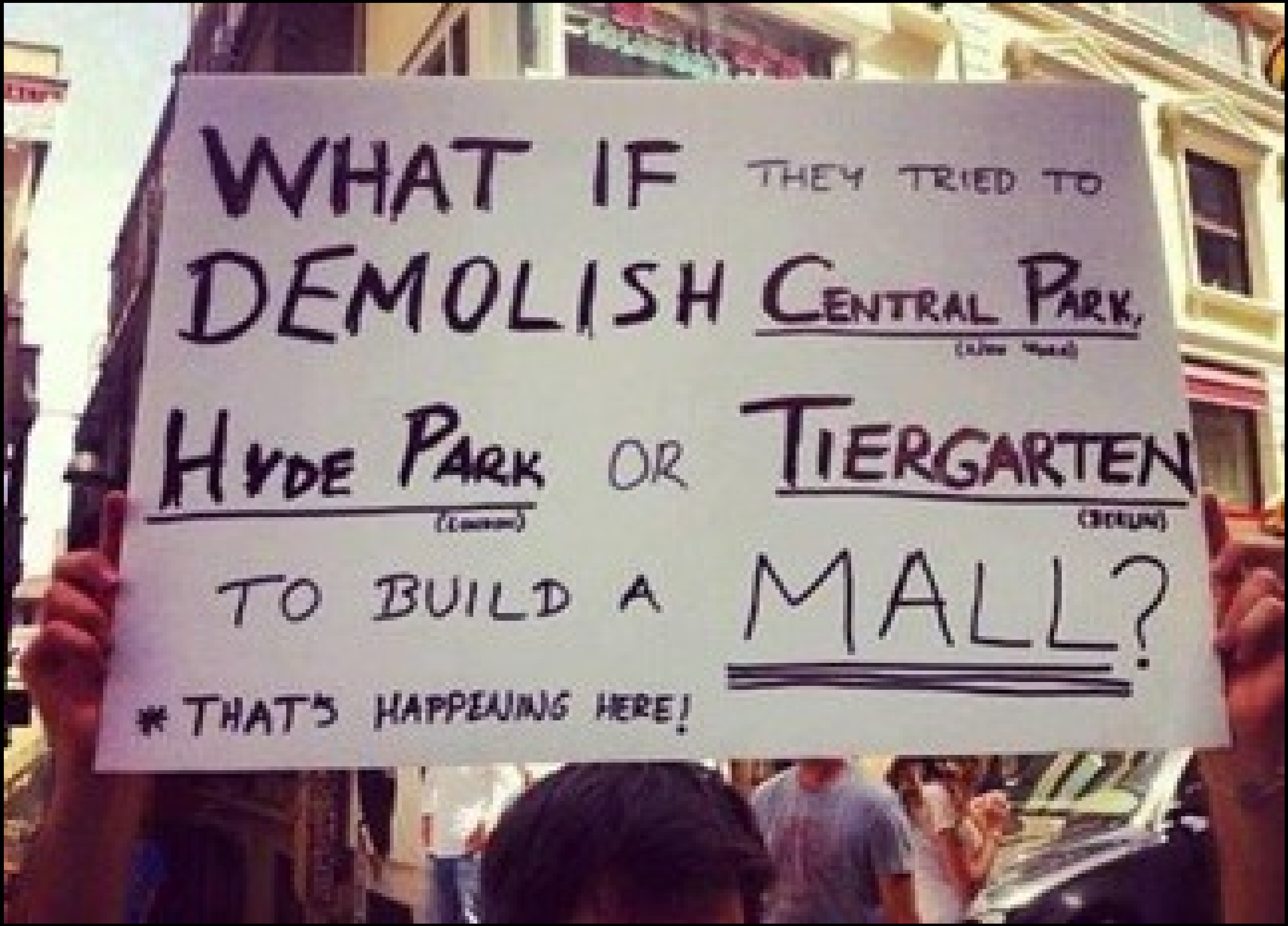
Hacking SIP Services Like a Boss

Fatih Özavcı

Information Security Researcher & Consultant

fatih.ozavci at viproy.com   viproy.com/fozavci

#occupygezi #direngezi



#occupygezi #direngezi

#occupygezi #direngezi

About Me

- 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 SIP Trust Relationships of SIP Gateways
- Blackhat Arsenal USA 2013 – Viproy VoIP Pen-Test Kit

- So, that's me

Agenda

- VoIP Networks are Insecure, but Why?
- Viproy What?
- Discovery
- Register/Subscribe Tests
- Invite Tests
- CDR and Billing Bypass
- Denial of Service
- Fuzzing
- Hacking SIP Trust Relationships
- Out of Scope
  - RTP Services and Network Tests
  - Management and Additional Services
  - XML/JSON Based Soap Services

SIP, NGN, VoIP

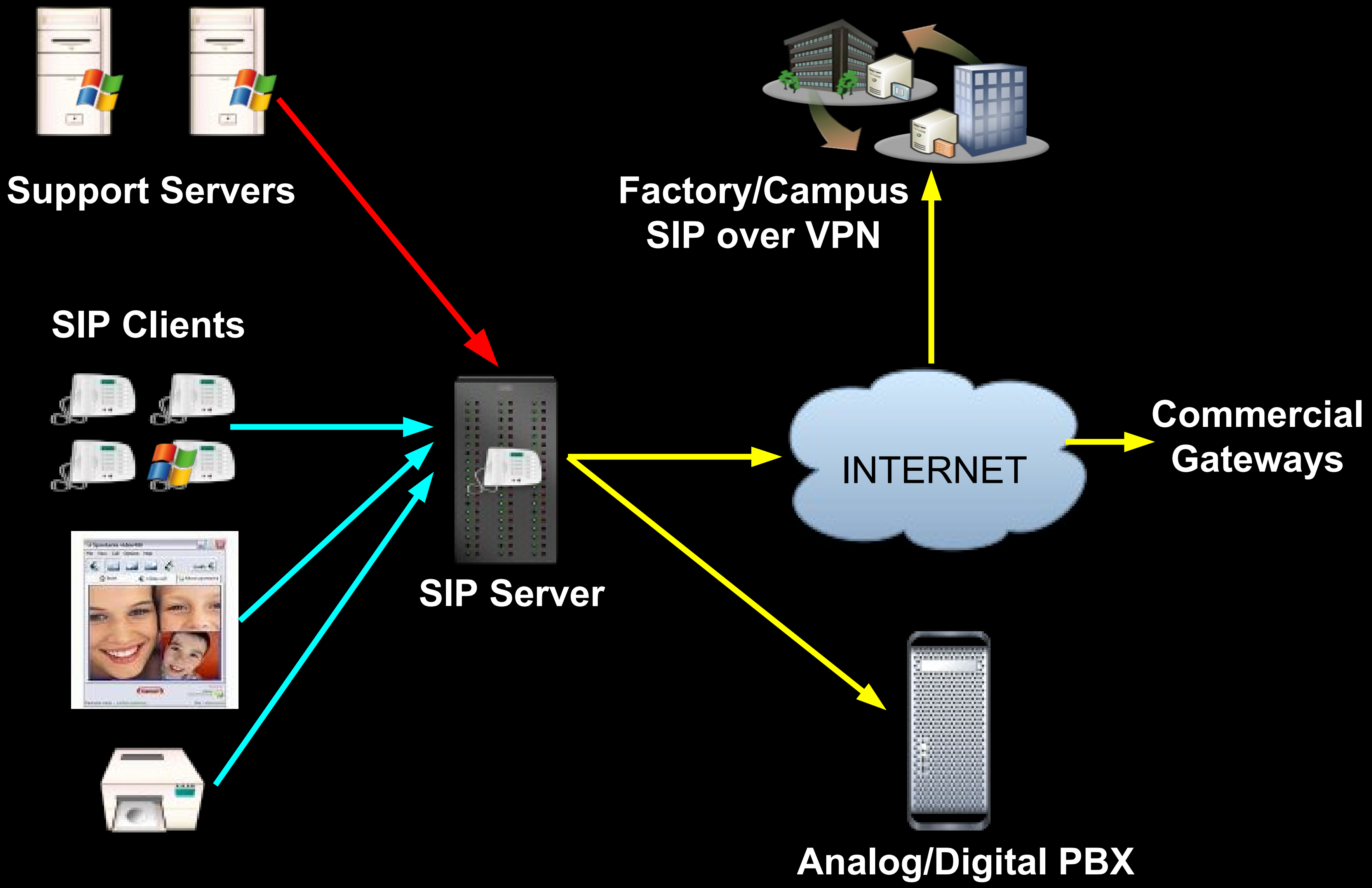
- SIP – Session Initiation Protocol
  - Only Signaling not Transporting Call
  - Extended with Session Discovery Protocol
- NGN – Next Generation Network
  - Forget TDM and PSTN
  - SIP, H.248 / Megaco, RTP, MSAN/MGW
  - Smart Customer Modems & Phones
  - Easy Management
  - Security Free, It's NOT Required?!

- Next Generation! Because We Said So!

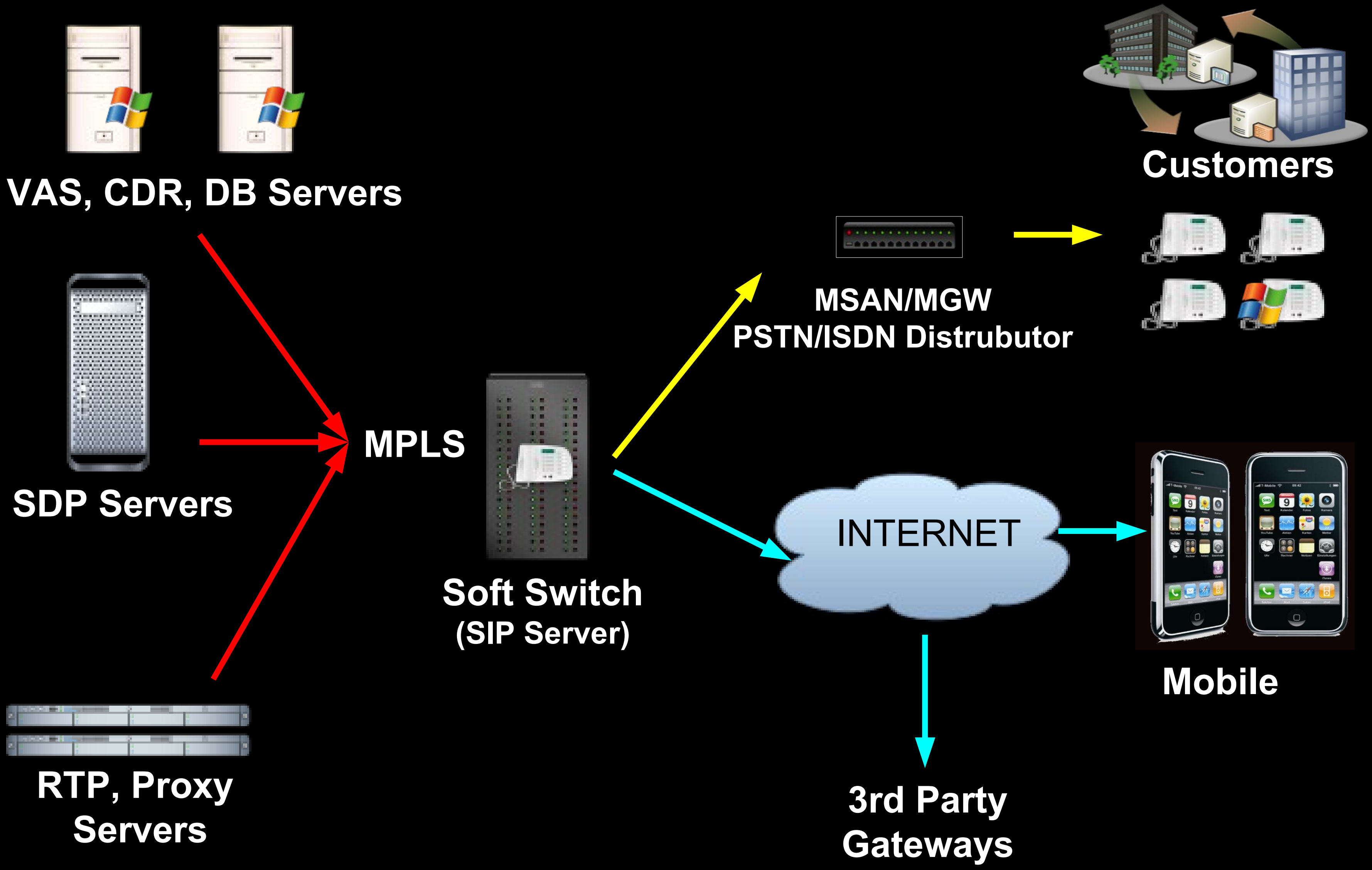
Administrators Think... Root Doesn't!

- Their VoIP Network Isolated
  - Open Physical Access for Many Network Operators
  - Insufficient Network Segmentation
  - Insecure VPNs (IPSec, MPLS)
- Abusing VoIP Requires Knowledge
  - It's Easy With Right Automated Tools, But That's the Case !
- Most Attacks are Network Based or Toll Fraud
  - Call Based DOS Attacks, Response Based DDOS Attacks,
  - Compromising Clients for Surveillance, Spying
  - Phishing, Fake Calls for Fun&Profit, Abusing VAS Services
- VoIP Devices are Well-Configured
  - Many Operators and Vendors Have No Idea About The Security Requirements
  - SIP Accounts without Passwords, Trunks, Management Problems
  - Old Version and Insecure Software (Especially VAS, CDR, DB, Operating System)
  - Insecure Additional Services (TFTP, Telnet, SNMP, FTP, DHCP, Soap Services)

SIP Services : Internal IP Telephony



SIP Services : Commercial Operators



Why Other SIP Tools are not Efficient ?

- Sipvicious, Sipsak, Sipp : Basic Tools, Basic Functions
- They Need Complete Protocol Information to Perform a Test
- They Prepared for Simple Tasks, not Complete Operation
- Performing Security Tests After Authentication is Painful
  - Call Spoofing, Bypassing CDR/Invoice, Spying
  - DOS Attacks for Call Limits, VAS Services, Toll Fraud
  - Special Tests Require 3-4 Steps
- They Don't Have Pen-Test Features
  - Database Support, Integration with Other Tools
  - Knowledge Transfer
  - Quick Action & Development for Specific Cases

Why Metasploit Framework or New Modules?

- Metasploit Has Many Penetration Testing Features
  - 1000+ Exploits & Tools, Database Support, Automated Tasks
  - Handy Functions for Development, Sample Modules, Less Code
  - Integration Between Tools and Exploits

- Why New Metasploit Modules?
  - There is NO SIP Library in REX, Auxiliary Development is Painful
  - There is NO Module for Testing SIP Services after Authentication
  - Presented SIP Auxiliaries are Useful Only Specific Tests
  - 8 Simple Modules and 1 Library, Less Code for SIP Tests
  - Integrated SIP Tests with Metasploit Framework Infrastructure

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, Port Scan
  - SIP Proxy, Fake Service

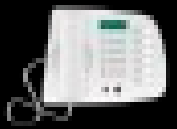
Discovery

- Finding and Identifying SIP Services
    - Different Ports, Different Purposes
    - Internal Communication Service or PSTN Gateway
- Discovering Available Methods
    - Register, Direct Invite, Options
    - Soft Switch, Call Manager, Mobile Client Software, IP Phone
- Discovering SIP Software
    - Well-Known Software Vulnerabilities
    - Compliant Softwares and Architecture
    - Network Points and 3rd Party Detection

Discovery

OPTIONS / REGISTER / INVITE / SUBSCRIBE

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



Clients

Gateways

Soft Switch
(SIP Server)

Collecting Information from Response Headers

- User-Agent
- Server
- Realm
- Call-ID
- Record-Route

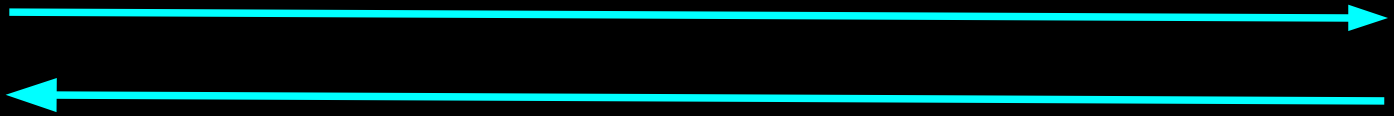
- Warning
- P-Asserted-Identity
- P-Called-Party-ID
- P-Preferred-Identity
- P-Charging-Vector

Register/Subscribe Tests

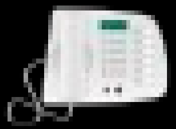
- Unauthenticated Registration
  - Special Trunks
  - Special VAS Numbers
  - Gateways
- Identifying Valid Target Numbers, Users, Realm
- De-Registration for Valid Users
- Brute Forcing Valid Accounts and Passwords
  - With Well-Known User List
  - Numeric User Ranges

Register/Subscribe Tests

REGISTER / SUBSCRIBE (From, To, Credentials)

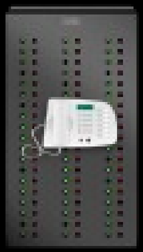


200 OK
401 Unauthorized
403 Forbidden
404 Not Found
500 Internal Server Error



Clients

Gateways



Soft Switch
(SIP Server)

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
- ….

Invite Tests

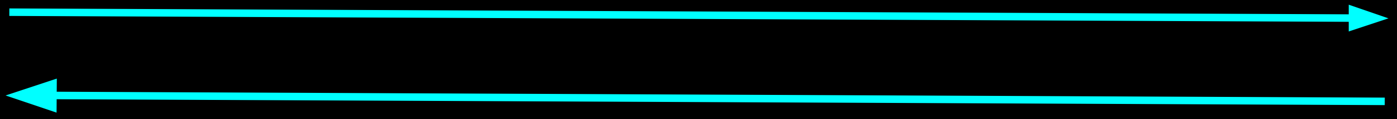
- Invite Without Registration
  - Client Software, IP Phone, Test SIP Server
  - Bypassing “After Register” Restrictions
- Direct Invite from Special Trunk (IP Based)
  - VAS Services, Trusted Soft Switches, Gateways, MSAN, MGW
- Invite Spoofing (After or Before Registration, Via Trunk)
  - For Phishing, Spying, Surveillance, Restriction Bypass, VAS
  - Via Field, From Field
  - P-Asserted-Identity, P-Called-Party-ID, P-Preferred-Identity
  - ISDN Calling Party Number, Remote-Party-ID

CDR and Billing Bypass

- Invite Spoofing (After or Before Registration, Via Trunk)
  - Via Field, From Field
  - P-Asserted-Identity, P-Called-Party-ID, P-Preferred-Identity
  - ISDN Calling Party Number, Remote-Party-ID
- Bypass Techniques
  - Faking as a Cheap Gateway, Another Customer or Trunk
  - Direct Call to Client, VAS Service or Gateway
- Call Count Information on Headers
  - P-Charging-Vector (Spoofing, Manipulating)
  - Re-Invite, Update (Without/With P-Charging-Vector)

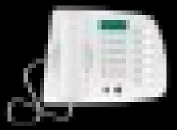
Invite, CDR and Billing Tests

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



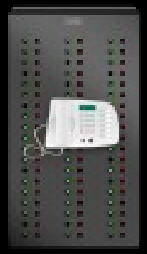
100 Trying
183 Session Progress
180 Ringing
200 OK

401 Unauthorized
403 Forbidden
404 Not Found
500 Internal Server Error



Clients

Gateways



Soft Switch
(SIP Server)

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
- ....

Denial of Service

- 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

Fuzzing SIP Services or Fuzz Me Maybe

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

Fuzzing SIP Services or Fuzz Me Maybe

- Request Fuzzing
  - Fuzzing Registration and Authentication Parameters
  - Fuzzing Invite Parameters
  - Fuzzing Options Parameters
  - Fuzzing Bye and Cancel Parameters
  - Fuzzing Authentication Functions
- Response Fuzzing
  - Authentication Options (Nonce, Digest, URI etc)
  - [1|2]0x 200 OK, 100 Trying, 180 Ringing, 183 Session Progress
  - 30x 301 Moved Permanently, 305 Use Proxy, 380 Alternate Services
  - 40x 401 Unauthorized, 403 Forbidden, 402 Payment Required
  - 60x 600 Busy, 603 Decline, 606 Not Acceptable

Static and Stateful SIP Fuzzers

- Static Fuzzers
  - Protos

    https://www.ee.oulu.fi/research/ouspg/PROTOS_Test-Suite_c07-sip
  - SipFuzzer

    http://code.google.com/p/sipfuzzer/
  - Asteroid SIP Fuzzer

    http://www.infiltrated.net/asteroid/
- Stateful Fuzzers
  - Interstate

    http://testlab.ics.uci.edu/interstate/
  - Kif

    http://kif.gforge.inria.fr/
  - Snooze

    http://seclab.cs.ucsb.edu/academic/projects/projects/snooze/

Missing Features in SIP Fuzzers

- Static Fuzzers
  - State Tracking is Biggest Problem
  - Missing Important SIP Features and Headers
- Stateful Fuzzers (Old Tools, Last Update 2007)
  - 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, Custom Headers, Invoice Headers
    - SDP and ISUP Support
  - Numeric Fuzzing for Services is NOT Buffer Overflow
    - Dial Plan Fuzzing, VAS Fuzzing

How This SIP Library Helps Fuzzing Tests

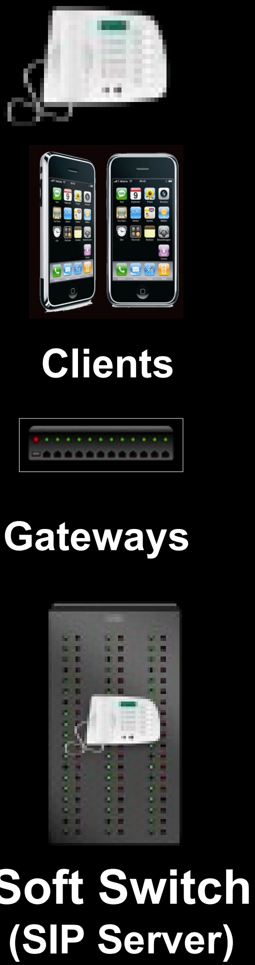
- Skeleton for Feature Fuzzing, NOT Only SIP Protocol
- Multiple SIP Service Initiation
  - Call Fuzzing in Many States, Response Fuzzing
- Integration With Other Metasploit Features
  - Fuzzers, Encoding Support, Auxiliaries, Immortality etc.
- Custom Header Support
  - Future Compliance, Vendor Specific 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 in Development

Fuzzing SIP Services : Request Based

OPTIONS/REGISTER/SUBSCRIBE/INVITE/ACK/RE-INVITE/UPDATE....

100 Trying
183 Session Progress
180 Ringing
200 OK

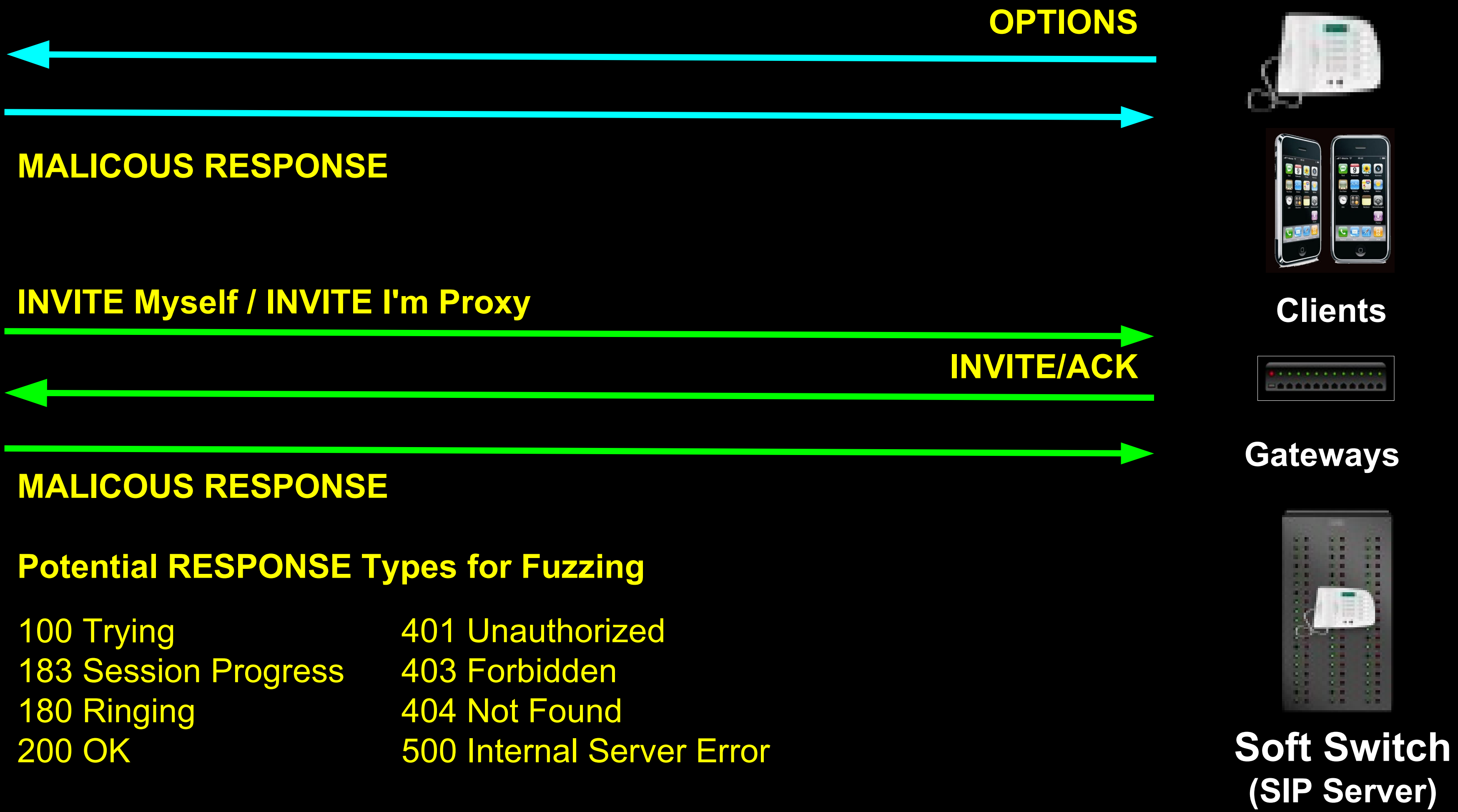
401 Unauthorized
403 Forbidden
404 Not Found
500 Internal Server Error



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 Different Requests (User, Pass, Realm, Nonce)
- Content-Type, Content-Lenth
  - SDP Information Fields
  - ISUP Fields

Fuzzing SIP Services : Response Based



OPTIONS

MALICOUS RESPONSE

INVITE Myself / INVITE I'm Proxy

INVITE/ACK

MALICOUS RESPONSE

Clients

Gateways

Soft Switch
(SIP Server)

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

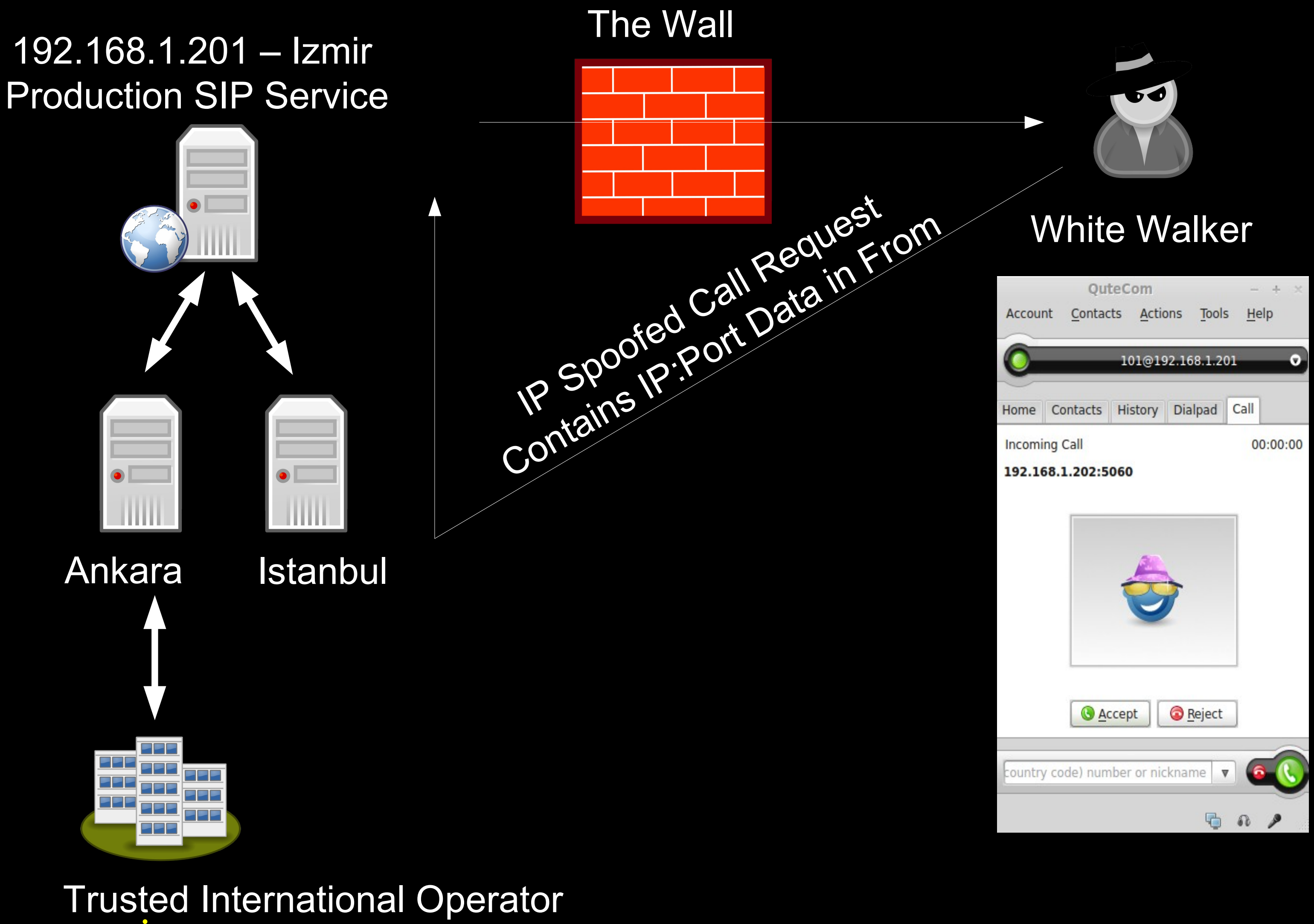
Hacking SIP Trust Relationships

- 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
  - Note The Trusted SIP Gateway When We Have a Call
  - 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

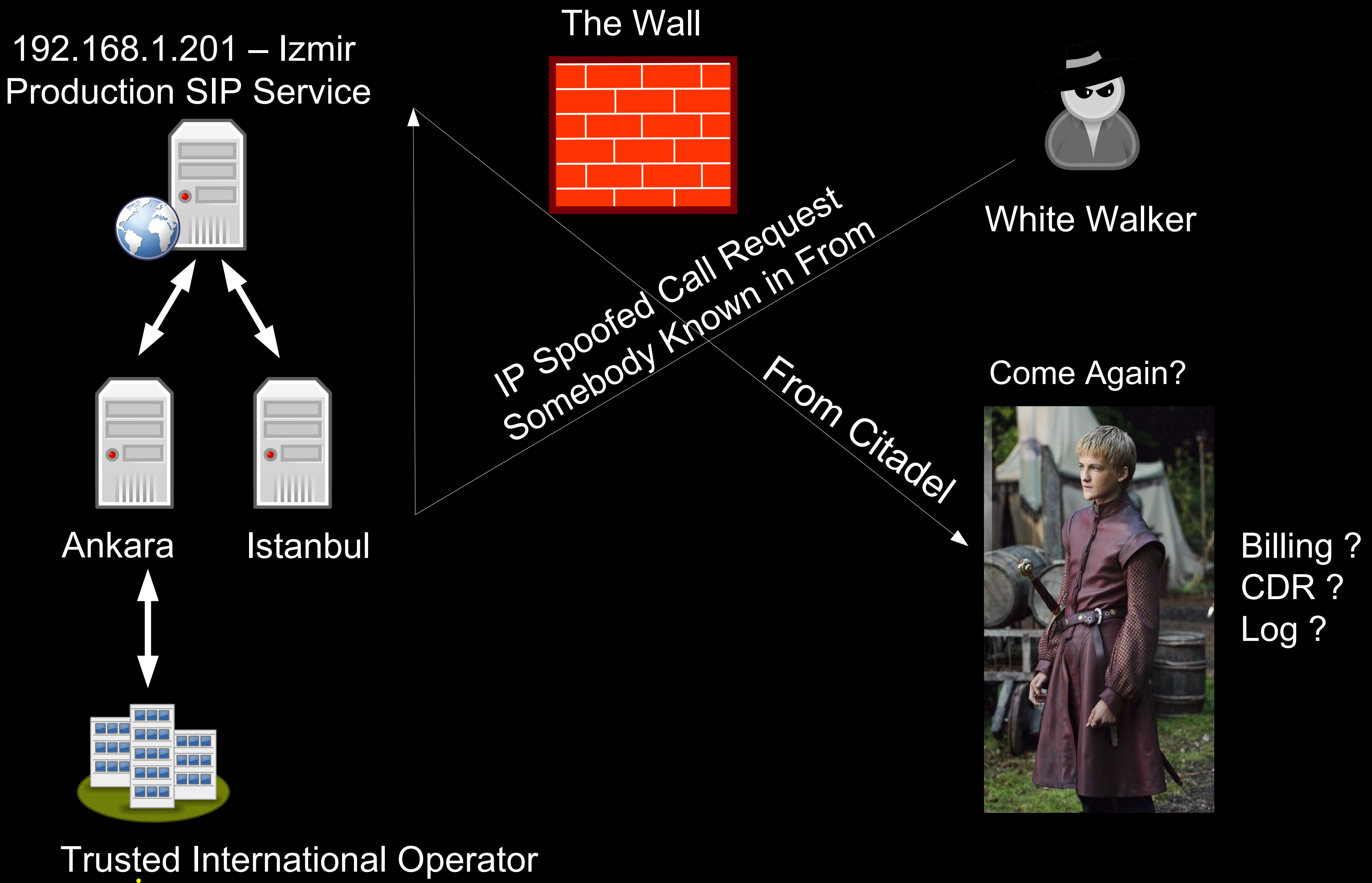
Istanbul

Trusted International Operator

Incoming Call 00:00:00
192.168.1.202:5060

# Hacking SIP Trust Relationships

Brace Yourselves The Call is Coming



The Wall

192.168.1.201 – Izmir
Production SIP Service

White Walker

IP Spoofed Call Request
Somebody Known in From

From Citadel

Come Again?

Ankara

Istanbul

Billing ?
CDR ?
Log ?

Trusted International Operator

References and Further Information

- My Personal Page (viproy.com/fozavci)
  - Hacking Trust Relationships Between SIP Gateways
  - SIP Pen-Testing Kit for Metasploit Framework
  - Pen-Testing Guide for SIP Services in English
  - Pen-Testing Using Metasploit Framework in Turkish (300 Pages)
  - Blog : fozavci.blogspot.com

- SIP Pen-Testing Kit for Metasploit Framework

  http://github.com/fozavci/viproy-voipkit

- Metasploit Project (www.metasploit.com)
- Metasploit Unleashed

  www.offensive-security.com/metasploit-unleashed/Main_Page

DEMO

Attacking SIP Servers Using Viproy SIP Pen-Testing Kit

http://www.youtube.com/watch?v=AbXh_L0-Y5A

Q ?

Thank You