FMC 환경에서 SIP 부가서비스 공격 시나리오 개발

조식완*, 이형우*, 김정욱**, 김환국**, 정현철**
*한신대학교 컴퓨터공학부
**한국인터넷진흥원 인터넷융합단 융합보호R&D팀
e-mail : hyungwoolee8299@hanmail.net

SIP Additional Service Attack Scenario on FMC Environments

Sik-Wan Cho*, Hyung-Woo Lee*, Jeong-Wook Kim**, Hwan-Kuk Kim**, Hyun Cheol Jeong**
*School of Computer Engineering, Hanshin University, Korea
**Convergence Security R&D Team, KISA, Korea

요 약

SIP 프로토콜 기반 VoIP 서비스는 편리함과 저렴한 통신비용으로 사용자 수가 급증하고 있다. 하지만 Text 형태의 SIP 헤더 정보를 UDP 방식으로 전송하기 때문에 손쉽게 위변조 할 수 있으며, 최근 SIP를 통해 제공되는 다양한 형태의 부가서비스에 대한 보안 위협이 증가하고 있다. FMC 폰을 통해 제공되는 동시착신, 착신전환, 3인통화 등과 같은 부가서비스에 대한 공격을 통해 과금우회 공격 등을 수행할 수 있다. 따라서 본 연구에서는 FMC 환경에서 제공되는 주요 SIP 부가서비스를 대상으로 각각의 취약성에 대해 조사 분석하였으며, 분석된 내용을 중심으로 SIP 기반 인터넷전화 부가서비스에 대한 공격 시나리오를 단계별로 설계 및 개발하였다.

1. 서론[1)]

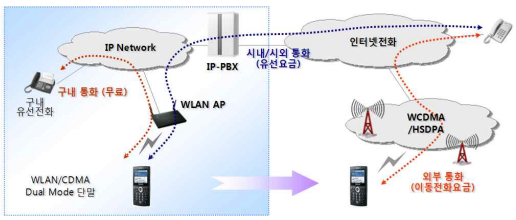
SIP(Session Initiation Protocol)는 음성을 포함한 화상, 텍스트 등 멀티미디어 통신 세션을 수정할 수 있는 프로토콜이다. 이를 이용하여 기본적인 통화 연결은 물론 컬러링이나 동시 착신, 통화중 대기 등 사용자의 편의를 위한 다양한 형태의 부가서비스를 제공할 수 있다. 이러한 SIP 프로토콜 기반 VoIP 서비스는 기존 통화 및 다양한 부가서비스들에 대한 편리함과 저렴한 통신 비용으로 인해 사용자가 급증하고 있으며 점차 상용화 및 고도화 되어가고 있다. 하지만 이러한 여러 장점들 때문에 오히려 새로운 문제점 및 서비스 취약점이 발견되고 있다. 컬러링 서비스 오용공격 및 SIP Packet Flooding 공격과 같은 취약성을 이용한 공격들이 생겨나고 있으며 그 정도가 점차 고도화 되어감에 따라 피해 사례가 늘어가고 있다. 이는 VoIP의 특성상 인터넷 프로토콜의 취약점이 그대로 존재하며 SIP 프로토콜을 통해 송수신되는 내용에 대한 수정/변경 등이 용이한 만큼 손쉽게 공격자에 의해 위변조가 가능함은 물론 인증 과정을 제공하고 있지 않기 때문에 다양한 공격 방법 및 위협에 그대로 노출된다는 한계를 갖고 있기 때문이다. 따라서 본 연구에서는 국내 SIP기반 VoIP 부가서비스별 Call Flow 및 취약성 분석을 통해 FMC폰 환경에서 현재 사용되고 있는 VoIP 부가서비스에 대한 공격 시나리오를 제시하고 각 방식별 취약점에 대해 제시하였다.

1) 본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업 일환으로 수행하였음. [KI001850, SIP기반 응용서비스 보호를 위한 침입대응기술 개발]

2. FMC 서비스

2.1 FMC 기반 VoIP 서비스

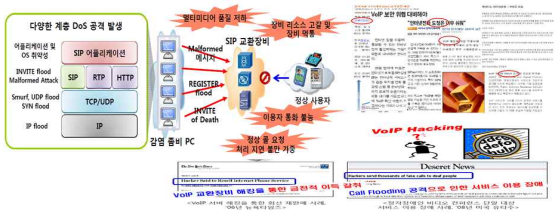
FMC(Fixed Mobile Convergence) 서비스는 FMC 전용 단말기를 이용해 평상시에는 3G망을 이용해 전화통화를 하며 전화요금도 이동전화요금을 사용한다. 그리고 무선 AP가 있는 지역으로 오면 FMC 전용 단말기가 VoIP 단말기로 변환되어 VoIP 전화요금을 사용하게 되며, 무선 AP를 이용해 무선인터넷도 데이터요금 없이 사용할 수 있게 된다.



[그림 1] FMC 서비스 구조도

2.2 FMC 환경에서 SIP 서비스 보안 취약성

VoIP에서 사용되는 기술 중, 현재 표준으로 널리 사용되는 SIP는 HTTP(HyperText Transfer Protocol)와 같은 텍스트 기반으로 정의되어 있어 확장이 용이하며, 경량화 되어 있고, 쉽게 사용할 수 있는 프로토콜이다. SIP는 기존에 사용하고 있는 E-MAIL 주소를 사용하고, 위치 지정 메시지를 통해 이동성을 제공하므로, 모바일 VoIP 서비스에 적합한 기술이라 할 수 있다. 하지만 FMC 환경에서 SIP 기반 VoIP 서비스에 적용하기 위해서는 새로운 문제들이 발생하고 있다.



[그림 2] FMC 환경에서의 SIP 프로토콜 취약성

SIP는 설계 당시 보안적인 요소가 고려되지 않아 항상 위협에 노출되어 있다. 실제로 SIP를 대상으로 하는 다양한 공격들이 가능하다. 대표적인 SIP 공격기법으로는 비정상 메시지 공격(Malformed Message Attack), SIP 메시지 폭주 공격(SIP Message Flooding Attack), SIP 스푸핑 공격(Spoofing Attack), 도청, DoS(Denial of Service) 등이 있다.

2.3 FMC 부가서비스

아래의 표에 나와 있는 다양한 부가서비스를 이용하여 서비스 사용자는 보다 향상되고 질 높은 통화 서비스를 이용할 수 있으며 최근 서비스 사용량이 점진적으로 늘어나고 있는 추세이기 때문에 개발 및 제공되고 있는 부가서비스의 종류가 점점 늘어나고 있다.

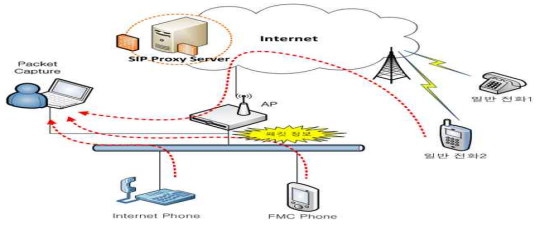
[표 1] FMC 부가서비스

부가서비스 명칭	설 명
컬러링	기존의 통화 연결음 대신 서비스 사용자가 등록한 메시지를 들려주는 서비스
착신전환	통화연결 요청을 다른 전화로 연결해주는 서비스
3인통화	2명의 수신자에게 통화연결 요청을 하여 3명이서 통화할 수 있도록 연결해주는 서비스
부재중 안내	부재시 미리 설정해 놓은 부재중 안내 메시지를 발신자에게 전해주는 서비스
통화중 대기	통화 중 다른 전화가 걸려왔을 시 현재의 통화를 잠시 대기시키고 걸려온 전화를 연결시키는 서비스
동시착신	등록한 모든 전화에 벨이 울리게 하여 먼저 받는 전화로 연결시키는 서비스
수신자부담 통화	요금을 수신자에게 부담하게 하여 통화연결을 요청하는 서비스

3. SIP 부가서비스 공격 시나리오

3.1 공격 시나리오 개발 환경

본 연구에서는 다음과 같은 구성도를 대상으로 FMC 환경에서의 VoIP 보안 위협에 대해 분석하였다.

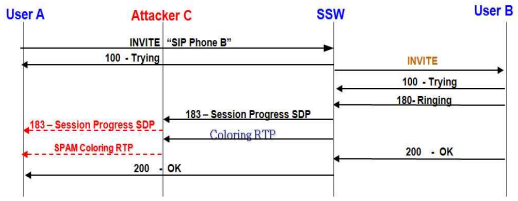


[그림 3] 서비스 취약점 분석 및 공격 시나리오 개발 환경 구조

FMC 기능을 지원하는 스마트폰을 통해 상용망에 접속하여 인터넷 전화 호를 발생토록 하였으며, 인터넷 전화나 3G망을 통해 핸드폰으로 전화를 걸었을 경우 발생하는 전체 호를 분석하는 것은 물론, 상용망에서 제공하는 다양한 형태의 부가서비스 등에 대해 취약점을 분석하고 이를 토대로 공격 시나리오를 개발할 수 있도록 구성하였다.

3.2 컬러링 서비스 공격

공격자에 의해 SSW에서 공격대상에게 전송되는 컬러링 메시지를 스팸 메시지로 변조하는 공격이다.

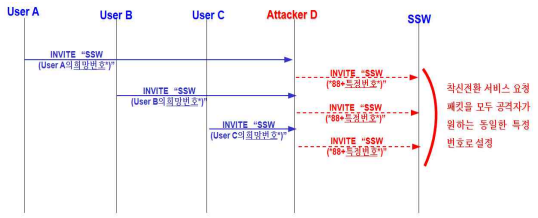


[그림 4] 컬러링 서비스 스팸 변경 공격

이 공격은 위 그림과 마찬가지로 SSW에서 보내지는 183 패킷 및 컬러링에 해당하는 RTP 데이터 패킷을 공격자가 임의의 183 패킷 및 스팸 컬러링 RTP로 변경하는 공격이다. 이 공격으로 인하여 공격대상에 해당하는 발신자는 컬러링 대신 스팸 메시지를 듣게 된다.

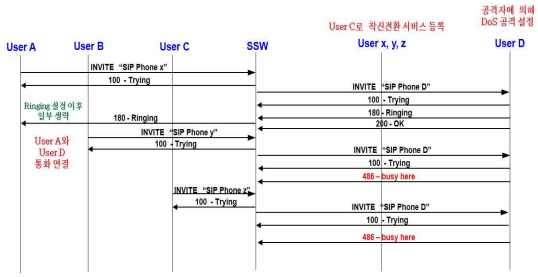
3.3 착신전환 서비스 공격

착신전환 서비스 변경 공격에서 범위가 커진 공격으로 각각 착신전환 서비스를 이용하고자 하는 착신전환 희망 번호를 모두 동일한 공격자 임의의 공격대상 번호로 변경하는 공격을 말한다.



[그림 5] 다중 사용자 착신전환 등록 공격 (1/2)

공격 대상들의 INVITE 패킷을 공격자가 원하는 공격대상 번호가 담긴 INVITE 패킷으로 변조하여 SSW에 전송한다. 한편 공격자에게 INVITE 패킷을 받은 SSW는 착신전환 서비스 데이터베이스에 각 공격 대상들의 착신 희망 번호가 아닌 공격자의 공격대상 번호로 등록하게 된다.

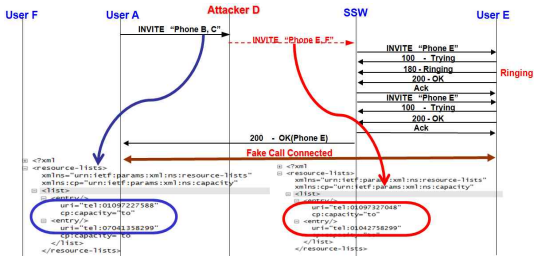


[그림 6] 다중 사용자 착신전환 등록 공격 (2/2)

이후 각각 공격 대상들에게 연결하고자 하는 발신자들은 모두 공격자가 등록해놓은 또 다른 공격대상 번호로 연결하게 되며 공격자에 의해 SSW에 등록된 공격대상은 착신전환 설정이 집중되어 있기 때문에 통화량을 폭주시키는 DOS형태의 공격이 가능해진다.

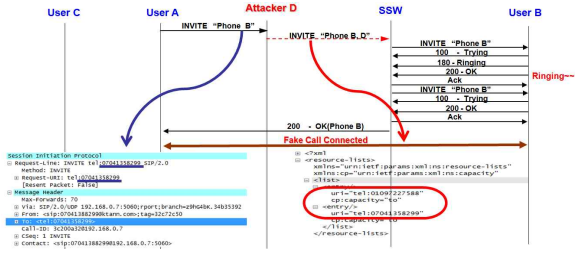
3.4 3인 통화 서비스 공격

공격대상이 3인 통화를 연결 요청하는 전화번호들을 공격자가 임의로 변경하여 공격자가 변경한 전화번호로 연결되게 하는 공격이다.



[그림 7] 통화연결 전화번호 변경 공격

위의 Call Flow에서 보여주는 것처럼 3인 통화의 경우 연결 요청하는 전화번호는 XML 형태로 INVITE 패킷을 통해 SSW에 전송된다. 공격자는 공격대상으로부터 INVITE 패킷을 수집한 후 패킷 안에 들은 XML 내용을 수정하여 SSW에 보냄으로서 통화연결 전화번호 변경 공격을 수행한다.

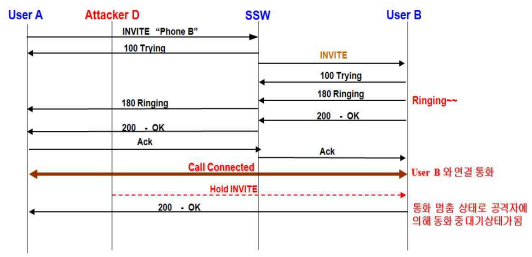


[그림 8] 통화연결 공격자 등록 공격

또한 일반통화 패킷에 공격자를 추가하여 3인 통화에 해당하는 패킷으로 변조해 전송할 수도 있다. 이 경우 SIP 패킷뿐 만이 아니라 안에 포함된 XML 메시지도 변조가 용이하기 때문에 공격자는 이를 이용한 도청이나 송수신자 모두에게 스팸 메시지를 전송하는 등의 공격을 할 수 있다.

3.5 통화중 대기 서비스 공격

송신자와 수신자가 일반통화를 하는 도중 공격자에 의하여 강제적으로 통화중 대기상태를 만들어 통화 연결을 방해하는 공격을 취할 수 있다.

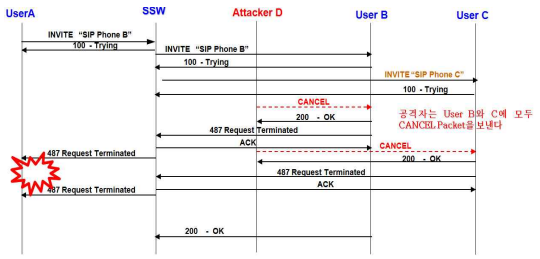


[그림 9] Hold INVITE 연결방해 공격

위의 Call Flow에서 보여주는 것처럼 User A와 User B는 통화연결 과정을 모두 마치고 정상적으로 연결이 되었다. 하지만 이후 공격자가 User A를 사칭하여 Hold INVITE를 보냄으로서 User B는 통화중 대기 상태가 되며 User A와 User B는 공격자에 의하여 연결 대기 상태가 된다.

3.6 동시착신 서비스 공격

동시 착신 부가서비스 사용 시 착신이 되지 못한 연결은 CANCEL 패킷을 보낸다는 것을 이용하여 공격을 취할 수 있다. 공격 대상이 통화 연결을 시도하였을 때 공격자가 동시 착신에 해당하는 모든 번호에 CANCEL 패킷을 보내어 통화연결을 방해할 수 있다.

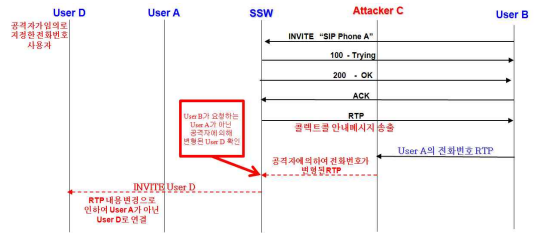


[그림 10] CANCEL 메시지 전송 공격

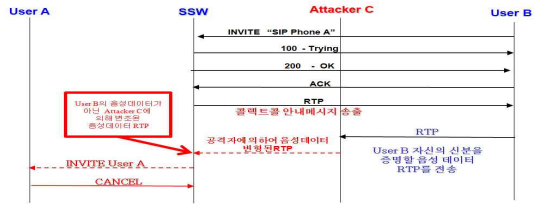
위의 Call Flow처럼 User A가 User B에 통화 연결을 요청하였을 시 SSW는 User B가 동시착신 서비스 가입자라는 것을 확인하고 서비스에 등록된 User C에게도 INVITE 패킷을 전송한다. 공격자는 User B와 C 모두 INVITE 메시지가 전송된 후에 SSW를 사칭하여 User B나 C에서 응답이 오기 전에 둘 다 CANCEL 메시지를 보냄으로서 두 연결을 모두 Terminated 시키는 공격을 할 수 있다.

3.7 수신자부담 서비스 공격

콜렉트콜 수신자부담 통화 서비스의 경우 서비스 사용할 경우 송신자가 데이터를 입력할 때는 연결할 수신자에 대한 전화번호를 입력할 때와 수신자에게 자신을 증명할 음성데이터를 입력할 때이다. 공격자는 이 데이터를 이용하여 공격을 취할 수 있다.



[그림 11] 수신자 전화번호 데이터 변경 공격

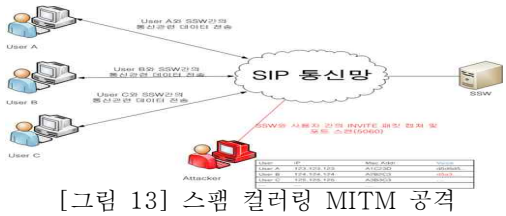


[그림 12] 송신자 음성데이터 변경 데이터 변경 공격

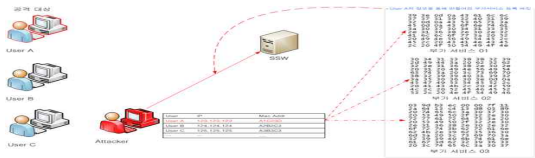
위에 Call Flow에도 잘 나와 있듯 공격 대상에 해당하는 User B는 먼저 SSW에 연결하여 안내메시지 RTP를 받는다. 그 후에 안내 메시지에 따라 연결 대상인 User A의 전화번호 RTP를 보내게 되는데 공격자는 이 RTP를 변조하여 SSW에 보내거나 User B의 음성 데이터를 변조된 데이터로 바꿔치기하여 전송한다. 그럼 SSW는 연결 요청 희망 대상이 아닌 공격자에 의해 변조된 INVITE 패킷을 보냄으로서 User B와 User D가 연결되게 하거나 변조된 음성데이터를 통해 수신자가 User A가 알아보지 못하게 하여 송신자를 인증 거부하도록 하는 공격을 취할 수 있다.

3.8 MITM 공격과 공격자에 의한 능동적 공격

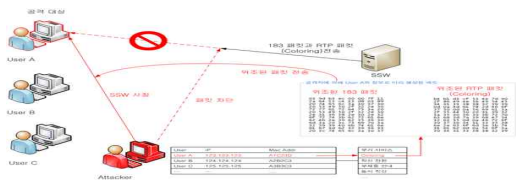
본 연구에서 분석한 취약점을 토대로 부가서비스 공격 시나리오를 개발 시 공격 방식은 크게 MITM 공격과 공격자에 의한 능동적 공격으로 나눌 수 있다. 먼저 MITM 방식의 공격은 공격자가 공격 대상의 SIP 통신망을 감시하고 있다가 공격자가 원하는 연결이 발생했을 시 이를 감지하여 패킷 차단 및 변조 등의 공격을 하는 방식을 말한다.



[그림 13] 스팸 컬러링 MITM 공격



[그림 14] 공격자에 의한 부가서비스 등록 공격 1단계



[그림 15] 공격자에 의한 부가서비스 등록 공격 2단계

스팸 컬러링을 공격 및 부재중 안내 사칭 공격 등 공격 대상을 감시하여 즉각적인 변조가 필요한 공격들이 이에 해당한다. 반면 공격자에 의한 능동적인 공격은 공격 대상의 SIP 통신망을 감시할 필요 없이 직접 공격 패킷을 보내는 공격 대상을 사칭하는 등의 공격 방식을 말한다.

공격을 하기 전 먼저 각 공격 대상들에 대한 정보가 필요하므로 공격 대상에 대한 정보를 먼저 수집한다.

대부분의 부가서비스 등록 및 해제 시의 취약점을 이용한 공격이 여기에 해당된다.

4. 결론

본 연구에서는 현재 상용되어 있는 대표적인 부가서비스에 대한 조사 분석 및 공격 시나리오를 개발하였다. 부가서비스 등록/해제 과정, 컬러링, 착신전환, 부재중 안내, 3인통화, 통화중 대기, 동시착신 및 수신자부담 통화 등 다양한 부가서비스를 대상으로 각 서비스별 흐름에 대해 공격이 가능한 시나리오를 Call Flow 형태로 제시하였다. 그 결과 대부분의 부가서비스가 통화연결 과정이 동일하게 나타났으며 연결 과정의 패킷 수집이 용이하고 수집된 패킷의 내용이 암호화되어 있지 않아 데이터의 기밀성이 없이 그대로 노출되어 있어 이를 통하여 송수신자의 정보 또한 쉽게 얻어낼 수 있다는 점을 알 수 있었다. 그 결과 분석한 부가서비스를 토대로 서비스 과정의 전체구조와 공격 대상에게 피해를 줄 수 있는 주요 취약점을 분석할 수 있었으며 각 부가서비스 별 시나리오 및 MITM 방식으로 공격을 수행할 경우 발생 가능한 시나리오와 공격자에 의한 능동적 공격 등을 수행하였을 경우 발생 가능한 공격 시나리오를 제시할 수 있었다.

참고문헌

[1] http://www.voip-forum.or.kr. VoIP 국내표준.「SIP 기반 인터넷 텔레포니 단말」. 2005.12

[2] 김지훈.「VoIP 보안 위협」. ASEC, 2008.

[3] 구자현.「서비스 거부 공격(Denial of Service)의 유형 및 대응」. 정보통신연구 진흥원, 주간기술동향. 2008.12.

[4] 구자현, "VoIP서비스 보안 취약성 분석", 한국정보보호학회지, 제 16권 1호, P.60~63, 2006.02

[5] 강신각.「VoIP 기술 현황 및 전망」. VoIP Grand Conference2005, 2005.

[6] 박진범 외 2인, "VoIP 보안 취약점 공격에 대한 기존 보안장비의 대응 분석 연구," 한국정보보호학회지, Vol.17, No.5, 2007.

[7] Sotillo S. Zfone.「A New Approach for Securing VoIP Communication」. ICTN 4040, 2006.

[8] Hemant Sengar.「VoIP Intrusion Detection Through Interacting Protocol State Machines」. 2006.

[9] Jean-Yves Migeon, "The MIT Kerberos Administrator's How-to Guide", Kerveros constortium, 2008, 6