Network Performance Measurement for IPsec

draft-ietf-ippm-ipsec-02

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

IETF 89

London, England

Background

- OWAMP [RFC 4656], TWAMP [RFC 5618]
  - 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

Q&A

- Q0: Is this a “new” protocol or an update to RFC 4656
  - A0: It is an update; we opted for backwards compatibility
- Q1: Can/should we use the “Unused” part of the Server Greeting?
  - A1: We opted not to; again favoring backwards compatibility

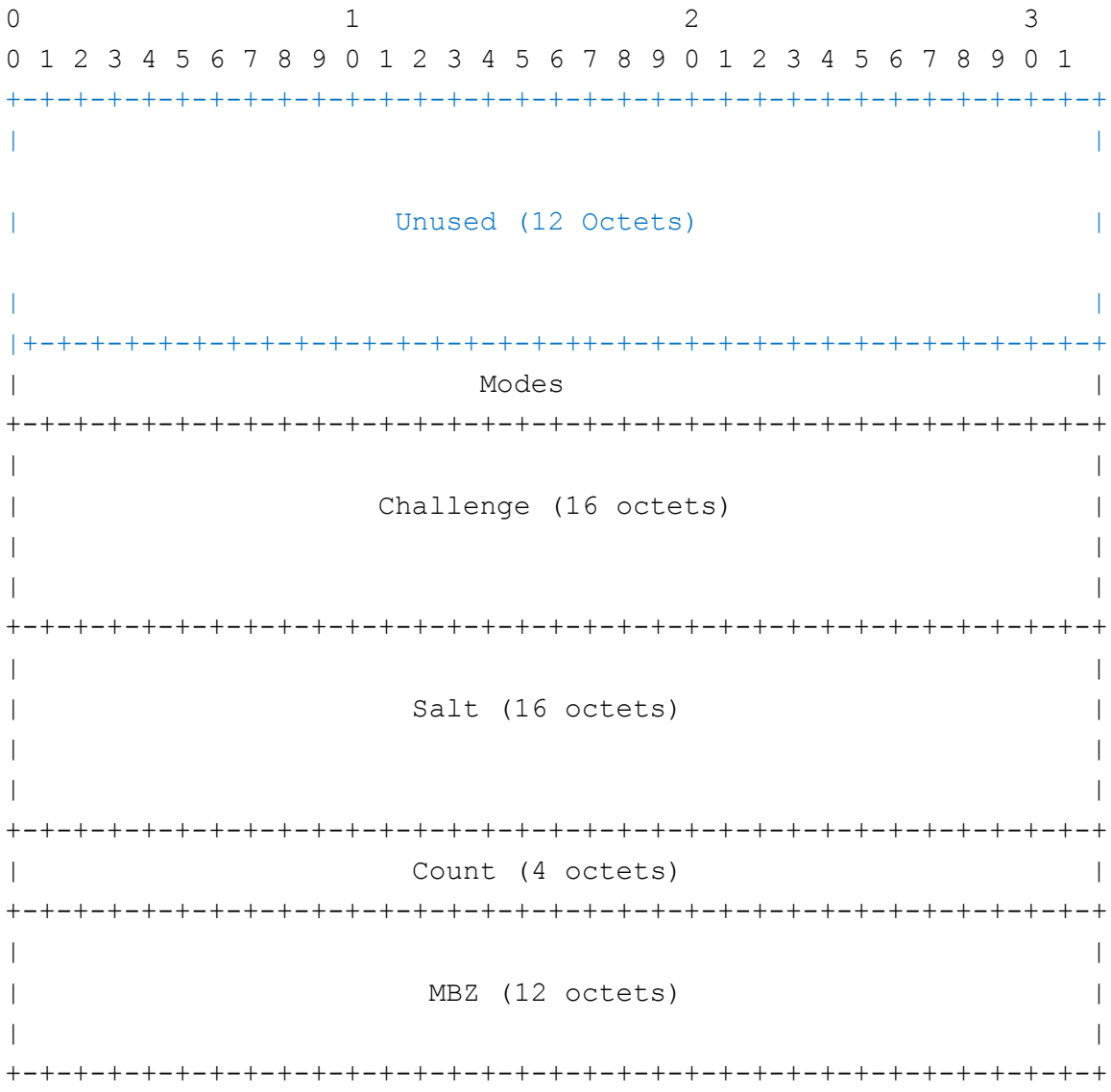
Draft Updates since IETF 88 (1)

- Introduction and Motivation
  - Large scale deployment of O/TWAMP is hindered significantly because of pre-shared key mode
  - Deriving shared key from IKE SA enables cert-based operation; key management can be automated and is more flexible
  - ~~Section 3.4 (“O/TWAMP and IPsec”)~~
- Simplification
  - Only one option for deriving shared secret key
  - ~~Section 4.3 (“Session Key Derivation”)~~

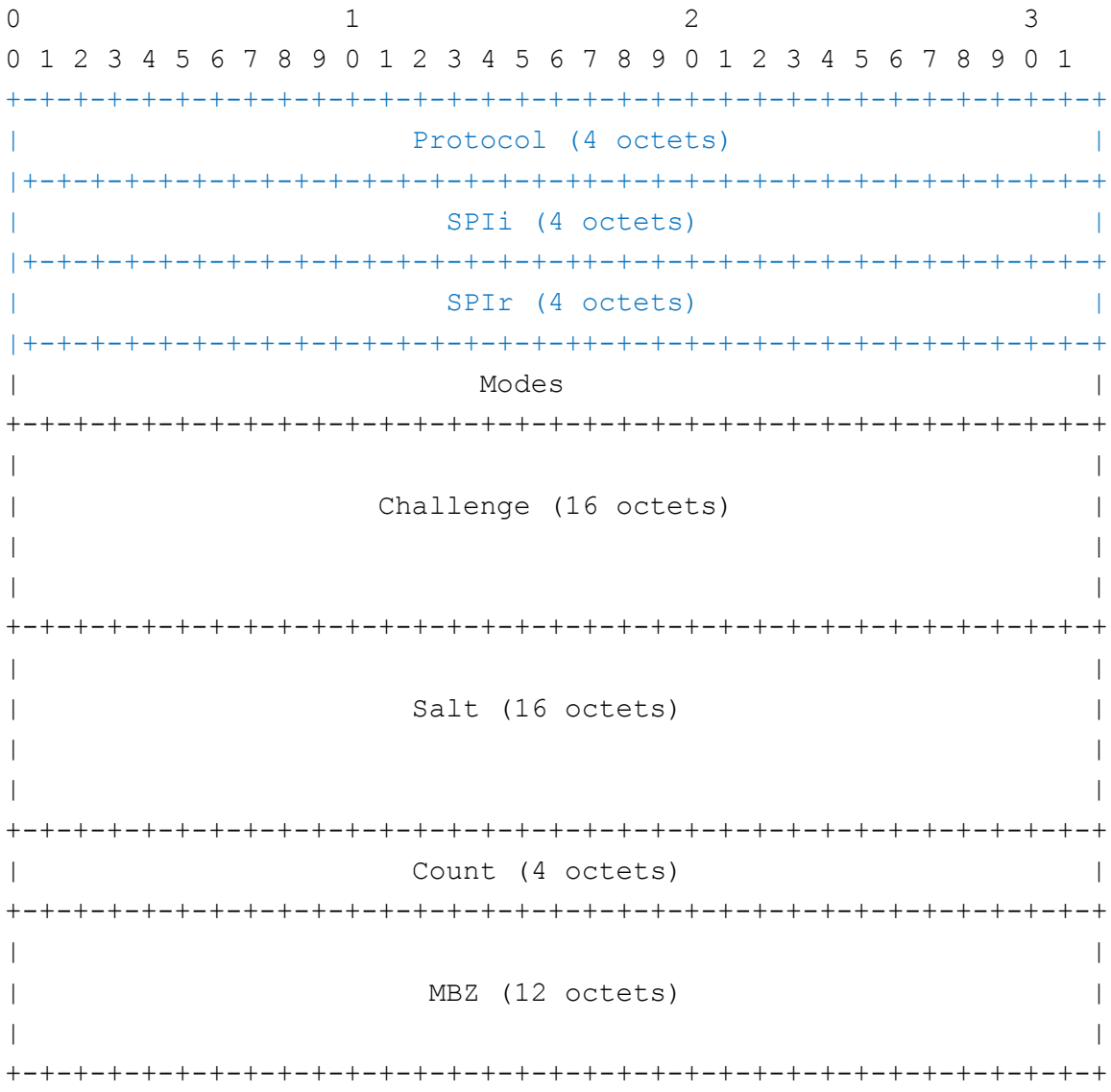
Draft Updates since IETF 88 (2)

- Shared secret key derivation in the IPsec layer
  - No key material exposure
  - IPsec and O/TWAMP implementation interaction is out of scope
- Backwards compatibility
  - New Modes
  - SPIs carried in Key ID field
- Clarifications and several editorial changes
  - TWAMP mixed mode clarification
  - Opt for deriving shared secret key from the IPsec SA

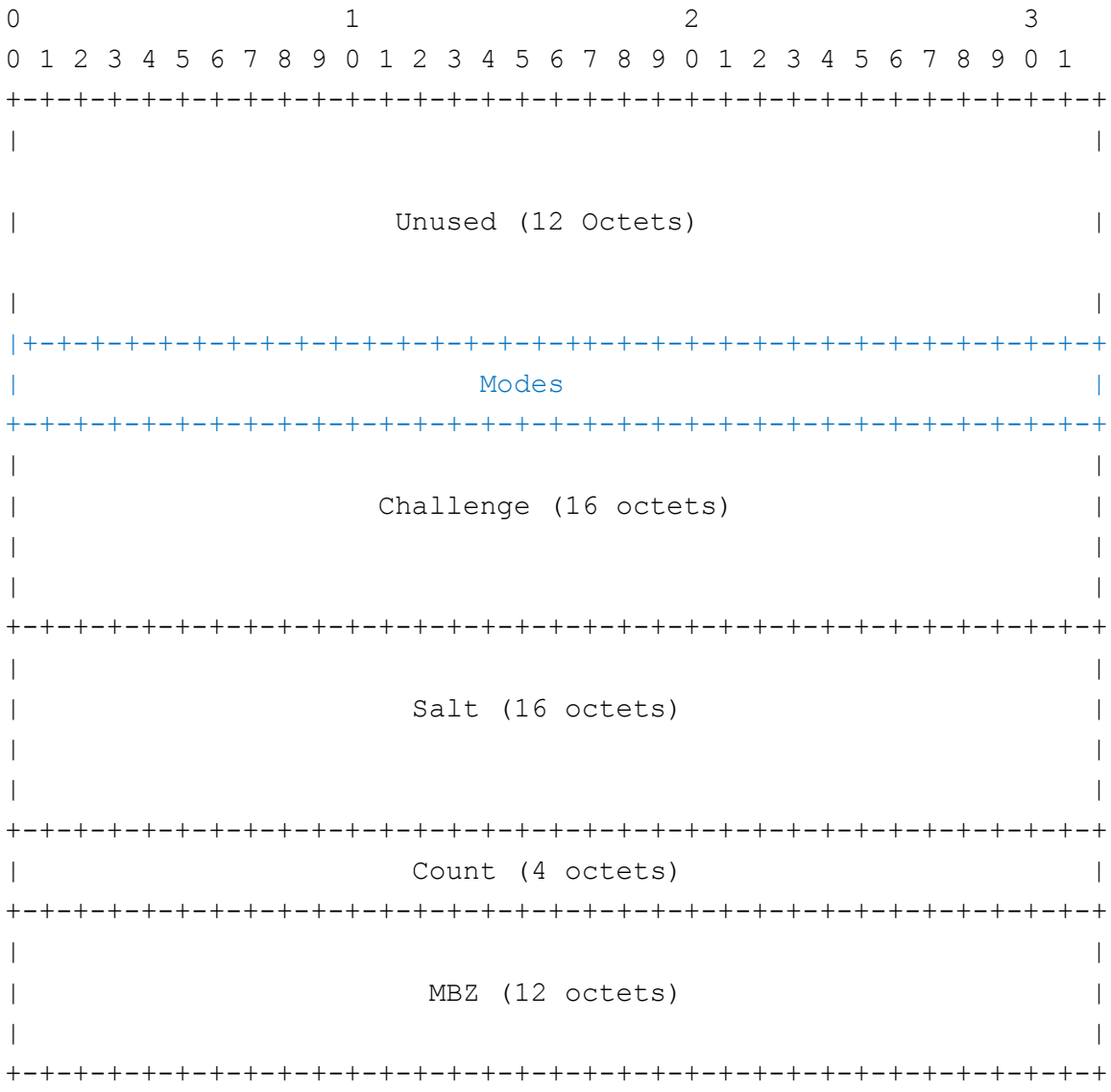
Server Greeting [RFC 4656]



Server Greeting [-ippm-ipsec-01]



Server Greeting [-ippm-ipsec-02]



New Modes

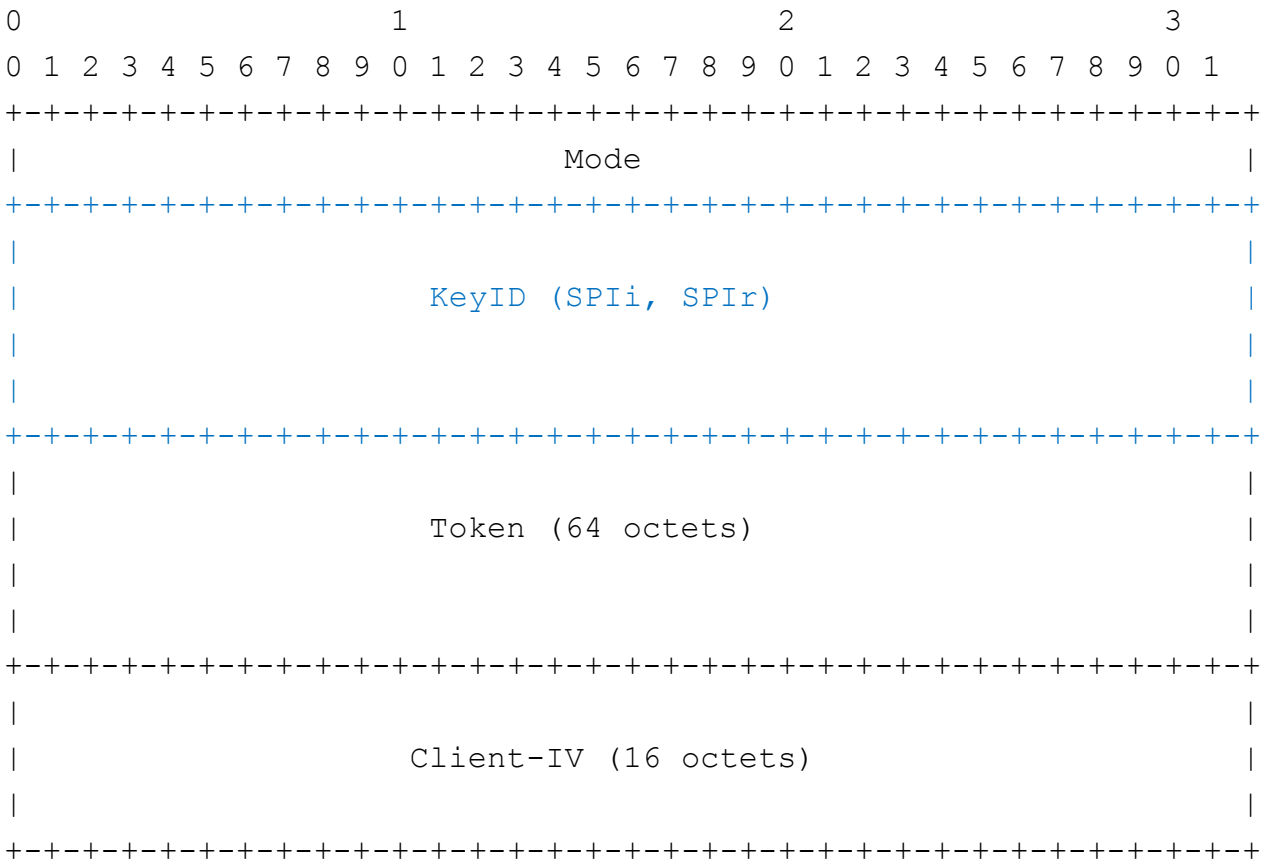
- ✓ Unauthenticated （value 1）
- ✓ Authenticated （value 2）
- ✓ Encrypted （value 4）
- ✓ Mixed （value 8）

Modes introduced in [RFC4656] and [5618]

- ✓ Authenticated using IKE （value 16）
- ✓ Encrypted using IKE （value 32）
- ✓ Mixed using IKE （value 64)

Modes introduced in [-ippm-ipsec-02]

Set-Up-Response [-ippm-ipsec-02]



Way Forward

- Feedback from WG on
  - simplified key derivation
  - new Modes
- Heading towards WGLC