Minutes - STIR Working Group at Virtual IETF 111

Summary

Rich Call Data PASSporT type

Chris Wendt presented an update on draft-ietf-stir-passport-rcd. It's currently on version 12. The updated integrity mechanism in version 10 has gotten good feedback. The draft has in general gotten quite a bit of discussion and implementation. The draft will go to WGLC shortly (The WGLC has since been announced and ends 19 August 2021)

STIR Interoperability Event

The chairs asked if people thought we were ready for a STIR interperability event. Interested parties should send email to the STIR list.

STIR for Messaging

Jon Peterson led discussion on using STIR for messaging (draft-ietf-stir-messaging). He noted the draft comprises two paths: Message sessions established with SIP, and individual messages sent via the SIP MESSAGE method.

People discussed whether it was acceptable to integrity protect the entire message MIME body as opposed to something more narrow. People included this was probably okay, but we need to do more homework. There was extensive discussion of the impact of message conferencing. More work is needed here. Next steps include those items, privacy considerations, and possibly more security considerations. More review is welcome. Jon thinks it will be ready for WGLC after a couple of more iterations.

Connected Identity

Jon Peterson led discussion on connected identity (draft-peterson-stir-rfc4916-update-04). The Internet-Draft adds identity headers for SIP responses. This version fleshed out pre-call scenarios with medialess dialogs to learn where a particular call will be routed. People discussed potential privacy issues, which could be mitigated by establishing pre-call dialogs anonymously. Directories for entites that want to advertise that they are responsible for a number would be complementary, but out of scope.

Jon proposed that centralized conferencing should be out-of-scope, and that decentralized conferencing would come for free. People noted that it would be useful to at least learn the identity of a converence service.

Jon proposed adoption, but noted a recharter would be needed. There was discussion of whether this should formerly update or obsolete RFC 4916, with a conclusion that we would worry about that later.

Potential Recharter

Jon has discussed potential new charter language with the chairs. The proposed changes would clarify development and maintenance of the core STIR RFCs and add work on extensions related to using STIR in a telephone number enviroment for security and and fraud-prevention purposes. If needed, we could discuss expanding the focus to non-telephone-number cases.

The discussion was cut short due to time constraints. The chairs will discuss with the area directors and on the STIR mailing list.

Identity Header Error Handling

The topic was deferred due to lack of time.

Detailed Notes

1. Administrivia
    - Agenda Bashing
    - Minute Taker
    - Jabber Scribe
    - Bluesheets

Adding potential charter update to the agenda. Jon does not plan to cover servprovider-oob, removed from agenda.

2. PASSporT Extension for Rich Call Data
    - Chris Wendt and Jon Peterson
    - draft-ietf-stir-passport-rcd
    - Resolve open issues from WG Last Call

Chris presents the version 11. He thinks it is getting close to done. Has gotten good feedback on updates to the integrity mechanism in v10.

Clarified "iss" subject identification, stated that the Subject Name field contents is out of scope for this document, and left to certificate governance policies and other specs.

Has had lots of industry discussion, implementation, and feedback. Ready for WGLC? Has not updated SIPCORE doc yet, but doesn't expect changes there. Will ask on SIPCORE list.

No one speaks against WGLC.

Robert Sparks: Do we have critical mass for interop event?

- CW: suspects so. Should ask people to commit.
- RjS: Can this be virtual on the public internet? Would be easier to setup if everyone does not need to be on same layer 2 network.
- RjS: Please send mail to the list to express interest.

3. Secure Reporting of Update Status
    - Jon Peterson
    - draft-ietf-stir-servprovider-oob
    - Prepare for WG Last Call

[Removed from agenda]

4. Messaging Use Cases and Extensions for STIR
    - Jon Peterson and Chris Wendt
    - draft-ietf-stir-messaging
    - Recently adopted; progress toward WG Last Call

Jon is in the middle of moving. Draft is now a wg item.

Two paths: 1) SDP Negotiated message stream security (session mode). Aimed at RCS and RTT like deployments. Esentially get that for free with STIR identity header. 2) Individual message security. Protect at MIME level.

Is it okay to have integrity protection over entire MIME body? Should it be more narrow?

- Ben Campbell: RFC 8591 section 9.1 talks about signatures with CPIM envelopes. May apply to some systems that use some CPIM metadata. Need to think about whether that applies here and how.
- Jon: For both paths, or just sessions?
- Ben: Probably mostly for sessions, but not sure.
- Jon: Can reference 8591.
- Jon: Should talk to GSMA about CPIM usage in RCS impact. Not sure if it needs formal LS. Jon knows people in GSMA to talk to.
- Jon: Doesn't think there's a lot of multi-part-ish things in messaging. Does anyone else?
- Brian Rosen: Some emergency messaging use multiple body parts. E.g. location and messages. Messages are only one part. Not sure if signature over entire body is a problem.
- Jon: Is it a problem protecting both location and message? Is that a feature or bug?
- Brian: Might be a feature.

Conclusion: Comfortable with protecting entire MIME body, but have homework to do to make sure it doesn't break anybody.

Added some text on RTT, meaning of end-to-end (inheriting constraints from SIPBRANDY)
Removed some TBDs, added some security consideratios, probably need more.

Probably need some privacy considrations. Jon doesn't think just adding a digest is a problem, but wants to think about it. Think about archiving of passports, exposing message content to signing oracle, etc.

Open issues:

conferencing/multi party messages. Proposes this be punted to connected-identity draft for path 1 (sessions). Depends on conferencing strategy. Centralized vs decentralized. Thinks RCS uses centralized. Need connected-identity for session establishment anyeay.
Thinks things just work for path 2 (MESSAGE), just send signed messages to right place. Might depend on

exploder location (inside vs outside AS).

- Chris Wendt: PASSporT does have multiple destination array capability. Not sure if it works here. Something to think about.
- Jon: Questions about whether an exploder may need to be able to sign across multiple domains.
- Jon: That might help with path 2. AS just needs to see dest list. Has authority for the identify of the sender of each individual thing.
- Jon: Gets harrier with an exploder, depending on where it is relative to AS. AS needs to be able to sign the identity of a sender of a message to someone in the group.
- Jon: These are important considerations for path 2. Needs to be minuted. An exploder may need to be behind AS that signs for a UE. Complicated for multiuser chats.
- Chris: Do you assume the sender knows all the recipients, or is that in the conferencing part?
- Jon: We have to worry about centralized vs decentralized conferencing for path 2. In decentralized, the UE knows the chat list. Should work fine. For centralized/exploder cases, could get hairy. Guests will fail if the sender doesn't know them.
- Roman: matching may be issue. In cases where you send to an group ID at exploder that explodes to a group, the sender may not know who all is in the group, but the recipient knows what number it needs to accept and match. Might be another consideration.
- Jon: Could use div. Show conversion between the destination as a group ID and the actual group of destination numbers.
- Roman: What about scenarios where sender is hidden. sending party verified but needs to be hidden. Some messaging is end-to-end, unlike most voice calls. May disclose personal information when all we should disclose is that the identity is verified.
- Jon: Depends on who does it. If UE, can probably use tranditional anonymization techniques. Stuff in 8224 about that. If exploder needs to conceal identites, there you are basicly in centralized conference. Should be using things like sip-event packages to notify sender what is going on.
- Roman: Consider impact on message size and added complexity for path 2.
- Jon: Wants people like Brian Rosen who worry about message size for emergency services to think about this.
- Paul Kyzivat: Is there really different between exploders and call forwarding for normal calls?
- Jon: That's why div might be the answer. Basically sending to a pseudonumber/chat ID at exploder, which then forewards to list. Can treat like call forwarding. Doesn't think anything in div prevents using it like this.
- Jon:Seeing div in production. May be other ways to do it that doesn't require using div. Depends on how you implement chat and where the conference is deployed compared to AS and VS.
- Brian Rosen: Vast majority of exploders are just customers of carriers. You just send to a phone number. 99.9% of cases already covered.
- Jon: Carriers want to be able to manage size of group, assert policy. Need to go through some sort of policy enforcement. But these are corner cases.

Next steps: Need to finish open issues, more work on conferencing. Had some reviews, more welcome. Not complicated document. Expects WGLC after one or two revs. Most of what we want to say will just sort of work.

- Ben: Is it time to think about identifiers that don't look like phone numbers. Email addresses, short codes, etc.
- Jon: Works for sip-like identifiers. 8224 not TN specific. Concerned about that email gateways are a slipery

slope--interactions with things like DKIM. Would rather not push a lot of email things into stir. Email mechanisms not aimed at end-to-end.
- Ben: short codes
- Jon: Short codes are like TNs. Managed in registries. Special cases of TNS. Not concerned with signing them. Thinks 10DLC messaging is getting more traction for enterprise use cases. Email is a different problem.
- Chris: The SHAKEN passport PKI is TN focused. May need to consider these things during recharder discussion.
- Jon: A lot of what SHAKEN accomplishs is the GA/PA, decides who should get credentials. Question of whether SHAKEN end-points will be willing to trust signatures with Verisign certs from someone like Apple. Complicated GA discussion. Doesn't think outcome for IETF is that we need a new set of CAs for email-like identifiers. Already have those.
- Chris: Regulated world vs unregulated world.
- Jon: Will talk about this during recharter discussion.

5. Connected Identity for STIR
    - Jon Peterson and Chris Wendt
    - draft-peterson-stir-rfc4916-update
    - Discuss open issues; get ready for WG call for adoption

Adding identity header on responses. Motivated by fraud scenarios, e.g. fraud alert in text message asking one to call a number. route hijacking, short-stopping, etc. Needed by SIPBRANDY. Not part of original threat model for STIR.

New version mostly cleanup. Mostly parked. Fleshed out info for pre-call scenarios. Medialess dialog. Can elevate to voice session if you decide called-party is legit. Demand for high-risk industries. Medical, financial, etc.

- RjS: Establish dialog with random number foo to see if it returns an identity you are willing to talk to? (Yes). May be used as liveness checks. May be concequences of poking bad guy. Need to document privacy consideration.
- Jon: Agrees there is a privacy dimension we should talk about.
- Roman: Some (e.g. financial, medical) scenarios require you to start talking with someone within a fixed period of time.
- Jon: Not really thinking about emergency scenarios. More for things like IRS scams. Non emergency scenarios. Assumes RCD is properly managed.
- Roman: Thinking about cases like HIPPA where you need to verify who you are talking to before disclosing info. But need to start talking before some time has expired.
- Jon: Proposing preflight checks. Phone wouldn't alert.
- Brian: Need to document case of placing anonymous call, getting connected ID back, placing reinvite with caller identity and media. E.g. Banks are probably willing to respond to a medialess anonymous call.
- Jon: Make sure that is minuted.
- Robert: Thinks we are talking about offering a service to say who is the legitimate user of a number. Setup dialog with full dialog mechanics where callee decides whether to admit to being responsible for number. Proposes a different mechanism for people who are *always* responsbible for the number.

- Jon: Thinking about something like a directory service for things like that. Back of mind. But looking for property of checking what would really happen if you place a call. Draft works without the directory but better with the directory.
- RjS: Highlight the real-time factor. What happens if call is routed right now.
- Jon: Yes. thinking about route hijacking attacks. Better with directory, but the directory is out of scope for this draft.
- Norbett Angell: (no audio)
- Jonathan Lennox: Norbett said he will send email. Brief discussion in chat--unless you are an institution or something, don't send RCD back for connected identity. Otherwise someone can war-dial identity checks to build up a directory.
- Jon: Aimed more at institutions. There is text on anonymity of responses. Don't want to enable wardialing.

Added text to think about conferencing, based on stuff considered for messaging draft. Suggests declaring centralized conferencing out-of-scope. Secured separately (e.g. sip-events) Get decentralized for free.

- Jonathan Lennox: There is a benefit from getting connected-id for conference bridge itself.
- Brian Rosen: Agrees. Would like to get the RCD from conference bridge. E.g. having confidential discussion over bridge, wants to know he has reached the bridge. Not worried about rosters, etc.
- Jon: Will try to get away with leaving conferencing out of scope.

Todos: Revise examples, any normative revisions to 4916, flesh out pre-call approach.

Should this be treated as a bis document? (4916bis?) Currently thinking it is not a bis.

- RjS: Seems like different usage. Not trying to change what 4916 says. Not asking 4916 implementations to change. Probably not even an UPDATES header.
- Brian Rosen: Contrarian view. 8224 obsoleted 4474. Aren't we doing the same thing? No use case for original 4916 if 4474 is obsolete.
- Jon related to gendispatch discussion.
- RjS: Deck chairs at this point.
- Jon: Believes 4916 really is effectively obsolete. No concerns making that official. Leave to ADs to figure out.
- Murray (AD): No preference. Does it matter if we obsolete 4916 without a replacement?
- Jon: This is not yet a wg item. Kick the can forward.

Next steps: Work to do. Adopt, pending recharter? Jon Thinks we should adopt, but that adopting requires a recharter. Proposes adding maintenance and extensions related to identity for telephone numbers to charter.

Jon has proposed a charter revision to chairs. Removed some aspirational parts that are done. Clarify dev and maint of 8224-8226. Consider extensions to leverage STIR for telephone calls and other TN based communication. Diversion, forwarding, rich identity presentation, messaging using TNs, etc. Connected identity and similar use cases related to fraud and security. If we want to ditch the TN-based part, we should discuss. Expands problem statement scope of STIR.

- RjS: Out of time. Will work with Murray and go to list. If anyone hates this speak now. RjS apologizes to Chris for not getting to the error handling topic.

6. Identity Header Error Handling

    - Chris Wendt
    - draft-wendt-stir-identity-header-errors-handling
    - Discuss open issues; get ready for WG call for adoption
7. Any Other Business (if time permits)