Connected Identity for STIR

• Good ol’ RFC4474 only worked for requests
  – Identity header not in responses: what authorization decision can you make about a response?
    • You can’t answer a 200 with a 403
  – John Elway wrote RFC4916 back in the day
  – Now we have RFC8224... also just for requests

• Responses really not in the RFC7340 threat model
  – Robocalling, voicemail hacking,

• But is there actually a callee impersonation problem?
  – Unfortunately, yes
  – Various hijacking attacks and vishing attacks
  – And the work we’re doing here could be applied to it
STIR Backwards

Did I actually reach the bank?
The big questions

• **What can we do to prepare before the call starts?**
  – Easy to imagine discovering keys, determining what security services are available offline before a call is placed
    • Especially for destinations in an address book
    • Could help to know when you need to fail the call

• **What will we use the results for?**
  – Authorization decisions about sending/receiving media
  – An approach: treat it like negotiating SRTP, in how failure is handled

• **What kind of user experience can we offer?**
  – Right now when you place a call you don’t always look at a display during alerting
    • Unlike the Caller ID case where users look at a display to decide how to answer
  – We won’t dictate a user experience, but we’ll at least provide cues it could follow
How Much of an Update?

• Generally, RFC4916 is still on the right page here
  – Lots of text about Identity-Info would no longer apply, obviously
  – Back in 2016, Adam identified one more piece of normative behavior we should fix in 4916
    • Relates to the re-sending mechanism we hacked into RFC8224 for compact form failures

• Big idea is the same: use an UPDATE request in the backwards direction while the dialog is being formed
  – Sign it with RFC8224, let the PASSporT reflect the connected identity in the “orig”
Next Steps

• Reasonable idea?
  – Useful for sipbrandy as well, if anyone uses it...

• If so, we’ll do some more work

• Later, adopt, milestone, etc.