Minutes for CFRG at Virtual IETF 111

RG Chairs:

- Alexey Melnikov alexey.melnikov@isode.com
- Nick Sullivan nick@cloudflare.com
- Stanislav Smyshlyaev smyshsv@gmail.com

- Thanks to Rich Salz for taking notes!

Agenda

No changes.

CFRG Update

Many documents in progress; see the slides.

Three errata verified; eight still to be verified.

New KEMs and AEADs for HPKE (Dan Harkins)

Problem: serialized public keys are more than twice as big as needed. Use "compact serialization" (per RFC 6090). Also it assumes guaranteed in-order delivery else tragedy.

Proposal: keep API (users not managing nonce is good, for example). So need deterministic authenticated encryption (DAE) cipher mode. See slides for paper reference including proof. This just *adds* things to HPKE, no changes.

CJPatton: Concerned about different code points providing different security guarantees to user. Does this push the AAD-uniqueness to the user.

Dan: Trying to make HPKE useful in a lossy network.

DKG: Requiring something "new" in each message seems very much like the nonce uniqueness that you don't like.

MT: Agree with dkg, this seems more dangerous than useful.

Further discussion on the list.

A “Duck Test” for End-to-End Secure Messaging (Alec Muffet)

Thesis: intuitive understands of E2EE is no longer politically sufficient. If you want something to *not* change, you must be able to measure it (riff off Drucker, etc.) Organizations looking to change include Unicef, GCHG “ghost” proposal, Indian government. All proposals say “this doesn’t break E2E security.” How can we tell?

Knodel document uses algorithms, etc. It proposes things in terms of user expectations.

This document talks about *messaging* and definition of end-to-end. Recipient isn’t protocol endpoint, but anyone who can see the message. If recipient was not known/visible to sender at time of creation, then E2EE isn’t there. Backdoor is also defined. Now surveillance orgs are *visible*

Eight nits pointed out; see the slides.

Desired next steps: adoption, work on it, and ship it as an RFC that provides *a* test, not *the* test.

Matthew Finkel: maybe we need a new term, or expand this to mean encryption. MT agrees.

Alec: I want to keep the scope well-defined.

MT: I think this should be IETF standard.

Alec: I think this fits right into the CFRG charter, but whatever.

dkg: E2EE is common term, we should use it.

Alec: Open to that.

VOPRFs (Armando Faz; Sofia Celi)

if “y=PRF(k,x)” Client learns y not k. Server learns nothing of x or y. (k is server private key; x is client input)

New: Blinding. Explicit errors. SHAKE-256 for decaf448. (which is not an HTML hex entity :).

New: Adding public metadata. Much math. Some considerations needed.

OPAQUE (Chris Wood)

Major changes: internal and external modes for key storage. Mitigations for client enumeration attacks (does this username exist on the server?), and “fake” test

vectors to test that code path. Replace app info with shared context string (like SPAKE2+) so all protocol messages are fixed-length.

Minor changes: text in security considerations, and other editorial improvements. Aligned with VOPRF draft.

Have many implementations; want more. Want Crypto Review Panel to (sic) review. After that, ready to ship.

Stanislav asked for some clarification about the enumeration attacks and trust boundary.

RSA blind signatures (Chris Wood)

Updates: Added recommendation to use deterministic signature, a test vector, and API considerations. Improved security section, editorial cleanup. More implementations.

Open questions: should we change the name? Should the draft support partially blind signatures? Add other signature schemes?

Read for RGLC?

Stanislav: Would like to see more review.

DKG: Are your implementations interoperable?

Chris: I believe we're full testing interop.

AEAD limits (Chris Wood)

Changes: Added analysis for TLS 1.2, example limits, editorial cleanup.

Coming: Updated TLS 1.2 numbers, updated ChaCha20/Poly1305 analysis (from upcoming paper)

Open issues: Account for AAD length in analysis; add SIV limits. Since SIV isn't in any major IETF protocol, unless someone provides a PR going to close that issue.

Other modes could be added if someone does the analysis.

Next steps: Resolve the open issues, RGLC.

Nick: We should get review from RG participants. These plans seem to make sense though.

CPace (Michel Abdalla)

New: paper submitted to ASIACRYPT 2021. Draft mostly unchanged; refined security analysis for some variants; clarified role of unique session identifiers (SIDs).

SIDs in practice: both users contribute randomness, agreement does not require secrecy, could be piggy-backed onto application messages. Working to provide security guarantees when unique SIDs aren't available. Will update the draft.

Watson Ladd: Is it OK that we wait for refined analysis for the case of SID negotiation for the protocol that has already been chosen in the selection? Michel Abdalla: I wasn't involved in the selection itself. But refined analysis in this sense would be useful for other PAKEs as well, not a big issue.

Chris Patton: Like to see game-based proof for both CPace and OPAQUE of the contest winners. Need to coordinate on SIDs story for both drafts.

Chris Wood: Do you want to block the draft for it? ChrisP: No. ChrisW: let's discuss.

HPKE (Chris Wood)

Registry conflicts: already an IANA AEAD algorithms registry, HPKE proposes a new one as it needs to add key and nonce lengths and that the cipher is IND-CCA2 secure.

Continue to use two registries or merge them? Plan is to create the new registry. Anyone disagree? Narrator voice: no.