FMC 기반 모바일 폰 환경에서 SIP 프로토콜 부가서비스 보안 취약성 분석

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

SIP Protocol Vulnerability Analysis on FMC based Mobile Phone

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

현재 FMC 폰을 통해 제공되는 동시착신, 착신전환, 3인통화 등과 같은 다양한 부가서비스가 제공되고 있어 보다 편리하면서도 다양한 기능을 제공하고 있다. 하지만 FMC폰에 적용된 SIP 프로토콜은 송수신 패킷에 대해 쉽게 위변조가 가능하고 송신자 인증기능에 문제점이 발견되고 있어 보안성이 취약하다. 또한 FMC 폰을 이용하여 여러 가지 부가서비스를 이용할 경우 서비스 자체의 취약점을 이용한 공격 등이 가능하다. 따라서 본 연구에서는 현재 상용화 되어 제공되는 SIP기반 주요 VoIP 부가서비스를 대상으로 각각의 Call Flow를 분석하였으며 이를 토대로 각 부가서비스에 대한 취약성에 대해 분석하였다.

1. 서론[1)]

FMC(Fixed Mobile Convergence) 서비스는 유무선 융합서비스로 유선전화를 무선전화 하나로 대체할 수 있고 편리성이 높은데다, 비용절감 효과가 상당히 큰 편이기 때문에 사용자가 급증하고 있는 서비스이다. 또한 사용자가 급증하고 있는 만큼 부재중 통화, 동시 착신, 통화중 대기 등 사용자의 편의를 위한 다양한 형태의 부가서비스를 제공하고 있기 때문에 대표적인 통화 서비스로 급부상하여 자리매김할 가능성이 크다. 하지만 오히려 이러한 여러 장점들 때문에 VoIP 서비스에 대한 취약성을 이용한 공격들이 생겨나고 있으며 그 정도가 점차 지능적이고 고도화 되어가고 있다. 이러한 공격기법의 근본적인 문제는 공격자가 정상적인 SIP 통신 패킷을 수정 및 삭제하고 이를 손쉽게 변경할 수 있기 때문이다.

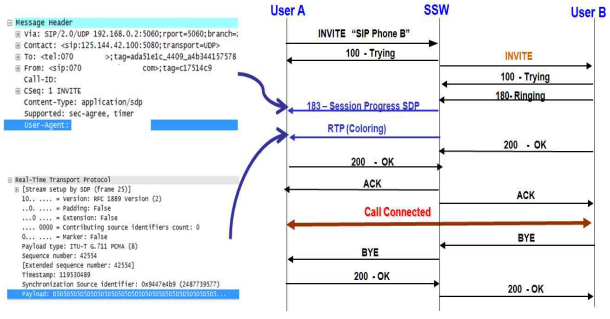
FMC 환경에서 VoIP 서비스의 보안 취약성을 해결하기 위해서는 인터넷전화 부가서비스 현황 및 특성과 FMC 서비스 보안 위협에 대해 분석하며, 이와 관련된 위협 사례에 대한 조사가 필요하다. 현재까지 수행된 대부분의 연구는 각기 유선 혹은 무선 네트워크 환경을 대상으로 한 취약성 분석이었기 때문에 FMC와 같이 유무선이 통합된 네트워크 환경에 대한 연구가 필요하다. 따라서 본 연구에서는 FMC폰 환경에서 제공되고 있는 국내 SIP기반 VoIP 부가서비스에 대해 각각의 Call Flow 구조에 대해 분석하고 주요 부가서비스별 취약점에 대해 분석하였다.

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

2. 부가서비스

2.1 컬러링 서비스

전화를 걸었을 때 기존의 통화 연결음 대신 음악이나 멘트, 효과음 등을 들려줌으로써 연결하는 동안 발신자를 지루하지 않게 해주는 부가서비스이다.

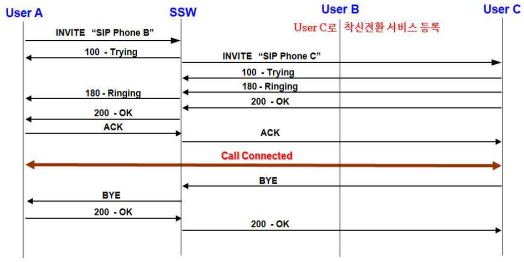


[그림 1] 컬러링 서비스의 Call Flow

컬러링의 경우 송신자가 INVITE 패킷을 보내면 SSW는 보내오는 INVITE 패킷을 받고 수신자인 User B에게 전송한다. 수신자가 이를 받고서 180 Ringing을 보내면 SSW에서는 컬러링 서비스 가입자라는 것을 확인하여 송신자에게 180 Ringing 대신 183 Session Progress SDP와 함께 컬러링에 해당하는 RTP를 전송한다. 이로 인하여 송신자는 컬러링 메시지를 듣게 된다.

2.2 착신전환 서비스

전화가 부재중이나 통화 중일 때 걸려오는 전화를 다른 전화로 연결 해주는 서비스를 말한다.

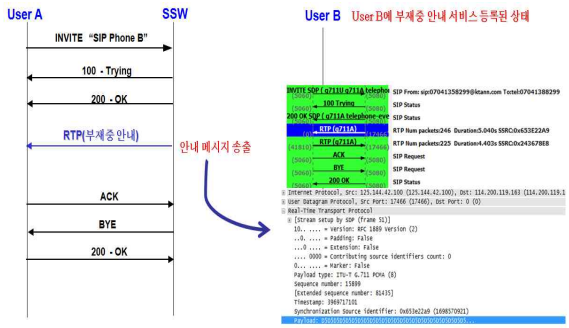


[그림 2 착신전환 서비스의 Call Flow

위의 Call Flow에서 보이는 것처럼 User A가 User B로 INVITE 패킷을 보냈을 시 SSW는 User B가 착신전환 서비스 등록자라는 것을 확인하여 User C로 INVITE 패킷을 전송한다. 이후 모든 통화 연결에 대하여 SSW는 User C로 전송하게 되며 과정은 일반통화와 동일하다.

2.3 부재중 안내 서비스

외출, 출장 등의 부재시 미리 설정해 놓은 부재중 안내 메시지를 발신자에게 전해주는 서비스를 말한다.

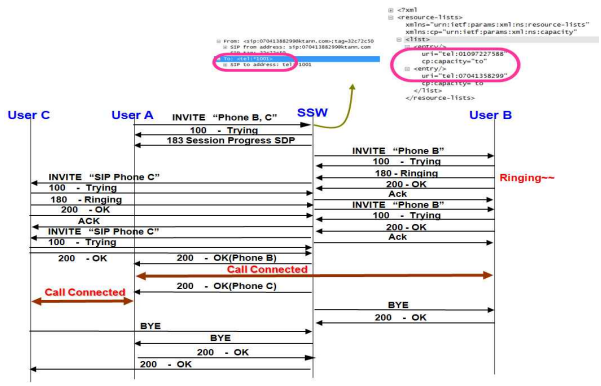


[그림 3] 부재중 안내 서비스의 Call Flow

송신자에 해당하는 User A가 User B와 연결하기 위해 INVITE 패킷을 보내면 SSW는 User B가 부재중 안내 서비스에 등록된 사용자라는 것을 확인하고 부재중 안내 메시지에 해당하는 RTP를 User A에게 전송한다.

2.4 3인 통화 서비스

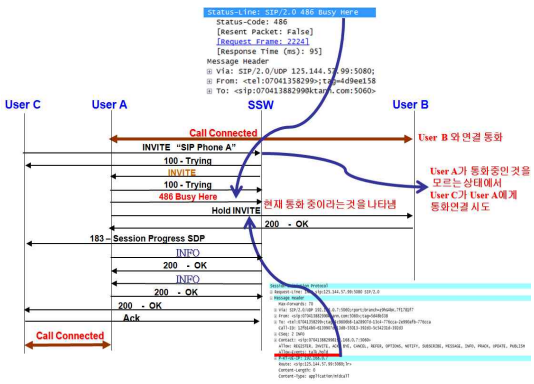
SIP 호 설정시 두 명의 전화번호를 입력하여 3인이 동시에 통화를 수행하는 부가서비스를 말한다. 다음에 제시된 Call Flow는 User A가 User B와 User C와 통화 연결을 하는 것으로 초기에 User A가 B와 C의 전화번호가 담긴 INVITE 패킷을 SSW에 전송한다. 이 때 INVITE 패킷은 도착지가 User B나 User C로 설정되어 있지 않고 SSW의 주소로 설정되어 있으며 User B나 User C에 대한 정보는 XML 형태로 INVITE 패킷 안에 담겨있다. 한편 User A에 의해 INVITE 패킷을 받은 SSW는 User B와 C에 연결을 하기 위해 먼저 183 Session Progress SDP를 User A에게 전송하며 그 후 User B와 User C에 대하여 각각 연결 과정을 수행한다.



[그림 4] 3인 통화 서비스의 Call Flow

2.5 통화중 대기 서비스

통화 중 다른 전화가 걸려와도 전화를 끊지 않고 뒤에 걸려 온 전화를 받으며 교대로 통화가 가능한 서비스이다.

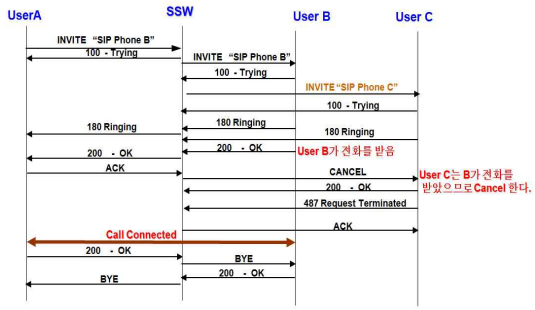


[그림 5] 통화중 대기 서비스의 Call Flow

통화중인 상태에서 SSW에 의해 타 사용자의 INVITE가 왔을 시 User A는 SSW에 '486 busy here'을 보내 SSW가 User C에게 183 패킷을 보낸 후 추가 연결과정을 수행할 수 있게 하고 User B에게는 Hold INVITE를 보냄으로서 User B를 통화 중 대기 상태로 만든 후 INFO 패킷을 통해 확인 과정을 거침으로서 User C와 연결한다.

2.6 동시착신 서비스

본래 쓰고 있는 수신자의 번호 외 타 유무선전화로 동시에 벨이 울리게 하여 먼저 받는 전화로 연결시키는 서비스이다.

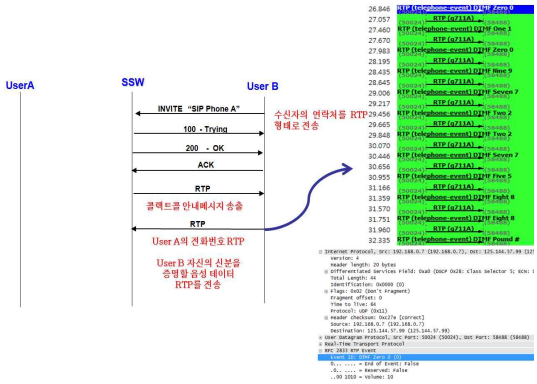


[그림 6] 동시착신 서비스의 Call Flow

User A가 User B에 연결하기 위하여 SSW에 INVITE 패킷 전송 시 SSW는 User B가 동시착신 서비스 가입자라는 것을 확인하여 동시착신 가입번호인 User C에게도 INVITE 패킷을 전송한다. 각각 INVITE 패킷을 받은 User B와 User C는 180 Ringing을 전송하고 그 중 먼저 전화를 받은 User B가 200 OK를 SSW에 전송하면 SSW는 User C에 CANCEL 패킷을 보냄으로서 연결을 종료되며 User A는 User B와 연결된다.

2.7 수신자 부담 통화 서비스

요금을 수신자에게 부담하게 하여 통화연결을 하는 서비스로 시내 및 시외전화가 가능하며 수신자에게 통화 의사를 확인 후 수신자가 통화를 거부하면 전화 연결 및 요금이 부가되지 않는 서비스이다.

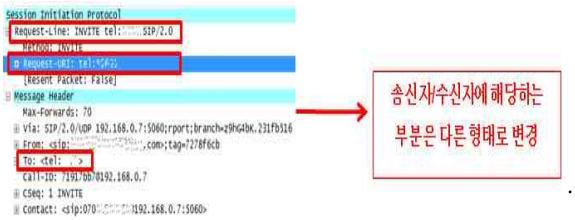


[그림 7] 수신자 부담 통화 서비스의 Call Flow

3. 부가서비스 취약성 분석

3.1 등록/해제 INVITE Packet 전송

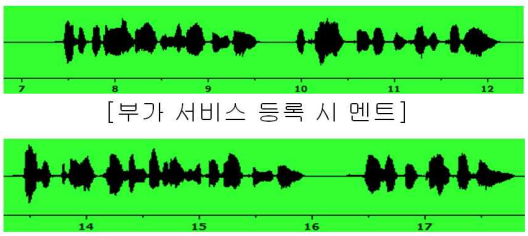
부가서비스를 사용하는 과정에서도 가장 중요한 패킷은 INVITE 패킷이다. INVITE 안의 메시지를 통해 송수신자의 정보 및 연결요청 상태를 알 수 있으며 특히 부가서비스 등록 및 해제의 경우 송신자가 어떠한 부가서비스를 요청하였는지에 대해서도 INVITE 패킷을 통해 알 수 있다. 결국 공격자에 의해서 부가서비스 등록 INVITE 패킷이 일반 사용자 대신 보내질 경우 부가서비스에 대한 공격이 가능하게 된다. 마찬가지로 일반 사용자가 부가서비스에 가입되어 있는 상황에서 공격자에 의해 부가서비스 해제 INVITE 패킷이 전송될 경우 마찬가지로 공격이 가능하게 된다.



[그림 8] INVITE 패킷의 취약성

3.2 고정된 RTP Packet 사용

부가서비스 등록 및 해제, 부재중 안내 등의 부가서비스는 SSW에서 보내오는 안내 메시지 RTP가 항상 고정되어 있다. 공격자가 이러한 고정 메시지를 수집하였을 경우 SSW인 것처럼 공격 대상에게 접근하여 RTP를 전송하는 SSW 사칭공격에 취약할 수 있다.



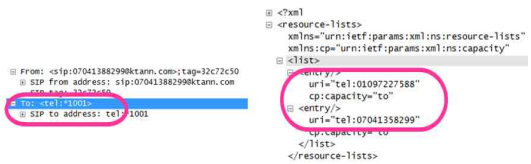
[부가 서비스 등록 시 멘트]

[부가 서비스 해제 시 멘트]

[그림 9] 부가서비스 등록/해제시 안내 메시지 RTP

3.3 XML 내용 변경

위의 INVITE Packet의 취약성에서도 설명했던 3인통화 및 통화중 대기에 쓰이는 INFO 패킷 안에는 XML 메시지가 들어있다. 이 XML 메시지 안에는 수신자에 대한 정보나 현재 상태 등이 들어가 있으며 수집 및 내용 변경이 용이하기 때문에 공격자에 의해 내용이 변조되었을 시 원치 않는 수신자와 통화하거나 통화 연결 방해 등의 피해를 받을 수 있다.



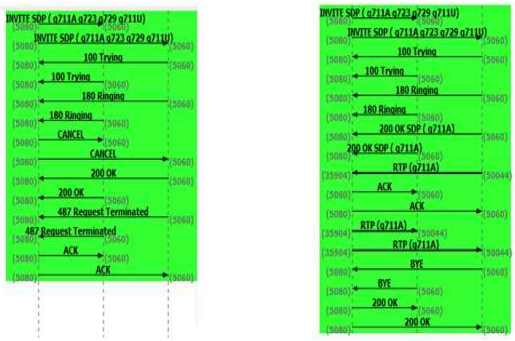
[그림 10] INVITE 패킷에 포함된 XML 메시지

3.4 486 Busy here packet

공격자가 SSW를 사칭하여 공격 대상에게 임의적으로 생성한 INVITE 패킷을 보낸다면 공격 대상은 SSW에 '486 busy here'을 보내면서 현재 연결 상태를 Hold 시킬 것이다. 따라서 공격자는 이러한 점을 이용하여 의도적으로 486 busy here을 생성하게 함으로서 현재 연결 상태를 Hold 시키고 통화 연결을 방해하는 공격을 할 수 있다.

3.5 CANCEL Packet 전송

동시착신 서비스의 경우 등록된 모든 번호에 벨이 울리게 하였다가 그 중 한 곳이라도 전화를 받으면 받은 전화번호를 제외하곤 모든 번호의 벨이 취소된다. 이 때 연결요청을 취소하는 패킷이 CANCEL 패킷이다.

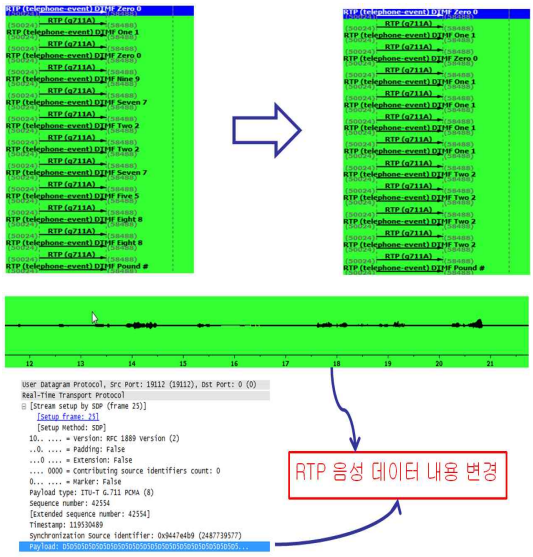


[그림 11] 동시착신 중 '받지 않음'과 '받음'의 호 분석

위의 그림처럼 CANCEL 패킷을 받은 각 수신자들은 487 Request Terminated 패킷을 전송하면서 연결을 종료한다. 이 점을 이용해 공격자가 SSW를 사칭하여 수신자들에게 CANCEL 패킷을 전송하게 되면 각 수신자들은 487 Request Terminated 패킷을 전송하면서 연결을 종료하게 될 것이다.

3.6 RTP 내용 변경

수신자부담 통화의 경우 송신자는 안내 메시지에 따라 연결할 수신자의 전화번호 및 수신자에게 자신을 증명할 음성 데이터를 RTP 형태로SSW에 전송한다.



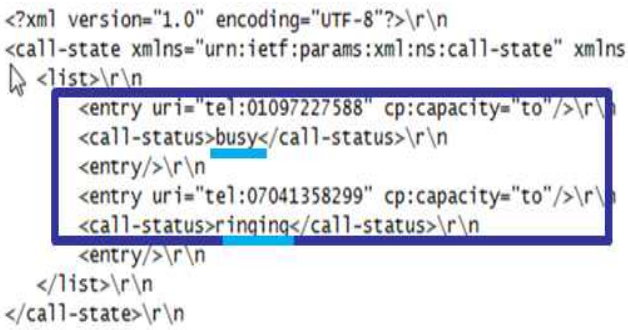
[그림 12] 동시착신 중 '받지 않음' 과 '받음'의 호 분석

공격자는 송신자의 희망번호를 공격자 희망번호로 변경 혹은 공격자 자신으로 변경하여 2차적 피해를 노리는 공격을 할 수 있으며 음성데이터 또한 공격자에 의해 수집 및 변경될 수 있기 때문에 이를 이용한 공격에 취약할 수 있다.

3.7 INFO Packet 변경

INFO 패킷은 통화중 대기 상태에서 연결을 요청

하는 송신자가 있을 시 수신자가 SSW에 보내는 SIP 패킷으로 안에는 xml 데이터가 저장되어 있다.



[그림 13] INFO패킷에 들어있는 XML 구조

수신자가 연결되는 송신자를 교체할 때마다 INFO 패킷이 생성하여 SSW에 전송하며 전송된 INFO 패킷은 SSW에서도 수신자에게 다시 전송하여 연결 상태에 대해 서로 확인이 가능하도록 한다. 이 점을 이용하여 공격자가 INFO 메시지 변경 혹은 삭제 등의 공격을 통해 통화 연결 방해 공격을 취할 수도 있다.

4. 결론

본 연구에서는 SIP 프로토콜에서 사용 가능한 부가서비스에 대한 Call Flow를 분석하였다. 부가서비스 등록/해제 과정, 컬러링, 착신전환, 부재중 안내, 3인 통화, 통화중 대기, 동시착신 및 수신자 부담 통화 등 많은 부가서비스를 대상으로 각 서비스별 Call Flow 및 각각의 특징에 대해 분석하였으며 패킷 구조 등에 대해서도 제시하였다. 그 결과 대부분의 부가서비스가 연결 과정이 동일하게 나타났으며 연결 과정의 패킷 수집이 용이하고 수집된 패킷의 내용에 암호화되어 있지 않아 데이터의 기밀성이 없이 그대로 노출되어 있어 이를 통하여 송수신자의 정보 또한 쉽게 얻어낼 수 있다는 점을 알 수 있었다. 특히 대부분의 정보는 초기 연결 설정을 위해 지나는 INVITE 패킷을 통해 얻을 수 있었으며 이를 통해 송수신자의 정보외에 현재 연결 요청에 대한 정보 및 각 연결 대상자의 상태까지 알 수 있었다. 또한 데이터 정보에 해당하는 RTP의 경우 각 통신사에서 고정된 멘트를 사용하기 때문에 INVITE를 비롯하여 이를 이용한 사칭 공격 등에 취약할 수 있다는 결과를 얻을 수 있었다.

그 결과 이렇게 종합적으로 연구 분석한 내용을 토대로 서비스 과정의 전체구조와 공격 대상에게 피해를 줄 수 있는 주요 취약점을 제시할 수 있었다.

참고문헌

[1] 김지훈.「VoIP 보안 위협」. ASEC, 2008.

[2] 최재덕 외 3인.「SIP 기반의 VoIP 보안 시스템 구현」. 한국통신학회 논문지, Vol.29, No.9B. 2004.9.

[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] 원용근 외 3인, "SIP프로토콜 기반 VoIP 서비스에서 DoS 공격 대응 방안 연구," 한국정보보호학회 동계학술대회, 2007.

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

[7] 신영찬 외 5인.「VoIP를 위한 보안 프로토콜 성능 평가」. 한국 정보보안학회 논문지, 제 18권 제 3호. 2008.6.

[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

[10] T. Dierks, E. Rescorla.「The Transport Layer Security(TLS) Protocol Version 1.1」. RFC4346, 2006.