CFRG Meeting Minutes
IETF 101 London, UK
March 19, 2018 15:50 - 17:20, Balmoral

Chairs: Alexey Melnikov and Kenny Paterson

CFRG status update
==================
presenters: chairs
slides: https://datatracker.ietf.org/meeting/101/materials/slides-101-cfrg-chairs-slides-00

The chairs summarise the status of the CFRG's drafts.

Hacspec
=======
presenter: Franziskus Kiefer
slides: https://datatracker.ietf.org/meeting/101/materials/slides-101-cfrg-1-hacspec-00
pointer: https://github.com/HACS-workshop/hacspec/tree/master/specs

Kiefer presented on the Haspsec initiative that addresses the challenges of verifying crypto implementations. This initiative attempts to reduce the cost of formal verifications.

Q: (Daniel Kahn-Gillmor): Thanks. Can you explain how to express the formal cryptographic properties?
A: (Kiefer): We have not yet formalized these.

Q: (Scott Floris): How do you handle side-channels? Is there a way to specify if this code has secret dependant branches/accesses?
A: (Kiefer) You can restrict what can be

compared. In things like big-nums, can't do it just yet. However, when you get to the machine integers it can be addressed.

Q: (Phil Hallam-Baker) It would be nice to have C# and Java support.
A: (Kiefer): Agreed.

Randomness Improvements for Security Protocols

presenter: Christopher Wood
slides: https://datatracker.ietf.org/meeting/101/materials/slides-101-cfrg-2-hashing-to-curves-02
draft: https://datatracker.ietf.org/doc/draft-cremers-cfrg-randomness-improvements/

Wood presented on the draft that improves the randomness of PRNGs based on the recommendation of SecDispatch at IETF 100.

Q: (Yoav Nir): Per slide 5, how bad can your PRNG be and your technique work? What about all zeros?
A: (Woods): Yes.
A: (Nir): How do you get a good secret key in the first place?
A: (Woods): We just assume it is good.

Q: (Thompson): Why did you choose concatenations?
A: (Woods): It seemed like the simplest.
A: (Thompson): You might want to include text about coordination.

Q: (Martin): You noted that is isn't a replacement for /dev/random? Do you have

results on how many random bytes you get?
A: (Woods): Not yet. Do you mean performance metrics?
A: (Martin): No security.
A: (Kenny Paterson): As many as you want if you do have a secure PRNG.

Comment: (Paterson): You used Dual EC as a motivation. You could detect this by just looking at source code, but if you don't have source code you can't detect it at all. Consider modifying your motivation.
A: ok.

Comment: (Paterson): Per slide 5, what if you used it in a hashing scheme?
A: (Smyshlyaev): Yes, this is an important aspect that we'll be addressing in the future versions of the draft.

Q: (Paterson): What is your intention with this draft?
A: (Woods): SecDispatch sent us here. We'd prefer to publish it.

Q: (Paterson) Consensus call to WG: should we adopt this draft?
[Yes] is the outcome of the consensus call.

Hashing to Elliptic Curves
==========
presenter: Christopher Wood
slides: https://datatracker.ietf.org/meeting/101/materials/slides-101-cfrg-3-hashing-to-curves-01
draft: https://datatracker.ietf.org/doc/draft-sullivan-cfrg-hash-to-curve/

Woods introduced a draft which describes algorithms to hash arbitrary strings to Elliptic Curves.

Q: (Paterson) to the WG: Is this useful?

Q: (Richard Barnes): In MLS BOF, there is a need to map from a random string to a curve point. Do you think this work would inform that draft?
A: (Woods): Let's talk. I would need to look at your draft.

Q: (): How does this work compare with other work?
A: (Woods) This isn't a proposal, but an aggregation of existing techniques.

Q: (Ella Berners-Lee): Were any of the curves mentioned pairing friendly?
A: (Woods): Not that I'm aware.
A: (Berners-Lee): There is related work and would you be interested in adding it to the draft?
A: (Woods): Yes.

Comment: (Dan Harkins): This is a very good idea and important.

Comment: (Scott Floris): If you have a method that misses half the points, that's important to point out.
A: (Woods): That would be an omission if we haven't said it. We'll check.

[none voiced]

Q: (Melnikov): Are there people willing to work?
[enough people]

Verifiable Oblivious Pseudorandom Functions (VOPRFs)

presenter: Nick Sullivan
slides: https://datatracker.ietf.org/meeting/101/materials/slides-101-cfrg-4-voprfs-00
draft: https://datatracker.ietf.org/doc/draft-sullivan-cfrg-voprf/

Sullivan introduced a draft that constructs VOPRF based on Elliptic Curves.

Q: (): What is the contents of the draft -- I didn't read it. You discussed several crypto primitives.
A: (Sullivan): A generic description of VOPRFs and a specific instantiation.

Q: (Melnikov): What are you interest in having happen to this draft?
A: (Sullivan): CFRG adoption.
A: (Paterson): How do you you see this and the above draft progressing given the dependency?
A: (Sullivan): They can proceed in parallel.

Q: (Gillmor): One of the concerns is how the key remains constant?
A: (Sullivan): You're noting the tagging attack. The signer's public key needs public verifiability -- maybe a transparency log or consensus protocol. Those are outside of the

scope of the draft.
A: (Gillmor): I was hoping to hear that they should be separate.
A: (Sullivan): We'll add language to the draft.
A: (Melnikov): Let's take further discussion to the mailing list.

VTBPEKE: Verifier-based Two-Basis Password Exponential Key Exchange

presenter: Guilin Wang
slides: https://datatracker.ietf.org/meeting/101/materials/slides-101-cfrg-5-pake-00
pointer: http://www.di.ens.fr/users/pointche/Documents/Papers/2017_asiaccsB.pdf

Wang provided background on Password-Authenticated Key Exchange (PAKE) and presented on a Verifier-based Two-Basis Password Exponential Key Exchange (VTNPEKE).

Comment: (Phil Hallam-Baker): I would like the IETF to only choose one approach and for this approach to be unencumbered.

Q: (Dan Harkins): Do you have IPR on these approaches?
A: (Wang): No.
Comment: (Dan Harkins): Per slide 9, SPAKE, SPAKE2, and SAE all provide perfect forward secrecy.
A: (Wang): Let's review and discuss.
A: (Smyshlyaev): I recommend a review of your various proposals. We should also take it to the mailing list.
A: (Melnikov): Let's take it to the mailing

list.

KangarooTwelve
==========
presenter: Benoit Viguier
slides: https://datatracker.ietf.org/meeting/101/materials/slides-101-cfrg-kangaroo12-01
draft: https://tools.ietf.org/html/draft-viguier-kangarootwelve-01

Viguier introduced the KangarooTwelve eXtendable Output Function (XOF), a hash function with arbitrary output length.

Q: (Paterson): You halved the number of rounds. How much of the performance gains come from that?
A: (Viguer): About 70% of the performance gains come from this change and also how blocks are processed.

Q: (Wang): Is this a complete function?
A: (Viguier): Yes, a complete function

Q: (Nick Johnson): It appears to be combining -- speed with parallelism with no cost to security; and then speed vs. security? Why do that?
A: (Viguer): The security is already conservative.
A: (Johsnon): Per slide 6, it looks like you are getting 100% speed-up from parallelism. I still don't understand why you're composing these two approaches.

(End of meeting.)