Ravage Unleashed: Tactical VoIP Assault Tool

the grugq <grugq@tacticalvoip.com >

April 9, 2007

Outline

Introduction

Presenter

- the grugq
- VoIP security researcher since 2001
- Director of Tactical VoIP

Presentation

- IP Telephony Security Threats
- Auditting Techniques

Outline

Public Switched Telephone Network (**PSTN**)

- Over a century old
- Acoustic based control system
  - Signaling is *In Band*
- First (known) attacks in the 1950's
- Secured (mostly) circa 2000

VoIP Functionality

What it is Multimedia content exchange over IP network(s)

That means Voice/Video calls over the internet

VoIP Functionality

What it is Multimedia content exchange over IP network(s)

That means Voice/Video calls over the internet

VoIP Benefits

- Significant cost savings
- Added functionality
  - portability
  - content tie-in
- Expanded multimedia capabilities
  - video
  - whiteboards

VoIP Costs

- No such thing as a free lunch
- Quality of service
  - Unreliable
  - Sound quality issues
  - "comfort noise"
- Security problems abound
  - All telephony assets are exposed
    including those on the PSTN

VoIP Costs

- No such thing as a free lunch
- Quality of service
  - Unreliable
  - Sound quality issues
  - "comfort noise"
- Security problems abound
  - All telephony assets are exposed including those on the PSTN

VoIP: Under the hood

- Several protocols providing different functionality
- Core IP Telephony requirements:
  - Signaling Call control
    - Lookup
    - Negotiation
    - Tear down
  - Media Call content
- Competing protocols for signaling

Major Signaling Protocols

H.323

- ASN.1 (binary) PER encoded protocol suite
- Proprietary vendor stacks not interoperable
- Common in Enterprise environments

Session Initiation Protocol SIP

- Bastard son of HTTP & email
- Plain text protocol over UDP
- Common on the internet due to interoperability and ease of development

Outline

The SIP Protocol

- Client-Server model
- Based on HTTP
- Defined in RFC 3261

Architecture Components

Telephone User Agent (UA)

- Hardware
- Software

Proxy Authorizes access to services

- Interface to a local VoIP Network

Registrar URI lookup to IP network address

- maps `bob@biloxi.com` to `bob@pc13.biloxi.com`

Gateways Convert call sessions from one network to another

SIP Message

Command Line `METHOD URI VERSION`

`INVITE bob@biloxi.com SIP/2.0`

Headers `Name : Value[, Value]`

Body `Mime content`

Example INVITE

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP localhost;branch=z9hG4bKaca45b4c3;rport=
To: ‘‘Bob’’ <sip:bob@biloxi.com>
From: siping <sip:siping@localhost>
Call-ID: eb92357c0ca7c60a
Max-Forwards: 70
Contact: siping <sip:siping@localhost>
CSeq: 1 INVITE
```

Outline

Outline

PSTN Phreaking

- Generate correct acoustic tone — issue control commands
- Hardware based phreaking
  - Blue Box 2600Hz to access trunk line
    - Captain Crunch
    - Steve Jobs & Steve Wozniak
  - Red Box imitate coins in a pay phone

Death of Phreaking

- Aggressive prosecution of caught phreakers
- Non technical fraud detection
- Command & Control system was moved to digital
  - *Out of Band*
  - Can't access it — Can't control it
- Process started in the 90's, mostly completed by 2000
  - Few hold outs across the world

Outline

Summary

Telephony . . .

- **Service** Access to services, e.g. PSTN, Voice Mail, etc.
- **Session** Phone call in progress
- **Identity** Phone number

Target: Telephony Services

Access to services

Toll Fraud free telephony services

- Long Distance (very important historically)
- PSTN access (land lines & mobile phones)

Revenue Generation toll fraud can be lucrative

- Resell stolen access/minutes
- Premium rate numbers
  - 900 numbers
  - SMS
- Toll mismatch:
  - Luxembourg example
    - Termination cost 2 euro
    - Origination charge 9 cents

Target: Telephone Session

Phone call in progress

Monitor

- Eavesdrop on call session content

Modify

- Inject new content
- Suppress existing content

Deny

- Tear down a session
- Degrade session quality

Hijack

- Combination modification/denial
- Malicious redirection

Target: Telephony Identity

Phone number

Impersonate

- Spoof out going call identification

Hijack

- Capture incoming calls

Deny

- Null route/re-route calls

Outline

Target: Service

Service Gain access to PSTN/VoIP network

- Toll Fraud
- Resell access to generate revenue

Architecture Targets

- Proxies
- Gateways

Session

Signaling manipulation of an existing sessions is limited to redirecting session members

Session Redirect in session content via malicious signals

- Man in the Middle
- Inject spurious messages

Architecture Targets

- Proxies
- User Agents

Identity

- Falsify outbound identity
  - Modify SIP "From" header
- Subvert URI lookups
  - Remove association = Denial of Service
  - Modify association = Hijack

Outline

Overview

The TacVTK provides:

Core Tools Specific assessment tasks

Framework Easy extention for custom audit requirements

- Addresses lack of definitive VoIP auditting tools
- First development in 2004
  - Under sporadic development ever since
- Developed in python
- Available at: `http://www.tacticalvoip.com/tools.html`

Outline

VoIPy: heart of the TacVTK

- Python module implementing core VoIP protocols
- Currently supports only SIP
- Enables rapid development of custom attack tools

Example VoIPy code

Send an INVITE

```
from voipy import sip
to_uri = ’‘‘Bob’’ <sip:bob@biloxi.com>’
from_uri = ’‘‘Alice’’ <sip:alice@atlanta.com>’

msg = sip.request.Invite(to=to_uri, from=from_uri, contact=from_

sock.sendto(str(msg), (’biloxi.com’, 5060))
```

Outline

Ravage: Registrar Assault Tool

- Core tool for auditting SIP registars
- SIP registrars are critical components for secure SIP networks
- Ravage provides several attack modes

Ravage: Attack Modes

Enum enumerate usernames on a Registrar

- `OPTIONS`
- `INVITE`
- `REGISTER`

Bruteforce guess user/pass combos for a Registrar

- `REGISTER`
- `INVITE`

Ravage: Subversion Attack Modes

Inject	insert a binding into a registrar
Remove	delete a binding from a registrar
Hijack	take over a binding in a registrar

Ravage **texttttENUM**

Enumerate usernames within a SIP environment

Techniques:

INVITE

- If response is not `404 Not Found` user exists

OPTIONS

- Identical to `INVITE`
- Less noisy, since `OPTIONS` doesn't initiate a call session

REGISTER

- If response is `401 Unauthorised` user exists

Ravage **texttttBRUTE**

Try username/password combinations to gain access
Techniques:

REGISTER

- Target a Registrar
- Attempt to insert/remove a binding

INVITE

- Target an authorising proxy
- Attempt to initiate a call session

Ravage Modification

Alter the bindings of within a SIP Registrar

Techniques:

Remove

- `REGISTER` with an `Expires` set to 0

Insert

- `REGISTER` with a new `Contact` URI

Hijack

- `REGISTER` with an `Expires` set to 0
- `REGISTER` with a new `Contact` URI

Toll Fraud for Dummies

- Enumerate accounts in a SIP environment
  - `$ ravage enum ...`
- Gain access to an account
  - `$ ravage brute ...`
- Create a trunk using the account
  - `asterisk`
- Sell access to the illicit trunk
- Profit!

Phishing Accelerator

- Directed attack against a financial institution
- Potential telephony infrastructure targets:
  - Call center logins
  - Telecos providing VoIP services
- Redirect incoming phone calls to VoIP harvester
- Victim calls phone banking hotline
  - *"Hallo. Welcome your bank. Please be entering pin number. Thanking you."*

Outline

siping

- Craft custom SIP messages on the command line
- Provides limited UA logic
- Useful for poking servers
- Capable of creating arbitrary SIP message content

siping example

Example INVITE

```
grugq@zer0gee:~/siping$ siping.py -v -mI sip:bob@biloxi.com
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP localhost;branch=z9hG4bKac2ba31c6;rport=
To:  <sip:bob@biloxi.com>
From: siping <sip:siping@localhost>
Call-ID: d42e27136a5dd71c
Max-Forwards: 70
Contact: siping <sip:siping@localhost>
CSeq: 1 INVITE
```

Outline

VoIP Security more Critical

- VoIP continues to gain traction
- VoIP security is still primitive
- TacVTK provides new capabilities to auditors
  - ravage: SIP registrar security analysis
  - siping: SIP signaling injection tool
  - VoIPy: flexible VoIP development framework
- VoIP makes phone calls as secure as email