

VoIP privacy

London CryptoParty 2013

Why?

- Because I don't like the NSA recording when I'm talking to my wife/daughter/dad
- Because in a private conversation, I can be myself
 - You think you don't self-censor?
 - Home vs in front of an audience

First, a little history...

Traditional phone calls

- Landline-to-landline
- Oh, my fair **analog** lines, RIP
- Internet rules all: “Unified Communications” means it all goes over the same wires
- => it’s all tappable.



Mobile phone calls



- GSM is “encrypted” – right?
- But, not end-to-end
- “Legal Interception Capabilities” **mandatory.**
- Also GSM encryption sucks
 - Publicly crackable since 2009

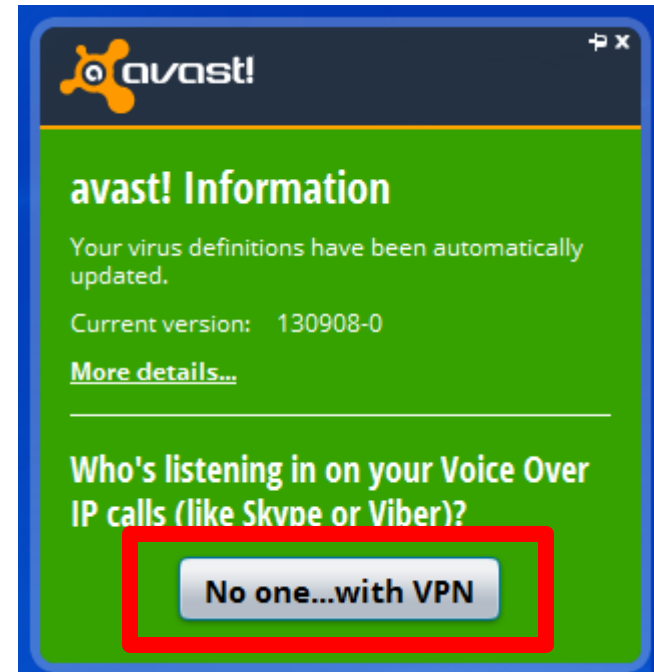
Traditional VoIP

- Promises of “end-to-end encryption” are false
- Provider (Microsoft, Apple etc) can always listen to what you say, record what your camera sees etc.
- ...and they are required to disclose it by law.



“Securing” traditional VoIP with a VPN

- SNAKEOIL ALERT!
- **This cannot be done.**
- Service provider still has full access to your calls.



A note on business models

- Google announced a \$10B revenue.
- With mostly “free” services? How is that possible?
- **We are the product.** Our spending preferences, habits, thoughts, are being sold to marketers. That’s worth *a lot of money*.

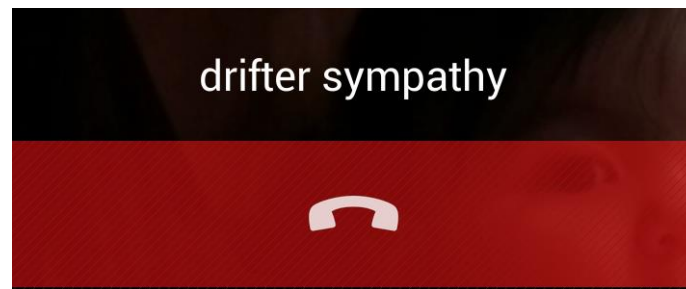
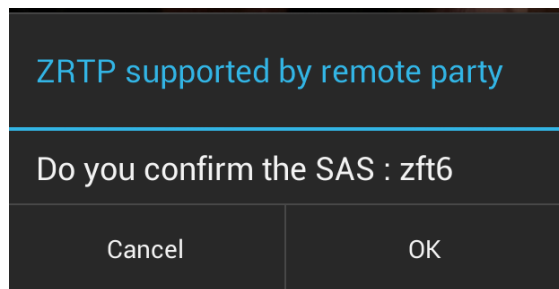
So now...

New-age VoIP: No trust


- Do not trust the network
- Do not trust the service provider
 - remember Hushmail?
- Use end-to-end encryption to verify that nobody else is listening in.

ZRTP

- RFC 6189 by Zimmerman & Callas (ex PGP)
- ZRTP assures that there is nobody listening between you and your partner, as long as you both see the same SAS (Short Authentication String)



ZRTP apps for desktops

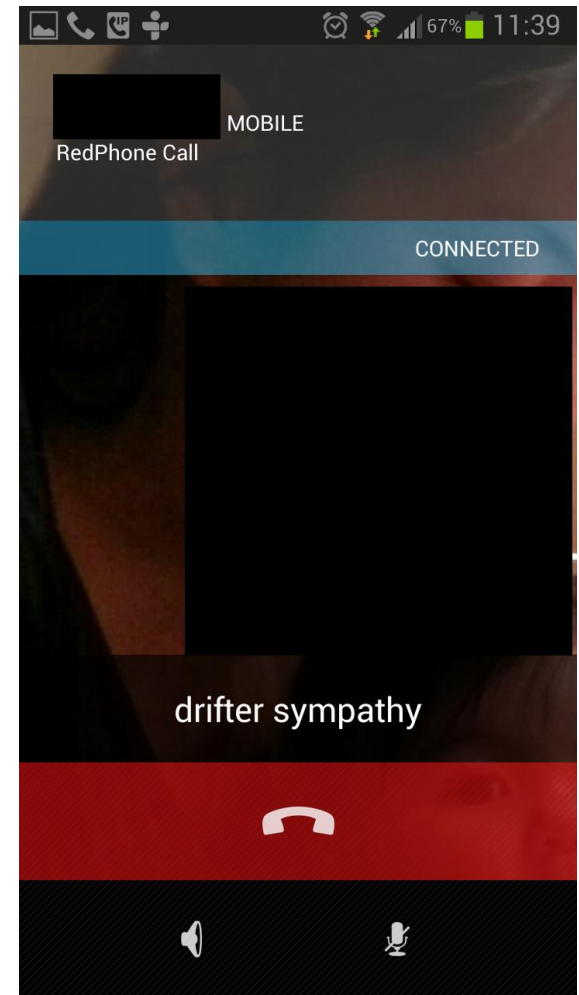
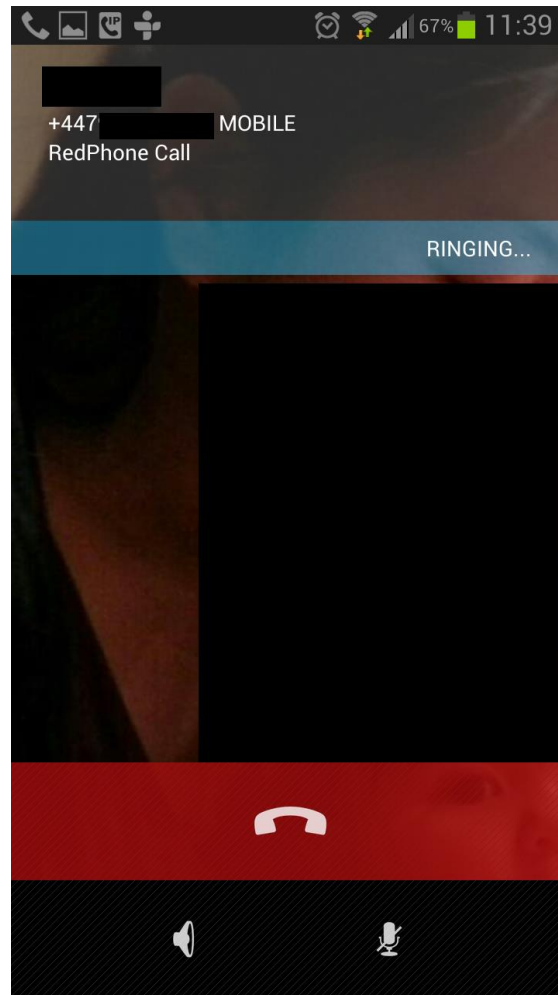
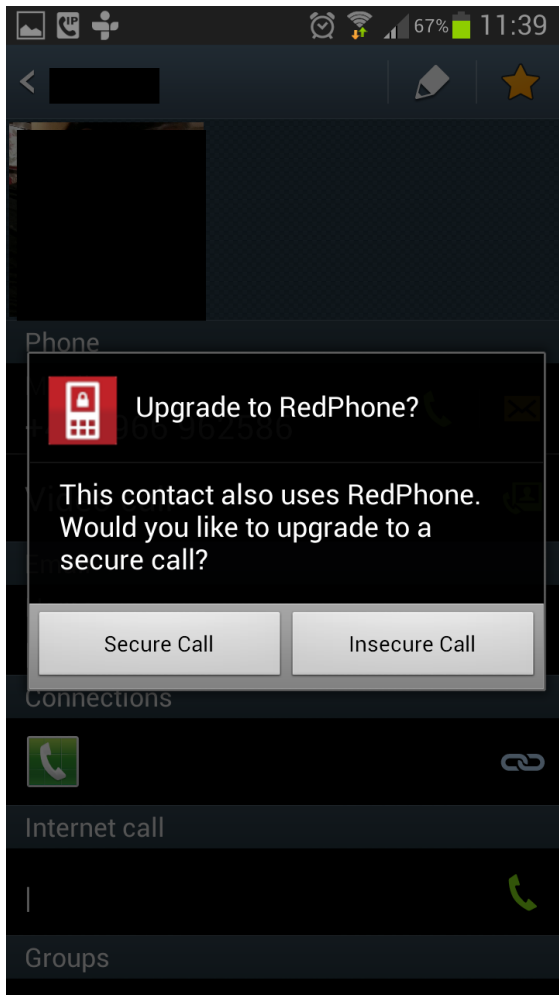
- Jitsi  jitsi.org
 - Runs on anything
 - Combine with an account from <https://ostel.co>
 - Loads of features => complexity
- The Zfone™ Project
 - By Zimmerman himself

Free ZRTP apps for mobile - RedPhone

- **Easy to use**
 - No configuration
 - No new usernames/passwords
- **But**
 - Android only
 - RedPhone-to-RedPhone only



RedPhone in action

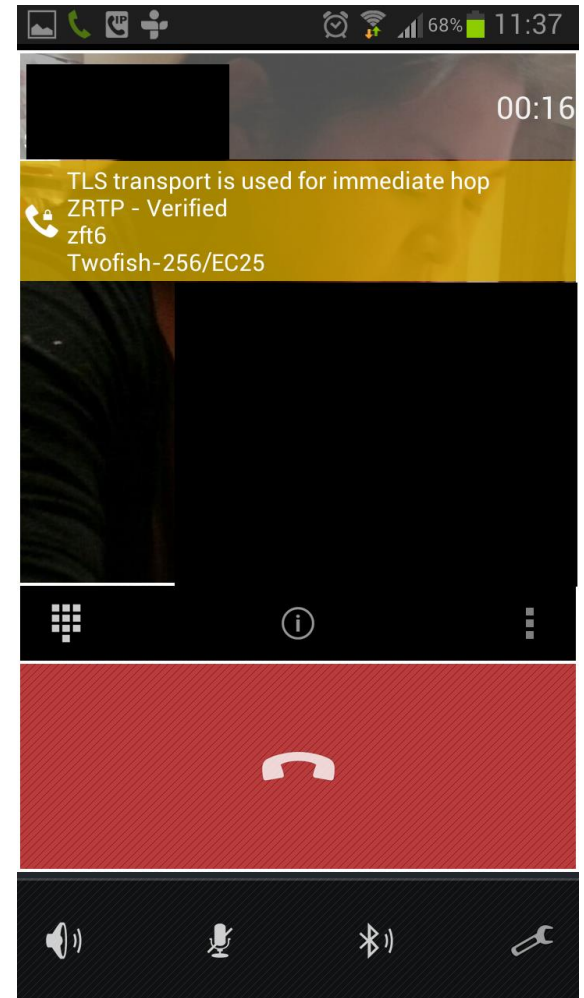
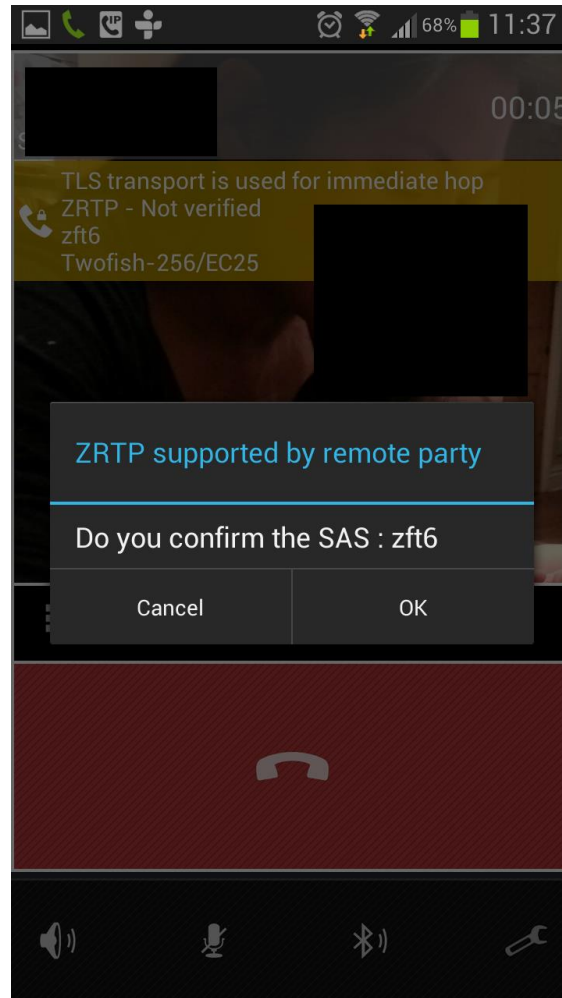
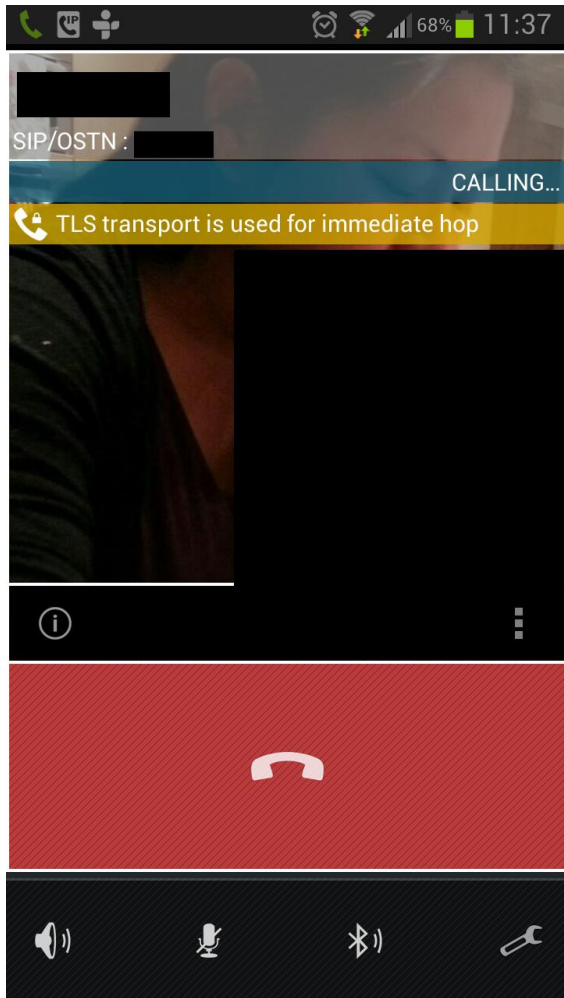


Free ZRTP apps for mobile - csipsimple

- Combine with an account from <https://ostel.co>
- You can talk to anyone who talks SIP (all mobile phones, PCs, Mac, Linux etc)



CsipSimple in action



Commercial ZRTP offerings

- Silent Phone (approx. £70/year)
 - SilentCircle-to-SilentCircle only
- Acrobits SoftPhone (£35)
 - iPhone & Android
 - Combine with account from <https://ostel.co>

It's demo time!

Questions?

A Skype alternative worth its salt: Jitsi

<http://apapadop.wordpress.com/2012/07/05/a-skype-alternative-worth-its-salt-jitsi/>

Continue the discussion at

<http://apapadop.wordpress.com>