다양한 스팸 공격 유형에 대한 분석이 필요하다. 특히 정상적인 스팸 공격 외에 비정상적인 과정을 거친 스팸 공격에 관한 구체적인 분석이 필요하다.

본 논문에서는 스팸 공격의 유형 및 분석을 위해 비정상적인 스팸 공격의 유형들을 설계하고 실제 스팸 발송을 통해서 스팸 공격의 위협 결과를 확인 하였다. 이를 위해 본 논문에서 설계한 스팸 공격 유형은 비정상적인 스팸 발송의 스니핑에서 스팸 발송까지의 전체적인 SIP 시그널링 과정을 설계하였다. 스팸 유형으로는 P2P 스팸 공격, 세션 가로채기를 통한 스팸 공격, 재전송 공격을 통한 스팸 공격, 프락시 위장을 통한 스팸 공격, 사전공격을 통한 스팸 공격 등이다. 또한 Spamtester는 VoIP 환경에서 스니핑이 가능하도록 구현 하였으며 자동으로 스니핑된 공격 대상자들의 ID 및 IP를 데이터베이스에 저장하며 SIP 메시지를 생성하여 공격 대상자들에게 발송 할 수 있도록 구현 하였다. 그래서 구축된 VoIP 실험 망을 통해 이와 같은 스팸 유형과 Spamtester를 이용해 스팸 발송을 해 보았고 표1과 같은 스팸 공격 결과를 확인 하였다. 또한 본 논문에서 구현된 Spamtester는 표2와 같이 관련된 도구들과의 비교에서 여러 장점이 있는 것을 확인 하였다. 따라서 추후 VoIP 스팸 대응 방안은 본 논문의 구체적인 스팸 공격 분석에 관한 정보를 이용하여 사전에 스팸 차단 방안을 만드는데 이용될 수 있기를 기대한다.

참 고 문 헌

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, SIP(Session Initiation Protocol), IETF RFC 3261, June 2002.

[2] J. Rosenberg, C. Jennings, and J. Peterson, The Session Initiation Protocol (SIP) and Spam,

IETF draft, October 2004.
[3] T. Dierks, and C. Allen, The TLS Protocol Version 1.0, IETF RFC 2246, January 1999.
[4] 장유정, 정수환, 문형권, 최재덕, 원유재, 조영덕, "SIP 기반의 VoIP 서비스 환경에서 스팸 방지를 위한 인증 기법," *한국통신학회논문지*, 제32권 제8호, pp.521-528, 2007년 8월.
[5] Yu-Sung Wu, S. Garg, and N. Singh, "SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architecture for Voice-over-IP Environments," *in Conf.* of International on Dependdable Systems and Networks, July 2004.
[6] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, S. Gritzalis, K.S Ehlert, and D. Sisalem, "Survey of security vulnerabilities in session initiation protocol," *IEEE Communications Surveys & Tutorials*, vol. 8, no 3, pp. 68-81, December 2006.
[7] D. Geneiatakis, G Kambourakis, C Lambrinoudakis, T. Dagiuklas, and S. Gritzalis, "SIP Message Tampering: THE SQL Code INJECTION Attack," *in Proc.* of 13th International Conference on Software, Telecommunications and Computer Networks IEEE, Sept. 2005.
[8] University of Colorado Policy Lab, http://www.colorado.edu/policylab/Papers/Univ_Colorado_VoIP_Vulner, April 2005.
[9] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart, HTTP Authentication Basic and Digest Access Authentication, IETF RFC 2617, June 1999.

저 자 소 개

최 재 식(학생회원)
2007년 숭실대학교 정보통신전자공학부 학사 졸업.
2007년~현재 숭실대학교 전자공학과 석사과정.
<주관심분야 : VoIP 보안>

정 수 환(평생회원)-교신저자
1985년 서울대학교 전자공학과 학사.
1987년 서울대학교 전자공학과 석사.
1996년 University of Washington 박사.
1996년~1997년 Stellar One SW Engineer.
1997년~현재 숭실대학교 정보통신전자공학부 교수
<주관심분야 : VoIP 보안, 차량 네트워크 보안, 이동 네트워크 보안, RFID/USN 보안>

최 재 덕(정회원)
2002년 숭실대학교 정보통신전자공학부 학사.
2004년 숭실대학교 정보통신공학과 석사.
2005년~현재 숭실대학교 전자공학과 박사과정.
<주관심분야 : VoIP 보안, 차량 네트워크 보안, 이동 네트워크 보안>