Viproy VoIP Penetration and Exploitation Toolkit

Fatih Özavcı

Security Consultant @ Sense of Security (Australia)

# whois

- Security Consultant @ Sense of Security (Australia)
- 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
- DEFCON 21 – VoIP Wars: Return of the SIP

- So, that's me

# traceroute

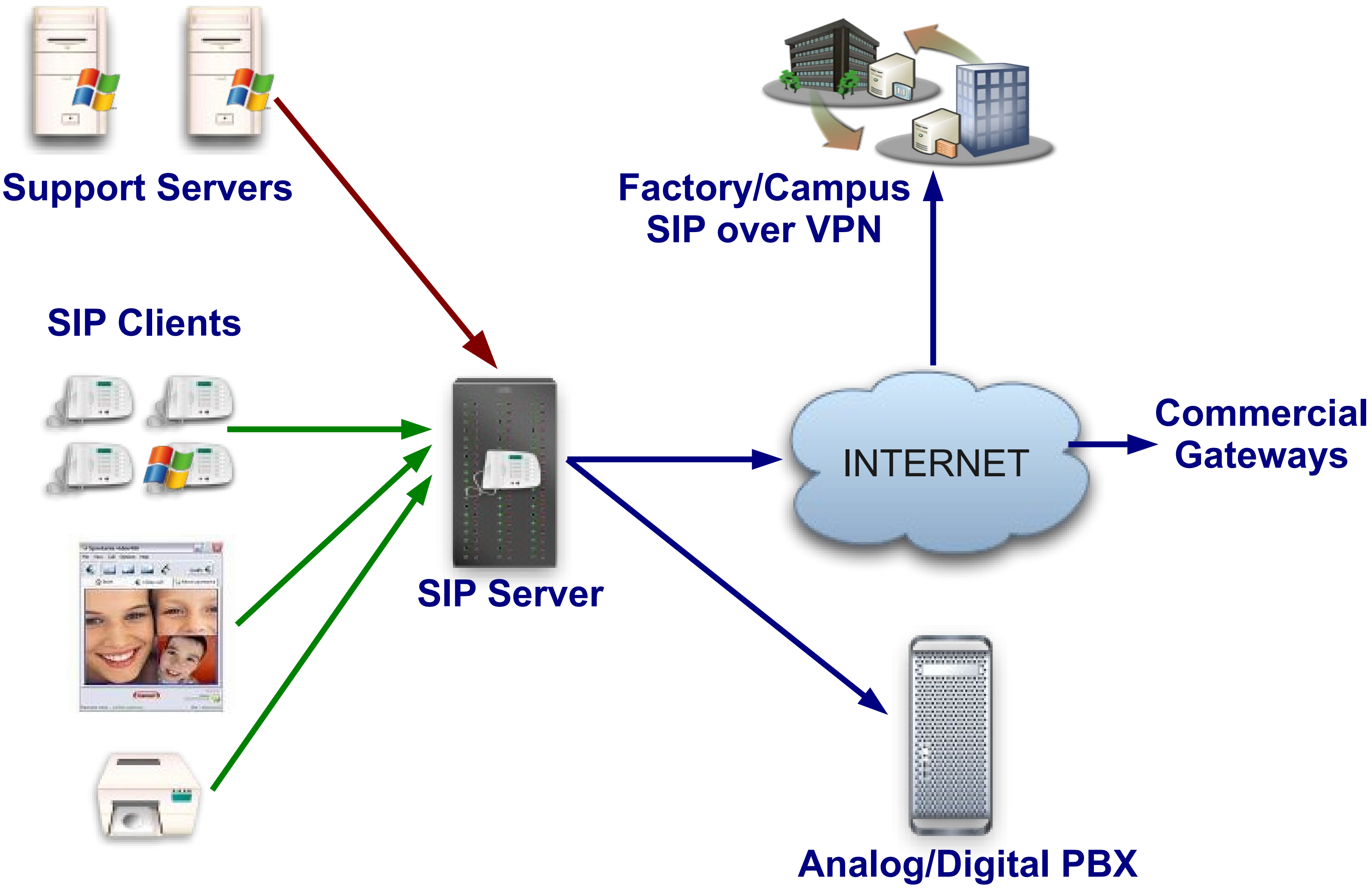
- Viproy What?
- SIP Services and Security Problems
- Basic Attacks but in Easy Way
- Modules for Basic Attacks
- SIP Proxy Bounce Attack
- Fake Services and MITM
- (Distributed) Denial of Service
- Hacking Trust Relationships of SIP Gateways
- Fuzzing in Advance

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

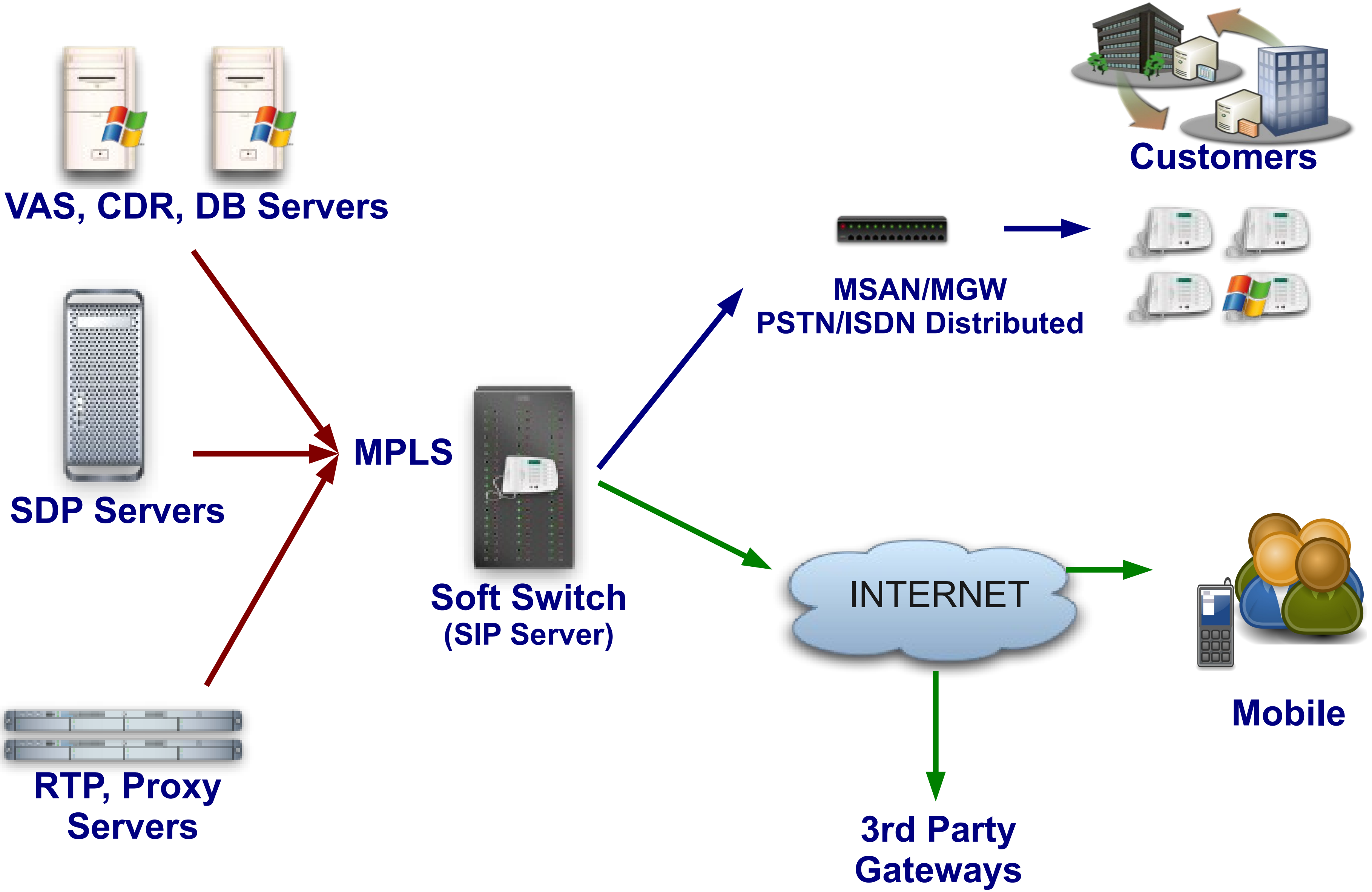
# Viproy What?

- 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

# SIP Services : Internal IP Telephony



# SIP Services : Commercial Services



# 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)

# Basic Attacks but in Easy Way

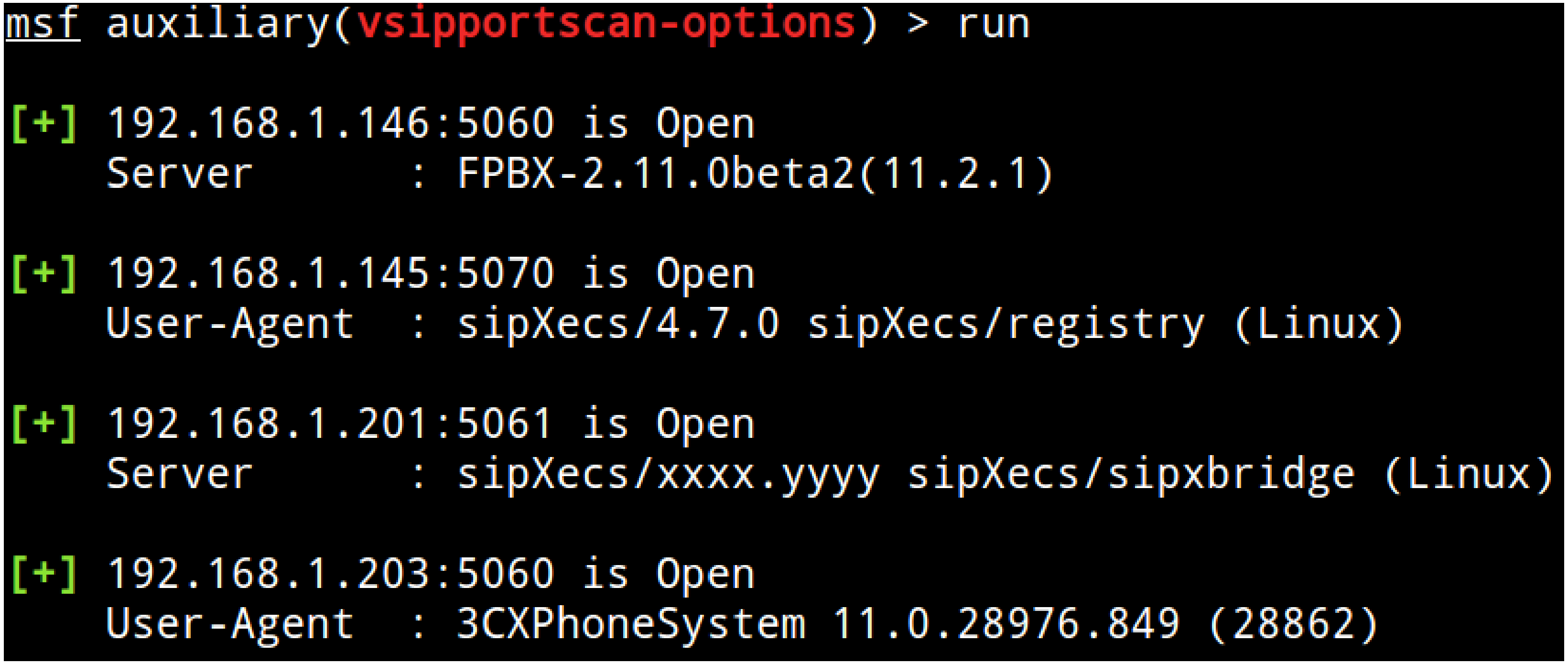
- this isn't the call you're looking for
- We are attacking for...
  - Free Calling, Call Spoofing
  - Free VAS Services, Free International Calling
  - Breaking Call Barriers
  - Spoofing with...
    - Via Field, From Field
    - P-Asserted-Identity, P-Called-Party-ID, P-Preferred-Identity
    - ISDN Calling Party Number, Remote-Party-ID
  - Bypass with...
    - P-Charging-Vector (Spoofing, Manipulating)
    - Re-Invite, Update (Without/With P-Charging-Vector)

# Basic Attacks but in Easy Way

- Modules for Discovery - Register, Enumerator, Options, Invite
- Modules to Obtain Information - Enumerator, Brute Forcer
- Modules to Attack VAS or Internal Services
  - Invite, Brute Forcer, Enumerator, Trust Analyzer
- Module to Initiate Calls, Billing Attacks and Privilege Analysis
  - Invite (Custom Header Support, Proxy Headers etc)
- Modules for Analyzing Trust Issues and Invite Spoofing
  - Invite, Trust Analyzer
- Module to Modify SIP Clients/Servers' Behaviors - MITM Proxy
- Modules for DDOS/DOS - All Modules

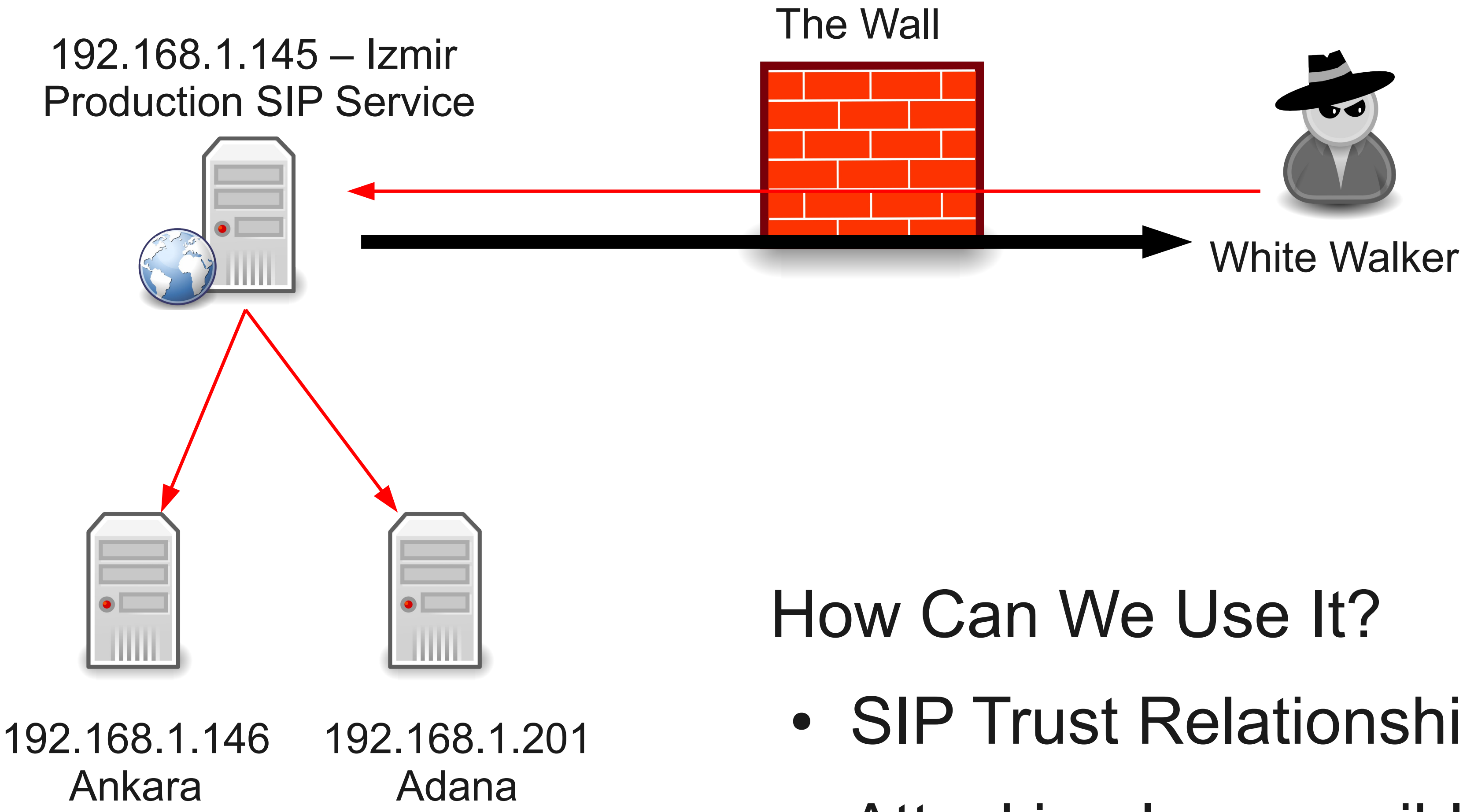
# SIP Proxy Bounce Attack

- 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



```
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

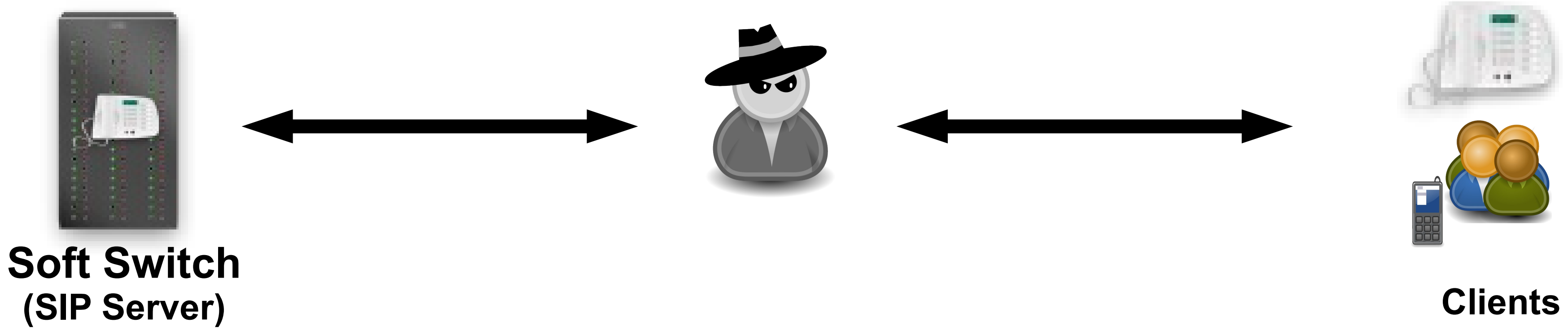


How Can We Use It?

- 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
  - Communiation 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 !

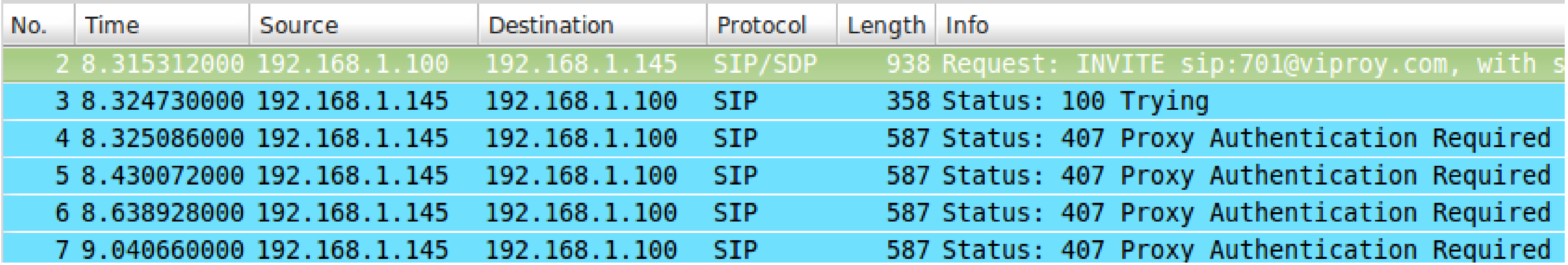
- SIP Amplification Attack

  + 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)



No.	Time	Source	Destination	Protocol	Length	Info
2	8.315312000	192.168.1.100	192.168.1.145	SIP/SDP	938	Request: INVITE sip:701@viproy.com, with s
3	8.324730000	192.168.1.145	192.168.1.100	SIP	358	Status: 100 Trying
4	8.325086000	192.168.1.145	192.168.1.100	SIP	587	Status: 407 Proxy Authentication Required
5	8.430072000	192.168.1.145	192.168.1.100	SIP	587	Status: 407 Proxy Authentication Required
6	8.638928000	192.168.1.145	192.168.1.100	SIP	587	Status: 407 Proxy Authentication Required
7	9.040660000	192.168.1.145	192.168.1.100	SIP	587	Status: 407 Proxy Authentication Required

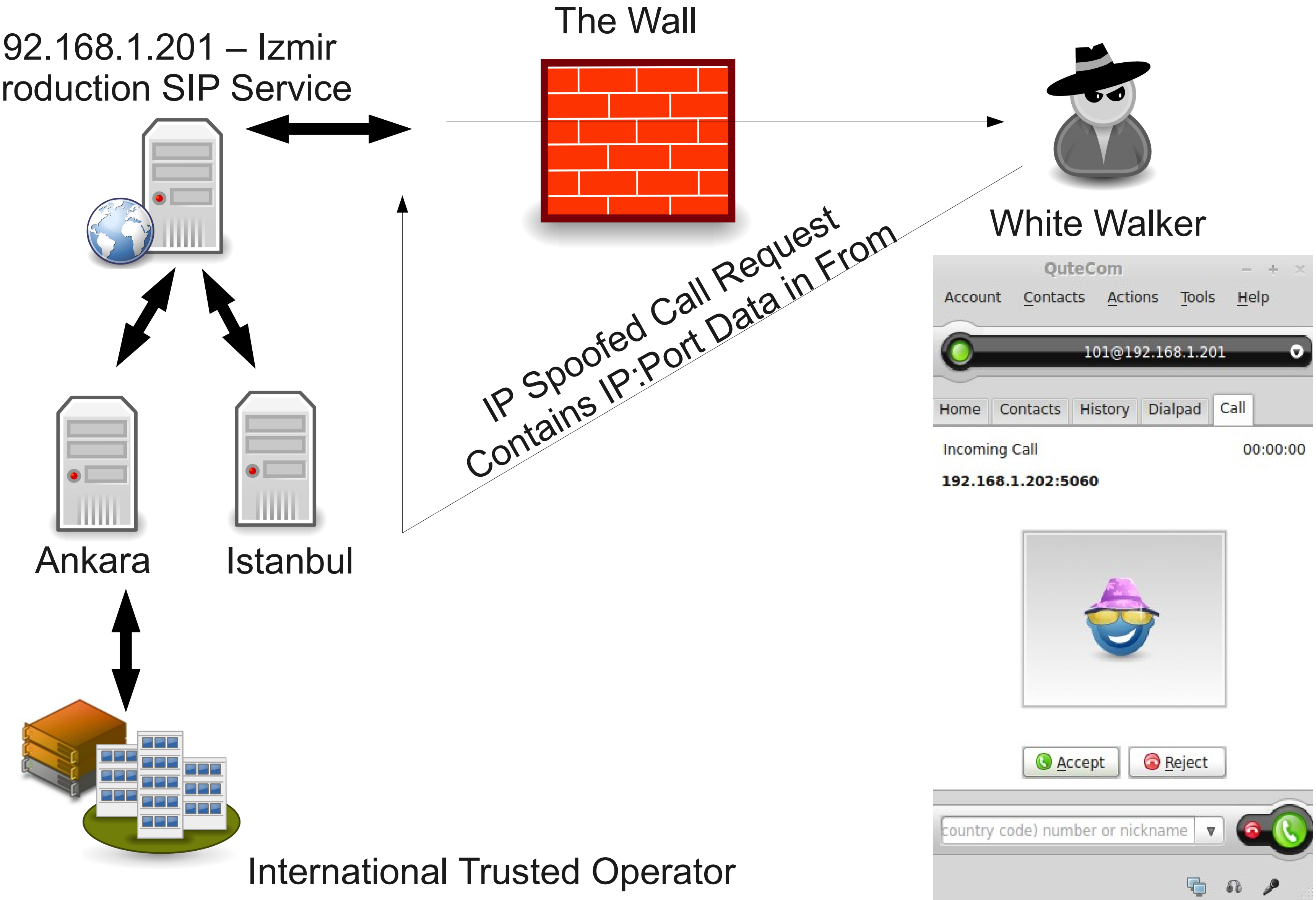
- Viproy Pen-Testing Kit Has a PoC DDOS Module
- Can we use SIP Server's Trust ? -wait for it-

# 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

White Walker

IP Spoofed Call Request
Contains IP:Port Data in From

Ankara

Istanbul

International Trusted Operator

101@192.168.1.201

Incoming Call 00:00:00

192.168.1.202:5060

# 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

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)

  http://viproy.com/files/siptrust.pdf

- VoIP Pen-Test Environment – VulnVoIP

  http://www.rebootuser.com/?cat=371

Q ?

Thanks