IPsecME WG
IETF 93, Prague

Paul Hoffman
Yaron Sheffer

WG Status Report

- draft-ietf-ipsecme-ikev2-null-auth in the RFC Editor's queue

- draft-ietf-ipsecme-chacha20-poly1305 in the RFC Editor's queue

  – Great turnaround!

- Our main item is still draft-ietf-ipsecme-ddos-protection

- And it is stalled

Agenda

- Process discussion – coming up
- DDoS (15)
- draft-nir-ipsecme-curve25519-00 (10)
- draft-tran-ipecme-yang-ipsec-00 (10)
- draft-wang-ipsecme-ipsec-yang-00 and draft-wang-ipsecme-ike-yang-00 (10)

ICMP Attacks

- draft-roca-ipsecme-ptb-pts-attack-00 was announced on the list

- TL;DR: unauthenticated well-crafted ICMP messages can DDoS an IPsec connection

- Recommended reading

- Will not be discussed today

Moving Forward

- Background: lack of energy around DDoS draft and several previous ones

- We propose to discuss several options
  - Decision will take place on the list

- Do nothing
- Close the WG and retain the mailing list
- Move to a more relaxed schedue
  - Once every second IETF
  - On demand