Minutes - STIR - IETF 110

Friday, 2020-11-20 at 15:30 UTC

Summary:

- STIR Certificate Delegation (draft-ietf-stir-cert-delegation): The document is with the IESG, and a recent revision was posted to address issues raised by IESG Evaluation. No one raised concerns with the changes.
- PASSporT Extension for Rich Call Data (draft-ietf-stir-passport-rcd): Several concerns were raised during WG Last Call, and the document was revised to address them. A hash value provides integrity for the whole jCard structure, and then a hash value for the content associated with each URL in the JSON-pointer-like structure. This is a significant change, so WG Last Call will be repeated.
- Out-of-Band STIR for Service Providers (draft-ietf-stir-servprovider-oob): A quick status was provided. More work is needed to get the document in shape for WG Last Call.
- Enhanced JWT Claim Constraints for STIR Certificates (draft-ietf-stir-enhance-rfc8226): The enhancements are straightforward, and the document is ready for WG Last Call.
- Messaging Use Cases and Extensions for STIR (draft-peterson-stir-messaging): There was a lot of interest in providing PASSporT authentication for the source of a text message. To provide integrity of the messages, a MIME-level security mechanism will be used. When TLS is used, it provides hop-by-hop integrity, but the MILE-level protection will be end-to-end. A WG call for adoption will take place shortly after IETF 110.
- Connected Identity for STIR (draft-peterson-stir-rfc4916-update): This document provides a PASSporT for the terminating telephone number for a call. With call forwarding and other mechanisms that can redirect a call, this is a very attractive capability. A re-charter will be needed to take on this work.

--- Raw Notes (from codimd) ---

STIR Working Group at Virtual IETF 110

Jabber: xmpp:stir@jabber.ietf.org?join
MeetEcho: https://www.meetecho.com/ietf110/stir
Notes: https://codimd.ietf.org/notes-ietf-110-stir

1) Administrivia

- Minute Taker - Jean Mahoney
- Jabber Scribe
- Bluesheets

- Agenda Bashing

Russ - If we don't get to everything, we'll schedule an interim.

2) STIR Certificate Delegation

- Jon Peterson
- draft-ietf-stir-cert-delegation
- Discuss issues raised by IESG Evaluation

Slides presented.

3) Assertion Values for a Resource Priority Header Claim and a SIP

Priority Header Claim in Support of Emergency Services Networks

- Chris Wendt and Martin Dolly
- draft-ietf-stir-rph-emergency-services
- Discuss issues raised by IESG Evaluation

Just went into the RFC Editor's queue.

4) PASSporT Extension for Rich Call Data

- Chris Wendt and Jon Peterson
- draft-ietf-stir-passport-rcd
- Discuss issues raised by WG Last Call

slide 3: sipcore-callinfo-rcd-02
See if you have any feedback on the new MUST for URI usage.

slide 7: "rcdi" claim extension - example
Would like comments on the extension to the JSON pointer.

Jon - if there's ambiguity or reordering, but that first line is a sufficient guarantee. Given the limited scope, should work ok.

Russ - 1st line required, others are optional?

Chris - yes, but I'll doublecheck.

Russ - the 1st line is a hash of the structure itself.

Chris - ...

Jon - this is secure.

Russ - seems fine to me.

Brian - JSON path (like xpath) has a lot more expressiveness, but don't remember if it would accomplish this, but you might want to look at it. JSON pointer is simpler.

Jon - it would nice if the keys could refer to "logo" etc, I think this is sufficient though.

slide 8: RCD integrity modes

Jon - the jwt constraints - you put them in the bucket, could you mix them up? The lexical ordering helps. Far as I can tell, it works.

Chris - it's the digest of the jcard claims itself.

slide 9: Questions?

Chris - this is substantive change.

Russ - we should redo WGLC. Is it ready for that?

Chris - I'll share this more broadly.

Russ - Next week will do a WGLC in STIR

Jack Rickard - iss claim - it MUST reflect the subject name of the certificate? "reflect" is vague.

Jon - we need to sort this out, has to be compatible for ATIS, what component? Who vets those?

Jack - can't really use it.

Chris - you need to be authorized to have a certificate.

Jon - want it to be not too prescriptive

5) Secure Reporting of Update Status

- Jon Peterson
- draft-ietf-stir-servprovider-oob
- Discuss open issues; get ready for WG Last Call

Slides presented.

6) Enhanced JWT Claim Constraints for STIR Certificates

- Russ Housley
- draft-ietf-stir-enhance-rfc8226
- Discuss open issues; get ready for WG Last Call

Is it ready for WGLC?

Jon, Chris - yes

Robert to confirm on list.

7) Messaging Use Cases and Extensions for STIR

- Jon Peterson and Chris Wendt
- draft-peterson-stir-messaging
- Discuss issues raised by WG call for adoption

slide 3: Is there really a problem?

Brian - I want it. I want it for 911

Ben Campbell - I support, there's bigger usecases - real messages are trusted - TFA

slide 4: Is it in scope of STIR?

Eric Rescorla - How would you scope the problem?

Jon - at full suite security at SIP. I'm not sure what the creep is.

Eric - I'm not worried about whether it's in scope for the WG, we can handle that.

Chris - This applies to the message came from this number, not beyond that.

Jon - Chairs, how do you want to do the check on whether this is in scope?

Robert - I think we just proceed. I'm not hearing dissent and concern.

slide 5: Integrity over messages

Jon - let's just do MIME-level security.

Russ - Ben agreed in chat, I agree also.

Brian - I would like it to work for URI, ... the geolocation case.

Christer - transport of MSRP over data channels - may not have impact, but keep in mind.

Jon - the message mime mode and the normal STIR mode. Anything we're negotiating with srtp...Are you not using TLS at all?

Christer - you are

Jon - it should work with mky then.

Chris - the mkey is for data channel or msrp?

Jon - if it's dtls, it should work okay.

Ben - too deep in the details for this part of the discussion. TLS is not E2E.

Jon - SIP brandy was supposed to get as close to E2E as possible.

Ben - things like message stores, I don't know the answer. Is mkey is security TLS or object-level security.

Jon - need assurance between VS and AS.

slide 6: Next steps

Jon - should we adopt? Chairs?

Russ - we will do that next week on the list. If you want to speak against the WG adopting, say so now.

8) Connected Identity for STIR

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

Jon - do we want to adopt?

Russ - Murray, do you have thoughts about the re-charter?

Murray - I'm happy to help you recharter, I'm not worried about this terribly.

Robert - Who in the room will put effort into exploring the problem.

Russ - several people in the chat have said this is good.

Jack (in chat) - not sure it's needed

Russ - not hearing anyone speak against.

Russ - we need to stop, continue on the list, and we'll be having an interim.

Rest of the items below not covered in meeting

9) Identity Header Error Handling

- Chris Wendt
- draft-wendt-stir-identity-header-errors-handling
- Discuss open issues; get ready for WG call for adoption

10) Any Other Business (if time permits)