Changes in ZRTP

draft-zimmermann-avt-zrtp-02.txt

Phil Zimmermann <prz@mit.edu>
Alan Johnston <alan@sipstation.com>
Jon Callas <jon@pgp.com>

Recent Changes

- Discussion of how ZRTP compares using the criteria in draft-wing-rtpsec-keying-eval-01.txt
- **Discovery and authentication of ZRTP through the signaling channel and the definitions and ABNF of three SDP attributes a=zrtp, a=zrtp-sas, a=zrtp-sasvalue**
- **New Multistream key agreement mode allowing SRTP keys for multiple media streams in a session to be derived from a single ZRTP DH exchange.**
- **CRC protection of ZRTP messages against transport errors using a 32 bit CRC algorithm**
- Simplified shared secret comparison algorithm
- New Stay secure and **Disclosure flags**
- More details on caching of retained shared secrets including expiration intervals
- Removal of Error message - Reason field added to GoClear
- **Discussion of the behavior of intermediary devices that might implement ZRTP**
- IPR declaration

Authentication Through Signaling

- ZRTP has three new SDP attributes
  - Discussed in detail in MMUSIC
- Short Authentication String (SAS) derived from DH public values exchanged over signaling *in addition to* being rendered to user.
- Allows
  - Discovery of support for ZRTP
  - Authentication by clients and servers.
  - SAS logging

Multistream Key Agreement

- Allows additional SRTP keys and salts to be derived from a previous DH calculation.
  - A Session key is calculated at time of initial DH
  - Multistream mode indicated in Commit message.
  - Skip DHPart1 and DHPart2 messages
    - No effect on retained shared secrets.
- Use cases:
  - Adding video stream to a voice call
  - Establishing multiple media streams in parallel
    - First one performs DH, upon completion, other streams use Multistream mode in parallel.

Disclosure Flag Background

- Goal of ZRTP Protocol – End-to-end media privacy
  - Absolutely No Back Doors within ZRTP!
- ZRTP still usable in environments where privacy is not assured, outside scope of ZRTP
  - Lawful intercept
  - Enterprise recording
- ZRTP requires endpoints to declare this capability by setting Disclosure Flag
  - Required for strict compliance to ZRTP protocol

Disclosure Flag

- Disclosure flag set by clients that have the capability to disclose SRTP keys out of band.
- Used to indicate capabilities of endpoint, not per call usage
  - Not in conflict with lawful intercept requirements

"If an endpoint stores or logs SRTP keys or information that can be used to reconstruct or recover SRTP keys after they are no longer in use (i.e. the session is active), or otherwise discloses or passes SRTP keys or information that can be used to reconstruct or recover SRTP keys to another application or device, the Disclosure flag D MUST be set in the Confirm1 or Confirm2 message."

CRC32 Checksum

- Added CRC32 checksum to all ZRTP messages.
- Needed to prevent a transmission bit error being misinterpreted as an active MitM attack.
- UDP 16 bit checksum not sufficient.

Behavior of Intermediaries

- No useful back-to-back ZRTP applications
  - Will be detected and identified as a MitM attack.
- Intermediaries should be transparent to ZRTP.
- Intermediaries may act as ZRTP endpoint, encrypting on behalf of user.
- ZRTP SDP attribute used by clients to tell intermediaries to act transparently.

Next Steps

- Continue list discussion on syntax
  - Everyone has an opinion on this ;-)
- Continue to incorporate feedback from deployed base. “Running code and rough consensus”