# Lawful Interception in German VoIP-Networks

22C3, Berlin

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

# Agenda

- What is Lawful Interception (LI)?
- Terms, Laws
- Lawful Interception in PSTN networks
- Lawful Interception in VoIP networks
- Countermeasures
- Interim Solution
- Upcoming Nightmares

# What is Lawful Interception?

- spying on users
- justified by the government
- goal: gain information about subject
- information: relationship rather than content
- target: 'account'
  - email, DSL, Usenet, phone number, SIP address
  - IRI: intercept related information

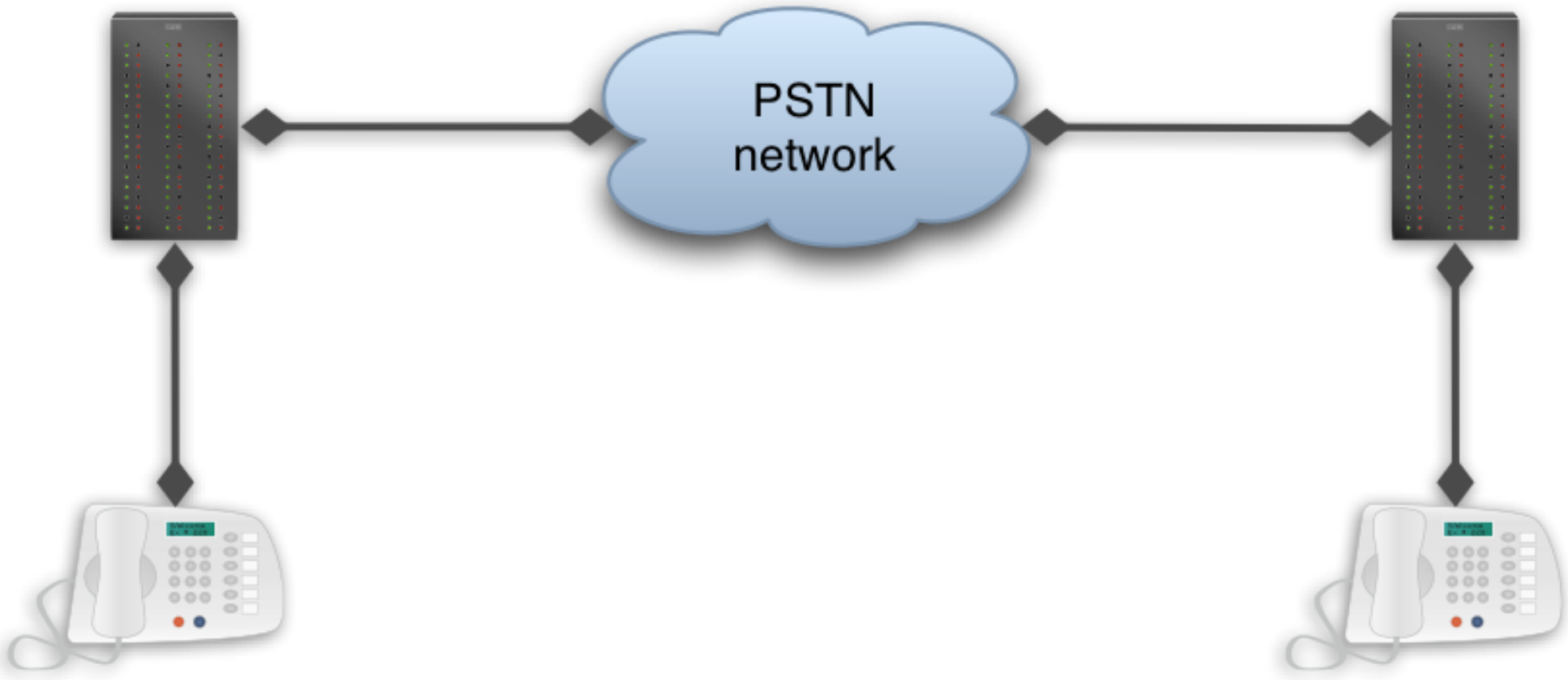
# Terms

- Bedarfstraeger, berechtigte Stelle
  - demand bearer, entitled agency
  - LEA: Law Enforcement Agency
- Massnahme
  - interception process
- Ausweisung
  - expulsion order
  - copying data
  - active vs. passive expulsion

# The Law

- Telekommunikationsüberwachungsverordnung
  - telecommunication surveillance ordinance
  - TKUeV
- Technische Richtlinie zur Telekommunikationsüberwachungsverordnung
  - technical guidelines
  - TR TKUeV
- Durchfuehrungsverordnung zur Telekommunikationsüberwachungsverordnung
  - rules of conduct
  - DV TKUeV

# PSTN network



# LI in the Old World

- signalling and voice parallel (ISDN)
  - D channel, multiple B channels
  - in-band singalling (analogue)
- LI on the upstream gateway (i.e. Siemens EWSD)
- in service since 20 years
- redirections not visible to user
  - no ping to measure round-trip times
  - no traceroute to record route

# VoIP Paradigm

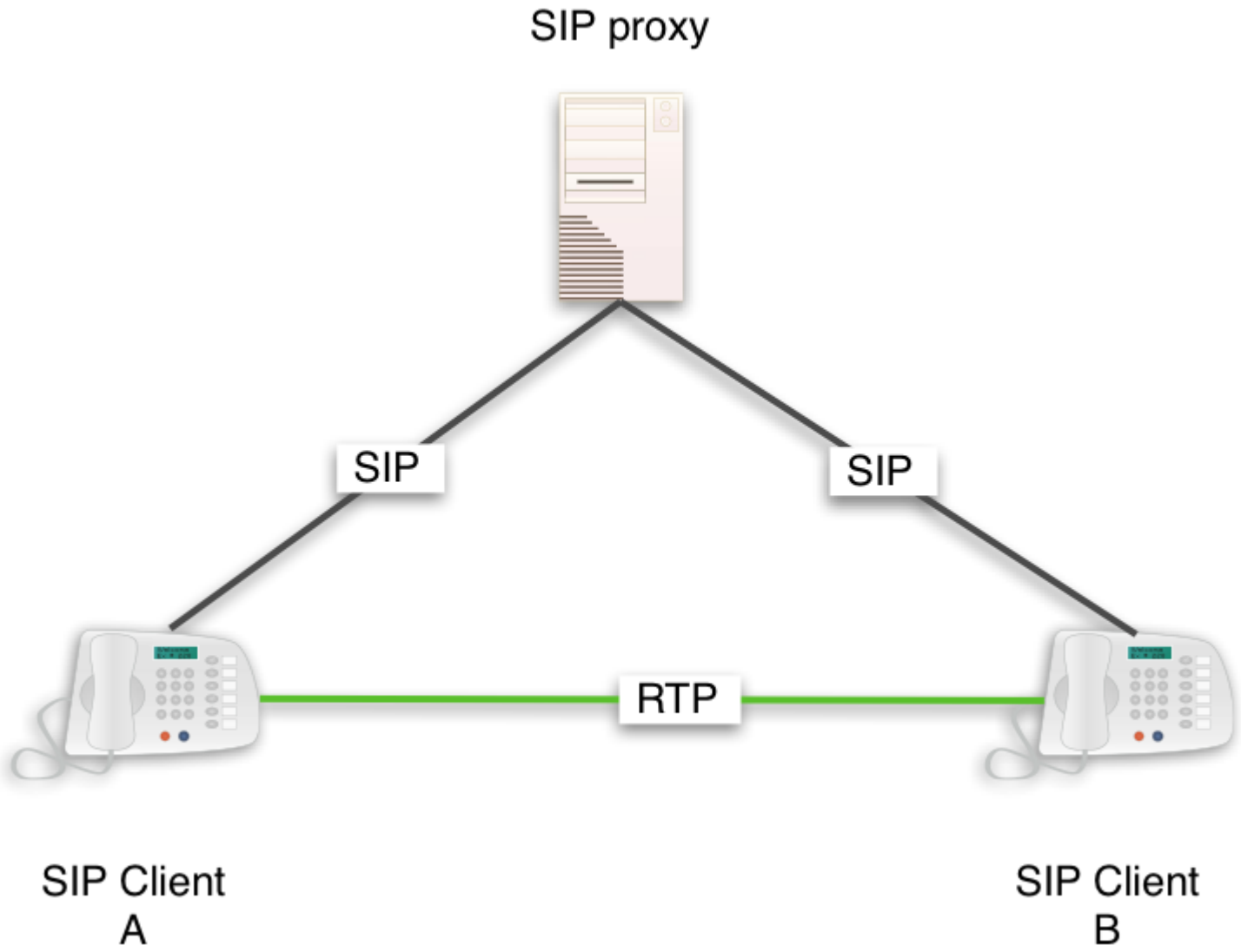
**VoIP should have all PSTN-LI-features**

- undetectable to user
- management (handover) interface
- security

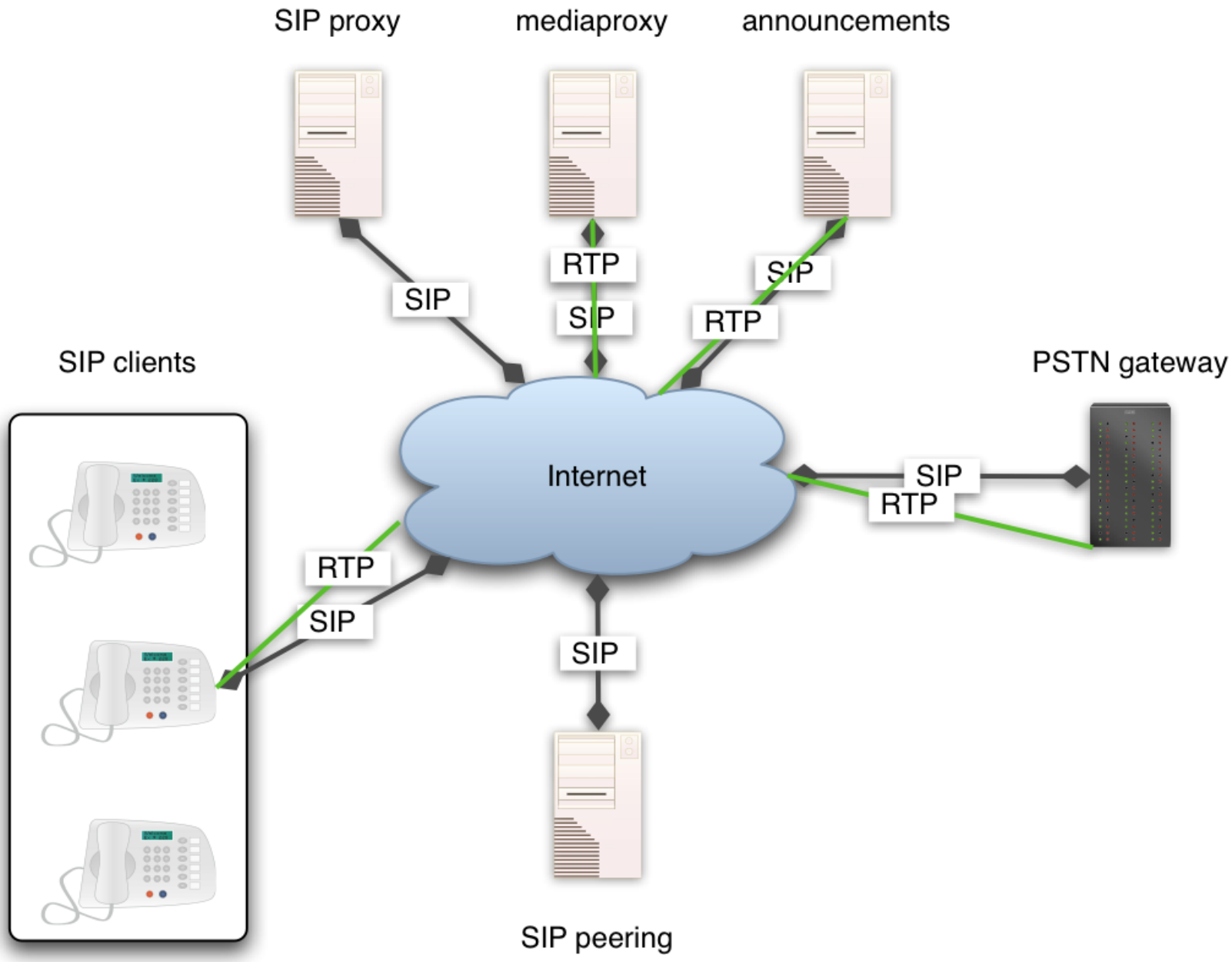
# The VoIP Universe

- signalling:
  - SIP
  - H.323
  - SCCP (Skinny)
- voice/media:
  - G.711 ulaw, alaw
  - G.723, G.726, G.729
  - GSM, iLBC, speex
  - proprietary

# simplified VoIP Setup



# standard VoIP Setup



# Solution: Conference Call

- each call becomes a conference call with a government official listening
  - implemented in client
- becomes visible in SIP: „Hi, I'm Eve and I'd like to get a copy of your voice stream“

# Solution: Media Gateway

- divert voice through a proxy that allows sniffing
- snignalling has to be modified
- „This is your SIP server speaking. You are being intercepted. Please send your data to the police. They'll forward it on for you.“
- easy to implement
- easy to detect in most cases

# Solution: PSTN Diversion

- divert outgoing call into the PSTN
- sniff data using well-known intercept access point (IAP)
- divert traffic back into the VoIP network
- requires transition SIP to {SS7|DSS1|MGCP}
- not all SIP-messages can be translated
- how about voice quality?

# Solution: passive Ausweisung

- add interception points (IAP) everywhere
  - in every POP -> expensive
- the right thing could sure be found in the mess
- eases abuse as everything is in place and waits to be used
- who controls what's intercepted?
  - hackers gaining access
  - management overhead, updates

# Solution: active Ausweisung

- drive to the POP when needed and install temporary hardware
- problems:
  - delay of up to 48h until device is in place
  - visible physically
  - what happens in long-term surveillance?
  - how about roaming users?

# ideas?

- don't do LI at all
- make the underlying 'access' ISP sniff the data
- Bedarfstraeger/government writes readable laws/instructions
  - ain't gonna happen
  - VoIP is kinda new to the government
  - define use-cases that can be intercepted
  - accept the fact of untraceable calls
- outlaw VoIP?

# bad ideas

- If you divert traffic from SIP to PSTN
  - Do not show diverted calls in records
  - Do not add cost announcement
  - Do not bill user for intercepted calls
- make it easy to use
  - abuse
- make it permanent (in-place)
  - security

# Countermeasures

- make fake calls and save
  - round trip times
  - Record-Route IP addresses
  - SDP header information
- alert user if things change

# Countermeasures cont'd.

- use random unsupported codec
  - PSTN gateway will drop call if used for interception
- add challenge authentication, checksums
  - DTLS
- TLS, SRTP
  - 'access' ISP has to provide data

# Poor man's LI

- record all data using libpcap
  - tcpdump -s 1500 -w foobar.cap udp
- use ethereal to reassemble RTP stream
  - save as audio file
  - nice statistics for debugging

# RegTP interim solution

- interim solution from July 2005
  - signalling only solution
  - based on ETSI TS 101 671
  - use SINA box (VPN tunnel) to send SIP signalling
  - totally bogus on first attempt
    - needed lots of discussion
- Meeting in Mainz early in June
- to be implemented by ISPs this year

# BNetzA Interim Issues

- sniffing based on account
  - how about in-band authentication?
    - authenticated using DTMF tones on mailbox
- delay
  - delay between call and data reception at LEA has to be very low (500ms)
- undetectable
  - doable in most cases

# Media solution

- RTP has to be interceptable by 2007
- BNetzA likes to have RTP media for intercepted calls
- some media is hard to capture
  - call scenarios yet to be specified
- lots of hardware needed in distributed systems
- LEA need to have bandwidth and equipment

# Upcoming Nightmares

- World of Warcraft 'Voice Chat'
  - this is VoIP?!
- 'Vorratsdatenspeicherung'
  - data warehouse containing user information, call logs
  - parameters:
    - European 'solution'
    - 12-36 months depending on government
    - ISPs have to store and provide data

# Resources

- RFC 3924, Cisco Architecture for Lawful Intercept in IP Networks
- http://bnetza.de/
- http://www.wormulon.net/ -> slides

# Questions?

**hscholz@raisdorf.net**