VoIP Phreaking

Introduction to SIP Hacking

Hendrik Scholz

hscholz@raisdorf.net

http://www.wormulon.net/

22C3, 2005-12-27

Berlin, Germany

Agenda

- What is Voice Over IP?
- Infrastucture
- Protocols
- SIP attacks
- Conclusion

VoIP is

- generally considered cheap
  - TCO
  - end user perspective
- in production use today
- undergoing explosive growth
- free calls

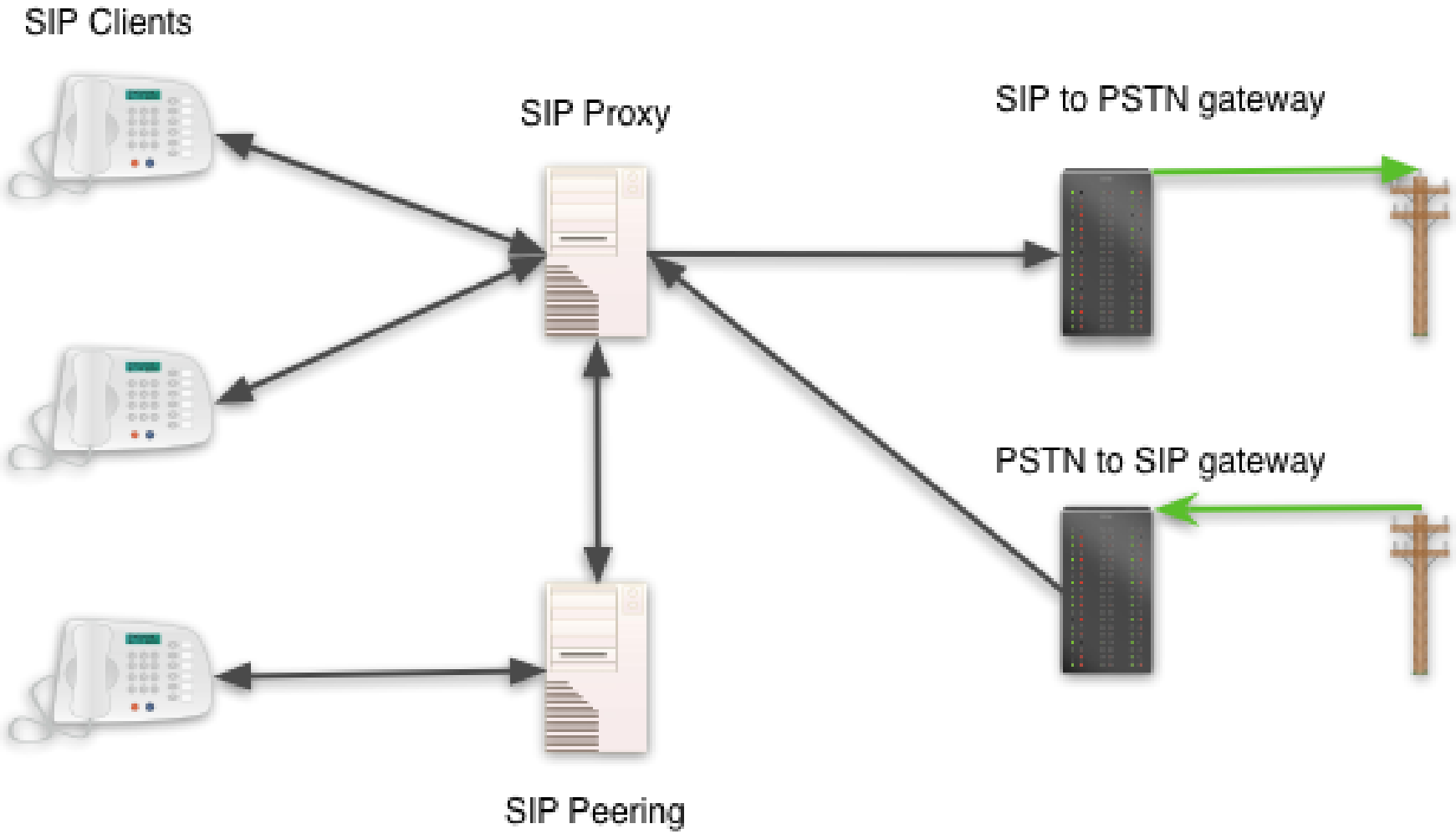
VoIP also

- converges with the PSTN
- replaces PSTN networks
- is growing rapidly
- is immature
- generally used without TLS

Infrastructure

- VoIP phones
  - hardware (Cisco, AVM, Snom, ...)
  - software (X-Lite, kphone, ...)
- Server software
  - registrar, route/proxy server, presence
- PSTN integration
  - VoIP->PSTN, PSTN->VoIP gateway
- misc services
  - billing, webinterfaces, media proxies, STUN

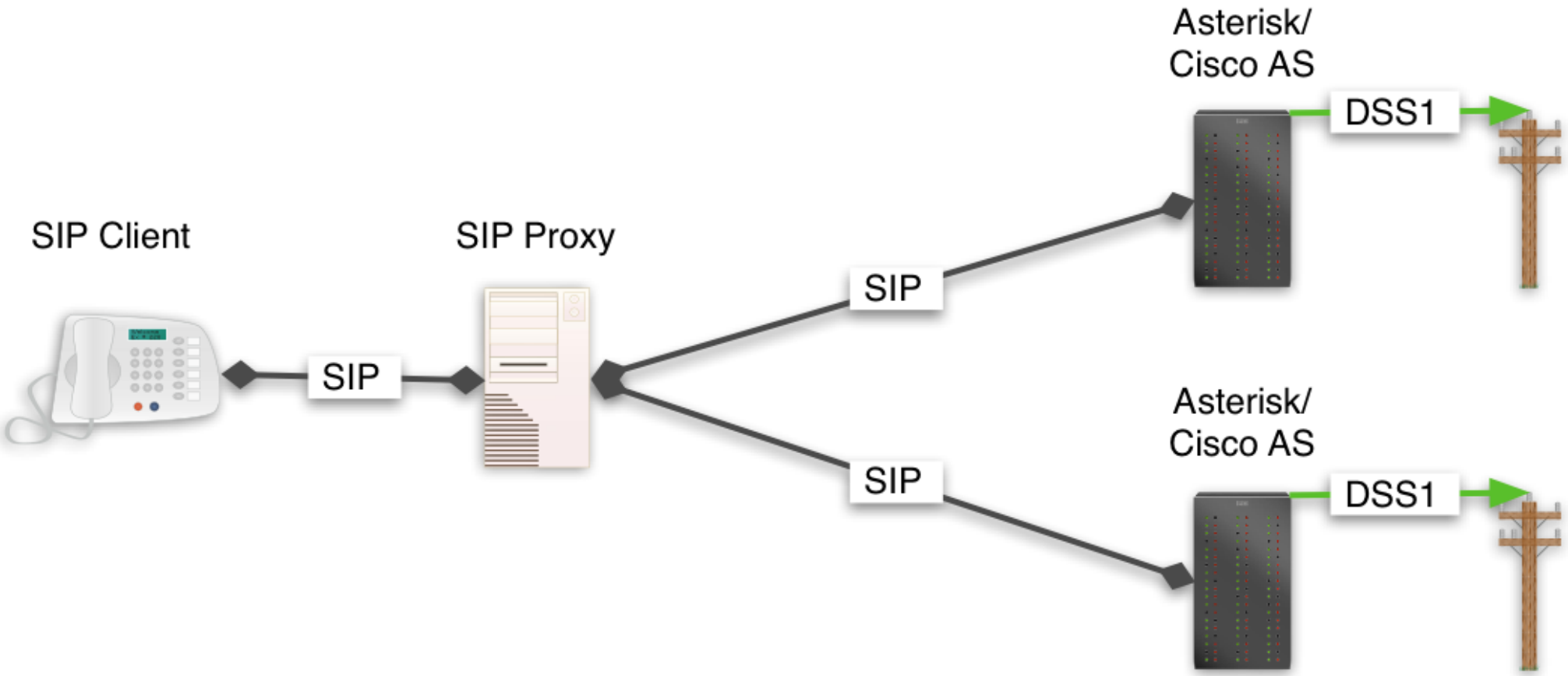
Infrastructure overview



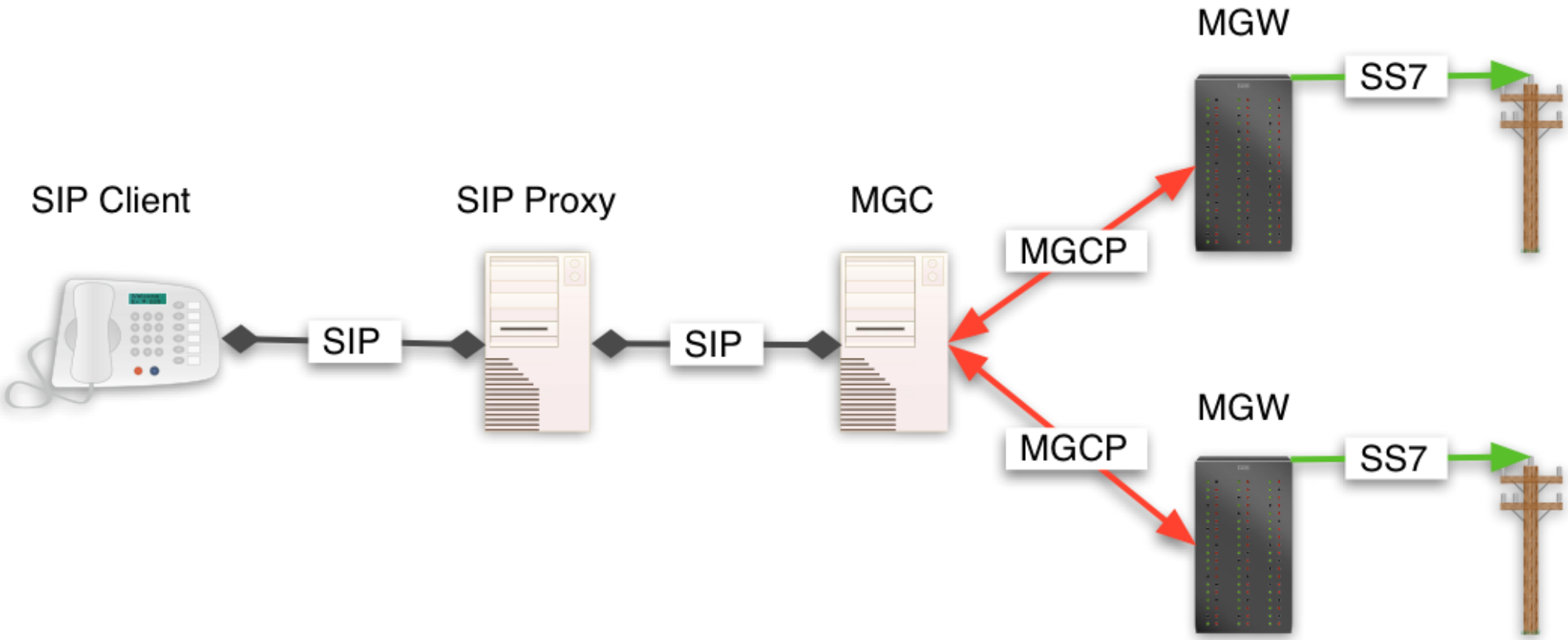
Protocols

- Separation of signalling and media
- Signalling
  - SIP, H.323
  - MGCP, Megaco
  - Skype
- Media w/ RTP
  - G711u/a, G7xx,GSM, iLBC, Speex, proprietary

SIP vs. MGCP


Asterisk/
Cisco AS
DSS1
SIP Client
SIP Proxy
SIP
SIP
Asterisk/
Cisco AS
SIP
DSS1

SIP vs. MGCP cont'd



Media Gateway Control Protocol

- Media Gateways are controlled by a Media Gateway Controller
- MGWC translates SIP/H.323 to MGCP
- RFC 3435, sect 5:

  „Any entity can send a command to an MGCP endpoint. If unauthorized entities could use the MGCP, they would be able to set-up unauthorized calls, or to interfere with authorized calls. We expect that MGCP messages will always be carried over secure Internet connections, as defined“

- MGCP is out of scope for this talk
- still it is VERY interesting

SIP

- SIP = Session Initiation Protocol
- RFC 3261 (superseded 2543)
- looks like http
  - plain text
  - status codes (200 OK, 404 Not Found)
  - key/value pairs
- transport: UDP (most common), TCP, TLS, DTLS

SIP cont'd

- complex state engine
- always changing due to additions
- hard to do complete implementation
  - different ways of doing things (Route header)
  - case insensitiveness, whitespaces

Open Source SIP software

- open source stacks
  - libosip, eXosip, reSIProcate, libdissipate
- clients
  - kphone, linphone, sfl-phone, PhoneGaim
- tools
  - sipsak, sipp, protos test suite, ngrep, ethereal
- server
  - SER, Asterisk, sipd, partysip, Vocal

Attack Vector: Signalling

- buffer overflows in all devices?
- race conditions
  - CANCEL during call-setup
  - media faster than signalling

SIP RE-INVITE (change codec, redirect media)

- Alert-Info header
  - change ringtone to a more distinctive one
    - internal symbol (bellcore-dr1)
    - http URL

Attack Vector: media/RTP

- injection of media
  - esp. premature media
- spoof receiver reports to fake bad quality and tear down the call
- various (private) tools exist
- recording of media streams
  - sniffing
  - proxying traffic

Attack Vector: Billing evasion

- make somebody other pay for the call
  - usually exploit ISP-related bugs/features
- get free calls
  - SIP based
  - MGCP based
- highjacking equipment
  - search for webinterface on hardware phone
  - initiate 3-party calls from webinterface

Attack Vector: SIP Spoofing

- SIP packets contain
  - To/From

```
To: <sip:0124@123.org;user=phone>
From: "Hendrik Scholz" <sip:0123@123.org>
```

  - Contact

```
Contact: <sip:0123@10.1.1.1:5060>
```

Attack Vector: SIP Spoofing cont'd

- To/From tags

```
From: "Hendrik Scholz"
  <sip:0123@123.org>;tag=000750c6848803683ac37
  616-1a257852
```

- Call-ID

```
Call-ID: 000750c6-84880034-5071af22-
  2898d775@10.1.1.1
```

- Cseq

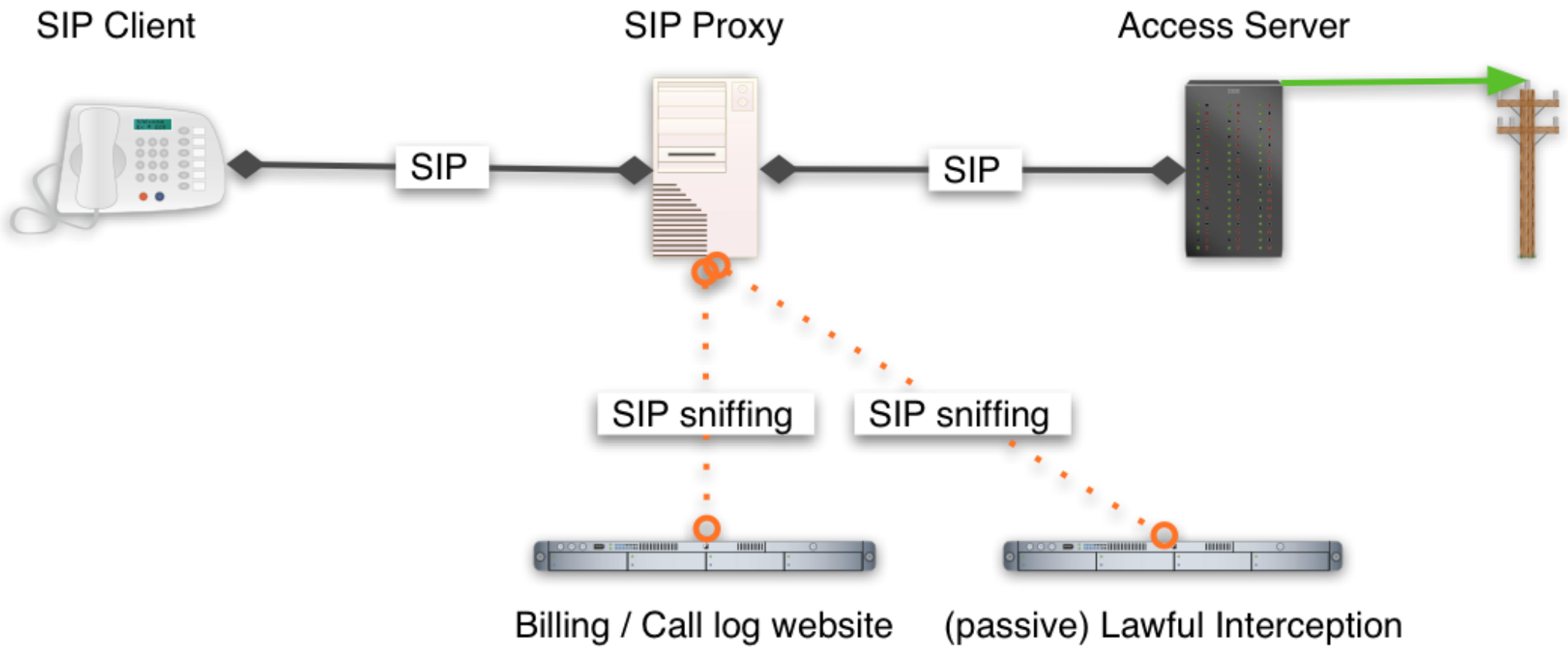
```
CSeq: 102 INVITE
```

- Record-Route

```
Record-Route:
  <sip:10.1.1.2;ftag=000750c6848803683ac37616-
  1a257852;lr=on>
```

Attack Vector: SIP Spoofing cont'd

- hard to guess all values
- luckly hardly any device checks all, Exploit!



Attack Vector: devices

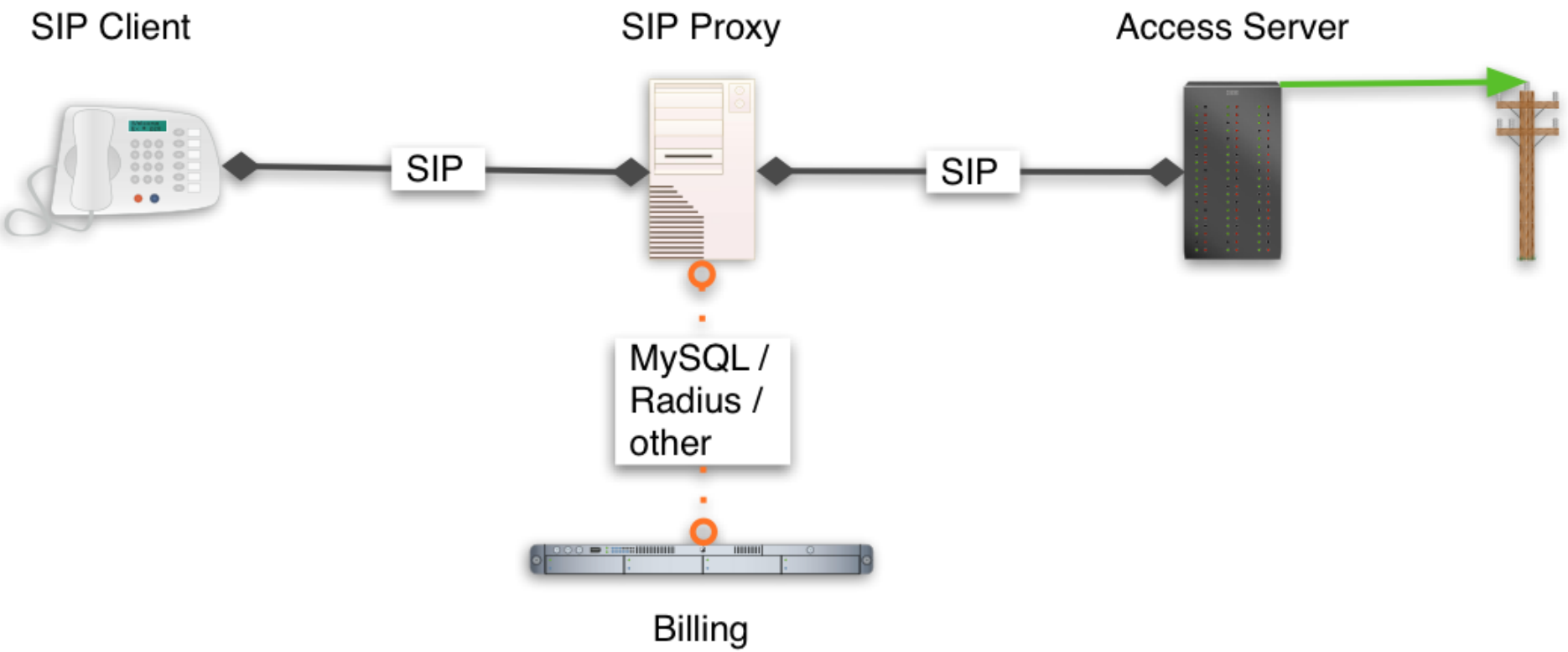
- SIP NOTIFY message w/ sync-check header
  - Event: check-sync
  - perform update/reboot
  - Cisco 79x0 related
- AVM 7050 'Bier holen'
  - „everything but the kitchen sink“
  - send #96*6* from an ISDN phone
  - phone displays 'Bier holen'

Attack Vector: Caller-ID

- messages contain
  - From
  - Remote-Party-ID
  - P-Asserted-Identity
- set and see what happens
- look for ISP proprietary extensions (P-Headers, SetCallerID header on nufone.net)
- use spoofed SIP Caller ID to call somebodies PSTN/cell phone voice mailbox

Easy Attack Example

- Route: caller -> proxy/billing -> PSTN -> callee
- Max-Forwards set too low on BYE
- packet expires on the way, cheap call



Resources

- RFCs: http://www.packetizer.com/voip/sip/standards.html
- http://iptel.org/
- Cisco Bugreports, esp. open bugs
- http://voip-info.org/
- http://onsip.org/

Conclusions

- VoIP is emerging while still under development
- convergence of trusted and untrusted networks
- TLS hardly used
- attack MGCP behind SIP
- attack applications (voice mail)