Debian's role in establishing an alternative to Skype

Motivation, Challenges and Tactics

Daniel Pocock daniel@pocock.com.au

http://www.OpenTelecoms.org

mini-DebConf, Paris, November 2012

Introduction

- *Motivation* – why do we need to do something? What happens if we do nothing?
- *Challenges* – why hasn't it been done already?
- *Tactics* – what can we do over the next 12 months?

- *Yes, you've seen me before* – in Managua. Slides and video are available and highly recommended.
- *Is there something new?* – yes.

- *Widely deployed* – hundreds of millions of users
- *Interdependency* – unlike other types of software, *interoperability* is a critical factor in the success of real-time communications software
- *Viber* – another proprietary solution that has quickly gained traction thanks to ease of use. The free software community missed the boat in the desktop VoIP arena, now the same may be happening for mobile.

- *Marketing* – Skype allows Microsoft to study your thoughts and emotions in real time. Feedback to advertisers.
- *Privacy* – Microsoft has patented a technique for monitoring Skype. Call records, friend lists, etc. Statistical techniques for identifying who is pregnant, who is a homosexual, have all been exposed recently.
- *Security* – the WhatsApp revelations, using IMEI as password.
- *Monopoly* – Skype depracating MSN, Lync integration on horizon, will open source solutions be locked out?

VoIP punished

Why VoIP has been held back

- *Codec mismatches* – not all products support the same codecs
- *Codec selection* – hard-coded codec settings not ideal for variable bandwidth (mobile/laptop/shared connection)
- *NAT incompatibilites* have undermined reliability and confidence, and caused many frustrations. Early solutions (STUN) were flawed.
- *Getting users registered* is not easy. Not like UNIX mailboxes (created by default).
- *Two protocols*, SIP and Jabber, to choose from.
- *Federation of VoIP networks* is not universal. Many networks are just islands or gateways to PSTN.
- *Backwards compatibility, holding on to phone numbers* and other traditions have muddied the waters: SMTP never attempted to replicate fax numbers.

VoIP punished

Why VoIP has been held back in UNIX

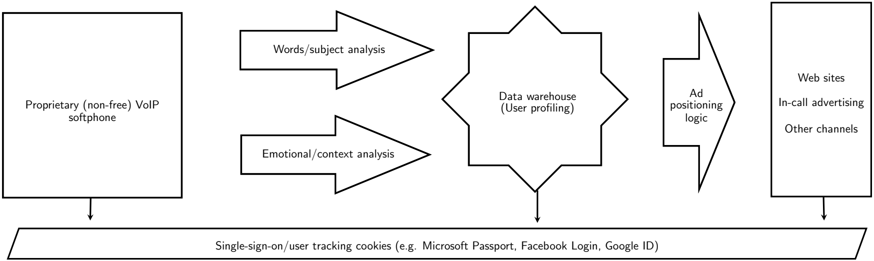
- *Asterisk* and similar products require much more setup effort
- *UNIX users* don't automatically become VoIP users, unlike for email, where a UNIX user automatically has a mailbox.
- *DIGEST hashes for passwords* — Different password hashing (similar to the HTTP DIGEST problem). Solutions for storing multiple hashes exist, users required to re-hash passwords during implementation. One possible workaround: client certificates instead of DIGEST.

How bad could it get?

The risk if action is not taken

- *Real-world examples* in other technologies should be a wake-up call
- *DVD CSS and DRM* has locked people out of their own DVD hardware
- *HDMI DRM* has extended the concept across the home entertainment domain
- *UEFI Secure Boot and TPM* is taking hold of the PC
- *What next?* Will Skype and Microsoft Lync operate as a closed system with similar DRM-like attributes?

The nightmare scenario
Advertising feedback possibilities



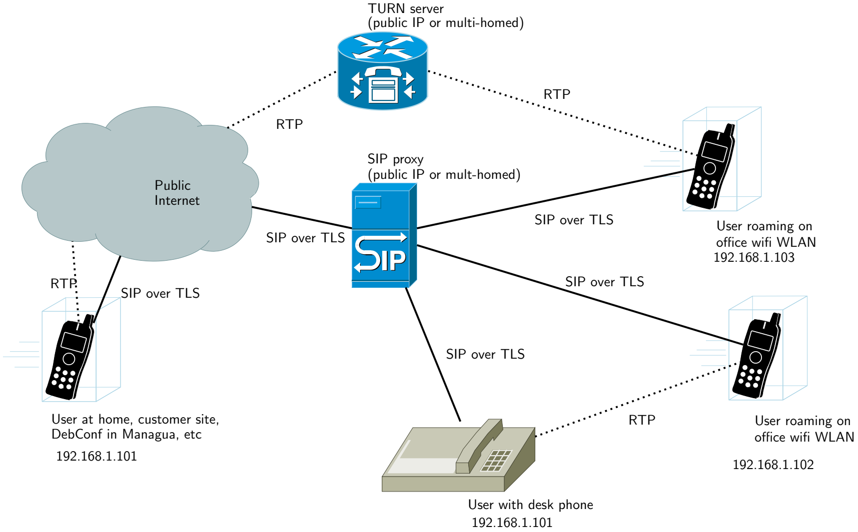
Peer pressure

Communications is a sore spot

- *Communications* is maybe the only pervasive technology that invokes more emotion than IT when users are dis-satisfied
- *Pressure* from personal and corporate peers is more intense due to the implicit need for interoperable solutions
- *A real danger* that users locked-in to the proprietary communications technology by their network of peers will be out-of-reach for free software like Debian

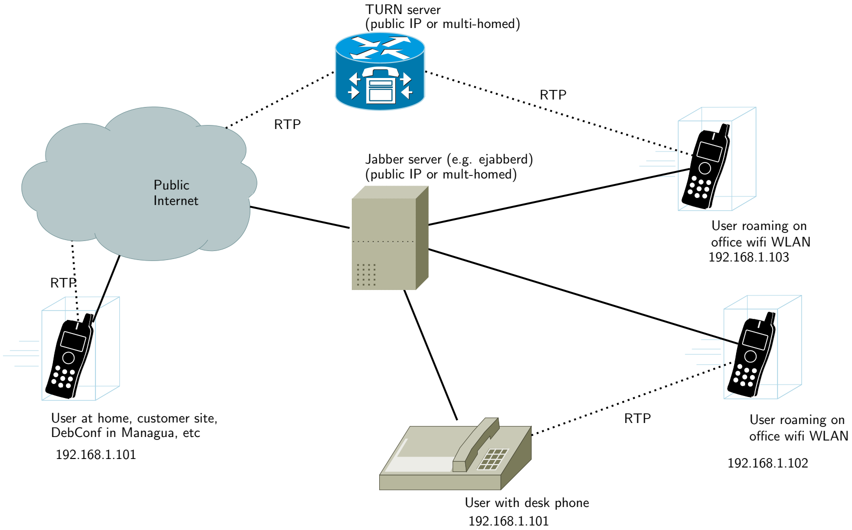
- *Maximising success of every call*
  - *Both protocols* (SIP and Jabber) in parallel
  - *Multiple codecs* supporting lowest-common-denominator
- *Easy server deployment* crucial — `repro` (SIP proxy) and `ejabberd` are both an order of magnitude easier than deploying a full soft-PBX
- *NAT headaches* must be addressed — ICE/TURN — `resiprocate-turn-server` on Debian (for both SIP and Jabber)
- *Phone spam* must be kept out — TLS — see OpenTelecoms.org TLS notes
- *Legacy* traditions like phone numbers can still be supported — ENUM — see `dlz-ldap-enum` for an instant solution

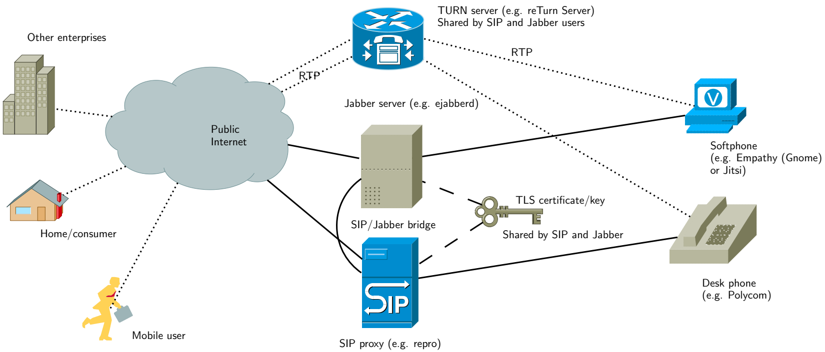
SIP deployment
Architecture diagram



Jabber (XMPP) deployment

Architecture diagram




Other enterprises
Home/consumer
Mobile user
Public
Internet
RTP
TURN server (e.g. reTurn Server)
Shared by SIP and Jabber users
RTP
Jabber server (e.g. ejabberd)
SIP/Jabber bridge
SIP proxy (e.g. repro)
TLS certificate/key
Shared by SIP and Jabber
Softphone
(e.g. Empathy (Gnome)
or Jitsi)
Desk phone
(e.g. Polycom)

Tactics

Must put federated VoIP first

- *Holding on to legacy concepts* like phone numbers has hamstringed VoIP
- *Many Asterisk installations* still use the phone number as the fundamental user identity
- *Lumicall* supports phone numbers with ENUM — but also attacks from the other flank, testing email addresses from the contact book, check for SRV records, offers pure-VoIP on every attempt to call
- *Thinking this way — Federation* — when designing or deploying any of Debian's great VoIP packages is the only way to seize the day
- *Start with SIP proxies and jabber servers* — to enable federation. Add functionality (e.g. Asterisk PBX) in a later phase.

Tactics

Things you can do now

- *If you have a server* — set up a SIP proxy, Jabber server and TURN server.
- *Family and friends* — share a server, domain, TLS certificate
- *IP phones* — a great desk phone. Push regular phones out of your home.
- *Try mobile VoIP* — On Android: Lumicall, CSIPSimple
- *Try softphones* — Empathy and Jitsi
- *Join the mailing list* — ask questions, help others
  - `free-rtc@lists.fsfe.org`
  - `lumicall-users@lists.lumicall.org`
  - `users@jitsi.java.net`

Tactics
Packages to watch

- *SylkServer* — conferencing server for SIP, Jabber and IRC. Alternative to Mumble.
- *Jitsi* — Java-based softphone. Comprehensive support for SIP, Jabber, TURN.
- Both packages are work-in-progress (hint: testing and contributions welcome)

- FOSDEM 2013 — February. Jabber and telephony devrooms, main track speakers, repeat of softphone integration tests
- DebConf13 — August. VoIP track is to be proposed

Useful links

- http://wiki.debian.org/UnifiedCommunications
- http://www.OpenTelecoms.org
- http://www.reSIProcate.org
- http://www.lumicall.org