CFRG @ IETF83

mcgrew@cisco.com
kmigoe@nsa.gov

Internet Research Task Force

- Focuses on longer term research issues related to the Internet
  - Sister organization to IETF
- RFC Editor publishes its documents on the IRTF Stream (RFC 5743)
- IRTF guidelines and procedures detailed in RFC 2014

IETF Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

CFRG Charter

The Crypto Forum Research Group (CFRG) is a general forum for discussing and reviewing uses of cryptographic mechanisms, both for network security in general and for the IETF in particular.

The CFRG serves as a bridge between theory and practice, bringing new cryptographic techniques to the Internet community and promoting an understanding of the use and applicability of these mechanisms via Informational RFCs, in the tradition of, e.g., RFC 1321 (MD5) and RFC 2104 (HMAC). Our goal is to provide a forum for discussing and analyzing general cryptographic aspects of security protocols, and to offer guidance on the use of emerging mechanisms and new uses of existing mechanisms. IETF working groups developing protocols that include cryptographic elements are welcome to bring questions concerning the protocols to the CFRG for advice.

The CFRG meetings, membership, and mailing list are open to all who wish to participate

Agenda

- Introduction and Welcome
- CFRG status
- Hash-based passwords (15 minutes, Bellovin)
  - `draft-bellovin-hpw-01`
- Password Authenticated Key Exchange (25 minutes, Harkins)
- PAKE discussion (5 minutes)
- Ciphers in Use on the Internet (10 minutes, Shen)
  - `draft-irtf-cfrg-cipher-catalog-00`
- OCBv3 (20 minutes, Rogaway)
  - `draft-krovetz-ocb-03`
- Elliptic curve considerations (20 minutes, Struik)
- CFRG review of IETF uses of crypto (time permitting)

Status

- One RG draft
- Requested by IETF Security Area:
  - [TLS] RG assessment of `draft-harkins-tls-pwd-02` and PAKE
    - Possibility of PAKE authentication in HTTP2 (June ‘12)
  - [JOSE] AEAD using generic composition of AES-CBC and HMAC-SHA
  - Secure hashing using block ciphers (as part of a minimal cryptosuite)
- In-person meeting at IACR conference?

CFRG Review of IETF Crypto

- Marshall, Joachim, David
  - Triaged ~ 50 MD5 drafts, 17 needed attention
  - More work than anticipated
- Ideas
  - Coordinate with SECDIR review?
  - Post drafts needing review to CFRG list?