Internet Telephony

mankin@psg.com Oct 17 2002

- WHAT is our desired outcome for IP telephony standardization?
- Two angles
  - Specific standards development intra-IETF (lead: Allison)
  - Organizations (lead: Jim)
  - Each part has a few slides, discussion
  - Conclusions together

Overview

- IP telephony is largely IETF technology
- Telephants' participation natural, but participants not ready (many young Internet folk too)
- Security and privacy case study of how to move forward

IP Telephony

Non-IETF

- ISUP
- H.323
- MGCP
- Y.???
- vomp

IETF

- RTP/RTCP
- SDP
- SIP
- SIP-ISUP
- ENUM
- CPL, TRIIP
- Seamoby, mobile IP
- Megaco
- Security protocols!
- IPPM metrics
- Diameter, LDAP etc. (so many)

Accept That This Happened

- Firmly standardize our protocols' telephony uses (simply) like any other use
  - If not, it's like two coders having the same function checked out at once
  - cf. draft-tsvarea-sipchange, IESG extensions policy in progress
  - Have discovered there are national variants of SDP by ITU and ANSI groups
- Understand people, specs that come with this

Security and Privacy Case

- Network Asserted Identity in PSTN
  - (draft-sipping-nai-reqs-02.txt)

Trust Domains are constructed by human beings who know the properties of the equipment they are using/deploying. In the simplest case, a Trust Domain is a set of devices with a single owner/operator who can accurately know the behaviour of those devices.

Such simple Trust Domains may be joined into larger Trust Domains by bi-lateral agreements between the owners/operators of the devices.

We say a node is ’trusted’ (with respect to a given Trust Domain) if and only if it is a member of that domain.

We say that a node, A, in the domain is ’trusted by’ a node, B, (or ‘B trusts A') if and only if:

1. there is a secure connection between the nodes, AND
2. B has configuration information indicating that A is member of the Trust Domain.

Understandings

- Authentication never meant cryptography in these specs; authors surprised that this surprised us, given that they wrote:

```
The authentication process used, or at least it’s
reliability/strength, is a known feature of the
Trust Domain
```

- Trust of end-user, equivalence of any node in net, with cryptographic security, is not valid to telephony folks
  - Perhaps our most serious problem in this space

Moving Forward: Goals on Security Stds

- ITU-T Study Groups adopt goals for their protocols compatible with Internet security goals and help us dissipate some of the tensions
- 3GPP adopt requirements matching (ending conflicts with IETF security/privacy
  - This is starting to happen
- Discussion: the end-system trust problem/privacy

Process Forward

- Spend time with PSTN (ITU-T) folks showing need for threat models, as a start
  - Help obtain pressures, decrease in special-casing of industry (e.g. “ss7 firewalls would be anti-cooperative”)
  - IP telephony they want makes them more at risk
- In IETF, engage over conflicting material as we did to understand NAI below its original surface

Other Cases

- Intercept
  - Privacy of end-users – view on much end-to-end security of our protocols by PSTN folks – unusable
  - They argue users will take protection related to unlawful wiretap
- ITU (and others, preface to Jim)
  - A standards reason why line getting a little hard to draw (pun not intended):