VoIP Wars : Return of the SIP

Fatih Özavcı
Information Security Researcher & Consultant
fatih.ozavci at viproy.com  viproy.com/fozavci
# whois

- Information Security Consultant @ Viproy / Turkey
- 10+ Years Experience in Penetration Testing
- 800+ Penetration Tests, 40+ Focused on NGN/VoIP
  - SIP/NGN/VoIP Systems Penetration Testing
  - Mobile Application Penetration Testing
  - IPTV Penetration Testing
  - Regular Stuff (Network Inf., Web, SOAP, Exploitation...)
- Author of Viproy VoIP Penetration Testing Kit
- Author of Hacking Trust Relationships Between SIP Gateways
- Blackhat Arsenal USA 2013 – Viproy VoIP Pen-Test Kit

- So, that's me
VoIP Networks are Insecure, but Why?
- Basic Attacks but in Easy Way
  - Discovery, Footprinting, Brute Force
  - Initiating a Call, Spoofing, CDR and Billing Bypass
- SIP Proxy Bounce Attack
- Fake Services and MITM
  - Fuzzing Servers and Clients, Collecting Credentials
- (Distributed) Denial of Service
  - Attacking SIP Soft Switches and SIP Clients, SIP Amplication Attack
- Hacking Trust Relationships of SIP Gateways
- Attacking SIP Clients via SIP Trust Relationships
- Fuzzing in Advance

Out of Scope
- RTP Services and Network Tests, Management
- Additional Services
- XML/JSON Based Soap Services
# info

- **SIP** – Session Initiation Protocol
  - Only Signaling, not for Call Transporting
  - Extended with Session Discovery Protocol

- **NGN** – Next Generation Network
  - Forget TDM and PSTN
  - SIP, H.248 / Megaco, RTP, MSAN/MGW
  - Smart Customer Modems & Phones
  - Easy Management
  - Security is NOT a Concern?!

- Next Generation! Because We Said So!
# Administrators Think... Root Doesn't!

- Their VoIP Network Isolated
  - Open Physical Access, Weak VPN or MPLS
- Abusing VoIP Requires Knowledge
  - It's Easy with Automated Tools, But That's the Case!
- Most Attacks are Network Based or Toll Fraud
  - DOS, DDOS, Attacking Mobile Clients, Spying
  - Phishing, Surveillance, Abusing VAS Services
- VoIP Devices are Well-Configured
  - Weak Passwords, Old Software, Vulnerable Protocols
# SIP Services : Internal IP Telephony

- Support Servers
- SIP Clients
- SIP Server
- Factory/Campus SIP over VPN
- INTERNET
- Commercial Gateways
- Analog/Digital PBX
# SIP Services: Commercial Services

- Soft Switch (SIP Server)
- MSAN/MGW
- PSTN/ISDN Distributed
- 3rd Party Gateways
- Customers
- Mobile
- RTP, Proxy Servers
- SDP Servers
- MPLS
- VAS, CDR, DB Servers
# Viproy What?

- Viproy is a Vulcan-ish Word that means "Call"
- Viproy VoIP Penetration and Exploitation Kit
  - Testing Modules for Metasploit, MSF License
  - Old Techniques, New Approach
  - SIP Library for New Module Development
  - Custom Header Support, Authentication Support
  - New Stuffs for Testing: Trust Analyzer, Proxy etc

- Modules
  - Options, Register, Invite
  - Brute Forcers, Enumerator
  - SIP Trust Analyzer, Service Scanner
  - SIP Proxy, Fake Service, DDOS Tester
# Basic Attacks but in Easy Way

- We are looking for...
  - Finding and Identifying SIP Services and Purposes
  - Discovering Available Methods and Features
  - Discovering SIP Software and Vulnerabilities
  - Identifying Valid Target Numbers, Users, Realm
  - Unauthenticated Registration (Trunk, VAS, Gateway)
  - Brute Forcing Valid Accounts and Passwords
  - Invite Without Registration
  - Direct Invite from Special Trunk (IP Based)
  - Invite Spoofing (After or Before Registration, Via Trunk)

- Viproy Pen-Testing Kit Could Automate Discovery
# Basic Attacks but in Easy Way

## Discovery

**OPTIONS / REGISTER / INVITE / SUBSCRIBE**

- 100 Trying
- 200 OK
- 401 Unauthorized
- 403 Forbidden
- 404 Not Found
- 500 Internal Server Error

**Collecting Information from Response Headers**

- User-Agent
- Server
- Realm
- Call-ID
- Record-Route
- Warning
- P-Asserted-Identity
- P-Called-Party-ID
- P-Preferred-Identity
- P-Charging-Vector
# Basic Attacks but in Easy Way

## Register

**REGISTER / SUBSCRIBE (From, To, Credentials)**

- 200 OK
- 401 Unauthorized
- 403 Forbidden
- 404 Not Found
- 500 Internal Server Error

**RESPONSE Depends on Informations in REQUEST**

- Type of Request (REGISTER, SUBSCRIBE)
- FROM, TO, Credentials with Realm
- Via

**Actions/Tests Depends on RESPONSE**

- Brute Force (FROM, TO, Credentials)
- Detecting/Enumerating Special TOs, FROMs or Trunks
- Detecting/Enumerating Accounts With Weak or Null Passwords
- ....
# Basic Attacks but in Easy Way

- this isn't the call you're looking for

- We are attacking for...
  - Free Calling, Call Spoofing
  - Free VAS Services, Free International Calling
  - Breaking Call Barriers

- Spoofing with...
  - Via Field, From Field
  - P-Asserted-Identity, P-Called-Party-ID, P-Preferred-Identity
  - ISDN Calling Party Number, Remote-Party-ID

- Bypass with...
  - P-Charging-Vector (Spoofing, Manipulating)
  - Re-Invite, Update (Without/With P-Charging-Vector)

- Viproy Pen-Testing Kit Supports Custom Headers
# Basic Attacks but in Easy Way

**Invite, CDR and Billing Tests**

**INVITE/ACK/RE-INVITE/UPDATE (From, To, Credentials, VIA ...)**

- 100 Trying
- 183 Session Progress
- 180 Ringing
- 200 OK
- 401 Unauthorized
- 403 Forbidden
- 404 Not Found
- 500 Internal Server Error

**RESPONSE Depends on Informations in INVITE REQUEST**

- FROM, TO, Credentials with Realm, FROM <>, TO <>
- Via, Record-Route
- Direct INVITE from Specific IP:PORT (IP Based Trunks)

**Actions/Tests Depends on RESPONSE**

- Brute Force (FROM&TO) for VAS and Gateways
- Testing Call Limits, Unauthenticated Calls, CDR Management
- INVITE Spoofing for Restriction Bypass, Spying, Invoice
- ....
# SIP Proxy Bounce Attack

- SIP Proxies Redirect Requests to Other SIP Servers
  - We Can Access Them via SIP Proxy then We Can Scan
  - We Can Scan Inaccessible Servers
  - URI Field is Useful for This Scan
- Viproy Pen-Testing Kit Has a UDP Port Scan Module

```bash
msf auxiliary(vsipportscan-options) > run

[+] 192.168.1.146:5060 is Open
    Server : FPBX-2.11.0beta2(11.2.1)

[+] 192.168.1.145:5070 is Open
    User-Agent : sipXecs/4.7.0 sipXecs/registry (Linux)

[+] 192.168.1.201:5061 is Open
    Server : sipXecs/xxxx.yyyy sipXecs/sipxbridge (Linux)

[+] 192.168.1.203:5060 is Open
    User-Agent : 3CXPhoneSystem 11.0.28976.849 (28862)
```
# SIP Proxy Bounce Attack

192.168.1.145 – Izmir
Production SIP Service

The Wall

192.168.1.146
Ankara

192.168.1.201
Adana

White Walker

How Can We Use It?

- SIP Trust Relationship Attacks
- Attacking Inaccessible Servers
- Attacking SIP Software
  - Software Version, Type
# Fake Services and MITM

Usage of Proxy & Fake Server Features

- Use ARP Spoof & VLAN Hopping & Manual Config
- Collect Credentials, Hashes, Information
- Change Client's Request to Add a Feature (Spoofing etc)
- Change the SDP Features to Redirect Calls
- Add a Proxy Header to Bypass Billing & CDR
- Manipulate Request at Runtime to find BOF Vulnerabilities
# Fake Services and MITM

- We Need a Fake Service
  - Adding a Feature to Regular SIP Client
  - Collecting Credentials
  - Redirecting Calls
  - Manipulating CDR or Billing Features
  - Fuzzing Servers and Clients for Vulnerabilities
- Fake Service Should be Semi-Automated
  - Communication Sequence Should be Defined
  - Sending Bogus Request/Result to Client/Server

- Viproy Pen-Testing Kit Has a SIP Proxy and Fake Service
- Fuzzing Support of Fake Service is in Development Stage
# DOS – It's Not Service, It's Money

- Locking All Customer Phones and Services for Blackmail
- Denial of Service Vulnerabilities of SIP Services
  - Many Responses for Bogus Requests → DDOS
  - Concurrent Registered User/Call Limits
  - Voice Message Box, CDR, VAS based DOS Attacks
  - Bye And Cancel Tests for Call Drop
  - Locking All Accounts if Account Locking is Active for Multiple Fails
- Multiple Invite (After or Before Registration, Via Trunk)
  - Calling All Numbers at Same Time
  - Overloading SIP Server's Call Limits
  - Calling Expensive Gateways, Targets or VAS From Customers

- Viproy Pen-Testing Kit Has a few DOS Features
# DDOS – All Your SIP Gateways Belong to Us!

- **SIP Amplification Attack**
  - + SIP Servers Send Errors Many Times (10+)
  - + We Can Send IP Spoofed Packets
  - + SIP Servers Send Responses to Victim
  
  => 1 packet for 10+ Packets, ICMP Errors (Bonus)

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>8.315312000</td>
<td>192.168.1.100</td>
<td>192.168.1.145</td>
<td>SIP/SDP</td>
<td>938</td>
<td>Request: INVITE sip:<a href="mailto:701@viproy.com">701@viproy.com</a>, with s</td>
</tr>
<tr>
<td>3</td>
<td>8.324730000</td>
<td>192.168.1.145</td>
<td>192.168.1.100</td>
<td>SIP</td>
<td>358</td>
<td>Status: 100 Trying</td>
</tr>
<tr>
<td>4</td>
<td>8.325086000</td>
<td>192.168.1.145</td>
<td>192.168.1.100</td>
<td>SIP</td>
<td>587</td>
<td>Status: 407 Proxy Authentication Required</td>
</tr>
<tr>
<td>5</td>
<td>8.430072000</td>
<td>192.168.1.145</td>
<td>192.168.1.100</td>
<td>SIP</td>
<td>587</td>
<td>Status: 407 Proxy Authentication Required</td>
</tr>
<tr>
<td>6</td>
<td>8.638928000</td>
<td>192.168.1.145</td>
<td>192.168.1.100</td>
<td>SIP</td>
<td>587</td>
<td>Status: 407 Proxy Authentication Required</td>
</tr>
<tr>
<td>7</td>
<td>9.040660000</td>
<td>192.168.1.145</td>
<td>192.168.1.100</td>
<td>SIP</td>
<td>587</td>
<td>Status: 407 Proxy Authentication Required</td>
</tr>
</tbody>
</table>

- Viproy Pen-Testing Kit Has a PoC DDOS Module
- Can we use SIP Server's Trust? -wait for it-
# DDOS – All Your SIP Gateways Belong to Us!

192.168.1.201 – Izmir
Production SIP Service

192.168.1.202 – Ankara
Production SIP Service

192.168.1.203 – Adana
Production SIP Service

White Walker

IP Spoofed Call Request

The Wall

Citadel
# Hacking SIP Trust Relationships

- NGN SIP Services Trust Each Other
  - Authentication and TCP are Slow, They Need Speed
  - IP and Port Based Trust are Most Effective Way
- What We Need
  - Target Number to Call (Cell Phone if Service is Public)
  - Tech Magazine, Web Site Information, News
- Baby Steps
  - Finding Trusted SIP Networks (Mostly B Class)
  - Sending IP Spoofed Requests from Each IP:Port
  - Each Call Should Contain IP:Port in From Section
  - If We Have a Call, We Have The Trusted SIP Gateway IP and Port
  - Brace Yourselves The Call is Coming
# Hacking SIP Trust Relationships

Slow Motion

192.168.1.201 – Izmir
Production SIP Service

The Wall

IP Spoofed Call Request
Contains IP:Port Data in From

White Walker

Ankara
Istanbul

International Trusted Operator
# Hacking SIP Trust Relationships

Brace Yourselves, The Call is Coming

192.168.1.201 – Izmir
Production SIP Service

The Wall

IP Spoofed Call Request
Somebody Known in From

From Citadel

Come Again?

- Billing ?
- CDR ?
- Log ?
# Hacking SIP Trust Relationships – Business Impact

● Denial of Service
  - Short Message Service and Billing
  - Calling All Numbers at Same Time
  - Overloading SIP Server's Call Limits
  - Overloading VAS Service or International Limits
  - Overloading CDR Records with Spoofed Calls

● Attacking a Server Software
  - Crashing/Exploiting Inaccesible Features
  - Call Redirection (working on it, not yet :/)

● Attacking a Client?
  - Next Slide!
# Attacking a Client via SIP Trust Relationships

- SIP Server Redirects a few Fields to Client
  - FROM, FROM NAME, Contact
  - Other Fields Depend on Server (SDP, MIME etc)

- Clients Have Buffer Overflow in FROM?
  - Send 2000 Chars to Test it!
  - Crash it or Execute your Command if Available

- Clients Trust SIP Servers and Trust is UDP Based
  - This module can be used for Trust Between Client and Server

- Viproy Pen-Testing Kit SIP Trust Module
  - Simple Fuzz Support (FROM=FUZZ 2000)
  - You Can Modify it for Further Attacks
# Attacking a Client via SIP Trust Relationships

Brace Yourselves 550 Chars are Coming

192.168.1.201 – Izmir Production SIP Service

White Walker

The Wall

IP Spoofed Call Request 550 Chars in From

Bogus Invite Request

CRASSSSH!

International Trusted Operator

Ankara Istanbul

AdorePhone Iphone App

- Command?
- Why Not!
# Fuzz Me Maybe

- Fuzzing as a SIP Client | SIP Server | Proxy | MITM
- SIP Server Software
- SIP Clients
  - Hardware Devices, IP Phones, Video Conference Systems
  - Desktop Application or Web Based Software
  - Mobile Software
- Special SIP Devices/Software
  - SIP Firewalls, ACL Devices, Proxies
  - Connected SIP Trunks, 3rd Party Gateways
  - MSAN/MGW
  - Logging Software (Indirect)
  - Special Products: Cisco, Alcatel, Avaya, Huawei, ZTE...
# Old School Fuzzing

- Request Fuzzing
  - SDP Features
  - MIME Type Fuzzing
- Response Fuzzing
  - Authentication, Bogus Messages, Redirection
- Static vs Stateful
- How about Smart Fuzzing
  - Missing State Features (ACK, PHRACK, RE-INVITE, UPDATE)
  - Fuzzing After Authentication (Double Account, Self-Call)
  - Response Fuzzing (Before or After Authentication)
  - Missing SIP Features (IP Spoofing for SIP Trunks, Proxy Headers)
  - Numeric Fuzzing for Services is NOT Memory Corruption
  - Dial Plan Fuzzing, VAS Fuzzing
# How Viproy Pen-Testing Kit Helps Fuzzing Tests

- Skeleton for Feature Fuzzing, NOT Only SIP Protocol
- Multiple SIP Service Initiation
  - Call Fuzzing in Many States, Response Fuzzing
- Integration With Other Metasploit Features
  - Fuzzers, Encoding Support, Auxiliaries, Immortality etc.
- Custom Header Support
  - Future Compliance, Vendor Specific Extensions, VAS
- Raw Data Send Support (Useful with External Static Tools)
- Authentication Support
  - Authentication Fuzzing, Custom Fuzzing with Authentication
- Less Code, Custom Fuzzing, State Checks
- Some Features (Fuzz Library, SDP) are Coming Soon
# Fuzzing SIP Services

## Request Based

Options/REGISTER/Subscribe/INVITE/ACK/RE-INVITE/UPDATE....

- 100 Trying
- 183 Session Progress
- 180 Ringing
- 200 OK
- 401 Unauthorized
- 403 Forbidden
- 404 Not Found
- 500 Internal Server Error

### Fuzzing Targets, REQUEST Fields

- Request Type, Protocol, Description
- Via, Branch, Call-ID, From, To, Cseq, Contact, Record-Route
- Proxy Headers, P-*-* (P-Asserted-Identity, P-Charging-Vector...)
- Authentication in Various Requests (User, Pass, Realm, Nonce)
- Content-Type, Content-Length
  - SDP Information Fields
  - ISUP Fields
# Fuzzing SIP Services

Response Based

### Potential RESPONSE Types for Fuzzing

- 100 Trying
- 183 Session Progress
- 180 Ringing
- 200 OK
- 401 Unauthorized
- 403 Forbidden
- 404 Not Found
- 500 Internal Server Error
DEMO

Attacking SIP Servers for Fun & Profit

Demo Sample
https://www.youtube.com/watch?v=AbXh_L0-Y5A
References

- Viproy VoIP Penetration and Exploitation Kit
  Author: http://viproy.com/fozavci
  Homepage: http://viproy.com/voipkit
  Github: http://www.github.com/fozavci/viproy-voipkit

- Attacking SIP Servers Using Viproy VoIP Kit (50 mins)
  https://www.youtube.com/watch?v=AbXh_L0-Y5A

- Hacking Trust Relationships Between SIP Gateways (PDF)

- VoIP Pen-Test Environment – VulnVoIP
  http://www.rebootuser.com/?cat=371
Q ?
Thanks