IP Telephony Security

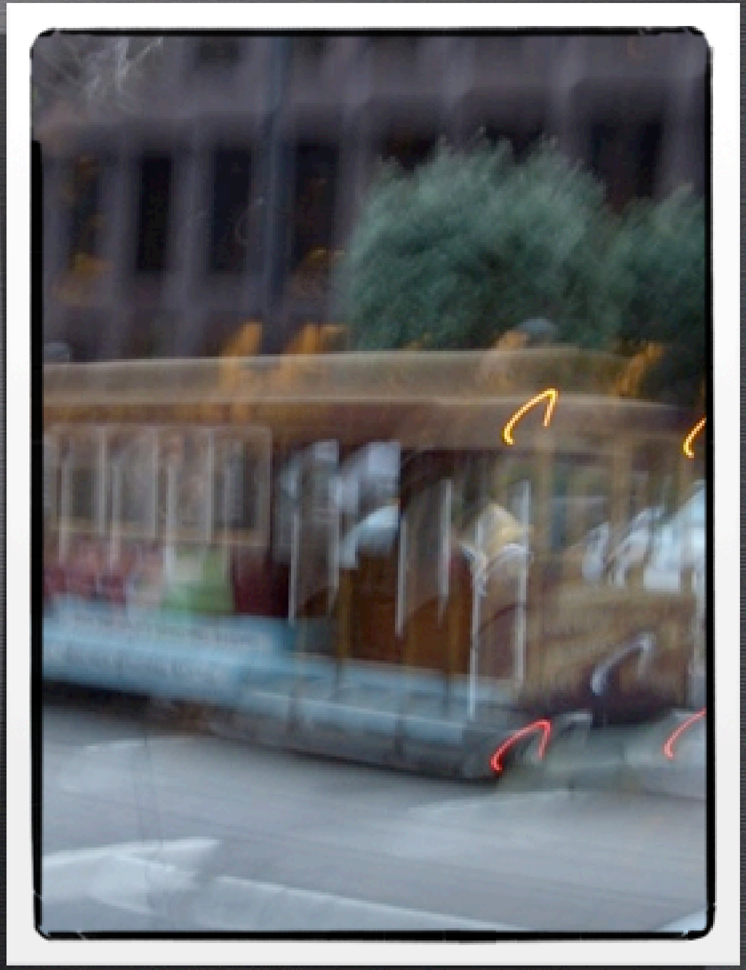
Johan Liseborn
CTO
Hotsip AB

Internetdagarna 2005

Agenda

- What’s this thing called “Security”?
- SPIT and SPIM
- PSTN Heritage
- SIP Security Mechanisms
- Summary

SPIT & SPIM



Definitions

- SPAM - Bulk Unsolicited Messaging
- Call SPAM - SPIT (SPAM for IP Telephony)
- IM SPAM - SPIM (SPAM for Instant Messaging)
- Presence SPAM

Content Filtering

- Analyze the content (e.g. Bayesian filter)
- You have to answer to “see” the content
- Content is sound or video, which is hard to analyze
- Could work for IM spam

Black Lists

- List addresses of spammers
- Easy to forge sender address
- Easy to obtain new addresses

White Lists

- List addresses of valid senders
- Needs strong identity to be effective
- “Introduction” problem
- A “buddy list” is close to a White List

Consent-Based Communication

- Used with White or Black Lists
- Widely used for presence and IM
- Needs strong identity
- Could generate “consent requests” instead of SPAM

Reputation Systems

- Used with White or Black Lists
- Seems to need a certain amount of centralization
- Reputation “mafias” may be a problem
- Might work well together with “Buddy Lists”

Address Obfuscation

- Prevent addresses to be harvested by bots
- Use e.g. “johan (at) hotsip dot com”
- ENUM might give easy access to addresses

Limited Use Addresses

- Use different addresses for different purposes
- Replace addresses that become SPAM-ridden
- Makes it more difficult to reach you (which address should I use? is the address still valid?)
- Presence could help

Turing Tests

- Give the sender a puzzle and see of he can answer
- If answer is correct, the sender is placed on your White List

Computational Puzzles

- Similar to Turing Test
- Force caller to solve an “expensive” puzzle
- Devices have widely varying computational power
- Spammers frequently have extensive computational power in the form of zombies

Payments at Risk

- Caller deposits a small sum when making a call
- If callee accepts the call, the caller is refunded
- Requires cheap micro-payment

Legal Action

- Make SPAM illegal
- Difficult to make it work in an international setting

Circles of Trust

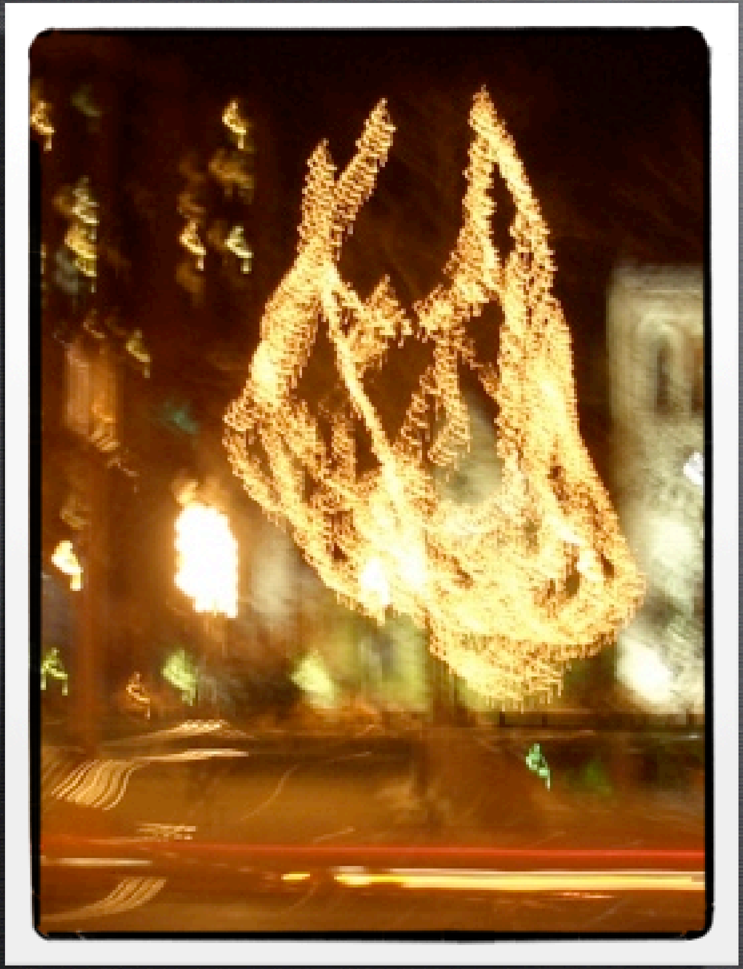
- Agree among a group of domains, not to SPAM
- Introduce a fine if someone breaks the trust
- Requires secure inter-domain authentication (could be TLS)
- Does it scale?

Centralized SIP Providers

- Similar to Circle of Trust
- All SIP providers connect through "inter-domain SIP Providers"
- Trust between inter-domain providers and "local" providers
- Works for the PSTN
- Stark contrast to original idea of SIP

Sender Checks

- Check senders, e.g. through DNS
- Possible also for SIP
- Use of certificates would probably be better for SIP



A bit of PSTN Heritage

Emergency Calling

- ECRIT is dealing with this for the Internet
- There is a requirements document
- There is regional input
- It is still early

Lawful Intercept

- RFC 2804: “The IETF has decided not to consider requirements for wiretapping as part of the process for creating and maintaining IETF standards”
- There are a number of more-or-less vendor specific solutions to LI, including the use of SBCs and/or RFC 3924
- From a SIP signaling perspective, it is not that difficult

SIP Security Mechanisms

- Digest Authentication
- S/MIME
- TLS
- IPSec
- SRTP

Summary

- SPIT and SPIM will become a problem
  - Solution proposals are numerous
- Emergency Calling is being worked on
- Legal intercept is already possible
- There are many other security related issues that we do not have time to cover today

Thank You

Johan Liseborn
johan@hotsip.com
johan@liseborn.se