Network Performance Measurement for IPsec

draft-ietf-ippm-ipsec-01

Kostas Pentikousis (Ed.), Yang Cui , Emma Zhang

IETF 88

Vancouver, Canada

Background

- OWAMP [RFC 4656], TWAMP [RFC 5357]
  - Discussion on security protection in the past
  - Decision to develop a dedicated security mechanism and give up on TLS, DTLS, IPsec
  - Unauthenticated, authenticated, and encrypted modes
- Today: interested in stats about the actual deployment of the authenticated and encrypted modes in practice
  - Cf. IKEv2/IPsec deployment

Draft Updates since IETF 87

- Proposal 1: “Backwards compatibility” option
  - Modes and Unused field interpretation
  - Backwards compatibility
- Proposal 2+3: Editorial changes
  - Add brief introduction for each section in the draft
  - Move figure 1 into section 3.1, restructure text
  - Adjust skeleton of section 4

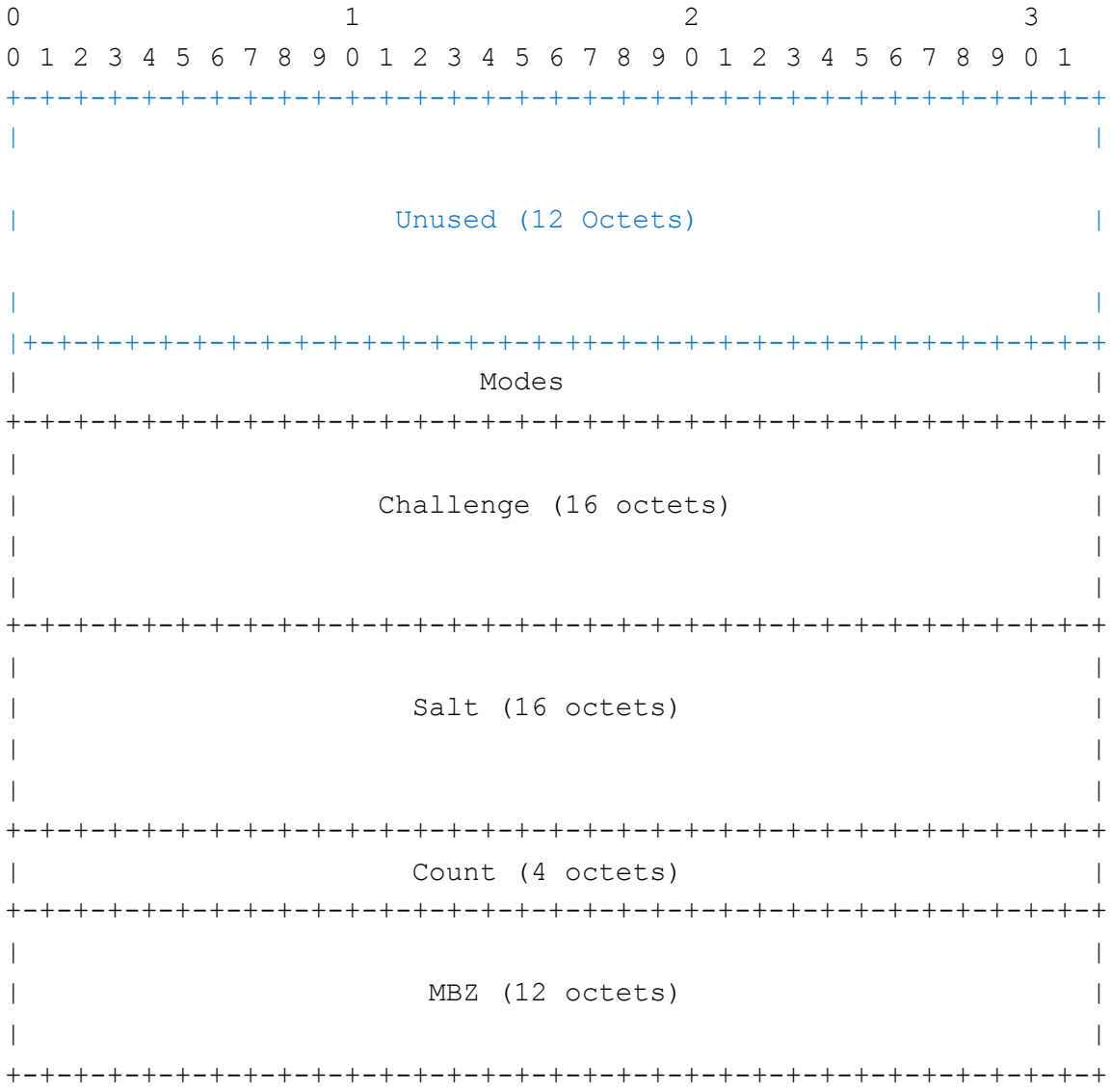
Question 0

- Does draft-ietf-ippm-ipsec define a “new” protocol?
- Or, will it “update” RFC 4656?

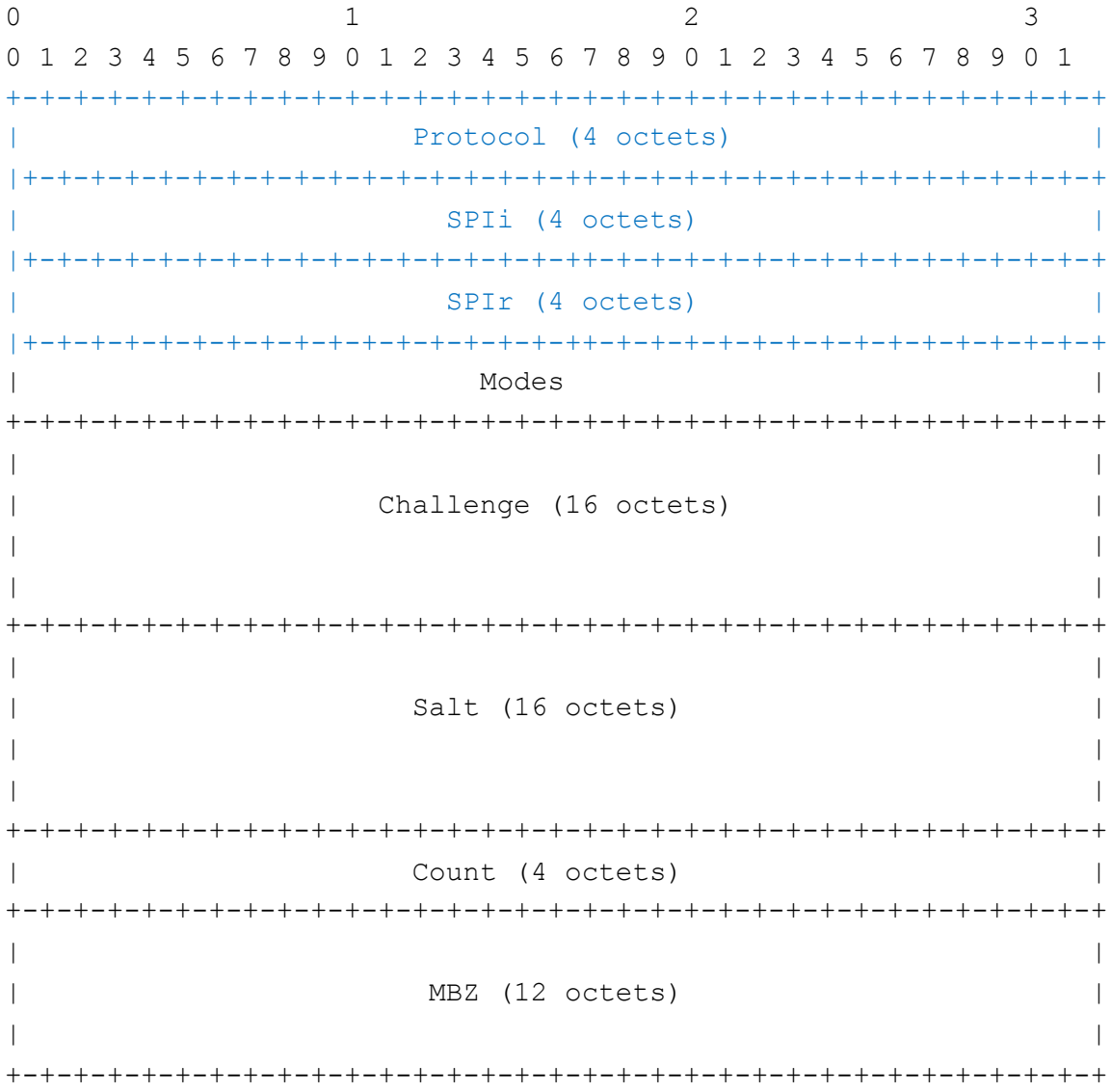
Towards a new Server Greeting?

- Unused 12 octets of Server Greeting interpreted as follows:
  - First 4 octets of Server Greeting indicate the protocol type
  - Next 8 octets indicate the initiator (SPIi) and responder (SPIr)
- Review from Al received on the value of Modes, will be integrated in -02, after the meeting
- "Compatible implementation" option
  - Pose the least backwards compatibility problems?
  - Avoid having parallel code bases

Server Greeting [RFC 4656]



Server Greeting [-ippm-ipsec]

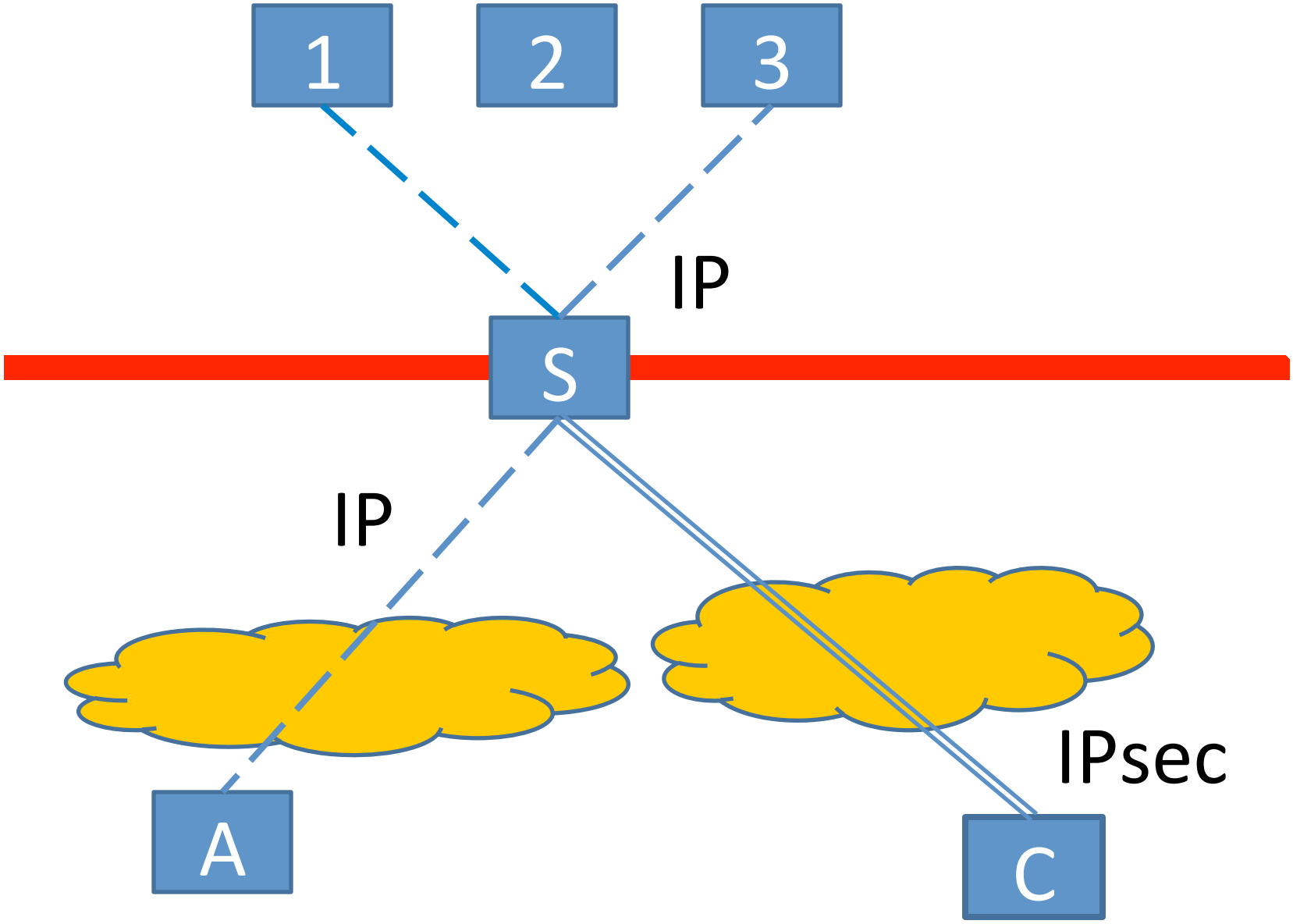


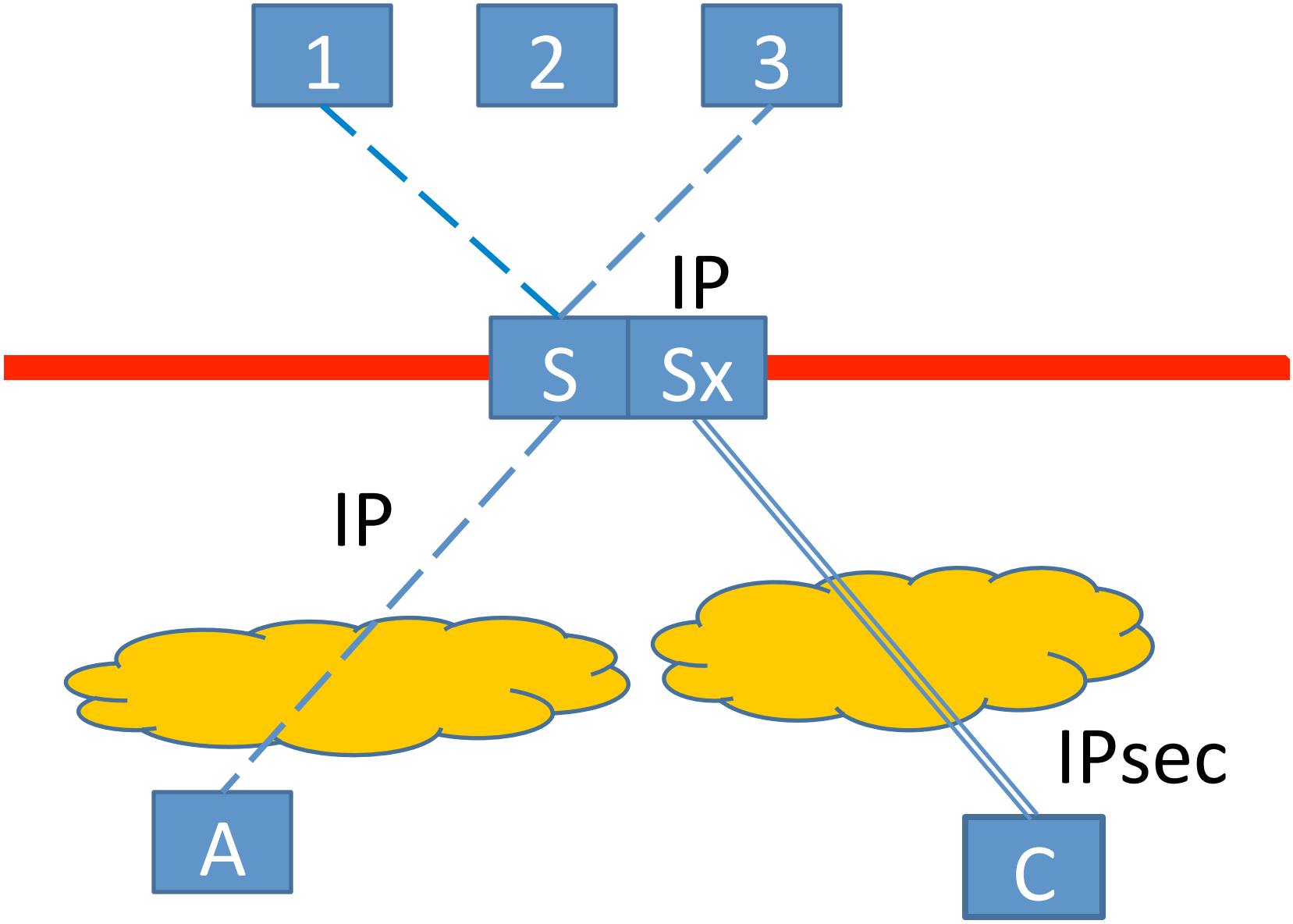
Question 1

- Can/should we use the “Unused” part of the Server Greeting?
  - So far, nobody has complained
  - But also nobody said that doing so (and hence serving backwards compatibility) would not break their implementation
- Please voice your concerns here and in the mailing list

Mailing List Feedback

- We have prodded both the ippm and ipsecme mailing lists a few times, but we received little feedback
  - Agreed, this draft addresses the intersection of two rather "esoteric protocols", but there was valuable Q&A in Berlin. Unfortunately the feedback momentum was not maintained since then
  - IPsec: Comments on the key derivation and IPsec part of the draft received from John Mattsson (Ericsson)—thanks!!!
  - IPPM: Thanks to the chairs for constructive side discussions and to Al Morton (AT&T) for his first public review of the draft!
    - We still wait for the opinion of other O/TWAMP experts


1
2
3
IP
S
IP
IPsec
A
C


1
2
3
IP
S
Sx
IP
IPsec
A
C

Way Forward

- Feedback from WG
  - Best option selection
    - Depending on the discussion and feedback finalizing the description is straightforward
  - Protocol fields definition
  - Edit the text in the draft for clarification, use of more accurate terminology, and to address comments
- Revision towards -02
  - Once IPPM makes a choice we tackle in parallel the key derivation part