SIP and PSTN Connectivity

Jiri Kuthan, `iptel.org`
sip:jiri@iptel.org
September 2003

Outline

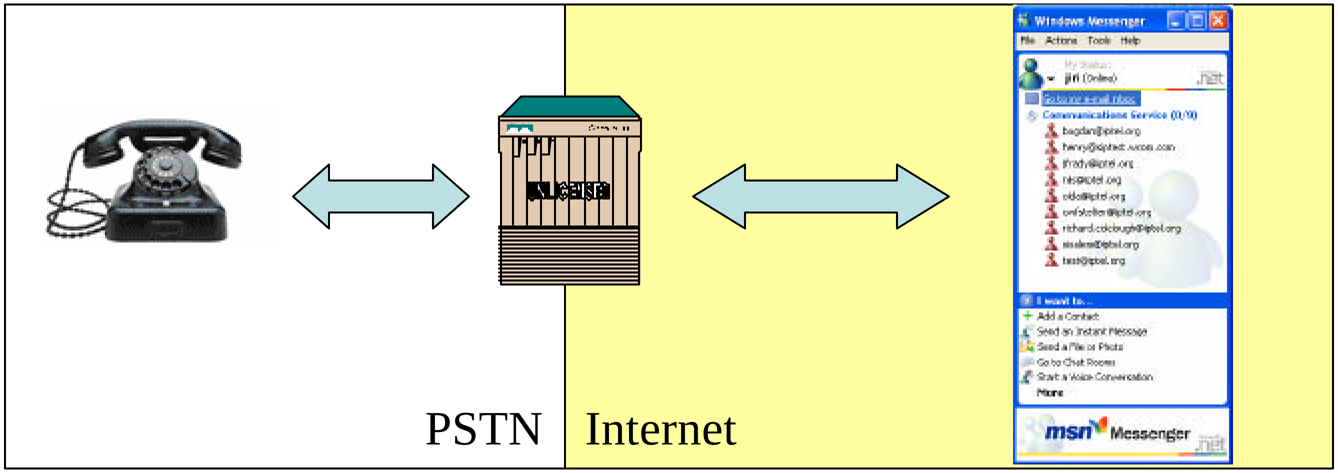
- PSTN Gateways.
- PSTN2IP Demo
- Integration challenges:
  - CLID
  - Interdomain Trust
  - Gateway Location
- Outlook: Reuse of Mobile Network Security
- Conclusions

About SIP-to-PSTN Connectivity

- SIP Telephony really nice. There are however still 200 million PSTN users hanging around and you would like to talk at least to some of them.

PSTN Gateways

- Problem #1: your device speaks a different language than your grandmother’s.
- Solution: use a gateway, i.e., adapter which converts signaling and speech from Internet to PSTN and vice versa.

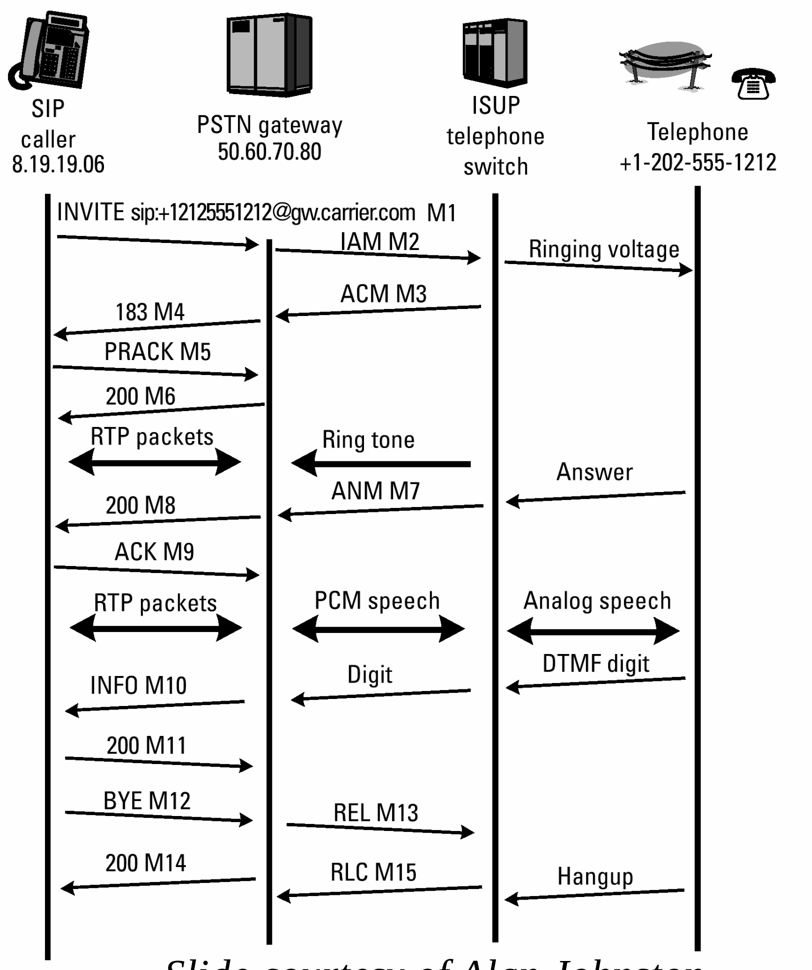


- Gateway market established: Cisco, Ericsson, Lucent. Sonus, Vegastream, etc. Open-source as well.

RFC 3398

Call Flow SIP to PSTN

- Request-URI in the **`INVITE`** contains a Telephone Number which is sent to PSTN Gateway.
- The Gateway maps the **`INVITE`** to a SS7 ISUP IAM (Initial Address Message)
- **`183 Session Progress`** establishes early media session so caller hears Ring Tone.
- Two way Speech path is established after ANM (Answer Message) and **`200 OK`**
- Gateways interfacing other PSTN dialects operate similarly.



SIP caller 8.19.19.06

PSTN gateway 50.60.70.80

ISUP telephone switch

Telephone +1-202-555-1212

INVITE sip:+12125551212@gw.carrier.com M1

IAM M2

Ringing voltage

ACM M3

183 M4

PRACK M5

200 M6

RTP packets

Ring tone

Answer

ANM M7

200 M8

ACK M9

RTP packets

PCM speech

Analog speech

DTMF digit

Digit

INFO M10

200 M11

BYE M12

REL M13

200 M14

RLC M15

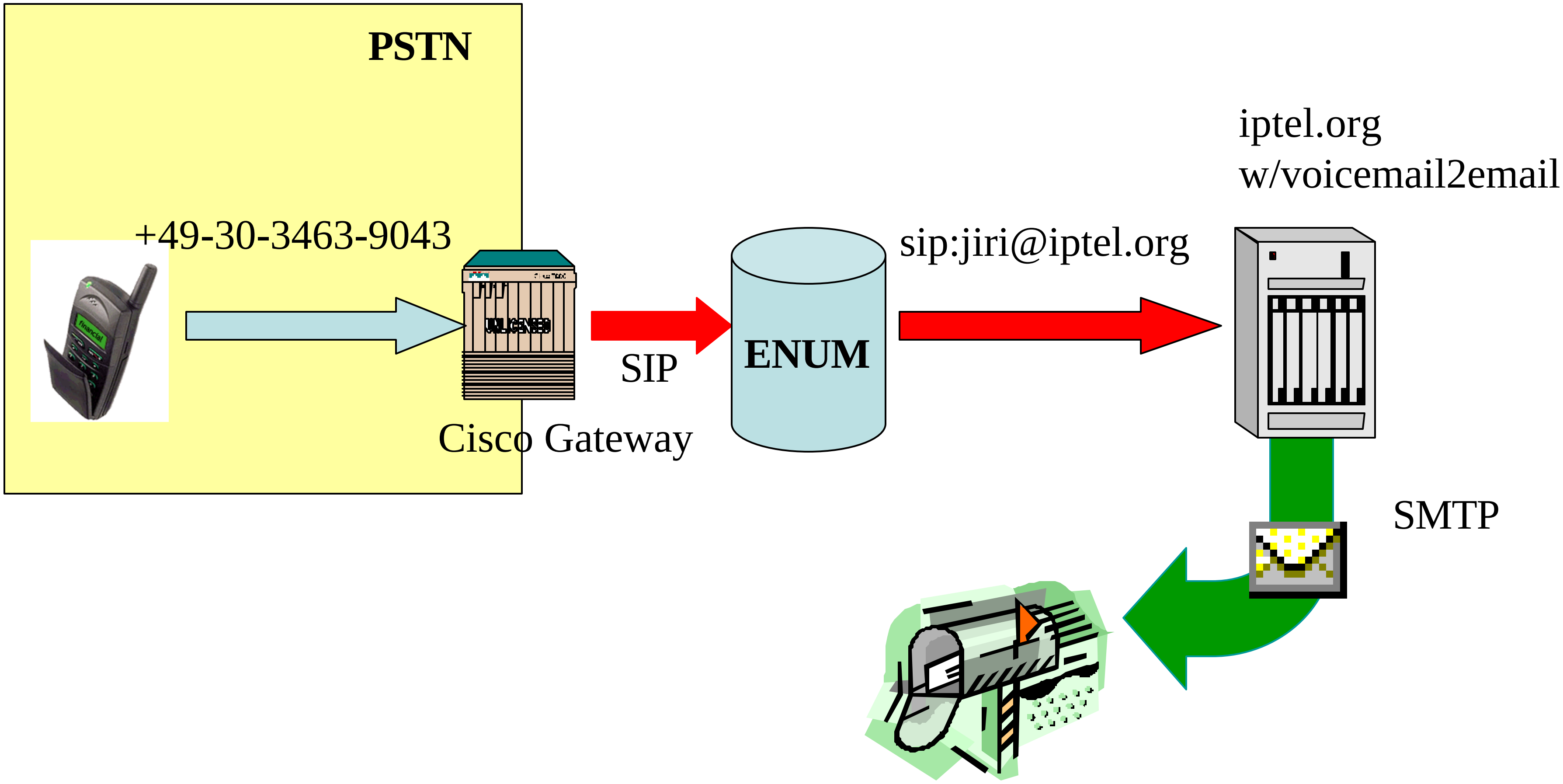
Hangup

Slide courtesy of Alan Johnston, WorldCom. (See reference to Alan's SIP book.)

A Possible Gateway Shopping Option…

- Size does matter: How to enlarge size of your network? Take MGCP/Megaco/H.248 and double the number of boxes today.
- Some vendors decompose gateways in two parts: signaling gateway and media gateway. These two parts are reconnected together through some of Megaco/MGCP/H.248 protocols.
- Don’t ask me what decomposition is here good for and why there are multiple protocols to choose from.

PSTN2IP Demonstration



PSTN

+49-30-3463-9043

Cisco Gateway

SIP

ENUM

sip:jiri@iptel.org

iptel.org
w/voicemail2email

SMTP

Gateways Ship Today, What Is the Problem Then? Integration!

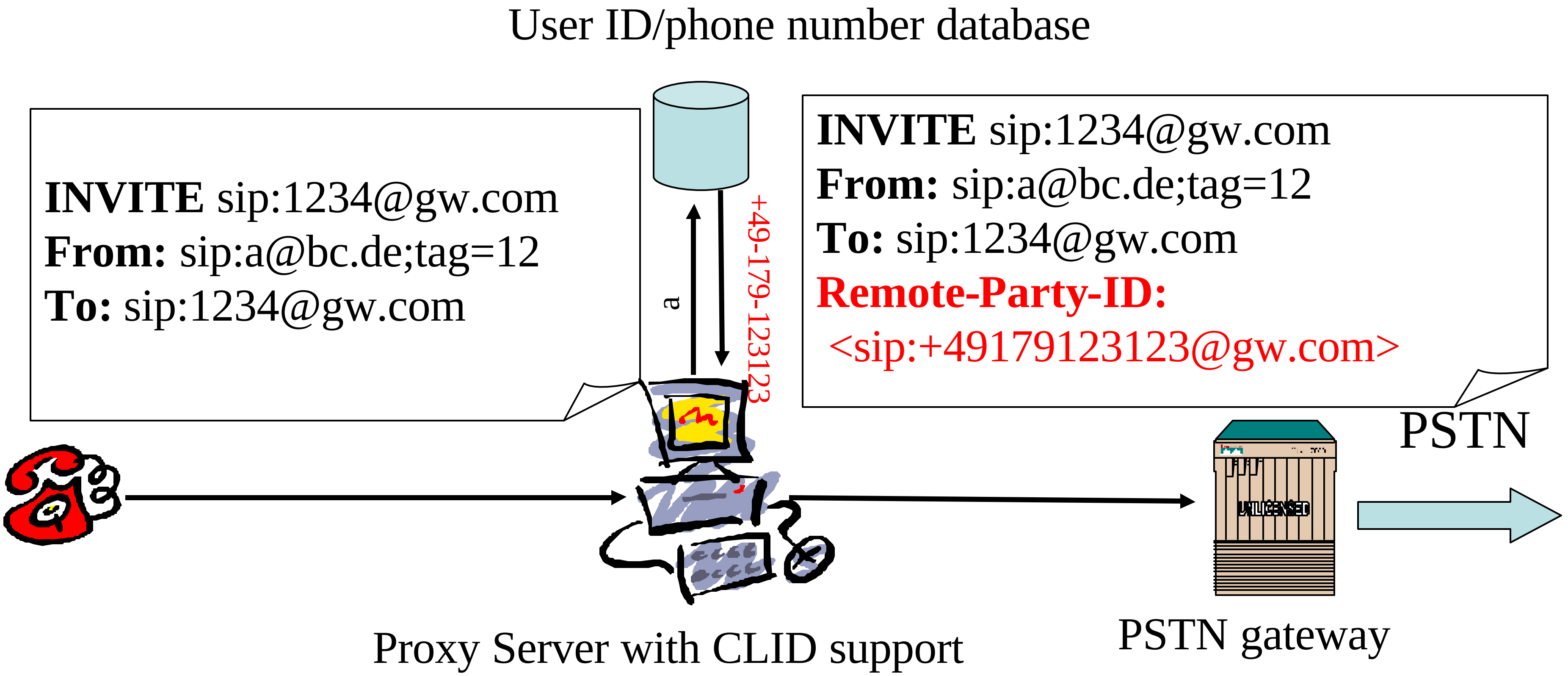
- Identity: jiri@iptel.org calls out through PSTN gateway. What Caller-ID will display down in PSTN?
- Interdomain settlement: your SIP service operator does not have the capability to terminate anywhere in world cheaply. How can he establish a secure channel to PSTN termination operators?
- How do you locate a proper PSTN termination gateway?
- And some other ugly legacy problems like DTMF, overlap dialing.

draft-ietf-sip-privacy

CLID

- Typical deployment problem: jiri@iptel.org (in possession of a valid PSTN number) would like to call to PSTN through his gateway operator – how does the gateway know which telephone number to display?
- Architecturally, proxy servers are highly programmable devices that can easily link SIP identity to PSTN numbers. Thus, that's the place for mapping of SIP identity to an "owned" PSTN number.
- Missing piece: communicating the PSTN number a server determined to gateway.
- Current standardization status: several competing documents. "Remote-Party-ID" deployed.

Remote Party ID



User ID/phone number database

INVITE sip:1234@gw.com
From: sip:a@bc.de;tag=12
To: sip:1234@gw.com

INVITE sip:1234@gw.com
From: sip:a@bc.de;tag=12
To: sip:1234@gw.com
Remote-Party-ID:
<sip:+49179123123@gw.com>

Proxy Server with CLID support

PSTN gateway

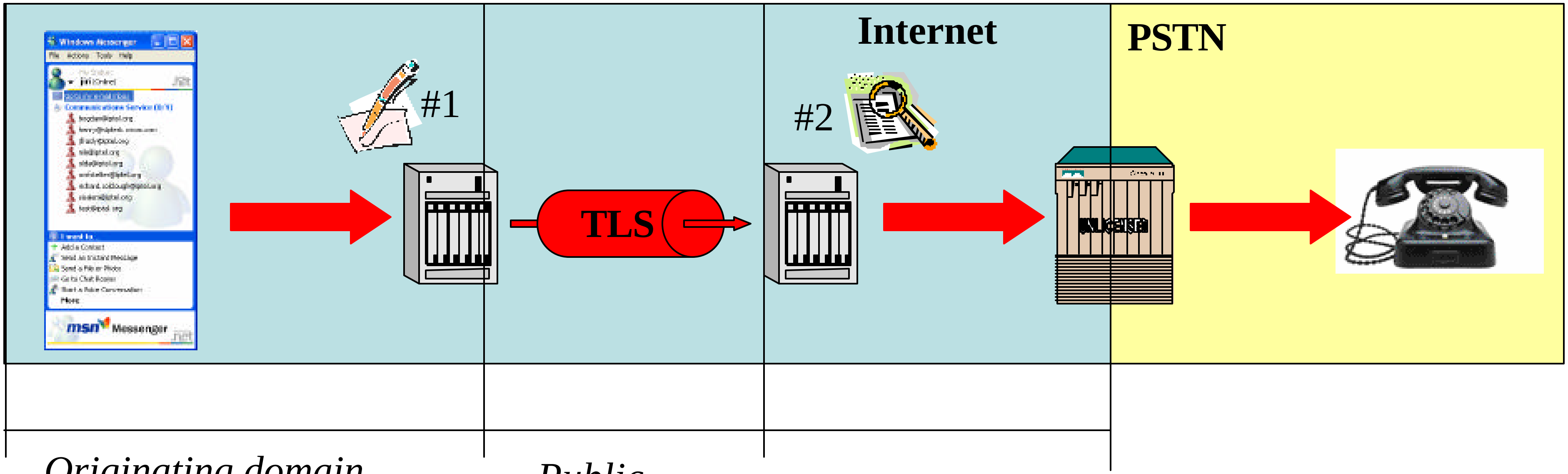
Problem of Trust

- Displaying proper caller ID is a legal requirement for operators. What happens if someone fakes the RPID and operator displays a wrong number?
  - Ask your lawyer or regulator, I better tell you how to ensure displaying correct number.
- It is about a reasonable trust model: a gateway may only display caller ID issued by a trustworthy source.
- Trust needed to solve other problems too: Does the call come from a source to whom my gateway can credit international calls?
- Establishing trust to individual users within a single domain almost easy…but what if multiple domains comes in?

Trust: Interdomain versus Intradomain

- Within single administrative domain, trust can be implemented using physical security and knowledge of identity of local users – proxy servers verify identity of local users using digest and gateways trust local proxies.
- Interdomain scenario example: iptel.org users terminate calls to US PSTN with National Gateways Inc. How do you export the trust then?
  - The terminating provider can't verify identity of remote users and can't trust information passed over the public Internet. RPID alone can't be trusted as it can be changed anywhere on the transit. Stronger security protocols come in for interdomain operation: TLS.

TLS Use for Interdomain Security



Originating domain

Public Internet

Terminating Domain With Local Trust

- Assumption: target domain trusts source domain to display proper CallerID and settle incurred costs.
- Step 1: originating domain verifies identity of local user (digest). If ok, it appends RPID and uses TLS for secure inter-domain communication.
- Step 2: terminating proxy verifies incoming TLS connection against list of trustworthy domains. If ok, SIP request is forwarded to PSTN gateway.

More on TLS Use

- TLS use for SIP solves other trust problems too:
  - With trust mechanisms, interdomain accounting can be also implemented securely
  - Signaling can be no longer sniffed during transport.
- Security Disclaimers:
  - Trust established hop-by-hop – it implies transitive trust along arbitrarily long proxy chains. Remember a chains is as strong as the weakest element in it. You have to trust next-hop not to pass your requests to questionable servers.
  - Privacy is not end-to-end: proxy servers along the signaling path do see SIP in plain-text,

Gateway Location

- Now, we have a plenty of gateways: which one to choose?
- Best Current Practice: static Least-Cost-Routing configuration in your signaling server.
- Concerns: static configuration doesn't scale (remember that /etc/hosts before DNS was invented?) – do we have future options?
  - One IETF's answer is Telephony Routing Protocol (TRIP) – it was (and probable will be) never deployed due to complexity and over-dimensioning.
  - Other possibility: ENUM.

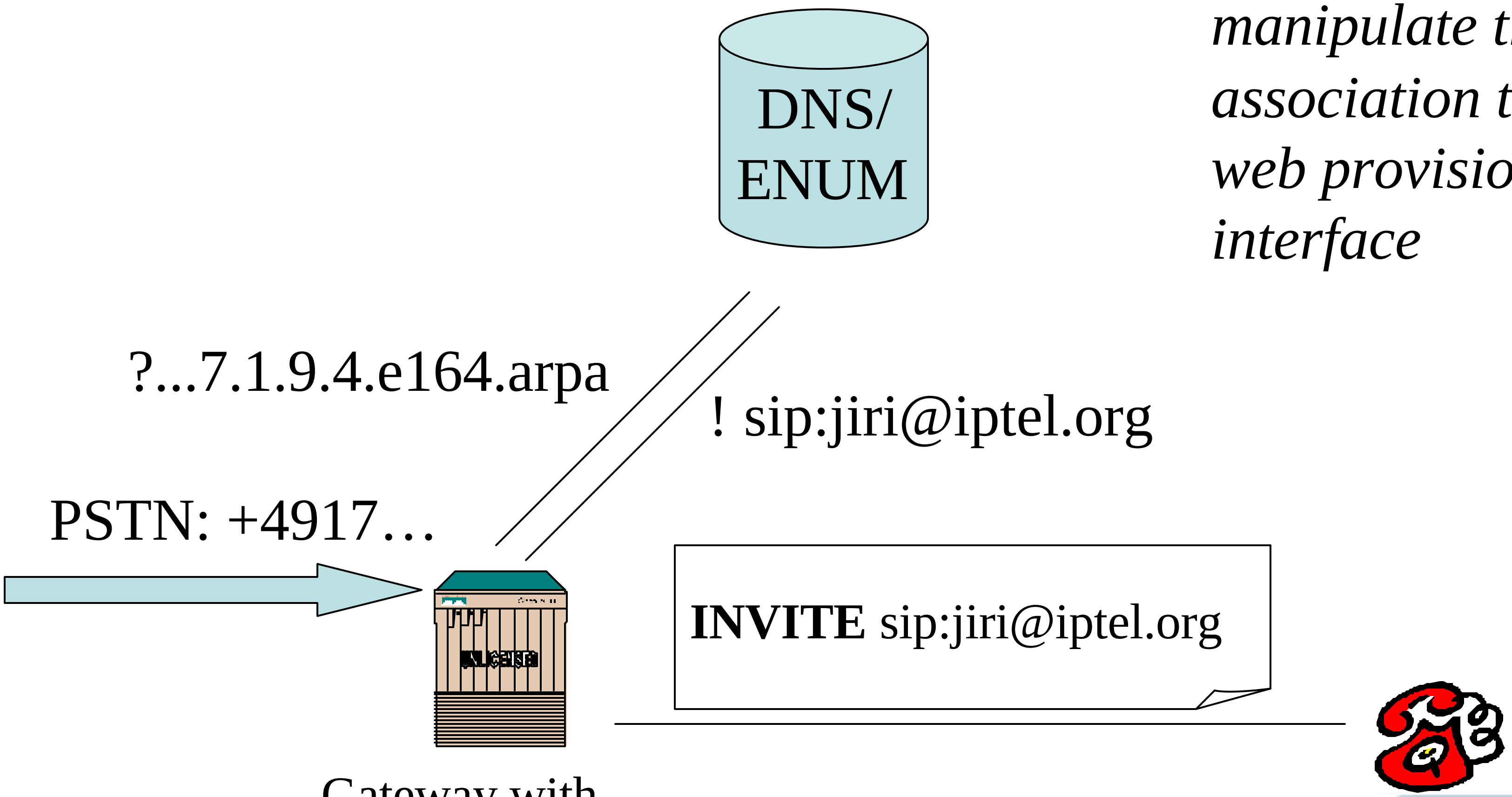
RFC2916

ENUM

- Problem: caller is in PSTN (can use only digit keys) and would like to reach a SIP callee
- Answer: ENUM. Create a global directory with telephone numbers that map to SIP addresses (or e-mail, etc.).
- Lookup mechanism: DNS maps E.164 numbers to a set of user-provisioned URIs
- The E.164 number queries are formed as a reversed dot-separated number digits, to which string ".e164.arpa" is appended, e.g.:
  - +4319793321 → 1.2.3.3.9.7.9.1.3.4.e164.arpa

ENUM Call Flow

- *DNS/ENUM helps ingress gateway to resolve SIP address from E.164 number*
- *Typically, owner of an ENUM entry can manipulate the address association through a web provisioning interface*



DNS/ ENUM

?...7.1.9.4.e164.arpa

! sip:jiri@iptel.org

PSTN: +4917…

INVITE sip:jiri@iptel.org

Gateway with ENUM resolution

RFC2833

DTMF Support

- Actually, I would wish this slide wasn’t here: IVRs are horribly inconvenient devices. I like voicemail message delivery by e-mail and flight-ticket shopping with web much better. But …
- … Large deployed base for telephony applications.
- Solution 1: include tones in audio. It works fairly well with G.711 codecs. More compressive codec may degrade quality so that tones are no longer recognized by receiver.
- Solution 2: special DTMF payload for RTP: RFC 2833. Reliability achieved through redundant encoding (RFC2198).

RFC3578

Overlapped Dialing

- Problem: ingress PSTN2IP gateway operates in overlapped dialing mode whereas SIP operates en-block;
- Solution #1: initiate en-block SIP dialing using knowledge of numbering plans or after a period of overlapped dialing inactivity; drawback: delay and knowledge of numbering plan catalogs.
- Solution #2: send a new INVITE for each new digit

Outlook: Leveraging the Mobile Network Security in SIP Devices

- Objective: transfer the mobile network security experience to IP telephony: Security keys used to authenticate users can be fairly long, users don’t need to remember them, and can use them with multiple devices
- The SIM stores other sensitive data too, Caller ID in particular.
- And of course it can keep user data such as phonebook as well.
- Obviously, reusing SIM cards with IP telephones lends itself.

SIP/SIM Works Today

- Within a trial, we developed a prototype which
  - Server side (SER), offers both traditional digest and “de-luxe” SIM-based authentication to callers
  - Client side (k-phone with a SIM-card reader), picks SIM-based authentication and submits proper credentials.
  - The server verifies phone’s credentials against its security database via RADIUS.
- Potential for enlightened telcos to bundle mobile phones with Internet access.
- Still on the agenda: maintenance of interdomain trust: each-to-each may be too hard (# of Internet domains >> # of cell operators) , some certification authorities may come in

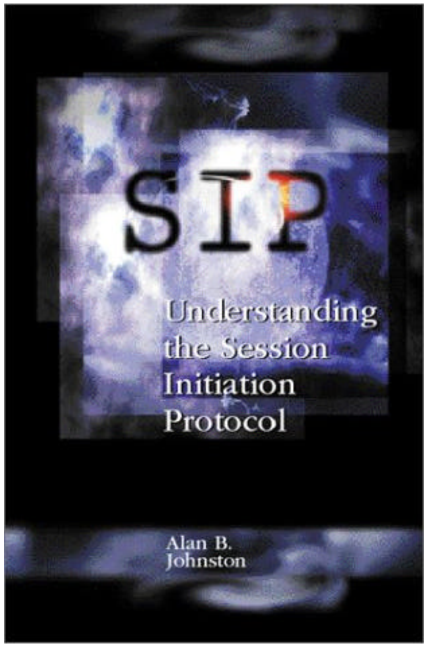
Concluding Observations

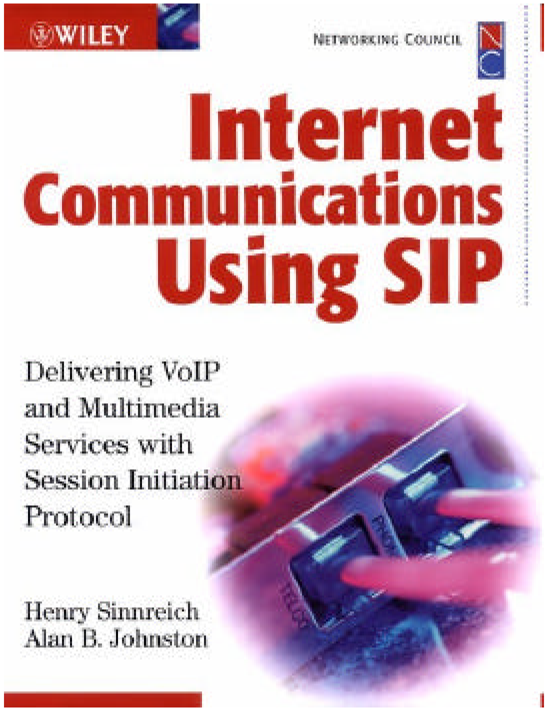
- PSTN/SIP interoperation works just fine today, the most troublesome are parts taking interdomain operation.
- Technologies applicable today: TLS interdomain-wise in combination with intradomain security protocols.
- Outlook: reuse of mobile network security protocols.

More PSTN-Related Reads

- Mapping of of Integrated Services Digital Network (ISUP) Overlap Signalling to the Session Initiation Protocol [draft-ietf-sipping-overlap]
- Session Initiation Protocol PSTN Call Flows [draft-ietf-sipping-pstn-call-flows]
- Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping [RFC 3398]
- Session Initiation Protocol for Telephones (SIP-T): (SIP-T): Context and Architectures [RFC3372]
- Interworking between SIP and QSIG [draft-elwell- sipping-qsig2sip]

There Are SIP Books!




WILEY
Networking Council
NC
Internet Communications Using SIP
Delivering VoIP and Multimedia Services with Session Initiation Protocol
Henry Sinnreich
Alan B. Johnston

- Alan B. Johnston: “SIP: Understanding the Session Initiation Protocol”
- Artech House 2001

- Henry Sinnreich, Alan Johnston: Internet Communications Using SIP: Delivering VoIP and Multimedia Services with Session Initiation Protocol
- John Wiley & Sons, 2001