Practical VoIP Penetration Testing Using Mr.SIP Pro: SIP-Based Audit and Attack Tool

- Ismail Melih Tas
- Kubilay Ahmet Kucuk

https://mrsip.pro/
https://mrsip.gitlab.io
https://github.com/meliht/mr.sip
https://twitter.com/mrsip_official
https://www.youtube.com/channel/UCgrl4qYdhrlPjxG8OtxqSkw
Content

- Introduction
- The story of the Mr. SIP
- VoIP Attack Surfaces
- Mr.SIP Pro Modules
- Lab Setup for VoIP Security Testing
- Hacking Story-1: Registration Hijacking for Long Distance Call Routing Fraud
  - BONUS: This is how hackers make millions of dollars in call frauds!
- Hacking Story-2: Caller-ID Spoofing for a Spear Phishing Campaign
- Hacking Story-3: Abusing Known Flood Based Telephony-DoS Vulnerability
- Advanced Novel Attacks
- VoIP Pentest Methodology w/Mr.SIP Pro
- Closing Thoughts
- Q&A!
About Melih

Ismail Melih Tas

• Offensive Security Researcher
  • Mostly offensive about VoIP/SIP
• Senior Pentest Expert @Private Bank
• PhD@BAU (Computer Eng. & Cyber Sec.)
• Entrepreneur @VulnHero
• Part-time Bug Hunter
• InfoSec Researcher & Trainer @SiberNinja
• Author of Mr.SIP (BlackHat USA/EU/Asia, Offzone)
• Author of National VoIP/UC Security Standard (coop with TSE)

• Contact : i.melih.tas@gmail.com
• LinkedIn : https://www.linkedin.com/in/melihtas/
• Twitter : https://twitter.com/artinscience
• Github : https://github.com/meliht
About Kubilay

Kubilay Ahmet Kucuk

- Security Researcher from Oxford, UK
  - Research Associate @ Cyber Security Centre, Oxford University
  - PhD Studentship from Intel ® Corporation, 2015-2018
- Interests:
  - Trusted Computing, Intel SGX, Hardware-assisted Security
  - Former Researcher from ETH Zürich
  - Industry 4.0, Manufacturing, Simulation, Production, C++
- Computer Engineer
- Contact : kucuk@cs.ox.ac.uk
- LinkedIn : https://www.linkedin.com/in/o1l/
# Introduction

From a hobby to the most advanced VoIP / SIP Pentest Tool ever.

https://github.com/meliht/Mr.SIP

- Developed to audit and simulate SIP-based attacks
- Originally used in academic studies
  To help developing novel SIP-based DDoS attacks
- Became a fully functional SIP Pentest Tool
- Can also be used as;
  - SIP client simulator
  - SIP traffic generator
Timeline for Mr.SIP – Dark Age/Closed Source

2011: First prototype developed by Melih
  • Winner in an innovation competition
  • Raised about $2m with research grants
2011: Prototype named as VZA
  • VoIP Vulnerability Tool in Turkish
2012: VZA is funded by the Turkish Government
  • Under a commercial company
  • Has one of the 10 biggest VoIP labs in the world
  • Research team founded
Timeline for Mr.SIP – Middle Age Battles
Fork, Competitors, Closed Source

2011: Independent competitor (SIPVicious) began.

2012: Wrong choice of team player caused fork:
• (Viproy, Fatih)

2012: The company kept initial tools private
2013: The company kept initial tools private
2014: The company kept initial tools private
2015: The company kept initial tools private

2015: Melih left the company
Timeline for Mr.SIP – Modern Age/Open Source

2016: Mr.SIP Open Source development began
2017: First public version appeared (3 modules)
2019: Presented at followings:
   • BlackHat USA/EU/Asia Arsenal
   • Offzone Moscow
2020: Pro version is now 10 modules
2020: Defcon28 Main Stage Talk (right here)
2021: Roadmap covers 5 new modules + GUI
2021: Built-in tool (public version) in Kali
2022: Attract and collaborate with major VoIP manufacturers
Facts about VoIP Security

Total Loss: 28.2B$
Media Mentions and Citations
Facts (Problems) about VoIP Sec

VoIP technologies are inherently weak
VoIP protocols are not designed securely
Manufacturers cannot meet today’s security needs
VoIP is not managed securely in companies generally
It will become an indispensable need in the near future

There is a need for a product that can detect and report security problems specific to VoIP.
‘Mr.SIP Pro’ 10 Modules (more to come)
https://github.com/meliht/mr.sip
Why to use Mr.SIP? State of Art in VoIP!

- High performance with multi-threading
- Hiding skills from security perimeters
- Advanced IP spoofing skills: random, subnet, manual
- Advanced intervention skills: MiTM, Intercepting Proxy
- On the fly cracking for SIP digest authentication
- Package injection and repeating skills
- Predefined original TDoS attack scenarios
- Advanced SIP packet generator (no trace, can generate based on vendor)
- Stateful, customisable, automated attack scenario development framework
Who is Using Mr.SIP? All in One Attack Tool

- Service providers and telecom operators at all levels
- Banking/finance and enterprise where security is critical
- All other institutions that manage their VoIP/UC infrastructure
- Integrators, security consulting firms and researchers
Where Mr.SIP is Used? Full Automated!

Use Cases:

• Penetration Testing
• Red Teaming Activities
• VoIP and Security Product Testing for R&D
  • Performance testing
  • Security testing
  • Load testing
  • Robustness testing etc.
• PoC and quality testing (purchase stage)
  • Both VoIP and security products such as firewall, DDoS mitigator, IPS etc.
• VoIP and/or security researchers
Typical VoIP Topologies

- Internal VoIP Implementations
  - (target in this presentation)
- Managed Services
- Online SIP Trunking Services
**SIP Basics**

The following request types are common within SIP:

- **INVITE** — Invites an account to join the call.
- **ACK** — Confirmation regarding the invite of joining the call.
- **CANCEL** — Canceling a queued call.
- **REGISTER** — Registering the user against the SIP server.
- **OPTIONS** — Shows the options the caller has.
- **BYE** — Ends the call between both sides.
- **REFER** — Shows that the receiver needs to communicate through a 3rd party by the information attached to the request.

**SIP Requests/Responses:**

- 1xx (Informational)
- 2xx (Success)
- 3xx (Redirection)
- 4xx (Failed requests)
- 5xx (Web server cannot complete request)
- 6xx (Global errors)
Basic SIP Call Flow

Typical SIP Interaction Structure:

1. Sender initiates an INVITE request.
2. Receiver sends back a 100 (Trying) response.
3. Sender starts ringing by sending a 180 (Ringing) response.
4. Receiver picks up the phone and a 200 success response is sent (OK).
5. ACK is sent by the initiator.
6. Call started using RTP.
7. BYE request sent to end the call.
Sample SIP INVITE

INVITE sip:6000@192.168.65.140;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 213.14.141.71:64116;branch=z9hG4bK-524287-1---d6078501e9ea7434;rport.
Max-Forwards: 70.
Contact: <sip:5000@213.14.141.71:64116;transport=UDP>.
To: <sip:6000@192.168.65.140;transport=UDP>.
From: <sip:5000@192.168.65.140;transport=UDP>;tag=3455a85b.
Call-ID: Fjad329igBhemWu1Vrhwv...
CSeq: 1 INVITE.
Allow: INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE.
Content-Type: application/scp.
User-Agent: Z 5.2.28 r2v2.8.115.
Allow-Events: presence, kpml, talk.
Content-Length: 510.

v=0.
o=Z 977115011 0 IN IP4 213.14.141.71.
s=Z.
c=IN IP4 213.14.141.71.
t=0 0.
m=audio 8002 RTP/AVP 106 93 111 0 8 97 110 112 98 101 100 99 102.
a=rtpmap:106 opus/48000/2.
a=fmtp:106 minptime=20; cbr=1; maxaveragebitrate=40000; useinbandfec=1.
a=rtpmap:111 speex/16000.
a=rtpmap:97 iLBC/8000.
a=fmtp:97 mode=20.
a=rtpmap:110 speex/8000.
a=rtpmap:112 speex/32000.
a=rtpmap:98 telephone-event/48000.
a=fmtp:98 0-16.
a=rtpmap:101 telephone-event/8000.
a=fmtp:101 0-16.
a=rtpmap:100 telephone-event/16000.
a=fmtp:100 0-16.
a=rtpmap:99 telephone-event/32000.
a=fmtp:99 0-16.
a=rtpmap:102 G726-32/8000.
a=sendrecv.
Basics About SIP Registration

- 3 cases for registration
  - First login
  - Each boot
  - 1 per hour (RFC 3261)

RFC 2617

HA1 = MD5(username:realm:password)
HA2 = MD5(method:digestURI)
response = MD5(HA1:nonce:HA2)
What Are We Demonstrating Today?

- Identifying SIP Servers and Enumerating Users
- Registration Hijacking via SIP Digest Authentication Cracking
- Sniffing via Application level MiTM
- Caller-ID Spoofing via SIP Signalling Manipulation
- Enumeration via Eavesdropping Calls
- Searching for Known Vulns & Exploits Based on Version Info
- TDoS Attacks including IP Spoofing
- BONUS: Disclosing background of Call Frauds where hackers made millions $$ $
Our Demo Lab Setup

Target Network

- Trix-1: 192.168.65.136
- Trix-2: 192.168.65.140
- FPBX: 192.168.65.145

- Softclients
- IP Phones
- More users
- More clients

Kali Linux (Mr.SIP Pro installed)
Mr.SIP Installation

Preferred OS: Kali Linux
Root privilege required
Use Requirements.txt for extra libraries!
#python3 mr.sip.py --help
#python3 mr.sip.py -usage

https://github.com/meliht/mr.sip
Hacking Story 1: Registration Hijacking for Long Distance Call Routing Fraud

- **Victim:** An enterprise running VoIP (SIP Trunk)
- **Impact:** Infrastructure abuse causing expensive bills
- **Cause:** Weak password policy, unencrypted UDP traffic
- **Attacker Motivation:** Carrier voice business w/o infrastructure
- **Attack Vector:** Authentication attack, registration hijacking
- **Techniques:** MiTM sniffing, digest auth. calculation, password cracking
Hacking Story 1: Setup & Steps

- Assumption-1: Hired to pentest on internal network
- Assumption-2: Target SIP server have outbound calls over internet
- Target Subnet: 192.168.65.0/24
- Attack Tool: Mr.SIP Pro, SIP (NES, ENUM, SNIFF, CRACK)
- Payloads: Dictionaries for (user extension, password)

Hacking Steps:
1. SIP servers identification
2. Valid user enumeration
3. MiTM sniffing
4. SIP Authentication Data collection
5. SIP digest authentication cracking
6. Registration hijack
Hacking Story 1: DEMO! (watch it on our youtube channel)

https://www.youtube.com/channel/UCgri4qYdhrIPjxG8OtqxSkw
Attack Conclusion

• Single registration barrier?
  • Perform Registration Erasure attack to drop existing one! Make it periodic for persistence!

• Run this attack architecture on wide range of network and hijack more users.

• Business opportunity:
  • Wholesale VoIP, Carrier Voice, Call Shop, Prepaid/Post-paid card.

• Millions of dollars profit!! without running any telecom infrastructure.
  • Based on REAL incidents!
Hacking Story 2: Caller-ID Spoofing for a Spear Phishing Campaign

- **Victim:** An enterprise running VoIP
- **Impact:** Enabling an attacker access (potentially), information disclosure
- **Cause:** Unencrypted UDP traffic for SIP, lack of security awareness
- **Attacker Motivation:** Malware infection, information stealing (credentials)
- **Attack Vector:** Caller-ID spoofing, social engineering (spear phishing)
- **Techniques:** MiTM sniffing, SIP signalling manipulation
Hacking Story 2: Setup & Steps

- Assumption-1: Hired to pentest on internal network
- Target Server: 192.168.65.140
- Attack Tool: Mr.SIP Pro, SIP (ENUM, EAVES)
- Payloads: User extension dictionary

Hacking Steps:
1. SIP servers identification
2. Valid user enumeration
3. MiTM sniffing
4. Call eavesdropping & enum.
5. Custom INVITE generation
6. Caller-ID spoofing
7. Mimic another user and phishing
Hacking Story 2: DEMO! (watch it on our youtube channel)

https://www.youtube.com/channel/UCgrl4qYdhrLPjxG8OtxqSkw

MrSIP: SIP-based Audit and Attack Tool

--- By Melih Tas (SN)---

Grants - Caner, Onur, Nesli
Maintainer - Semih, Besir, Kutuk

[*] Client Interface: ethe0
[*] Client IP: 192.168.65.148
[*] SIP SM simulation process started.
A spoofed message was successfully sent.
time duration: 0.06
root@kali-64:~> Desktop/Mr_SIP_Proj python3 mr_sip.py --sim --caller-id=1234 --coa=1000 --tm=192.168.65.148

MrSIP: SIP-based Audit and Attack Tool

--- By Melih Tas (SN)---

Grants - Caner, Onur, Nesli
Maintainer - Semih, Besir, Kutuk

[*] Client Interface: ethe0
[*] Client IP: 192.168.65.148
[*] SIP SM simulation process started.
A spoofed message was successfully sent.
time duration: 0.06
root@kali-64:~> Desktop/Mr_SIP_Proj python3 mr_sip.py --sim --caller-id=1234 --coa=1000 --tm=192.168.65.148
Attack Conclusion

- Emulate insiders and perform spear phishing activities.
- SPIT idea (robocall): Create a list of victim users, perform automated calls (SIP-SIM supports that), play pre-recorded media content (advertisement)
- It is possible to make WAN-based Caller-ID Spoofing!
- Wait for it!
Hacking Story 3: Abusing Known Flood Based TDoS Vulnerability

- Victim: An enterprise running VoIP
- Impact: Overloading SIP server capacity
- Cause: Known DoS vulnerability of the SIP server
- Attacker Motivation: Distrupt the service availability
- Attack Vector: Version-based vulnerability scan, TDoS attack
- Techniques: Flood based TDoS, IP spoofing
Hacking Story 3: Setup & Steps

- Assumption-1: Hired to pentest on internal network
- Target Server: 192.168.65.140
- Attack Tool: Mr.SIP Pro, SIP (VSCAN, DAS)
- Payloads: N/A

Hacking Steps:
1. SIP servers identification
2. Scan for known vulns & exploits
3. Check for vulns & exploit details
4. Perform spoofed SIP INVITE flood
5. Exhaust the resources of target server
Hacking Story 3: DEMO! (watch it on our youtube channel)

https://www.youtube.com/channel/UCgrl4qYdhrlPjxG8OtxqSkw
Attack Conclusion

- Main Problem: Running vulnerable version? TDoS in UDP usage?
- Manipulate attention with TDoS
  - and perform another insidious attack at the time!
Advanced Attacks w/ SIP-ASP (Attack Scenario Player)

Attacking w/ Specially Crafted Call Scenarios

Predefined Attack Scenarios:
1. Incomplete INVITE Transaction DoS with Non-responding Destination Attack
2. Incomplete INVITE Dialog DoS without ACK Attack
3. SIP Request Collection Attack
4. SIP Request Reflection Attack
5. Registration Ensure Attack (Unexpected to Call Center)
6. TearDown Attack Using SIP Message
7. TearDown Attack Using CANCEL Message
8. Registration Hijacking
Advanced Attacks w/ SIP-ASP (Attack Scenario Player)

- Incomplete INVITE Transaction DDoS with Nonresponding Destination Attack
- Incomplete INVITE Dialog DDoS without ACK Attack
Advanced Attacks w/ SIP-ASP (Attack Scenario Player)

IEEE Access 2020-25937 "A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism"


• **SIP Request Reflection Attack (SRDoS in short)**

---

**A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism**

I. MELIN TAN1, BASAK GENCER UNSALER1, AND SELCUK BAKIR1, 2, (Member, IEEE)

1Department of Computer Engineering, Faculty of Engineering and Natural Sciences, Bilkent University, Ankara, Turkey

2College of Engineering and Technology, American University of the Middle East, Kuwait

Corresponding author: SelcuK Bakir (selcuK.bakir@Aum.edu.kw)

**ABSTRACT** We introduce a novel SIP based attack, named the SR-DRDoS attack, that exploits some less-known SIP features by using the IP-spoofing techniques, the reflection-based attack logic and the DRDoS attack logic. Furthermore, we develop a SIP-based DoS/DDoS attack simulator, named Mr. SIP, and use it to implement our SR-DRDoS attack. Our attack is shown to dramatically increase the CPU load of a SIP server from 0% up to 100% in only 4 minutes after the attack is initiated. Since our intelligent attack creates legitimate traffic on the SIP network by using reflection methods, it bypasses blacklists as well as to IP, packet-cast or session/transaction-based rate limiting and automatic message generation detection systems which exist in state-of-the-art security perimeters such as firewalls, intrusion detection/prevention systems and anomaly detection systems. Moreover, we propose a novel defense mechanism that effectively mitigates our proposed DRDoS attack. Our defense mechanism is shown to successfully reduce the CPU load of a SIP server under attack from 71% down to 18% within 3 minutes after it is initiated.

**INDEX TERMS** VoIP, voice over IP, SIP, session initiation protocol, SIP-Security, DoS, DDoS, DRDoS, distributed reflection denial of service attack, reflection attack.
VoIP Pentest Methodology w/ Mr.SIP Pro

- Identifying SIP Servers & Versions
  - SIP-NES
- Enumerating Users & Authentication Info
  - SIP-ENUM
- Identifying Known Vulns & Exploits
  - SIP-VSCAN
- Man in the Middle Attack
  - SIP-MANMID
- Sniffing the SIP Traffic
  - SIP-SNIFF
- Eavesdropping Calls & Enumeration
  - SIP-EAVES
- Cracking SIP Digest Authentication Realtime
  - SIP-CRACK
- Caller-ID Spoofing Attacks
  - SIP-SIM
- Denial of Service Attacks and Message Generation
  - SIP-DAS
- Attacking with Specially Crafted SIP Scenarios
  - SIP-ASP
Closing Thoughts

Lead Maintainer: Hakki Riza Kucuk
- Computer Science (Informatik) Student in University of Zurich (UZH)
- [https://github.com/hrkck](https://github.com/hrkck) (available for hire!) 😊

Special Thanks (Neslisah, Onur, Caner)

Call for Contribution
  Meaningful wordlists for username, passwords, user-agents
References


https://www.cfca.org/fraudlosssurvey
Thanks!

https://mrsip.pro/
https://mrsip.gitlab.io
https://github.com/meliht/mr.sip
https://twitter.com/mrsip_official
https://www.youtube.com/channel/UCgrl4qYdhrIPjxG8OtxqSkw

Contact: i.melih.tas@gmail.com
LinkedIn: https://www.linkedin.com/in/melihtas/
Twitter: https://twitter.com/artinscience
Github: https://github.com/meliht