Hash BoF

63rd IETF

Paul Hoffman, VPN Consortium

Why we are here

- Intro to hashes: **http://www.vpnc.org/hash.html**
- Deal with recent attacks on *collision resistance* in widely-used hash functions
- Determine whether there should be an IETF working group to discuss and/or standardize changes in current hash functions and/or new hash functions
- Continue conversation from the mailing list: **https://www1.ietf.org/mailman/listinfo/hash**

Today's agenda

- Presentations (60-70 minutes)
- Charter discussion (remainder)

Presentations (60 minutes)

- Bill Burr on the upcoming NIST workshop
- Russ Housley on a new proposal for message preprocessing in hash functions
- Ran Canetti on draft-irtf-cfrg-rhash-00.txt for signatures
- Steve Bellovin and Eric Rescorla on IETF protocols and new hashing mechanisms
- Tim Polk on what NIST is working on in this area
- If there is time: general discussion on tradeoffs of mechanisms and functions

Charter discussion (30 minutes)

- What are the short term and long term objectives in this area for the IETF?
- Is it possible to set IETF requirements for hash functions?
- Is a Working Group useful to the IETF? Can it be useful to the outside world?
- If so, should this be in the IETF or IRTF?
- Continue conversation from the mailing list: **https://www1.ietf.org/mailman/listinfo/hash**

URLs

- Continue conversation from the mailing list: **https://www1.ietf.org/mailman/listinfo/hash**
- Intro to hashes: **http://www.vpnc.org/hash.html**
- Description of collision attack issues: **draft-hoffman-hash-attacks-04.txt** (in RFC Editor queue)