VoIP Security Issues

Hendrik Scholz
<hscholz@raisdorf.net>
http://www.wormulon.net/

Agenda

- VoIP Overview
- Security Threads
- Locating Devices
- Fingerprinting Devices
- Specific Attacks
- SBCs – Cure or Curse?
- Conclusions

VoIP Overview

VoIP for Managers

- VoIP equals
  - cheap: run PSTN on Internet infrastructure
  - ISDN features + more
- in production use today
- Google/Skype cannot be wrong
  - explosive growth
  - huge market for hardware

The Dark Side

- PSTN converges with the Internet
  - more old hardware to take care of
- PSTN features need to be implemented
  - fundamental differences

clever network + dump terminals

goes

dumb network + clever applications

SIP Standards - Feel Lost?

1847, 2045, 2046, 2047, 2048, 2198, 2327, 2543, 26**16**, 2617, 2633, 2733, 2791, 2833, 2848, 2959, 2976, 3087, 3050, 32**04**, 3219, 3261, 3262, 3263, 3264, 3265, 3266, 3310, 3311, 3312, 3313, 3319, 3320, 3321, 3322, 33**23**, 3324, 3325, 3326, 3327, 3329, 3361, 3351, 3372, 3388, 3389, 3398, 3407, 3420, 3428, 3455, 3468, 3485, 35**15**, 3550, 3551, 3555, 3556, 3605, 3606, 3608, 3611, 3702, 3711, 3725, 3764, 3824, 3840, 38**42**, 3856, 3857, 3890, 3891, 3903, 3911, 3959, 3960, 3968, 3969, 3976, 4028, 4077, 4**08**3, 4091, 4092, 4117, 4123, 4145, 4168, 4189, 4235, 4240, 4244, 4245, 4317, 4320, 4321, 4353, 4354, 4411, 4412

http://www.packetizer.com/voip/sip/standards.html

- 'some' additional drafts
- new RFCs/drafts on a weekly basis

Session Initiation Protocol

- Requests
  - i.e. INVITE, REGISTER, CANCEL
- Responses
  - i.e 200 OK, 403 Forbidden, 404 Not Found
- lots of additions
  - Caller ID (Remote Party ID, RFC 3323, RFC 3325)
  - supplementary services (HOLD, MCID, CCBS)
- complex state engine

Security Threads

Security Threats

- Interception & Modification
  - RTP/media attacks
  - re-routing
- Eavesdropping
  - call pattern tracking
  - number harvesting
  - communication reconstruction

Security Threats (cont)

- Social Threads
  - Theft of Services
  - Unwanted Contact (SPIT)
  - Identity Theft
- Denial of Service
  - Flooding
  - Malformed Services
- Combinations
  - Spoofed identity + RTP replay

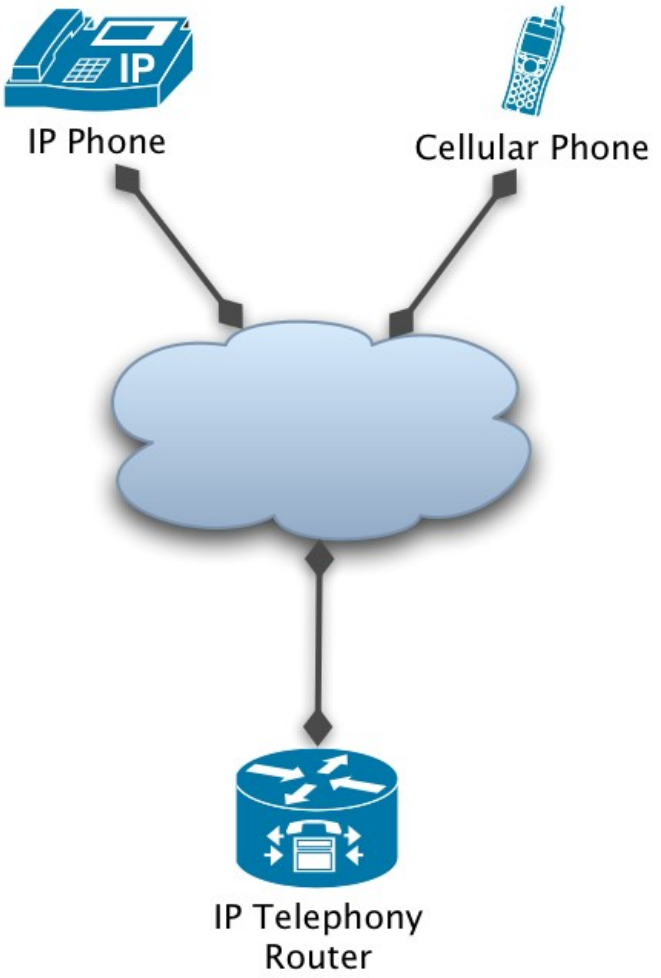
Attack Vectors

- Singalling
- End Devices
- Protocol Independent Attacks
- Implementation specific issues
- Configuration Bugs
- Session Border Controllers
- SIP Neigborhood: Billing, PSTN, MGWC

SIP Signalling

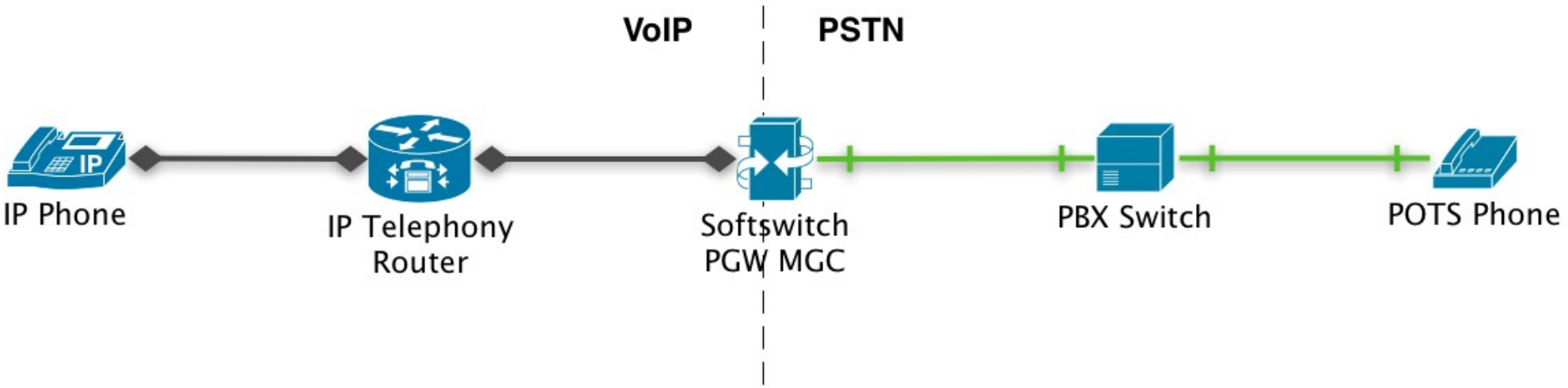
Singalling: Call Forking

- Call Forking
  - parallel/serial forking
  - wanted behaviour
- possible problems
  - traffic amplification
  - resource starvation (if statefu



User	Contact
adam	adam@10.1.1.1:5060;tag=value
john	john@172.30.1.1:5060;opaque=123
john	john@192.168.1.1:18123;foo=bar

Signalling: Call Forwarding



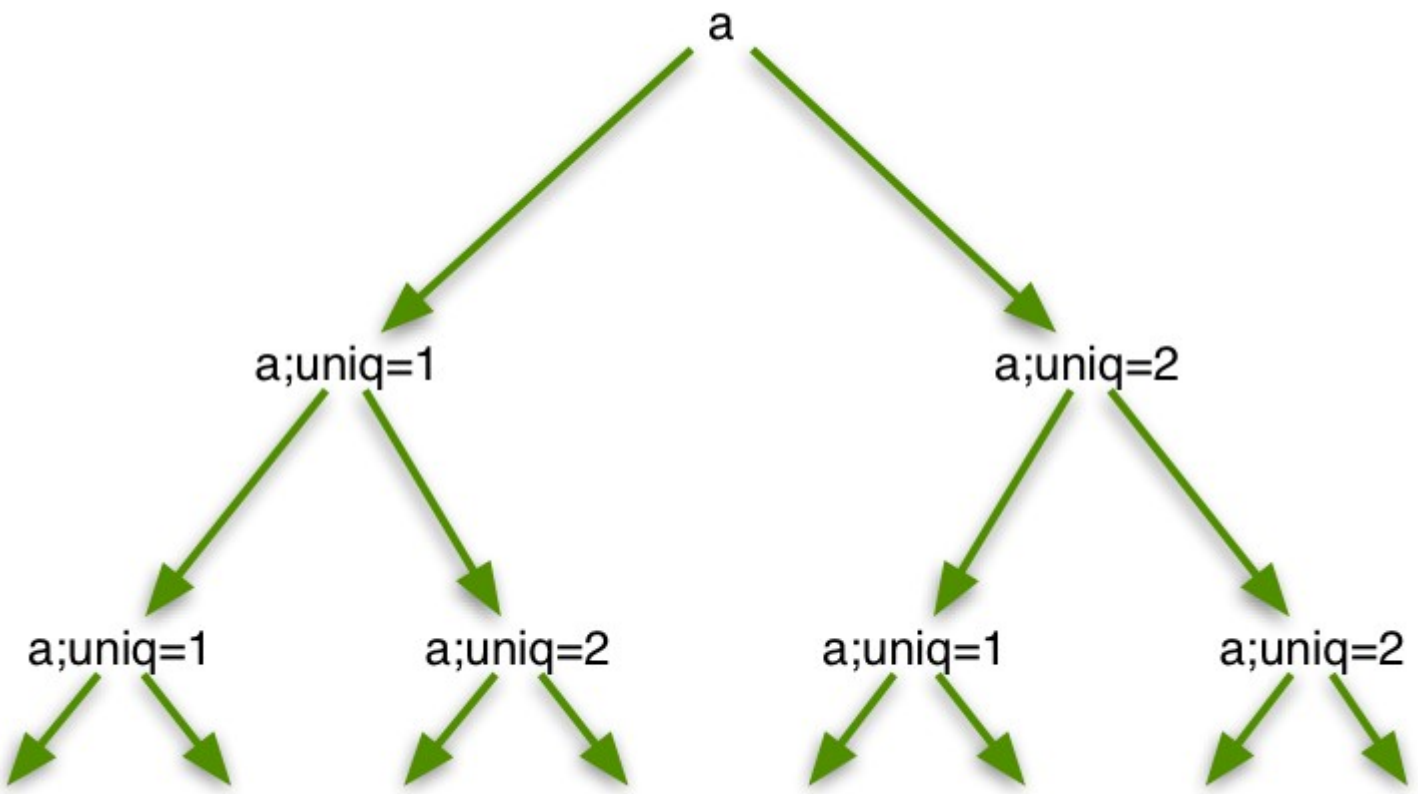
- Time To Live:
  - SIP: Max-Forwards (counts down)
  - SS7/ISUP: Redirect counter (counts up)
- Loops? they do happen

Fork Loop: Ingredients

- parallel call forking
  - two contacts for one user
- add the loop
  - strip IP from contact and add local domain
  - add tag to keep contact fields different

User	**Contact**
a	a@wormulon.net;uniq=1
a	a@wormulon.net;uniq=2

Fork loop: Tree



source: draft-ietf-sip-fork-loop-00

Fork loop: Preparation

- REGISTER users
  - http://sipp.sf.net/
  - http://sipsak.org/
- single call to user A
  - use your phone ;)
- wait for 2^70 INVITEs to be processed
  - 1180591620717411303424 INVITEs
  - 408 timeout will be triggered -> attack torn down

Fork loop: Improvements

- TCP contact
  - SYN flood a random website
- PSTN contact
  - forward to cell phone
  - cell phone forwards back to SIP proxy
  - results in new calls, fresh timeout, full TTL (Max-Forwards)
- Announcement contact
  - announcement starts playing immediately
  - redirect RTP/media to victim using SDP

End User Devices

End User Devices

- routers/modems/PBXs/ATAs
  - Operating System
  - Unpatched
  - No logging/notification
  - Web interface
  - ISP-wide monocultures

End User Devices: Attacks

- unprotected
- little CPU power, limited number of lines
  - resource starvation
- no inbound Authentication
  - needed for ENUM, P2P SIP et al.
  - SPIT
- remote management
  - reboot, config change, **call control, click to dial**

End User Devices: Goals

- Locating devices
  - IP address
  - phone numbers
  - Contact headers
- Fingerprinting devices
  - type of device (proxy, end user devices)
  - brand, version
  - firmware

Locating Devices

- smap
  - mashup of sipsak and nmap
  - http://www.wormulon.net/files/pub/smap-syscan.tar.gz
  - utilizes various SIP requests
  - banner grabbing
  - active fingerprinting (currently 35 fingerprints)
- scan DSL 'dial up' ranges
- 60-70% hit ratio based on ISP

Locating Devices: smap ouput

```
$ smap 89.53.17.16/29

smap 0.3.4 <hscholz@raisdorf.net> http://www.wormulon.net/

Host 89.53.17.16:5060: (ICMP untested) SIP enabled
Host 89.53.17.17:5060: (ICMP untested) SIP enabled
Host 89.53.17.18:5060: (ICMP untested) SIP enabled
Host 89.53.17.19:5060: (ICMP untested) SIP timeout
Host 89.53.17.20:5060: (ICMP untested) SIP timeout
Host 89.53.17.21:5060: (ICMP untested) SIP enabled
Host 89.53.17.22:5060: (ICMP untested) SIP enabled
Host 89.53.17.23:5060: (ICMP untested) SIP timeout

8 hosts scanned, 0 up, 5 SIP enabled
$
```

Whitehat Rationale

- Tracking down interworking issues
- Identification of malicious devices
- Prevention/detection of attacks
  - drop INVITEs of non-interoperable devices
  - lower impact of faulty clients
- SPIT bots will be small, not feature-blown

Blackhat Rationale

- Identify and locate specific devices
- Identify exploitworthy boxes
  - 4 T1 lines vs. 2 analogue lines
- Disguise program as being legit
  - honeypot nmap feature

Fingerprinting devices

```
...
Host 194.97.1.66:5060: (ICMP untested) SIP enabled
device identified as:
  Asterisk PBX 1.2.7

FINGERPRINT information:
newmethod=501
allow_class=201
supported_class=NR
hoe_class=2
options=200
brokenfromto=404
prack=501
invite=100
headers found:
  User-Agent: Asterisk PBX


1 hosts scanned, 0 up, 1 SIP enabled
$
```

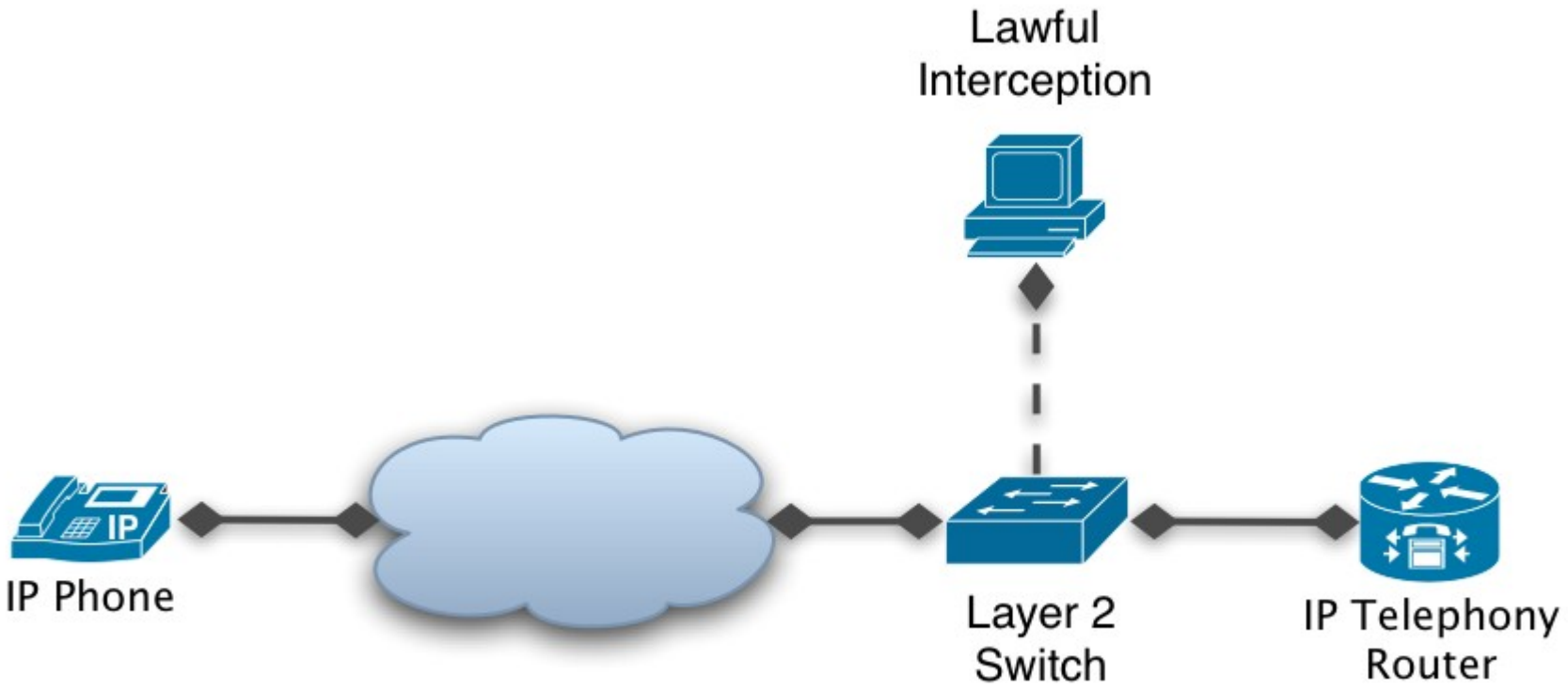
Protocol Independent Attacks

Timing Attacks

- exploit UDP defragmentation timer
- evade billing & Lawful Interception
- inspired by Van Hauser's IPv6 talk at 22C3

- goal: fool passive Lawful Interception

Timing Attack: LI Setup



Timing Attack: LI Box

- receives mirrored traffic
- use libnids defragmentation in userland
- parse SIP messages (i.e. using libosip)
- check username/phone # against DB
- copy message to LEA if needed

Timing Attack: Timers

- two different IP stacks
  - different implementation
  - different configuration
- LI Box might drop fragments too early
- … or too late
- goal: prevent a messages from being de-fragmented on LI system

LI timer < LIVE timer

- inject 1st fragment
  - LI stores fragment
  - LIVE stores fragment
- wait for fragment to expire on LI system
- inject 2nd fragment
  - LIVE de-fragments successfully
  - LI system stores second fragment

LI timer > LIVE timer

- inject 1st fragment: fill both buffers
- wait for LIVE system to drop fragment
- inject 2nd fragment
  - LI box de-fragments successfully
  - LIVE stores fragment
- inject 3rd fragment
  - LI box stores fragment
  - LIVE de-fragments and initiates call

SIP Implementation-specific Bug

RFC 3261 Implementation

- RFC 3261 To/From 'Displayname'
- Displayname considered a comment
- libosip bails out on comma in Displayname
- osip_message_parse() fails

- add comma in Displayname and break LI system previously described

SIP Implementation Differences

Implementation: Caller-ID

- Different implementations
  - From displayname or URI
  - Remote-Party-ID
  - P-Preferred-Identity/P-Asserted-Identity
  - ISP proprietary extensions, i.e. SetCallerID:
- Threads
  - Caller-ID used for Authentication
  - Misrepresentation

Implementation: Caller-ID

- spoof Caller-ID using different implementation
- set to cell phone number, call voice mail

INVITE sip:0049311@123.org
From: "foo" <0049199123@123.org>
Remote-Party-ID: <sip:**001800999**@123.org>
P-Asserted-Identity: <sip:**001800999**@123.org>
Authorization: ... username="foo" ...

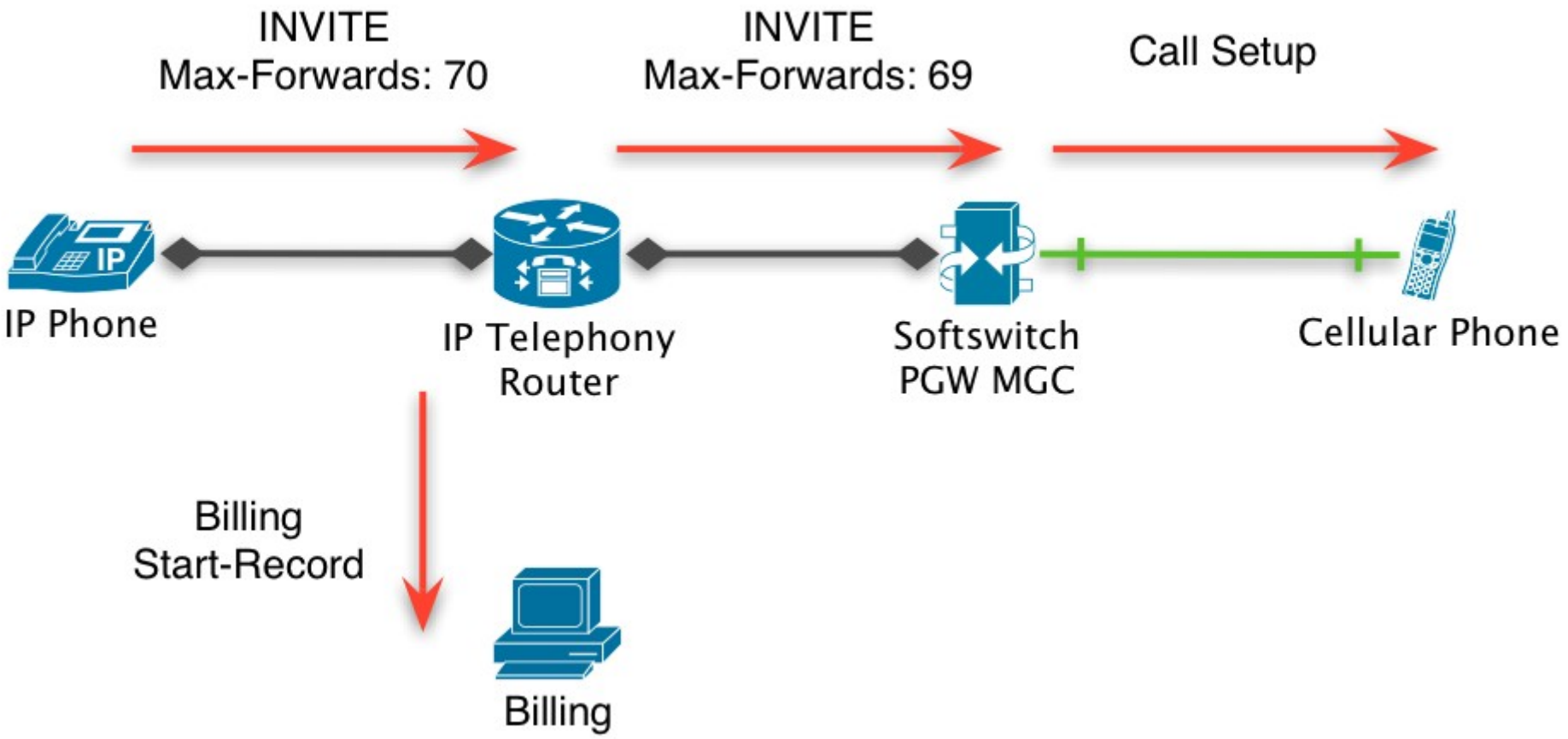
INVITE sip:0049311@123.org
From: "foo" <0049199123@123.org>
Remote-Party-ID: <sip:**0049199123**@123.org>
P-Asserted-Identity: <sip:**001800999**@123.org>

Configuration Bugs

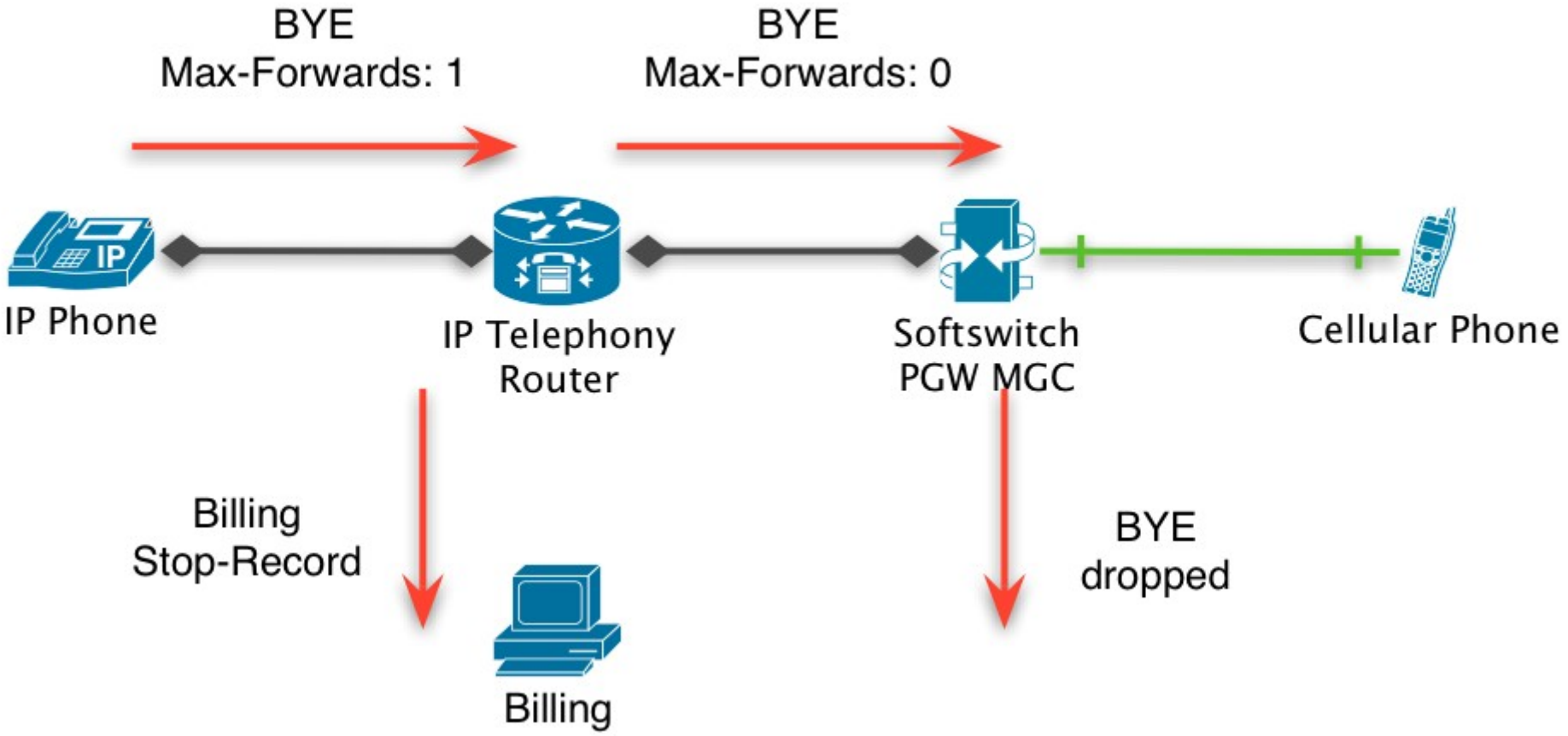
Configuration Bugs

- abuse of (misconfigured) SIP features
- examples
  - mimic Call-Forwarding to prevent correct billing
    - REFER
    - Diversion header
  - Route headers
    - bypass authentication
  - prematurely discard messages
    - Max-Forwards header

Max-Forwards: cheap calls

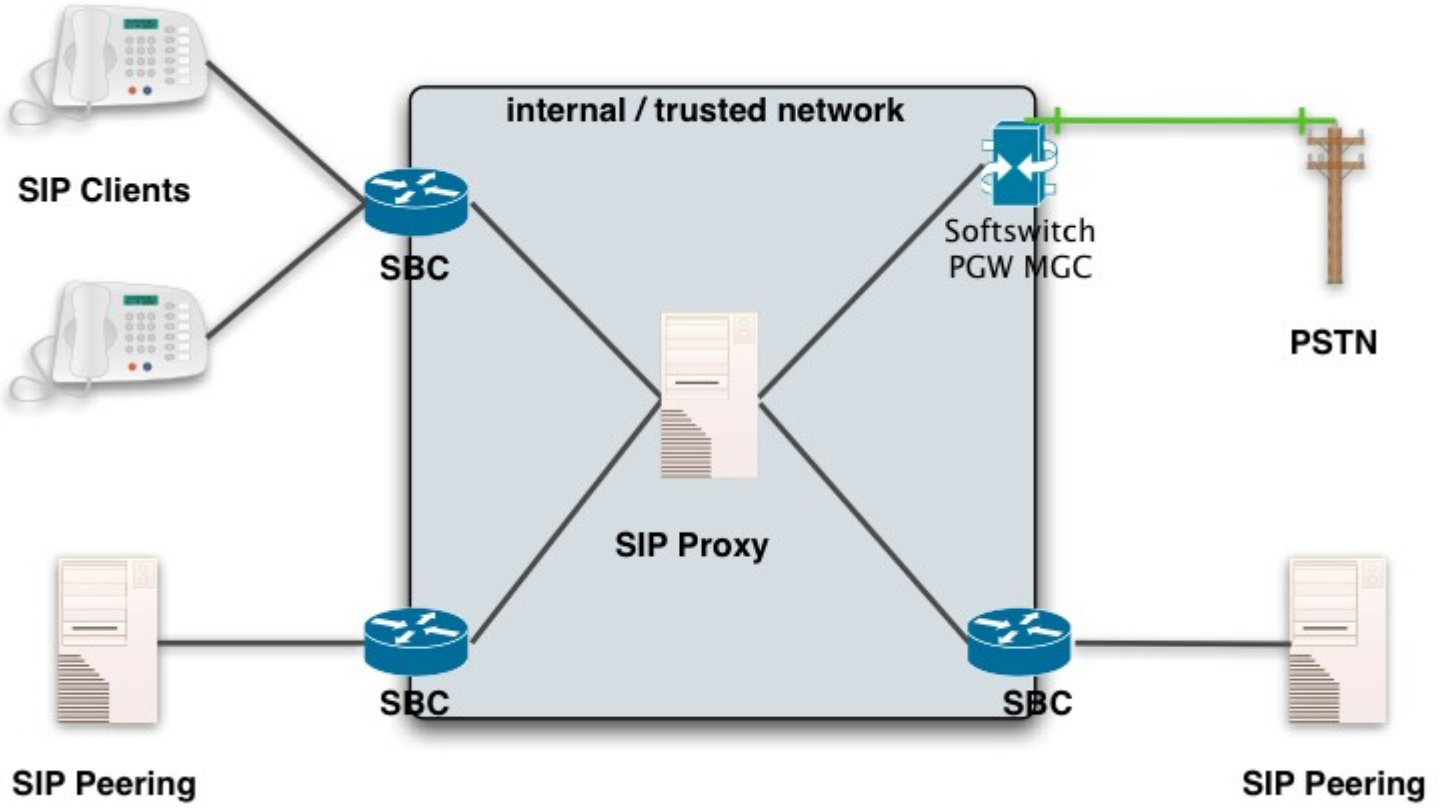


Max-Forwards: cheap calls



Session Border Controllers

Session Border Controllers



Protection of internal/trusted network

SBC: Functionality

- Inside Singalling and Media streams
  - fix NAT issues
- Single Point of Contact
  - Peering Partners
  - User Agents
- SBCs are commercial products
  - $$$
  - Tech Support, anyone?

SBC: Cure?

- Fix NAT issues
  - always on non-RFC1918 address
- Simplicity
  - Single Point of Contact for Peering
- (D)DOS-Attack mitigation
- Filter superfluous messages
  - i.e. REGISTER every 30 seconds
- Filter broken/unsupported messages
  - lessen load on call control proxies

SBC: Curse?

- Quality of Service
  - added latency for SIP + RTP
- Single Point of Failure
  - Availability
  - Scalability
- SBC vs. new standards/extensions
  - MWI, Messaging
  - broken clients
  - innovation blocked by SBC

Newport SBC Via header

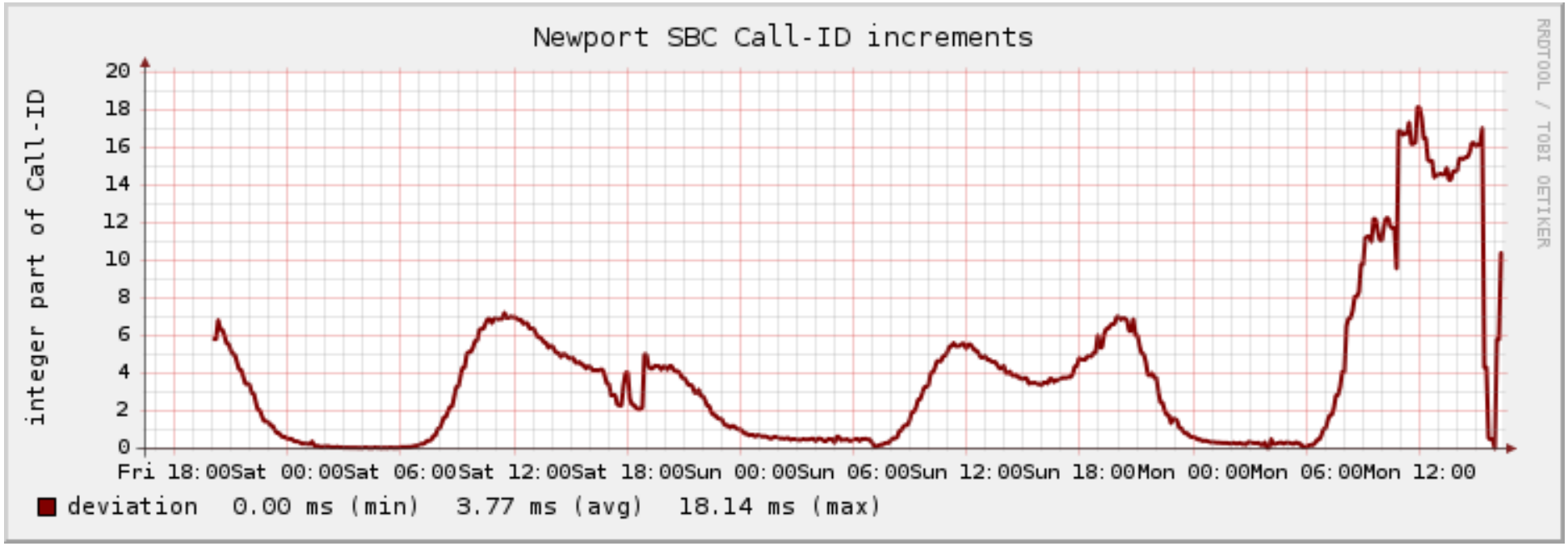
- branch leaks information

```
Via: SIP/2.0/UDP 10.1.1.66:5060;branch=z9hG4bKterm-1845fb0-
  49310995520-49310995108.
Via: SIP/2.0/UDP 10.1.1.66:5060;branch=z9hG4bKterm-1845fb1-
  493142973448-4931422104.
```

- contains A + B party number
  - even when CLIR set
- incrementing counter
  - calls per second

Newport SBC: calls per second

- obtain calls per second
  - even if INVITEs are not visible
  - OPTIONS sent by SBC itself(!)

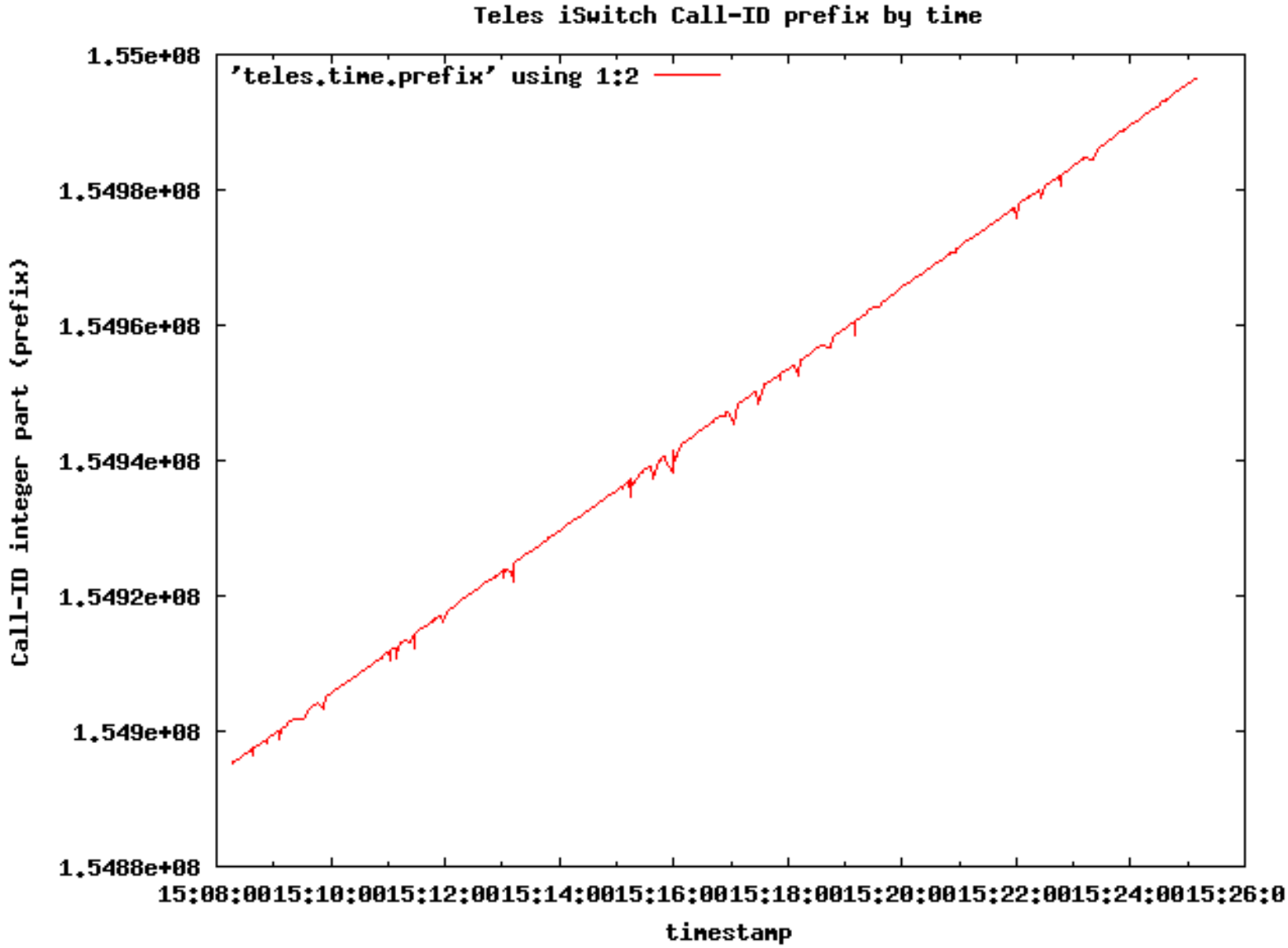


Teles iSwitch

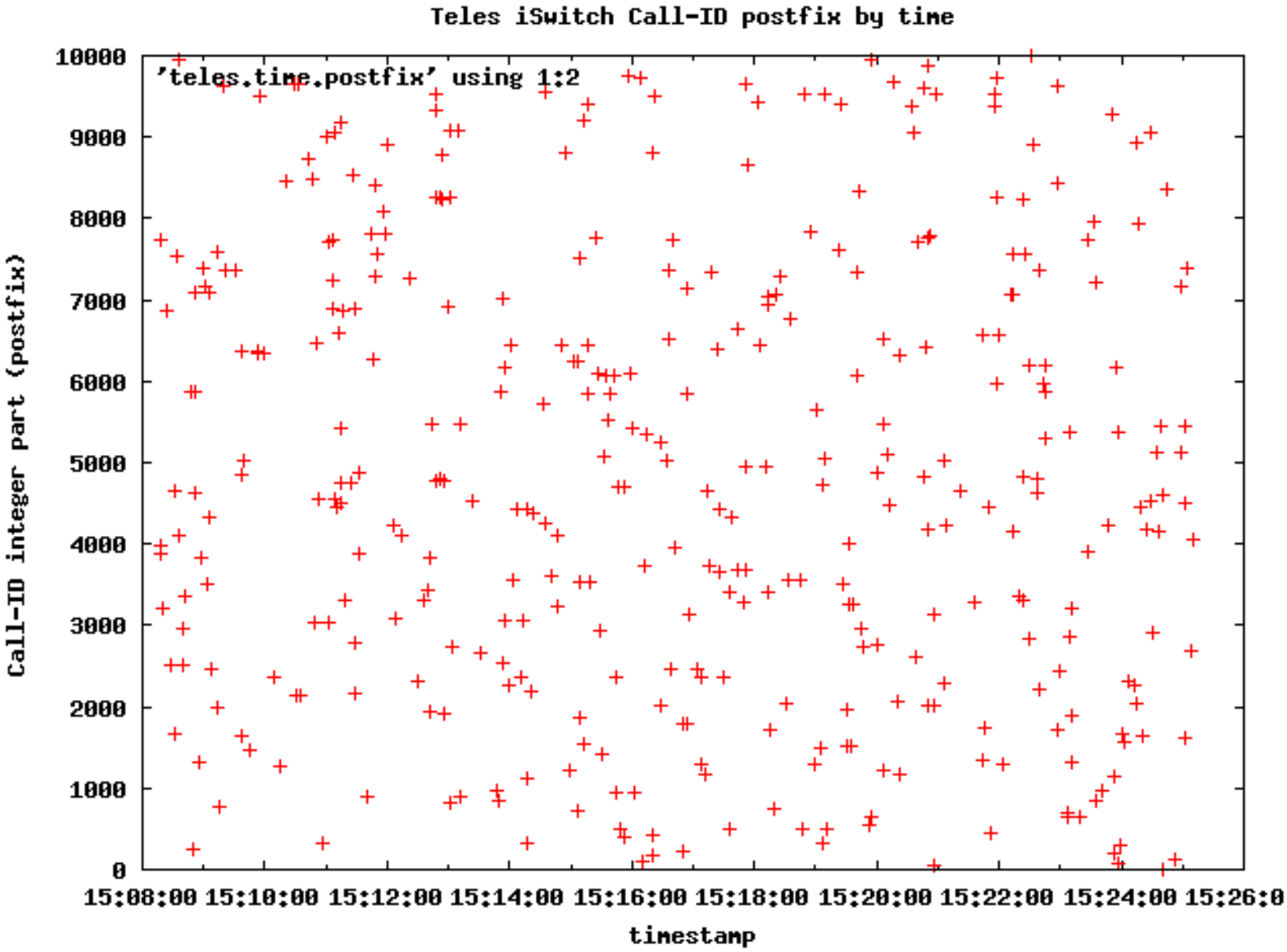
- Call-ID contains MAC-Address
  - identification of physical hardware
  - randomness limited to a few bytes
- Call-ID prefix is recycled in
  - branch
  - To/From tag

008082384A39**093B8B14**000**26E4**@10.1.1.1

Teles iSwitch: Call-ID Prefix



Teles iSwitch: Call-ID Postfix



Conclusions

Conclusions

- VoIP Security is a challenge
  - new hardware (and old PSTN cruft)
  - new RFCs (ISDN supplementary services)
  - regional laws
- Research to be done
  - SIP Fingerprinting
  - Stack Interworking
  - PRNG analysis (Blackhat in two weeks)
  - SPIT will come (2-3 years?)

Resources

- Call Cases: http://www.tech-invite.com/
- Documentation: http://www.softarmor.com/
- SIP software
  - SER: http://iptel.org/
  - OpenSER: http://openser.org/
  - Asterisk: http://asterisk.org/
  - sipp, sipsak
  - Protos Test Suite, RFC 4475

Questions & Answers

Q&A

hscholz@raisdorf.net