CFRG Research Group

Online Agenda and Slides at:

https://datatracker.ietf.org/doc/agenda-104-cfrg/

Data tracker: http://datatracker.ietf.org/rg/cfrg/documents/

Agenda

https://datatracker.ietf.org/doc/agenda-104-cfrg/

IETF Note Well

This summary is only meant to point you in the right direction, and doesn't have all the nuances. The IETF's IPR Policy is set forth in BCP 79; please read it carefully.

The brief summary:

- **By participating with the IETF, you agree to follow IETF processes.**
- **If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.**
- **You understand that meetings might be recorded, broadcast, and publicly archived.**

For further information, talk to a chair, ask an Area Director, or review the following:

BCP 9 (on the Internet Standards Process)

BCP 25 (on the Working Group processes)

BCP 78 (on the IETF Trust)

BCP 79 (on Intellectual Property Rights in the IETF)

Also see: http://www.ietf.org/about/note-well.html:

Administrative

- Audio Streaming/Recording
  - Please speak only using the microphones
  - Please state your name before speaking

- Minute takers & Etherpad
- Jabber

CFRG Research Group Status

Chairs:

Kenny Paterson <kenny.paterson@inf.ethz.ch>

Alexey Melnikov <alexey.melnikov@isode.com>

RG Document Status

Document Status

- New RFC (since Bangkok)
  - None
- In RFC Editor's queue (since Bangkok)
  - draft-mcgrew-hash-sigs-15 (**AUTH48, document shepherd: Paul Hoffman**): Hash-Based Signatures
  - draft-irtf-gcmsiv-09: AES-GCM-SIV: nonce misuse-resistant authenticated encryption
- In IRSG review
  - draft-irtf-cfrg-re-keying-14 (**in IESG conflict review**): Re-keying Mechanisms for Symmetric Keys
- Completed, waiting for chairs
  - draft-irtf-cfrg-spake2-08 (**document shepherd to check changes** (Kenny), then will be ready for ISRG): SPAKE2, a PAKE
  - draft-irtf-cfrg-argon2-04 (**document shepherd to check changes** (Alexey)**, then will be ready for IRSG**): memory-hard Argon2 password hash and proof-of-work function
- Active CFRG drafts
  - draft-irtf-cfrg-vrf-04 (**updated**): Verifiable Random Functions (VRFs)
  - draft-irtf-cfrg-hash-to-curve-03 (**updated**): Hashing to Elliptic Curves
  - draft-irtf-cfrg-randomness-improvements-04 (**updated**): Randomness Improvements for Security Protocols
  - draft-viguier-kangarootwelve-04 (**newly adopted work item**): KangarooTwelve eXtendable Output Function
  - draft-arciszewski-xchacha-03 (**newly adopted work item**): XChaCha: eXtended-nonce ChaCha and AEAD_XChaCha20_Poly1305
  - draft-hoffman-c2pq-04 (**expired**): The Transition from Classical to Post-Quantum Cryptography
- Related work/possible work item
  - draft-hoffman-rfc6090bis-02: Fundamental Elliptic Curve Cryptography Algorithms
  - draft-barnes-cfrg-hpke-00: Hybrid Public Key Encryption
- Expired
  - draft-irtf-cfrg-cipher-catalog-01: Ciphers in Use in the Internet
  - draft-irtf-cfrg-webcrypto-algorithms-00: Security Guidelines for Cryptographic Algorithms in the W3C Web Cryptography AP
  - draft-irtf-cfrg-augpake-09: Augmented Password-Authenticated Key Exchange (AugPAKE)

PAKE selection process

- After receiving several PAKE proposals recently and seeing several CFRG documents complete, chairs want to announce PAKE selection process.
  - The aim is to select 1 or more PAKE to recommend to the wider IETF community
- All submissions need to satisfy RFC 8125 (Requirements for Password-Authenticated Key Agreement (PAKE) Schemes).
- Upcoming presentation in this session.

Crypto Review Panel

- Formed in September 2016
  - Wiki page for the team: <https://trac.ietf.org/trac/irtf/wiki/Crypto%20Review%20Panel>
  - Mailing list for internal communications was requested
- May be used to review documents coming to CFRG, Security Area or Independent Stream.
- **Lots of good reviews done, including recent work on Independent Stream submissions.**

AOB