STIR Problem Statement

IETF 88 (Vancouver)

Tuesday Session

Jon Peterson

draft-ietf-stir-problem-statement

- -00 issued (after -02 of secure-origins-ps)
- Incorporated comments on previous drafts

- Milestone for this was September…

- So really, let's try to work through whatever else we need today

What's New in -00?

- Added a section about PAI
- Tried to reduce language about certificates and focus on "credentials"
- Removed references to CNIT
- Tried to be less judgmental about SBCs
- Trying to balance in-band and out-of-band

Random Cleanup for -01

- Many nits from Phillipe Fouquart (thanks!)
  - Perhaps some language too US-specific
    - "Certificated"
- Some fixes from Andrew Allen as well
- Adding a ref to RFC5039 (sipping-spam)
- Hadriel wanted some text added about call forwarding scenarios
  - How to differentiate a cut-and-paste from a legit call forward
- Should add some language about texting

VIPR and iMessage

- Been list discussion about these
  - Existence proofs from the deployment world are helpful to articulate the problem
- Proposal is to make iMessage one example among several
  - BB Messenger, Whatsapp, etc
- VIPR is as much a cautionary tale as an existence proof
  - Necessary to understand the privacy edges we need to avoid
- Neither iMessage nor VIPR are STIR solutions
  - But this ain't a solution document
  - They do however have components salient to STIR

Distinctions, distinctions

- Currently problem-statement has definitions of in-band and out-of-band
  - Cannibalized from old “roadmap” section
- However there many hybrid ideas out there
  - Tunneling in-band information in non-SIP protocols
  - Doing out-of-band at gateways rather than at/near endpoints
- A simple proposal: in-band means in SIP
  - Out-of-band means everything else

More Open Issues

- Privacy
  - Preventing attackers from learning what numbers are being called
  - The VIPR Achilles heel – a risk for out-of-band STIR?
- How much message overhead are we willing to tolerate?
  - problem-statement today says “must” stay within UDP bounds
- Be explicit about whether STIR is interdomain or intradomain (or both)?

draft-ietf-stir-threats

- -00 issued
  - Text stripped out of problem statement document
- Received some review and comment

- Deliverable for this is November…
  - (not late yet!)

- Hopefully we're close, here

Overview

- Text broken out from problem-statement into its own draft
- Defines actors, attacks and scenarios
  - Roles of endpoints and intermediaries
  - Attacker can observe and inject traffic
  - Two basic attacks:
    - Voicemail hacking
    - Spam (both voice and text)
  - Several scenarios
    - IP-PSTN, PSTN-PSTN, IP-IP, PSTN-IP, IP-PSTN-IP

Scope of Work

- Assume robocalling can't be "prevented"
  - It can only be detected and policy can block it
- Anonymity is not an attack
  - Some networks don't provide identity
  - We may lose identity in gateways, etc, as well
- Connected identity out of scope
- Assume operators are not attackers
  - Intermediaries modifications are unbounded, and are not attacks
- Much depends on verifiers knowing when to expect identity

What's New

- Helpful reviews from Brian Rosen, Alex Bobotek, Steve Kent
  - Reviewers noted the problems drift into solutioneering from time to time
    - Some facts about the problem space suggest solutions
    - For example, we have persistent relationships with voicemail services, and resulting solution opportunities
- Updated language on "threats" versus "attacks"
- Fixed language about choosing numbers for attacks
  - Are the "valid" or "assignable" or what have you
- Removed countermeasures descriptions that identified solutions

Now what?

- No comments on the new version, yet
- So we’re done, right?
- A few things we could discuss

Some Open Issues

- Biggest TBD: Should this draft include threats against the solutions?
  - Outlines of in-band and out-of-band mechanisms
  - If so, it will deliver late…
- Text message spam
  - Scenario should be IP-PSTN or IP-IP?
- Text about swatting (suggested by Brian)
  - Is CPN spoofing germane to swatting?

Dancing around MitM?

- Question about both threats and problem
- Threats:
  - In call paths with intermediaries and gateways (as described below), there may be no way to provide any assurance in the signaling about participants in the media of a call. In those end-to-end IP environments where such an assurance is possible, it is highly desirable.
- Similar text about support for non-TN identifiers
  - It's not a requirement that we do it, but it's not a requirement that we remove it either