VoIPhreaking

How to make free phone calls and influence people

by

the grugq

Agenda

- Introduction
- VoIP Overview
- Security
- Conclusion

Voice over IP (VoIP)

Good News

- Cheap phone calls
- Explosive growth in recent years
- Internet telephony converging with the PSTN

Other News

- Immature security best practises
- Free, anonymous, phone calls

VoIP Overview

Agenda

- Infrastructure
- Protocols
- Signalling protocols
- Media protocols
- PSTN integration protocols

How VoIP Works

- Mimics traditional POTS service
- Multiple interconnecting protocols
  - Protocol realms of responsibility
    - Signalling
    - Media
    - PSTN integration
- An example, in detail...

How VoIP Works, cont.

- Alice “dials” Bob
  - Signalling Protocols:
    - Location
      - “Alice is @ aaa.bbb.ccc.ddd”
      - “Where is Bob?”
    - Presence
      - “Is Bob available?”
  - Media Protocols
    - Codec
    - Stream location

How VoIP Works

- Bob picks up the phone
  - Signalling protocols
    - Location
      - “Bob is at aaa.bbb.ccc.ddd”
    - Presence
      - “Bob is available” (he picked up the phone, duh)
  - Media Protocols
    - Codec
      - Negotiated shared codec capabilities
    - Stream location

More 'how it works'

- Bob hangs up
  - Signalling
    - Terminate the call
  - Media
    - Stop receiving the stream

Infrastructure

Components which implement VoIP

Infra. Short list

- VoIP Phones
  - Software
  - Hardware
- Internet technology
  - Routers
  - DNS
- PSTN integration technology
  - Media Gateway
  - Signalling Gateway

VoIP Protocols

Signalling & Media

Protocols

- Separation of signalling and media
- Several competing standards
  - Signalling
    - SIP vs. H.323
  - PSTN integration
    - MGCP vs. Megaco
- Proprietary protocols as well
  - Skype
    - Recently cracked by a Chinese company.

Signalling Protocols

H.323

- Early VoIP protocol set
- ASN.1 PER encoded protocol
  - Convoluted, complex, broken implementations
- No two H.323stacks seamlessly interoperate
- Open Source stacks are... not ideal
- No public attack tools to speak of

SIP

- Session Initiation Protocol
  - RFC 3261
- Based on HTTP
  - Error codes will look familiar
    - `200 OK`, `404 Not Found`, `403 Forbidden`, etc.
  - Plain text protocol
- Usually transported via UDP
  - Can use TCP and TLS as well

SIP, cont.

- Complex state engine for call handling
- Multiple open source SIP stacks
  - Most are poor for attack tool development

SIP Spec

- SIP packet comprised of command line and header fields
- Command line made:
  - Method and URI or,
  - Response code and response
- Header fields are ':' name value pairs
  - Value component can be a list with each element possessing parameters

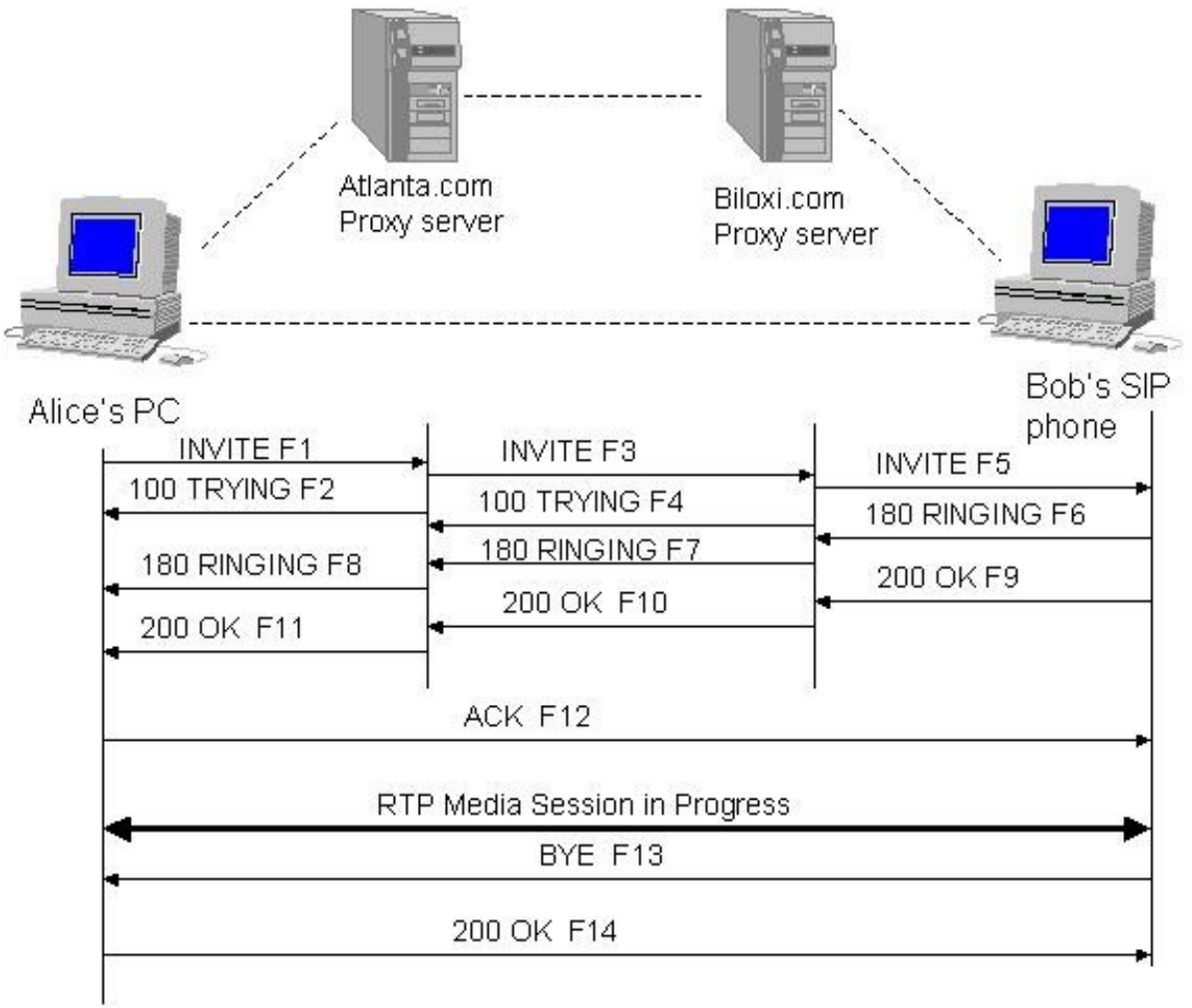
SIP Packet Example

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
```

Interesting SIP Methods

- `INVITE`
  - Set up a call session
- `REGISTER`
  - Update a registrar binding
- `BYE`
  - Terminate a call session
- `OPTIONS`
  - Query a SIP device for supported operations

SIP Call Setup



SDP

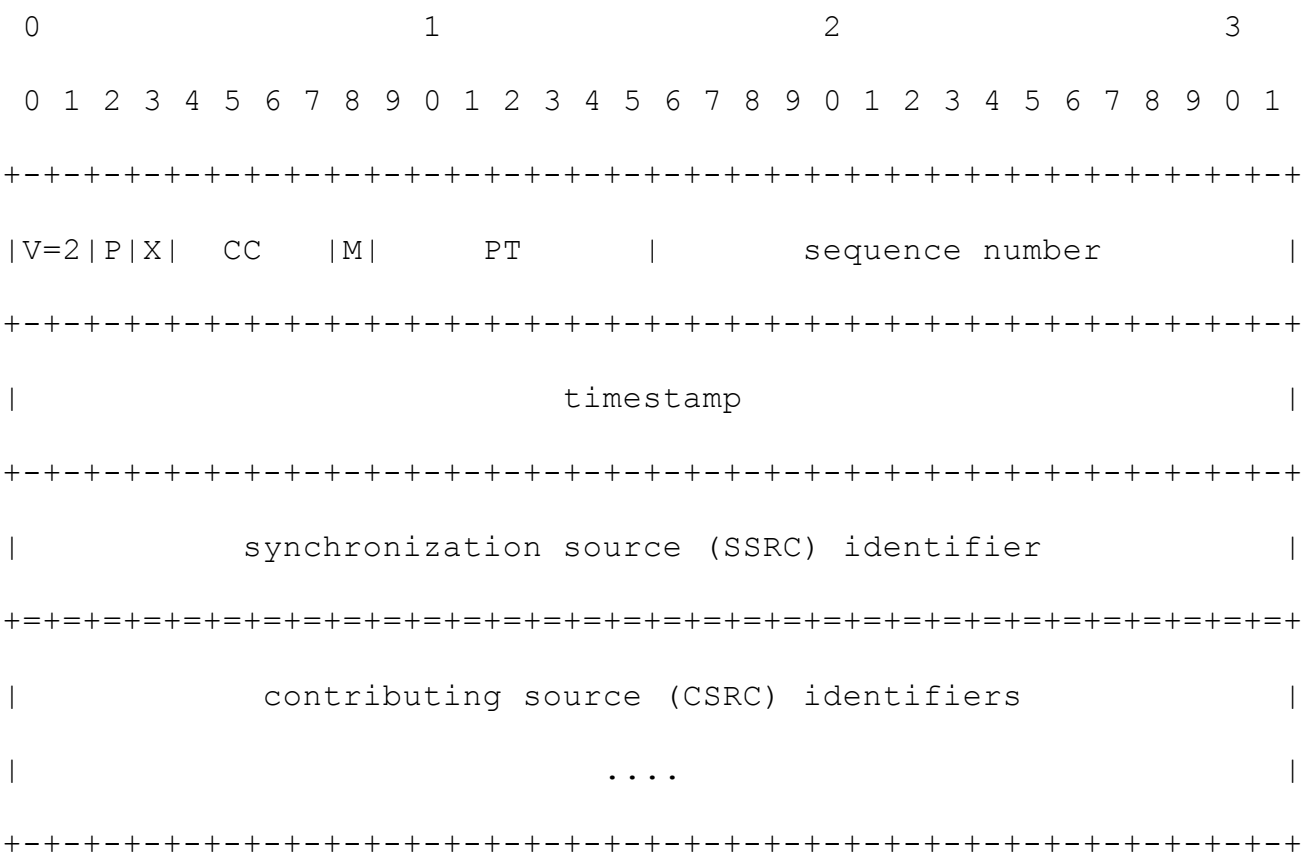
- Session Description Protocol
  - RFC 2371 – Obsolete
  - RFC 3262
- Plain text protocol
- Defines media stream parameters
  - Codec
  - Protocol
  - IP address and port (range)

Media Protocols

RTP

- Real Time Protocol
  - RFC 1889 – Obsolete
  - RFC 3550
- Supports multiple codecs for audio, video
- Layered on top of UDP
  - For speed
- Uses ID numbers for syncronisation
  - Not robust as security measure

RTP Packet


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
|V=2|P|X| CC |M| PT | sequence number |
| timestamp |
| synchronization source (SSRC) identifier |
| contributing source (CSRC) identifiers |
| .... |

VoIP Infrastructure

SIP Entities

- User Agent
  - Softphone
  - Hardware phone
  - Program
- Proxy
  - Provides single entry/exit point for local VoIP network
  - Often treated as VoIP firewall
  - Can provide NAT functionality

SIP Entities, cont.

- Registrar
  - Maps SIP URIs to IP addresses
    - These are called “bindings”
  - Allows SIP UAs to roam
    - Enabled via frequent bindings updates
  - Should require authentication to update bindings

Gateway Devices

- Gateway devices convert between IP encapsulated data and PSTN data
- Media Gateway
  - Converts RTP and PSTN voice traffic
- Signalling Gateway
  - Converts SIGTRAN/SCTP to SS7

VoIP Security

Nature of vulnerabilities

- Generic software problems
  - Memory corruption bugs
    - Buffer overflows, format strings, int wraps
  - Race conditions
- Application specific problems
  - Web App
    - SQL injection, LDAP injection
  - VoIP infrastructure
    - Telephony attacks

VoIP Concerns

- VoIP end users
  - Quality of Service (QoS)
  - Privacy
  - Authentication
- VoIP service providers
  - Billing
  - Quality of Service

Internet Telephony Attacks

Historic telephony attacks

- Signalling and media over same line
  - In band
- Original phreaks exploited access to signalling band
  - Blueboxing
- Eradicated with separation of signalling and media
  - Out of band

Attacks against VoIP users

- Session Hijacking
  - RTP Hijacking
  - SIP redirection hijacking
    - Re-`INVITE`
- Spam over Internet Telephony (SPIT)
  - SIP '`Alert-Info`' header
  - Not entirely sure of the economics of SPIT

Against VoIP users, cont.

- Media stream injection
  - Various private tools exist
- Media stream monitoring
  - RTP stream sniffing
  - SIP redirection
  - SIP 3rd party injection
- Denial of service

Attacking VoIP service providers

- Billing attacks
  - Mis-charged calls
    - Various SIP attacks involving spoofing
  - Free phone calls
    - MGCP attacks
    - SIP attacks
- Hijack equipment
  - Usually very insecure “embedded” devices

SIP spoofing

- SIP packets provide two core identifier URIs
  - From
  - Contact
- Mismatches between the two can exploit poorly developed software

SIP spoofing example

MGCP Attacks

- MGCP spec on “security considerations”:

  Security is not provided as an integral part of MGCP. Instead MGCP assumes the existence of a lower layer providing the actual security.

MGCP Attacks -- Techniques

- Hijacking active calls
  - MDCX – modify connection
- Creating new (free) calls
  - CRCX – create connection
- Denial of service attacks
  - DLCX – delete connection

MGCP Attacks Example

Attacks using VoIP service providers

- Caller-ID spoofing
  - Impersonate phone numbers
    - Voicemail
    - Credit card authorisation
    - Etc. etc. etc.
- Full ANI spoofing
  - Anonymous phone calls
  - Mis-billed phone calls
  - Scams involving 'pay by phone' services

Abusing nufone.net

- Allows caller ID spoofing by default

```
SetCallerID (<Insert a valid 10
  digit US48 caller ID>)
```

- Combined with a misconfigured VoIP calling card – Full ANI spoofing
  - Empty portions of the ANI are filled in from the Caller ID information
- FBI currently investigating nufone.net

Phone Attack Conc.

- Multiple VoIP attack usages
  - Against VoIP end-users
  - Against VoIP service providers
  - Using VoIP service providers
- VoIP attacks enable additional criminal activities

Conclusion

- Existing security solutions are immature
- Convergence of (trusted) PSTN and (untrusted) IP networks happening rapidly
- Brave new world of VoIPhreaking is emerging

Q & A

- I can't hear any of you, and I don't speak Mandarin. Please submit all questions in writing to:

  /dev/null

Cash for 0day exploits

thegrugq@gmail.com