Diffie Hellman Tests for IKEv2

`draft-ietf-ipsecme-dh-checks-00`

Scott Fluhrer
Yaron Sheffer

Presented by Tero Kivinen

IETF-86, Orlando

Draft Overview

- Some tests are missing in IKEv2
- Recipient should verify the sender's DH public key
  - Both Initiator and Responder
- The tests are required if **both** are true:
  - Using ECDH
  - The DH private key is reused for multiple sessions, as allowed by the protocol
- If both conditions apply then the tests are **critical** for security

Changes in the WG -00 Draft

- Describe the situation for MODP groups
  - Traditional groups: we only need simple range tests
  - Groups with small subgroups (22-24): reuse doesn't make sense, unless you're performing the self tests anyways
- Explain that some groups are not covered in the document, specifically even-characteristic groups
- Clarify the IANA actions:
  - Add a "Recipient Tests" column to the IKEv2 IANA registry – must be specified for any new groups
  - Specify values for existing groups

Open Issues and Next Steps

- One outstanding open issue
  - What do do if the test fails (probably: send INVALID_SYNTAX and drop the SA)
- Would like to WG LC soon after Orlando