STIR Out-of-Band: Threat or Menace?

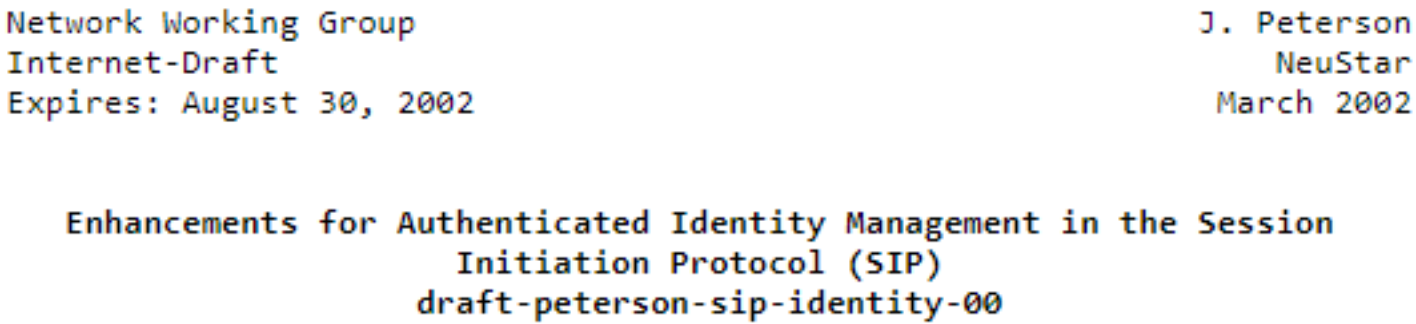
Tuesday, December 3, 2019 9:15 - 9:45 AM

Jon Peterson Fellow, neustar

A Long Time Coming

The basic idea of an authentication service which signs over a subset of a SIP request has been around for a while

- Note RFC3261 issued in June 2002 – it was before then
- Fifteen years ago, SIP adoption was still modest, as was robocalling
- The robocalling epidemic forced us to revisit the problem



Network Working Group — J. Peterson
Internet-Draft — NeuStar
Expires: August 30, 2002 — March 2002

Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)
draft-peterson-sip-identity-00

Great Strides

Much implementation work has been done on AS and VS solutions in the past couple years

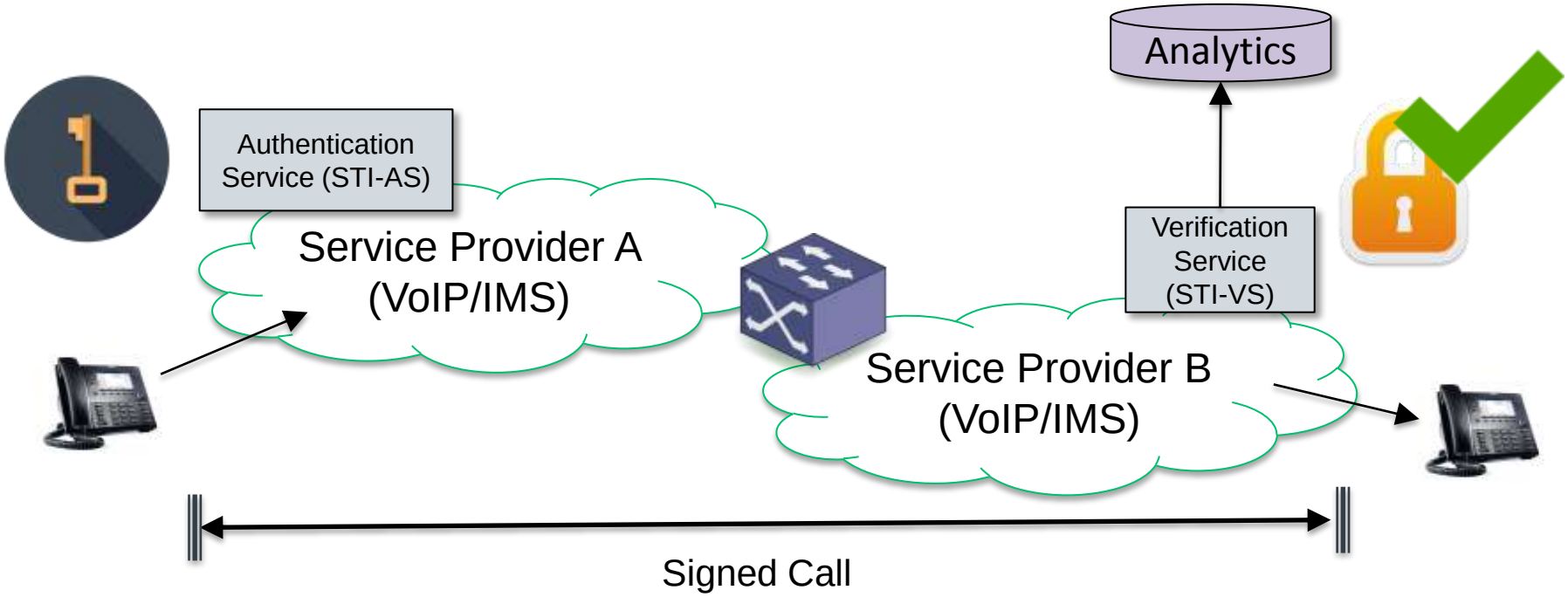
The SHAKEN GA/PA is ramping up, CAs (and real certs) are coming

Legal and regulatory support is growing

So we're done, right?

- Only if we're confident we're putting a big dent in illegal robocalling
- And if we're concerned about that, do we need a fallback?

Where STIR/SHAKEN Works: the IP-NNI



A threat looms on the horizon…

Not all telephone calls go end-to-end over SIP

Exactly how many do?

Why don’t calls go SIP E2E?

There are still plenty of non-SIP PSTN calls

- Yes, there is VoLTE, and SIP trunking, and residential carrier VoIP
- But outside the IP-NNI, a lot of lingering POTS and non-VoIP mobile

Not all VoIP calls are SIP calls

- Still a lot of proprietary protocols, or integrated VoIP applications
  - Not all calling methods even use telephone numbers

Not all SIP calls actually begin or end with SIP

- Even if they do, what lives in the middle?
  - Many IMS networks remain highly mediated, and SBCs are everywhere
  - But there is a bigger problem still…

The Real Problem: the DFZ

Term from Internet routing, the “default-free zone”

- Usually when you route a packet, you have a default place to send it, an upstream provider
- But when there are no more upstreams, just peering, you hit the default-free zone

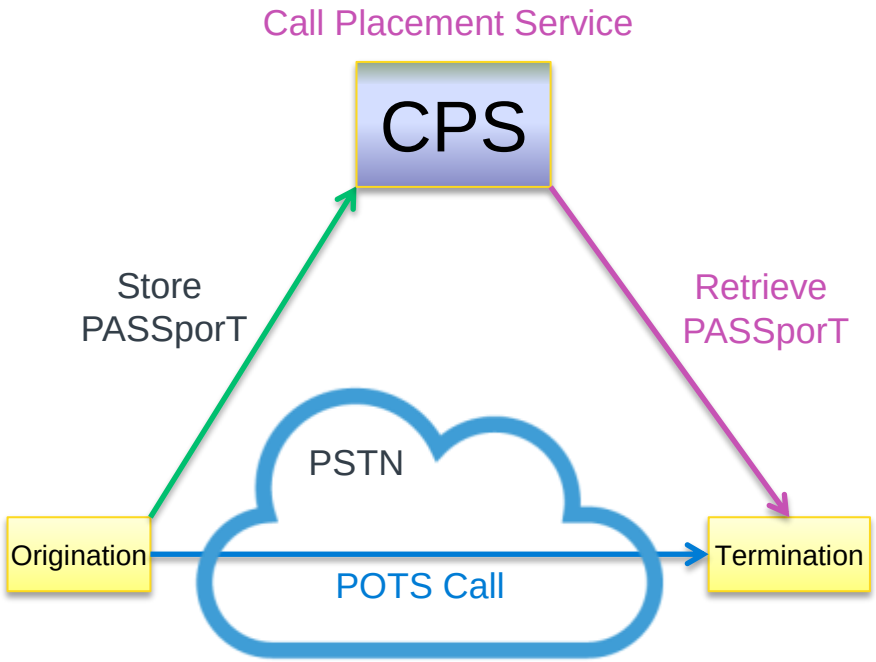
Telephone call routing on the Internet has its own DFZ: it’s called the PSTN

- When you don’t know how to route a number any further, you drop it to the PSTN
- But then you lose all the advanced features of the IP world – including STIR/SHAKEN

The irony is that the originating and terminating side often have IP connectivity, just not a way to leverage it for these orphan calls

- Maybe there’s a simpler problem than call routing to be solved

STIR Out-of-Band



Could be any sort of device storing and retrieving PASSporTs

Does OOB work?

Basically, yes, it's not that complicated

- OOB is just a surrogate for a rendezvous protocol
- Substitutes the problem of routing a call for storing the PASSporT to a cloud service
  - It is a more tractable problem because it lets the two ends meet halfway
  - Also because it leaves carrier policy enforcement to the actual call path

The tough part is security

- More work in some environments than others

But on security, there is nothing magical about attaching a PASSporT to an INVITE

- Cut and paste attacks using that PASSporT are just as available to eavesdroppers on SIP as on a CPS
- Security environment is not as dissimilar as it might look – in some ways, OOB may be better

Flavors of OOB

There has been some talk about a “**public option**” for OOB

- Making a federation of public CPS’s discoverable
  - There are workable approaches to that: bootstrapping from credentials is my favorite
- Difficult threat environment, however
  - Tough to manage who can store and retrieve PASSporTs, and to prevent passive monitoring of calls
  - Requires encryption, which adds no small complexity to STIR

Also, there has been some work towards “**private**” CPS deployment

- Sort of an intradomain overlay network over PSTN calling
  - Some code on both the originating and terminating side is controlled by a single domain
- Does not require a discovery process, security requirements are less stringent
- Motivated by enterprise fraud requirements, branded call display, and so on

Beyond the DFZ

The lack of end-to-end SIP traffic is the ultimate motivation for OOB

Can we fix it?

- Having public TN routing databases would be a good first step
- ENUM, and the more recent MODERN project, would be candidates
  - But public ENUM never took off, and private deployments thrive

More importantly, the full “IP transition” requires a lot of infrastructure upgrades

- They are both costly and time-consuming to deploy
- Unclear where that money and time will come from

Perhaps best to view OOB as a stopgap for environments where the IP transition is prohibitively difficult

- It is certainly easier to do, and less expensive

In the Standards

The OOB framework is on the IETF ballot this Thursday to go to RFC

- Really more of an architecture document than a protocol specification – some assembly required

Future work will focus on more concrete deployments

- Likely that “intradomain overlays” are the low-hanging fruit
- Still plenty of questions: should the retrieval be a push or pull function, say

If there’s a will for it, we can do a public OOB specification as well

- Not necessarily incompatible with SHAKEN or its assumptions
- Originally OOB was called “fallback” and was intended to be used in concert with in-band
  - There are strategies along those lines we could explore, if people wanted to
    - Think of it like a safety net, just in case your call gets caught in the DFZ

Which is the real menace?

Out-of-Band will go away as soon as E2E SIP calls are universal

So… when is that?