IPsecME WG IETF 96, Berlin, Germany

ipsec@ietf.org

Tero Kivinen

David Waltermire

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.

Logistics

- Blue Sheets
- Two note takers
- One jabber scribe

Agenda

1. Logistics, agenda, WG status – Chairs - 10 minutes
2. Status of draft-ietf-ipsecme-ddos-protection-07 - Yoav Nir – 5 minutes
3. Status of draft-ietf-ipsecme-rfc4307bis-09 - Tero Kivinen – 5 minutes
4. Discussion of draft-mglt-ipsecme-rfc7321bis - Daniel Migault – 10 minutes
5. Status of draft-ietf-ipsecme-safecurves-01 - Yoav Nir – 5 minutes
6. Discussion of draft-ietf-ipsecme-tcp-encaps-00 - Tommy Pauly - 15 minutes
7. Discussion of draft-fluhrer-qr-ikev2-01 / Next steps – Chairs – 25 minutes
8. Review of charter text - Chairs – 20 minutes
9. Discussion of draft-pauly-ipsecme-split-dns - Paul Wouters – 10 minutes
10. Discussion of draft-mglt-ipsecme-implicit-iv - Yoav Nir – 10 minutes
11. Diet-ESP in 6lo WG - Daniel Migault – 5 minutes

Charter – Summary of Changes

- Removed opportunistic – “Done”
- To be added:
  - Mandatory to implement algorithm documents
  - New algorithms (curve25519, EdDsa etc)
  - Quantum Resistance for IKEv2
  - TCP Encapsulation
- New work?
  - Split DNS
  - Yang models
  - Others?

WG Presentations

Charter Discussion

Charter

The IPsec suite of protocols includes IKEv1 (RFC 2409 and associated RFCs), IKEv2 (RFC 7296), and the IPsec security architecture (RFC 4301). IPsec is widely deployed in VPN gateways, VPN remote access clients, and as a substrate for host-to-host, host-to-network, and network-to-network security.

The IPsec Maintenance and Extensions Working Group continues the work of the earlier IPsec Working Group which was concluded in 2005. Its purpose is to maintain the IPsec standard and to facilitate discussion of clarifications, improvements, and extensions to IPsec, mostly to IKEv2. The working group also serves as a focus point for other IETF Working Groups who use IPsec in their own protocols.

Charter New Work Items (1 of 2)

The current work items include:

IKEv2 contains the cookie mechanism to protect against denial of service attacks. However this mechanism cannot protect an IKE end-point (typically, a large gateway) from "distributed denial of service", a coordinated attack by a large number of "bots". The working group will analyze the problem and propose a solution, by offering best practices and potentially by extending the protocol.

IKEv2 utilizes a number of cryptographic algorithms in order to provide security services. To support interoperability a number of mandatory-to-implement (MTI) algorithms are defined in RFC4307 and RFC7321. There is interest in updating the MTIs in RFC4307 and RFC7321 based on new algorithms, changes to the understood security strength of existing algorithms, and the degree of adoption of previously introduced algorithms. The group will revise RFC4307 and RFC7321 proposing updates to the MIT algorithms used by IKEv2 and IPsec to address these changes.

Charter New Work Items (2 of 2)

The current work items include:

There is interest in supporting Curve25519 and Curve448 for ephemeral key exchange in the IKEv2 protocol. The group will extend the IKEv2 protocol to support key agreement using these curves and their related functions.

IKEv1 using main mode and shared secret was partially resistance to quantum computers. IKEv2 removed this feature to make the protocol more usable. There as been interest to add a mode to IKEv2 to be quantum resistant.

There have been middle boxes blocking IKE negotiation over UDP. To make IKE work in these environments, IKE packets need to be encapsulated in a TCP tunnel. The group will define a mechanism to tunnel IKE and IPsec over a TCP-based connection. This method is intended to be used as a fallback when IKE cannot be negotiated over UDP.

This charter will expire in December 2017. If the charter is not updated before that time, the WG will be closed and any remaining documents revert back to individual Internet-Drafts.