IP Security Maintenance and Extensions (IPsecME) WG

IETF 120, Tuesday,July 23th, 2024

Chairs: Tero Kivinen
Yoav Nir

Responsible AD: Deb Cooley

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

• By participating in the IETF, you agree to follow IETF processes and policies.

• If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.

• As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.

• Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.

• As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:
•BCP 9 (Internet Standards Process)
•BCP 25 (Working Group processes)
•BCP 25 (Anti-Harassment Procedures)
•BCP 54 (Code of Conduct)
•BCP 78 (Copyright)
•BCP 79 (Patents, Participation)
•https://www.ietf.org/privacy-policy/ (Privacy Policy)

Administrative Tasks

We need volunteers to be:

- Two note takers

MeetEcho: https://meetings.conf.meetecho.com/ietf120/?session=33058

Notes: https://notes.ietf.org/notes-ietf-120-ipsecme

Agenda

- Note Well, technical difficulties and agenda bashing – Chairs (2 min) (15:30-15:32)
- Document Status – Chairs (3 min) (15:32-15:35)
- Presentations
  - Delete info -- Paul Wouters (3 min) (15:35-15:38)
  - SA TS Payloads opt -- Paul Wouters (4 min) (15:38-15:42)
  - Anti replay notification -- Paul Wouters (4 min) (15:42-15:46)
  - Child PFS info -- Paul Wouters (4 min) (15:46-15:50)
  - ESP Echo Protocol -- Jen Linkova (10 min) (15:50-16:00)
  - Encrypted ESP Ping -- Antony Antony (10 min) (16:00-16:10)
  - Beet mode -- Antony Antony (10 min) (16:10-16:20)
  - Multiple sequence counters -- Steffen Klassert (5 min) (16:20-16:25)
  - WESPv2 -- Steffen Klassert (15 min) (16:25-16:40)
  - Diet-ESP -- Daniel Migault (5 min) (16:40-16:45)
  - FrodoKEM in IKEv2 -- Wang Guilin (5 min) (16:45-16:50)
  - PQC Auth -- Valery Smyslov (10 min) (16:50-17:00)
- AOB + Open Mic (0 min) (16:50-17:00)

WG Status Report

- Published as RFCs
  - Internet Key Exchange Protocol Version 2 (IKEv2) Support for Per-Resource Child Security Associations (SAs) RFC9611
  - Announcing Supported Authentication Methods in the IKEv2 RFC9593

WG Status Report

- Waiting for write-up / AD Followup:
  - draft-ietf-ipsecme-g-ikev2
- Work in progress:
  - draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt
  - draft-smyslov-ipsecme-ikev2-qr-alt
  - draft-mglt-ipsecme-ikev2-diet-esp-extension
  - draft-mglt-ipsecme-diet-esp

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• ESP Echo Protocol	Jen Linkova
• Encrypted ESP Ping	Antony Antony
• Beet mode	Antony Antony
• Multiple sequence counters	Steffen Klassert
• WESPv2	Steffen Klassert
• Diet-ESP	Daniel Migault
• FrodoKEM in IKEv2	Wang Guilin
• PQC Auth	Valery Smyslov

Presentations

Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	**Paul Wouters**
ESP Echo Protocol	Jen Linkova
Encrypted ESP Ping	Antony Antony
Beet mode	Antony Antony
Multiple sequence counters	Steffen Klassert
WESPv2	Steffen Klassert
Diet-ESP	Daniel Migault
FrodoKEM in IKEv2	Wang Guilin
PQC Auth	Valery Smyslov

Minor IPsec updates

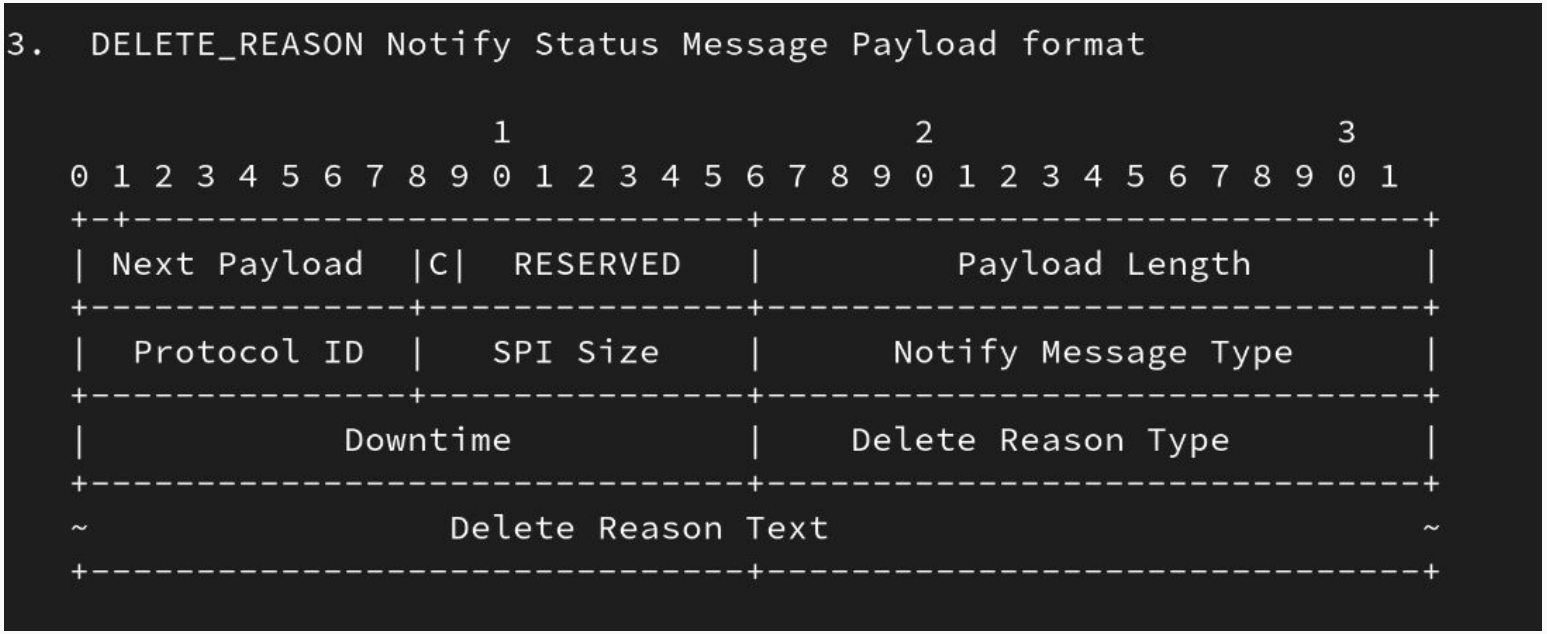
draft-pwouters-ipsecme-delete-info
draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt
draft-pan-ipsecme-anti-replay-notification
draft-pwouters-ipsecme-child-pfs-info

Paul Wouters
IETF 120 Vancouver
23 July 2024

draft-pwouters-ipsecme-delete-info-02

- **Enum list or free text? people wanted both.**
  - enum plus optional text field
  - Example section changed to initial IANA Registry

3. DELETE_REASON Notify Status Message Payload format



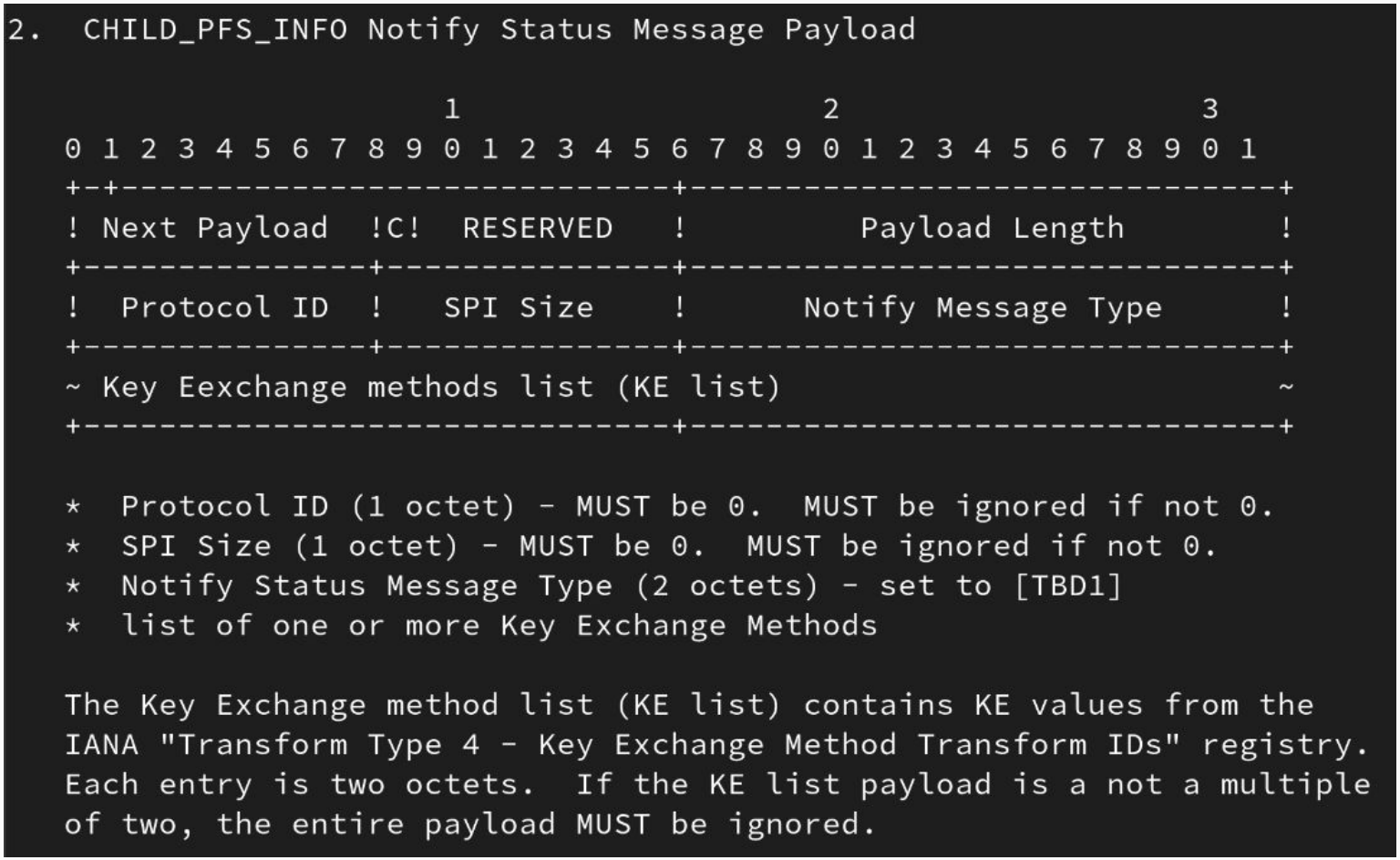
draft-ietf-ipsecme-ikev2-sa-ts-payloads-opt-03

- **Fixed Protocol ID and SPI Size to be 0**
  - As it is a regular NOTIFY payload
- **Renamed SPI to “new SPI” to avoid confusion**
- **Very minor textual fixups**
- **Would like interop tests, then WGLC**
  - Please implement so we can interop test :)

draft-pwouters-ipsecme-child-pfs-info-00

- **Convey PFS/KE for Initial IPsec SA**

2. CHILD_PFS_INFO Notify Status Message Payload



* Protocol ID (1 octet) - MUST be 0. MUST be ignored if not 0.
* SPI Size (1 octet) - MUST be 0. MUST be ignored if not 0.
* Notify Status Message Type (2 octets) - set to [TBD1]
* list of one or more Key Exchange Methods

The Key Exchange method list (KE list) contains KE values from the IANA "Transform Type 4 - Key Exchange Method Transform IDs" registry. Each entry is two octets. If the KE list payload is a not a multiple of two, the entire payload MUST be ignored.

IETF

draft-pwouters-ipsecme-child-pfs-info-00

- **Currently only coves basic case**
- **Cannot convey info on INTERMEDIATE params**
- **Cannot convey info on multiple KE**

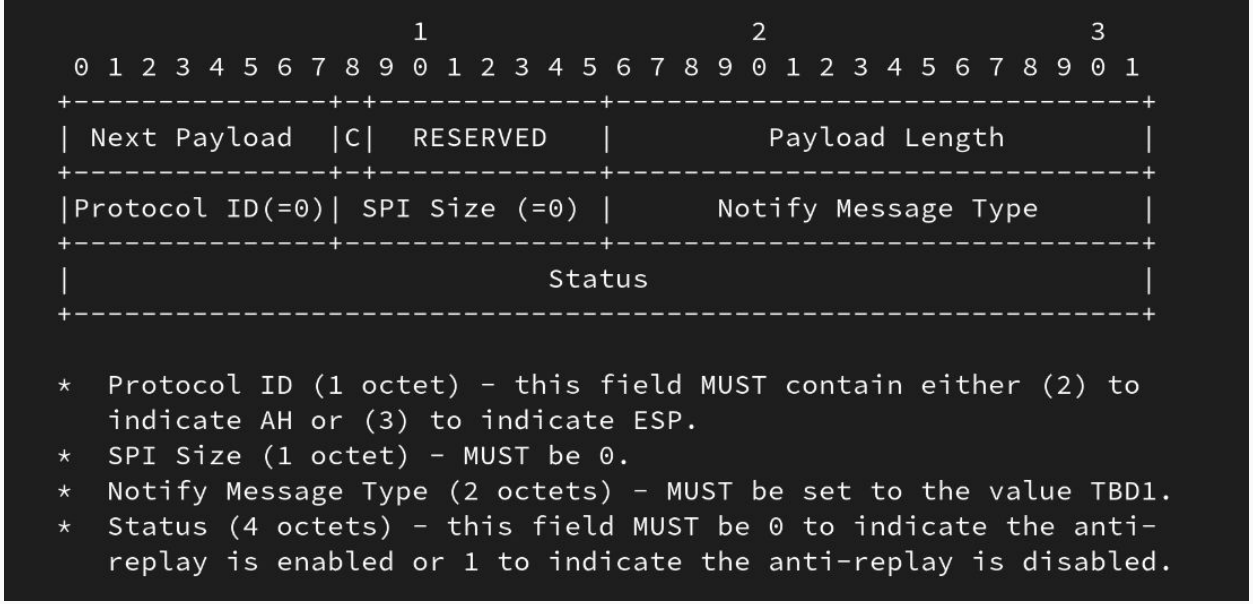
- **Leave for only simply case or make complicated?**

draft-pan-ipsecme-anti-replay-notification-00

- **Missing method to convey “no replay support”**
- **Should we add value for “ESN separate from anti-reply”**

4. ANTI_REPLAY_STATUS Notify Payload Format

The ANTI_REPLAY_STATUS Notify Message type notification is used by the initiator and responder to indicate their own anti-replay status to each other when creating the Child SAs.



* Protocol ID (1 octet) - this field MUST contain either (2) to indicate AH or (3) to indicate ESP.
* SPI Size (1 octet) - MUST be 0.
* Notify Message Type (2 octets) - MUST be set to the value TBD1.
* Status (4 octets) - this field MUST be 0 to indicate the anti-replay is enabled or 1 to indicate the anti-replay is disabled.

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• **ESP Echo Protocol**	**Jen Linkova**
• Encrypted ESP Ping	Antony Antony
• Beet mode	Antony Antony
• Multiple sequence counters	Steffen Klassert
• WESPv2	Steffen Klassert
• Diet-ESP	Daniel Migault
• FrodoKEM in IKEv2	Wang Guilin
• PQC Auth	Valery Smyslov

ESP Echo Protocol

draft-colitti-ipsecme-esp-ping-02

Lorenzo Colitti , Jen Linkova , Michael Richardson
IETF120, July 2024

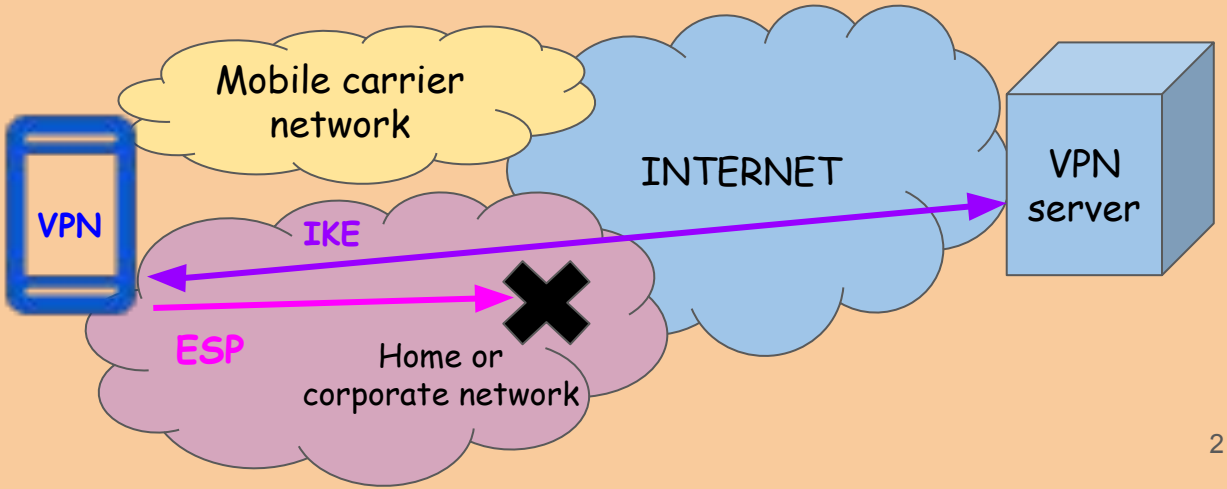
Problem Statement

ESP packets do not share fate with IKE

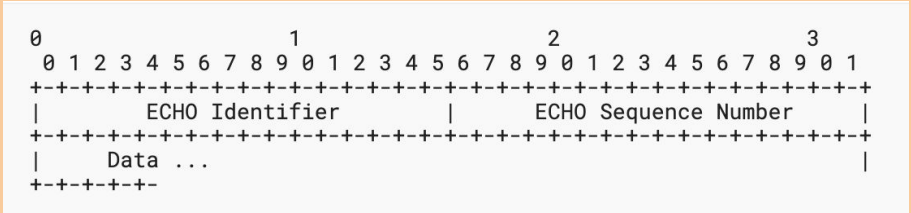
IKE might succeed but ESP packets are dropped

Hard to detect and recover

Data traffic is blackholed



Solution Overview



The node MAY send an IPv6 ESP Echo Request packet:

- SPI = 7, Next Header = 59

The peer SHOULD respond with an ESP Echo Reply packet:

- SPI = 8, Next Header = 59
- MUST copy the data from Echo Request up to the MTU

Changes since the IETF119: Use Cases

- A node discovering if the network could carry ESP packets
- Troubleshooting mechanism for network administrators
- Keepalives, to maintain firewall state entries

Fallback Scenarios: ESP Ping failures

- Senders MAY use other means of sending ESP packets:
  - encapsulation
  - use a different IP protocol
  - use a different server or interface.
- Senders SHOULD still attempt to use ESP if no alternative means are available

Questions? Comments?

Adoption?

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• ESP Echo Protocol	Jen Linkova
• **Encrypted ESP Ping**	**Antony Antony**
• Beet mode	Antony Antony
• Multiple sequence counters	Steffen Klassert
• WESPv2	Steffen Klassert
• Diet-ESP	Daniel Migault
• FrodoKEM in IKEv2	Wang Guilin
• PQC Auth	Valery Smyslov

Encrypted ESP Ping

draft-antony-ipsecme-encrypted-esp-ping

Antony Antony <antony.antony@secunet.com>

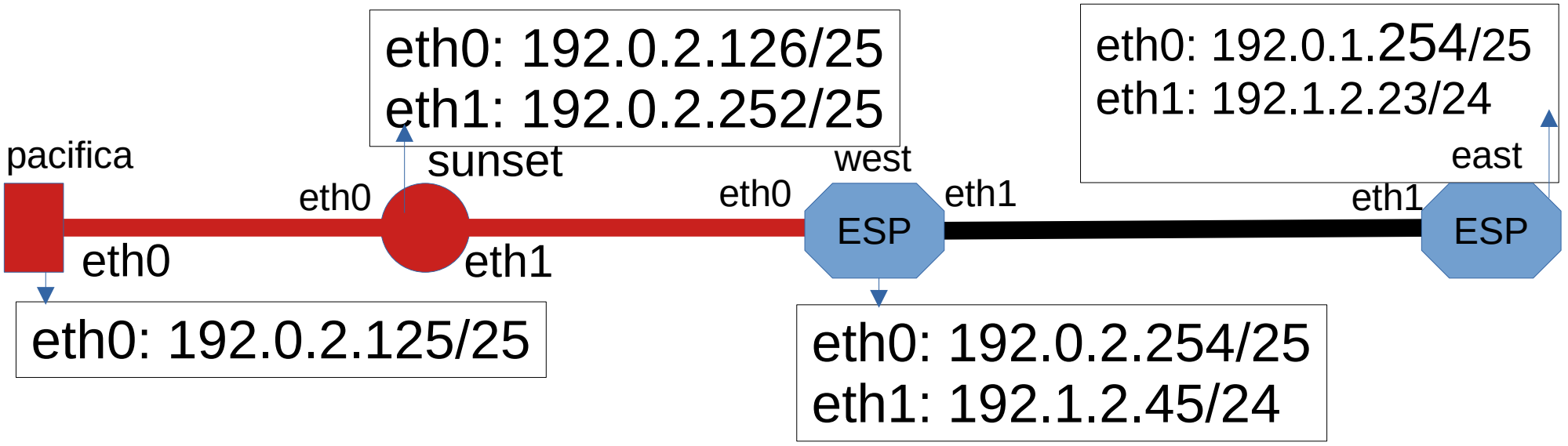
IPsec Background

- IKE is control plane (UDP 500 or UDP 4500)
- ESP is Data plane (ESP or ESP-in-UDP 4500)

Problem Statement

- Diagnose after IKE is established
- ESP packets do not share fate with IKE
- IKE might succeed but ESP packets are dropped
- Hard to detect and recover
- Data traffic is blackholed
- Why Not Use Existing IP Tools?

Why not ping over IPsec?




```
xfrm policy 192.0.2.125/25  <-> 192.0.2.125/25
Xfrm state  192.1.2.23 <=> 192.1.2.23
espping  -I 192.1.2.45  192.1.2.34 <data>
```

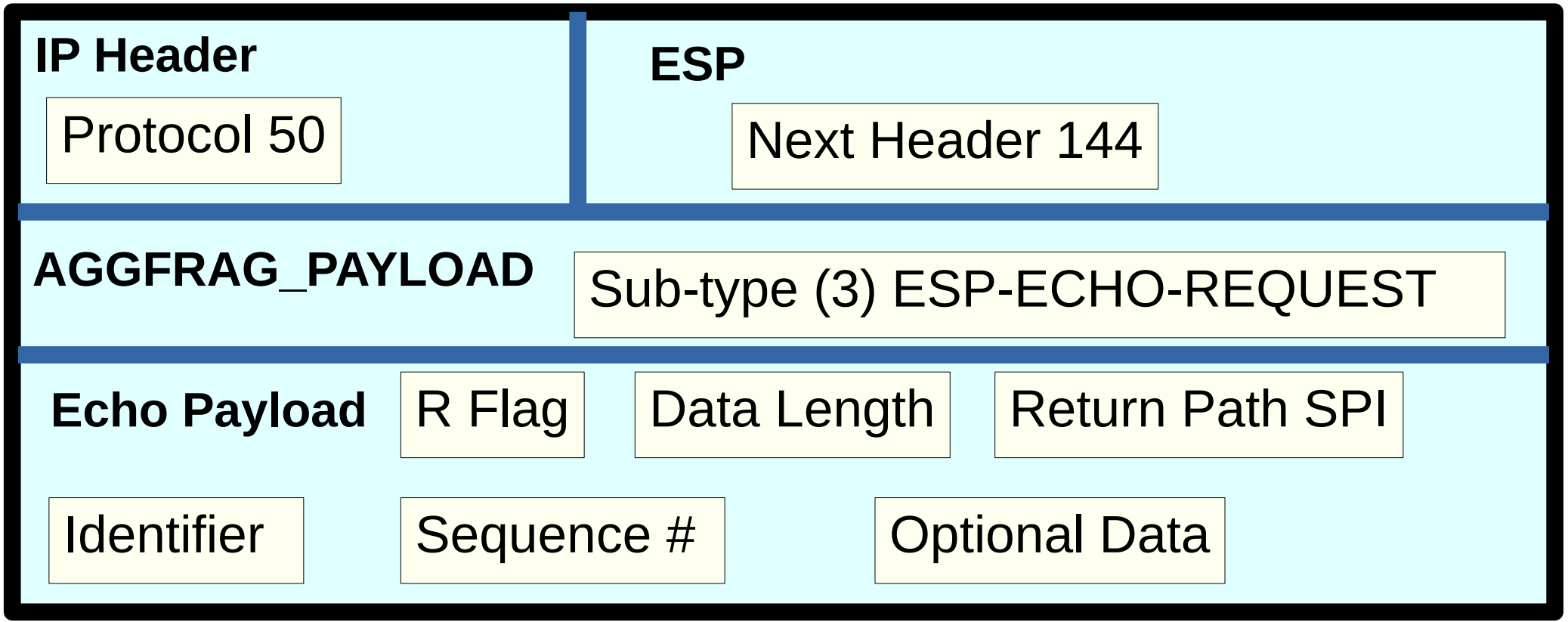
Use cases

- Diagnose ESP Blocked or Filtered
- Probing Multiple ESP Paths to same end point
- Probe Return Path
  - ESP is two unidirectional Security Associations

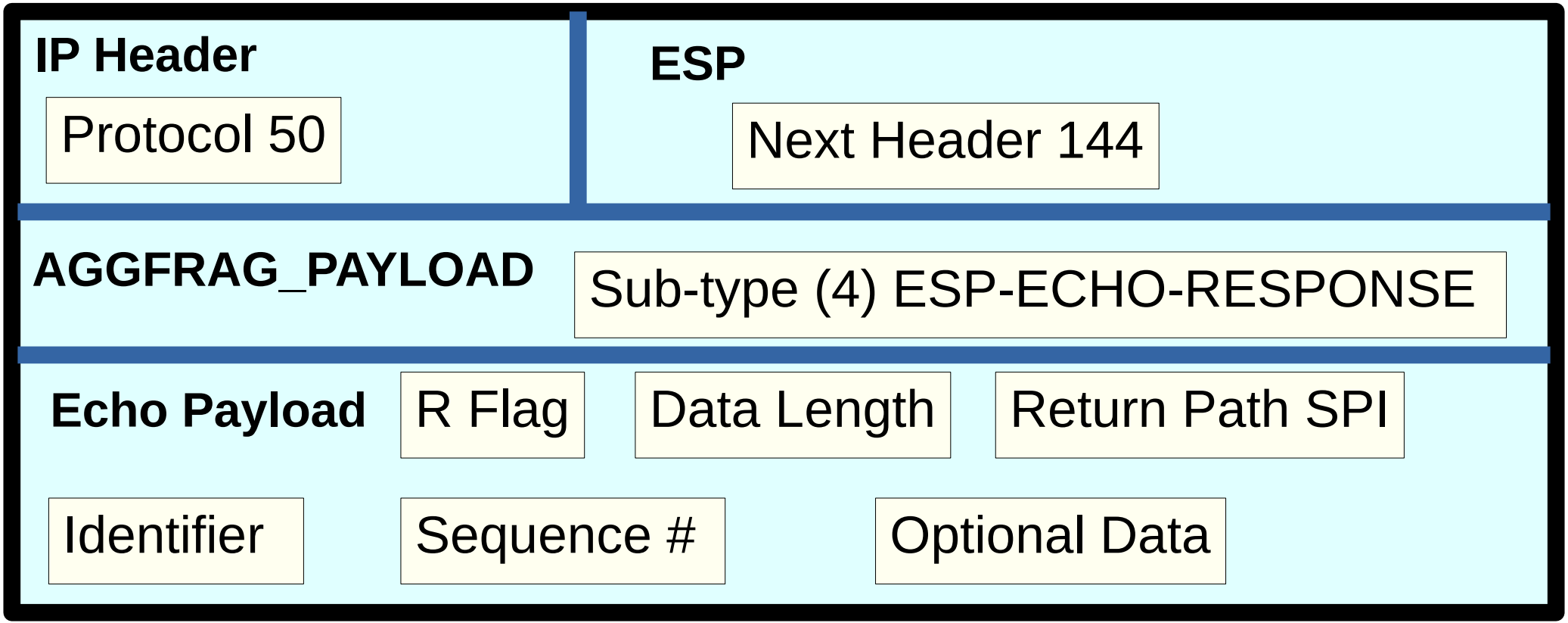
Example

- espping -s <size> -I <src ip> [--spi <spi>] <dst ip>
- espping -I 192.1.2.23 –spi 0xAABBCCDD 192.1.2.45

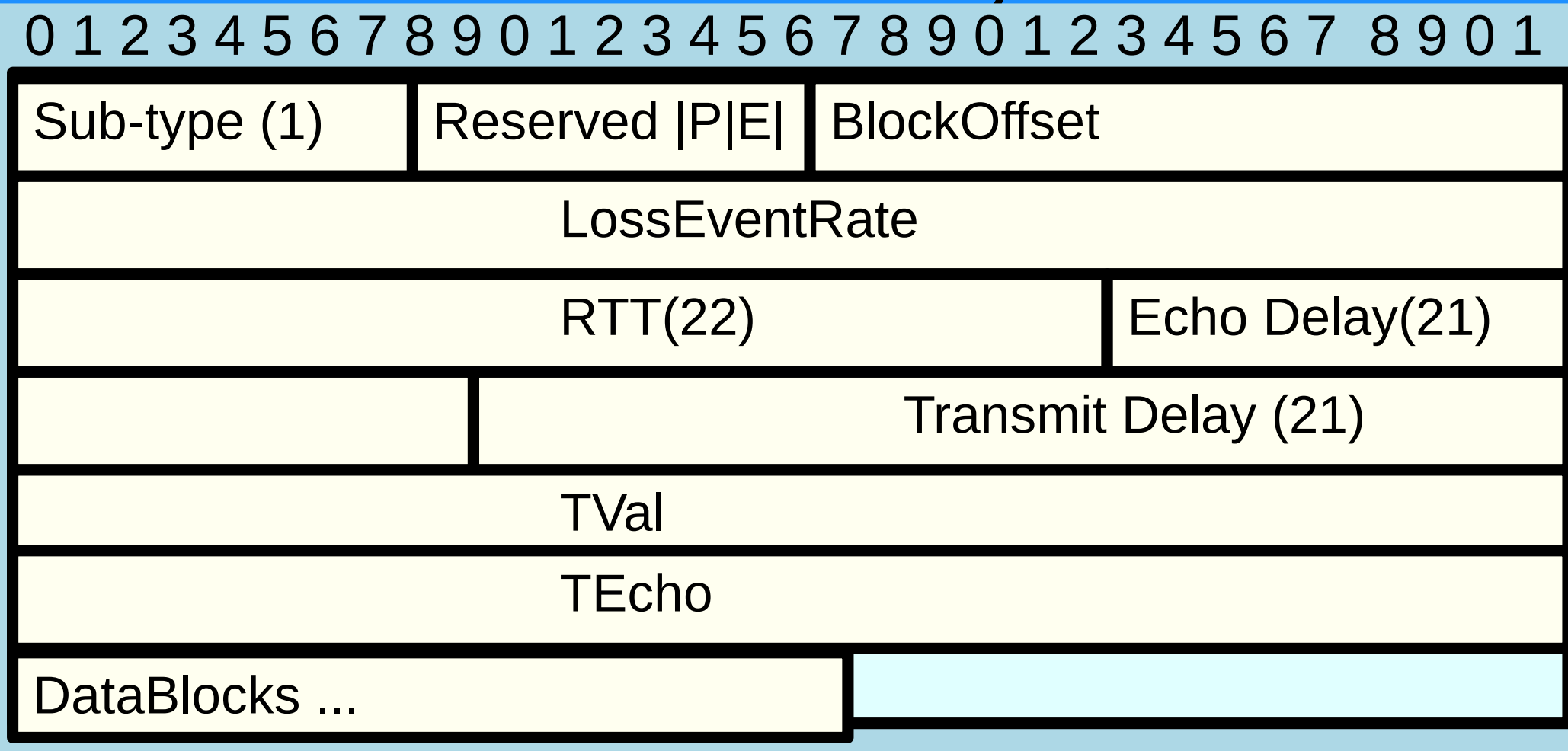
Packet format : Request



Packet format : Response



RFC 9347 CC Payloads



IP-TFC Congestion Control Payload

- CC payload helps to discover path properties:
  - One way delays,
  - loss rate.
  - estimate bandwidth
- Useful to probe manually even when IP-TFS is not negotiated

IKEv2 Notify to announce support?

Add IKEv2 Notification in -03 I.D.

ENCRYPTED_PING_SUPPORTED

SADB Implementation on receiver

- How to validate Return Path requested?
  - SADB is unidirectional
  - Especially when there are multiple SAs
  - Only IKEd knows the return path in its peer DB

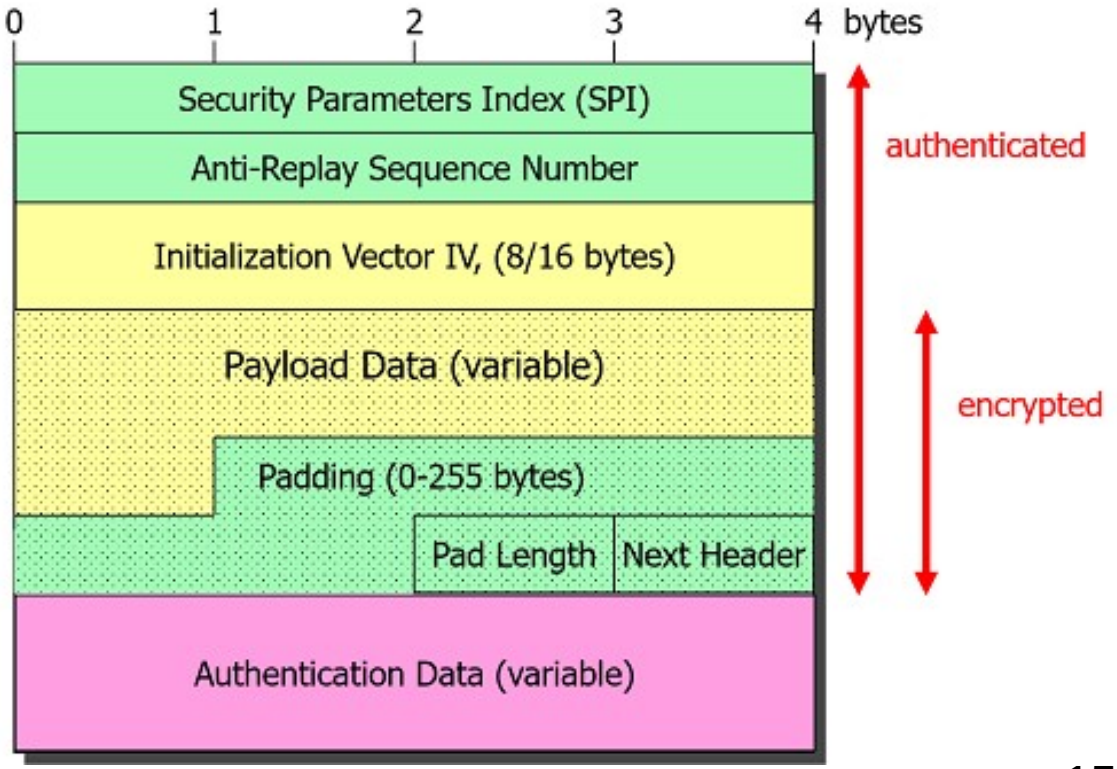
Questions / Feedback?

Adoption?

Similar ideas

- MPLS LSP ping with return path : RFC 7110
- Bidirectional Forwarding Detection (BFD)
  - IP only (Not suitable for Encrypted ESP Ping)
  - https://www.rfc-editor.org/rfc/rfc8562

ESP Message


0
1
2
3
4 bytes
Security Parameters Index (SPI)
Anti-Replay Sequence Number
Initialization Vector IV, (8/16 bytes)
Payload Data (variable)
Padding (0-255 bytes)
Pad Length
Next Header
Authentication Data (variable)
authenticated
encrypted

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• ESP Echo Protocol	Jen Linkova
• Encrypted ESP Ping	Antony Antony
• **Beet mode**	**Antony Antony**
• Multiple sequence counters	Steffen Klassert
• WESPv2	Steffen Klassert
• Diet-ESP	Daniel Migault
• FrodoKEM in IKEv2	Wang Guilin
• PQC Auth	Valery Smyslov

IKEv2 negotiation for BEET Mode

draft-antony-ipsecme-iekv2-beet-mode

IETF 120, Vancouver, July 2024

Antony Antony

secunet

Since IETF 118

Focus only on IKEv2 negotiation for BEET

Goal

- Code Point for IKEv2 BEET mode negotiation
  - BEET defined in Appendix B of RFC 7402

Current Use cases

- For End-to-end tunnels BEET saves bytes.
  - About 20 bytes for IPv4 (without IPv4 options)
  - 40 bytes for IPv6
- HIP RFC 7402, RFC 5202
  - HIP use BEET mode without IKE
- Minimal IPsec RFC 9333

Software support

- Linux initial commit 2006
  - Linux kernel sees several related fixes
- strongSwan supports using private IKE Notify
- Linux iproute2 command line tool to setup SA
  - (ip xfrm mode beet)

Next Steps

- Requesting adoption of this I.D.

- Interest to write RFC 7402 Appendix B bis?
  - Write bis document for just for the Appendix B?
  - Especially to RFC 7402 authors?
    - Would you like to write a BEET mode I.D.?

Questions / Feedback?

Adoption?

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• ESP Echo Protocol	Jen Linkova
• Encrypted ESP Ping	Antony Antony
• Beet mode	Antony Antony
• **Multiple sequence counters**	**Steffen Klassert**
• WESPv2	Steffen Klassert
• Diet-ESP	Daniel Migault
• FrodoKEM in IKEv2	Wang Guilin
• PQC Auth	Valery Smyslov

ESP Problem Statement

draft-mrossberg-ipsecme-multiple-sequence-counters-02

Steffen Klassert

Authors think the draft is complete!

Status

- Version -02 (Feb.)
- Presented at IETF 117 and IETF 118
- Intended status: Informational

What to do now?

- Working group adoption (Informational Draft)
- Anyone gives further feedback
- Let it expire (next month)
- Anything else ???

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• ESP Echo Protocol	Jen Linkova
• Encrypted ESP Ping	Antony Antony
• Beet mode	Antony Antony
• Multiple sequence counters	Steffen Klassert
• **WESPv2**	**Steffen Klassert**
• Diet-ESP	Daniel Migault
• FrodoKEM in IKEv2	Wang Guilin
• PQC Auth	Valery Smyslov

Wrapped ESP v2

draft-klassert-ipsecme-wespv2-01

Steffen Klassert

Why a new security protocol?

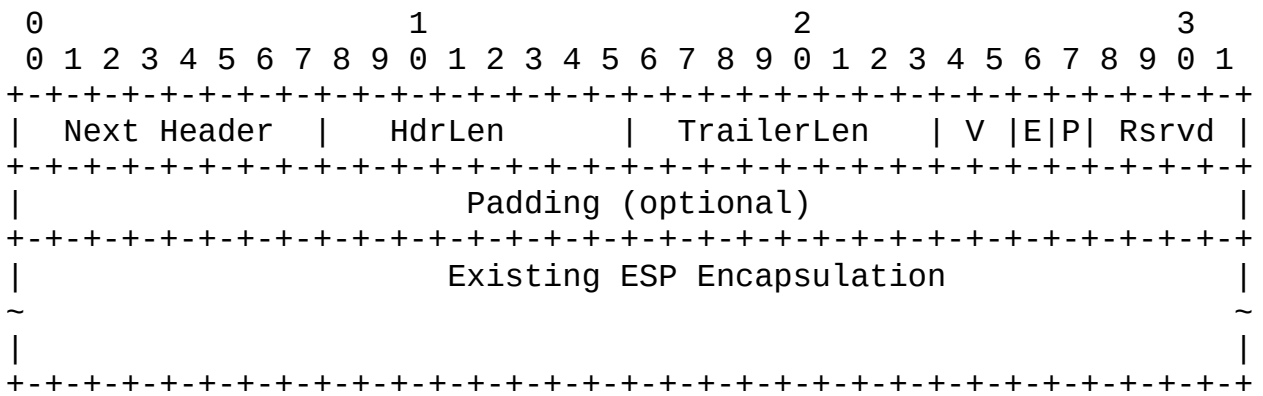
- ESP is unflexible
  - No version number
  - New features must be negotiated
  - Not transparent to the network
- Lot of proposals to extend ESP
  - Suffer from ESP limitations
- Need to be HW offload friendly: Google PSP
  - Similar to ESP but more flexible
  - No standard!

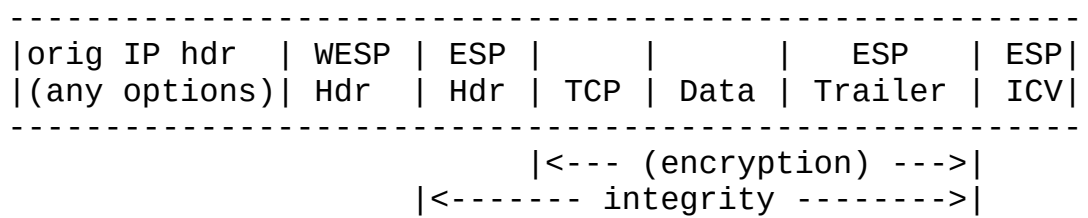
Wrapped ESP (WESP)

WESP

- RFC 5840
- ESP wrapper
- AH replacement
- Has an encryption (E) Flag
    - If set: Packet is authenticated **and** encrypted
    - If not set: Packet is authenticated **but not** encrypted
- Inner packet can be parsed if E is not set
- Has 2 bit version number (version 00 currently)

WESP


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Next Header
HdrLen
TrailerLen
V
E
P
Rsrvd
Padding (optional)
Existing ESP Encapsulation

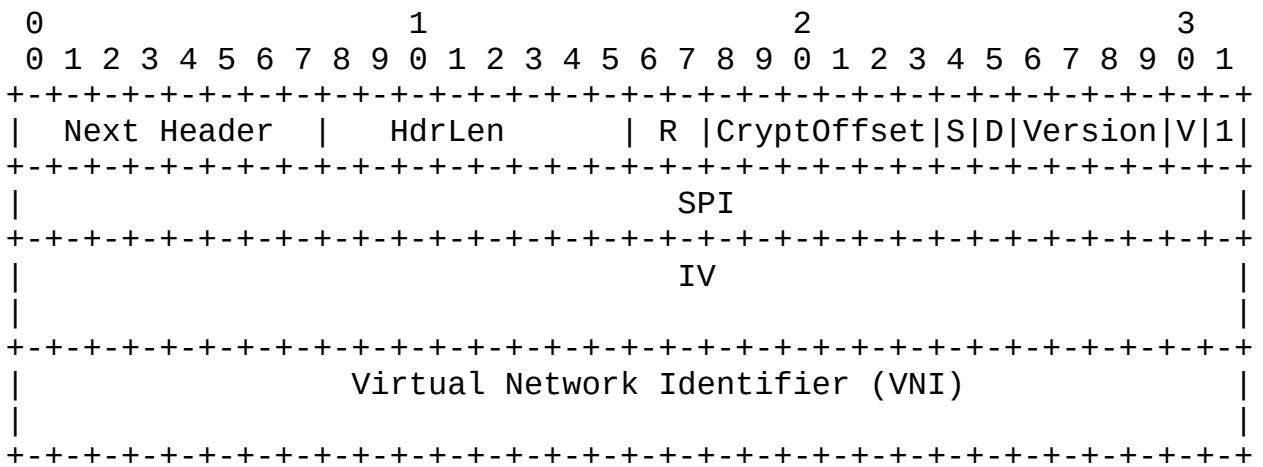

orig IP hdr (any options)
WESP Hdr
ESP Hdr
TCP
Data
ESP Trailer
ESP ICV
<--- (encryption) --->
<------- integrity ------->

Google PSP

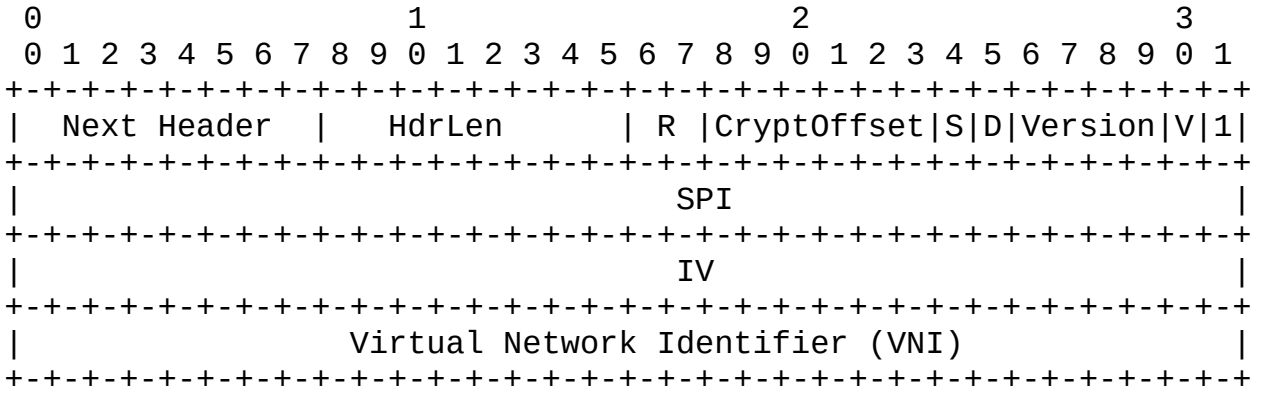
PSP

- Inspired by IPsec/ESP
- Hardware offload friendly
- Used for datacenter security
- Widely deployed at datacenters

PSP


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Next Header
HdrLen
R
CryptOffset
S
D
Version
V
1
SPI
IV
Virtual Network Identifier (VNI)
orig IP hdr (any options)
PSP Hdr
TCP
Pyld Data
PSP ICV
<- encryption ->
<------- integrity ------->

PSP



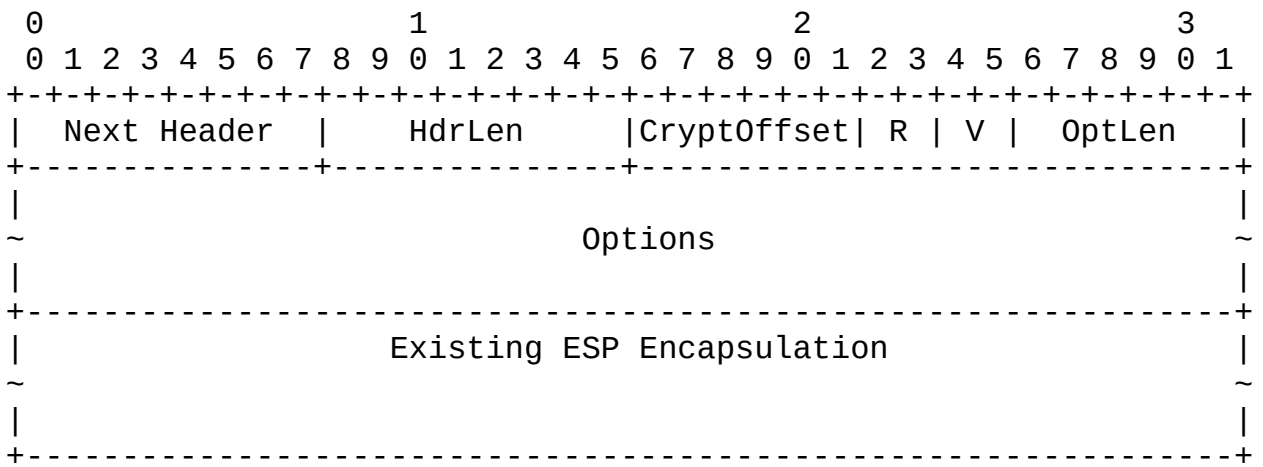
- CyptOffset – Can expose inner headers
- Version – Crypto parameters (algorithm type, keylen)
  - Stateless decryption on RX side
- VNI – Flow Identifier
- No sequence number
  - No replay protection

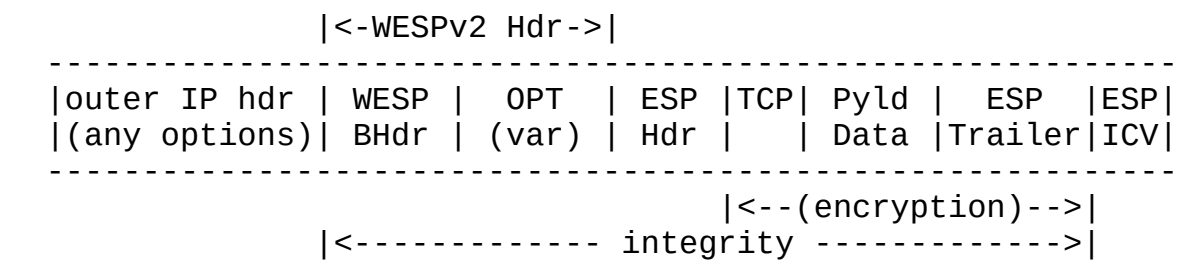
Wrapped ESP v2 (WESPv2)

WESPv2

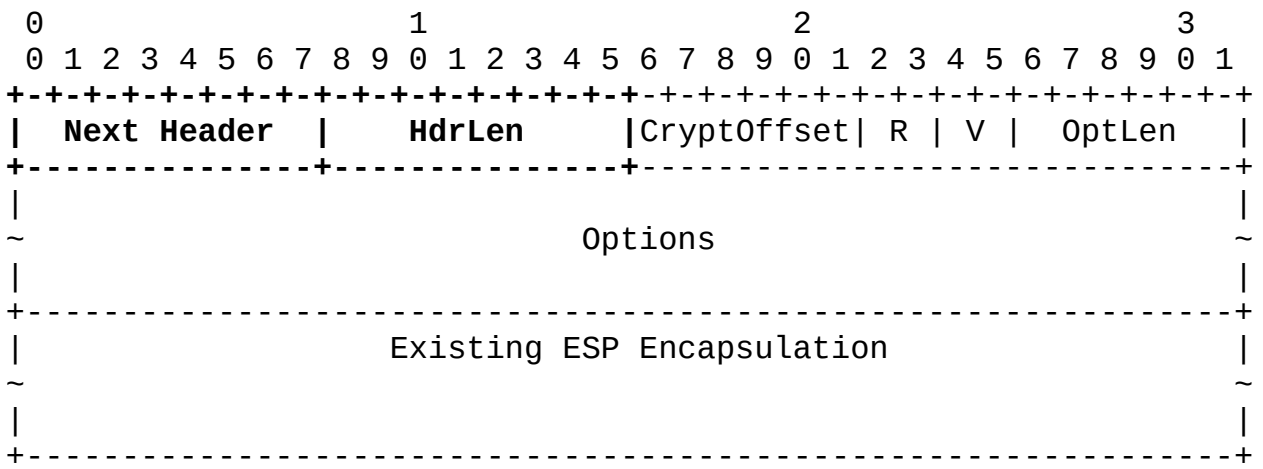
- WESP not widely used
- Has protocol number (141)
- Has version number
- Can match all PSP usecases
- Can carry integrity protected flow information
- Preserves original WESP usecase (partially)

WESPv2


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Next Header
HdrLen
CryptOffset
R
V
OptLen
Options
Existing ESP Encapsulation

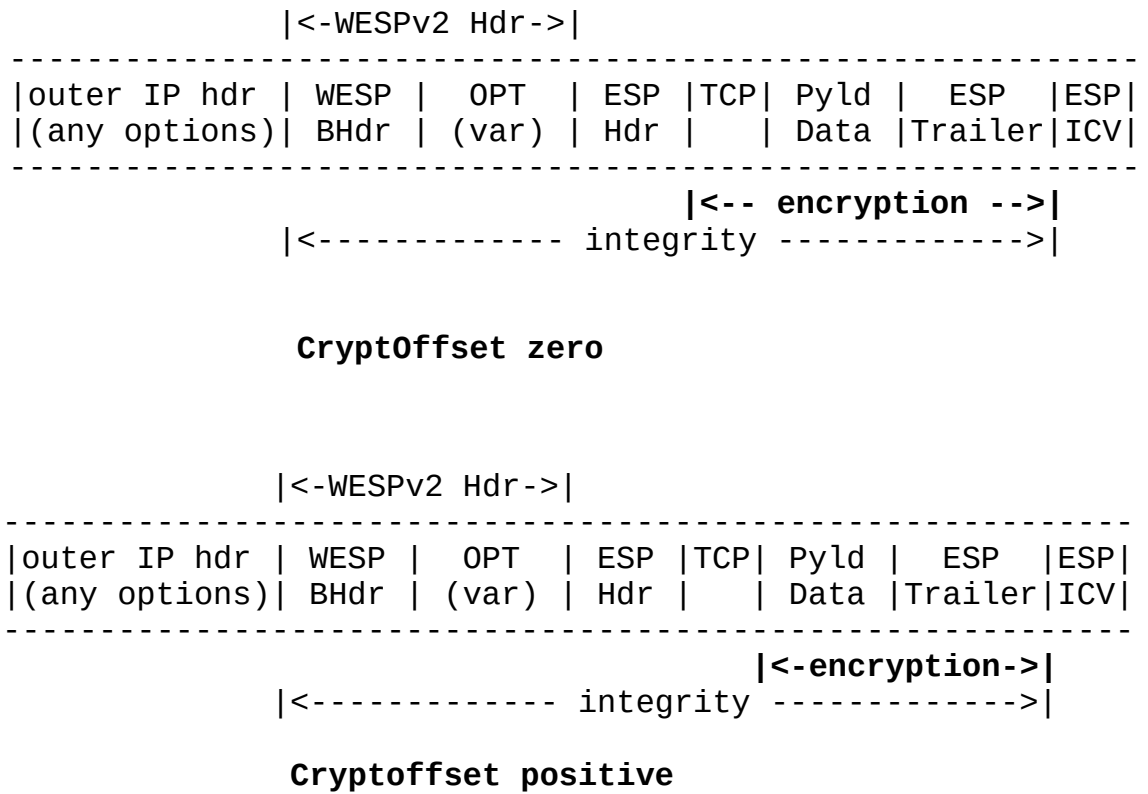

|<-WESPv2 Hdr->|
outer IP hdr (any options)
WESP BHdr
OPT (var)
ESP Hdr
TCP
Pyld Data
ESP Trailer
ESP ICV
|<--(encryption)-->|
|<------------ integrity ------------>|

IPv6 Extension Header Style

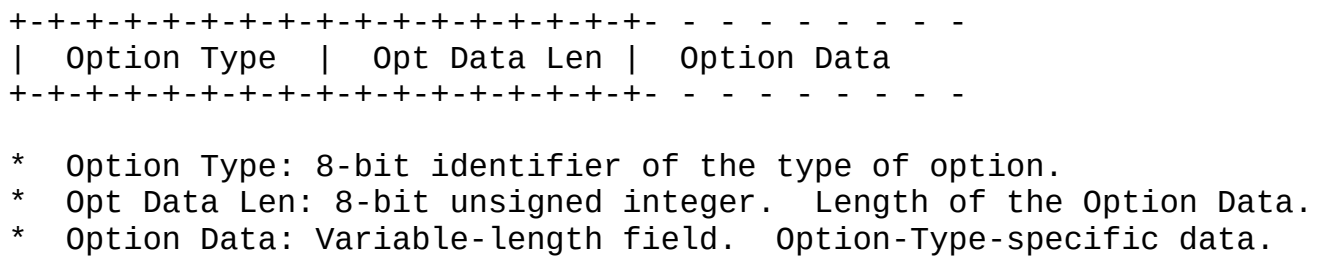


- Complient to RFC 8200 Section 4.8 (Defining new IPv6 Ext. Headers)

CryptOffset



WESPv2 Options



- Options are Type Length Values (TLV)
- Adapted from IPv6 Extension Header Options (RFC 8200 Section 4.2)
- Multiple Options can follow the header
- Future documents can define new Options
- Reserved space for private Options

Option Types

- Padding Options
- Flow Identifier Options
- Private Options
- Future documents can define new Option Types

Padding Options

- Used to align following header (4 byte IPv4, 8 byte IPv6)
- Future usecase: Ciphertext alignment (for SIMD, AVX)

Flow Identifier Options

- Must carry characteristic information of the inner flow
- Detailed specification of Flow Identifiers not in this draft
  - Must be provided by future documents
- Can be used by intermediate devices
  - ECMP
  - RSS

Private Options

- Reserved for private use
- Used for any purposes that are out of scope for standardization
- Can be used to encode hardware specific information

Usecases for Options

- Sequence number subspaces
  - draft-ponchon-ipsecme-anti-replay-subspaces-03
- VPN IDs
  - draft-he-ipsecme-vpn-shared-ipsecsa-00
- Padding for ciphertext alignment

Takeways from IPsec Workshop
and
Netdev Conference

Takeways

- WESPv2 design fits the PSP usecases
- PSP users are willing to migrate to a standardized packet format
- Cryptoffset is needed for telemetry
    - Mandatory for PSP usecase
    - Need to parse L4 headers
    - Never parses more then L4 header

Questions, suggestions?

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• ESP Echo Protocol	Jen Linkova
• Encrypted ESP Ping	Antony Antony
• Beet mode	Antony Antony
• Multiple sequence counters	Steffen Klassert
• WESPv2	Steffen Klassert
• **Diet-ESP**	**Daniel Migault**
• FrodoKEM in IKEv2	Wang Guilin
• PQC Auth	Valery Smyslov

ESP Header Compression Profile

`draft-ietf-ipsecme-diet-esp`

Migault, Hatami, Cespedes, Atwood, Guggemos, Bormann, Schinazi

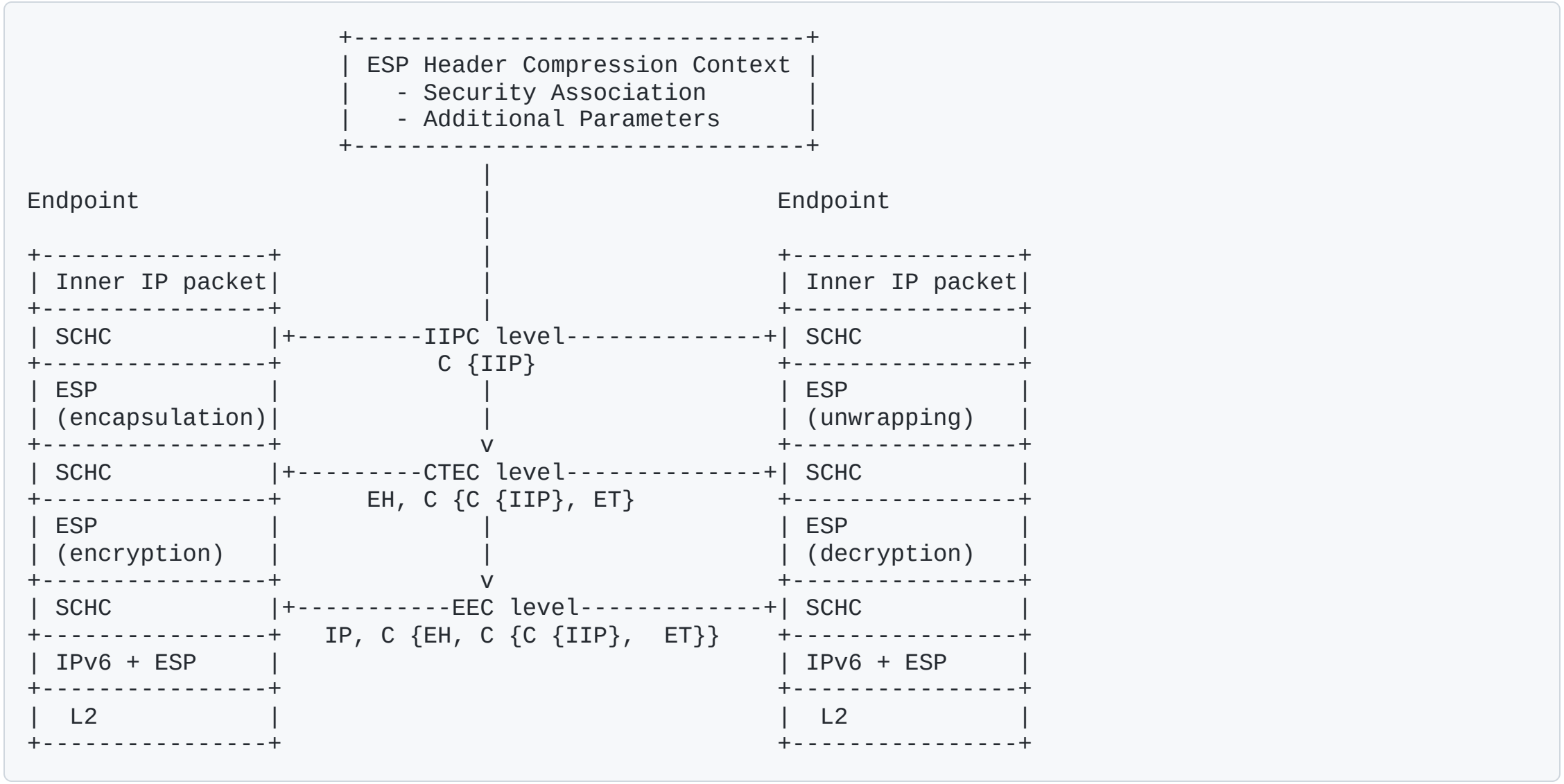
ESP Header Compression Profile (EHCP) defines a profile to compress IPsec/ESP communications.

The description of the Compression / Decompression uses the Generic Framework for Static Context Header (SCHC) [RFC8724].

- Implementations are not expected to use SCHC.

This is a joint work with the SCHC WG

Architecture



Inner IP compression (Tunnel Mode)

ECN (2 bits) is currently uncompressed:

- Should we leave uncompressed ?
- Should we read it from the Tunnel IP Header ?

Unless defined DSCP (6 bits) is read from the Tunnel IP header.

- Should we leave it uncompressed ?
- Does reading DSCP from the Tunnel IP header causes any issue ?

Flow Label (20 bits) can either be uncompressed or completely regenerated by the receiving node.

- Does regenerate it seems an acceptable option ?

Clear Text ESP Compression

In IPv6 and Transport mode, the Next Header (8 bits) MAY designates an IPv6 Extension and so cannot be compressed even if we know the packet is UDP or TCP.

- How much traffic encrypts IPv6 Header Extensions in ESP ?
- Should we spend more effort to compress this ?

- pyesp integrates specs with openschc
  - Plan to finalize pyesp and the specs by the end of the year.
- openschc integrating the parsing of ESP fields.
- (contiki - without SCHC) Diet-ESP: IP layer security for IoT Journal of Computer Security, vol. 25, no. 2, pp. 173-203, 2017 (deprecated)

Thanks!

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• ESP Echo Protocol	Jen Linkova
• Encrypted ESP Ping	Antony Antony
• Beet mode	Antony Antony
• Multiple sequence counters	Steffen Klassert
• WESPv2	Steffen Klassert
• Diet-ESP	Daniel Migault
• **FrodoKEM in IKEv2**	**Wang Guilin**
• PQC Auth	Valery Smyslov

Post-quantum Hybrid Key Exchange in the IKEv2 with ECDH, ML-KEM, and FrodoKEM

IETF 120, IPSECME

Guilin Wang

Wang.guilin@Huawei.com

IKEv2 with FrodoKEM

❑ Information of our daft

- **Title**: Post-quantum Hybrid Key Exchange in the IKEv2 with ECDH, ML-KEM, and FrodoKEM (draft-wang-hybrid-kem-ikev2-frodo-01)
- **Author**: Guilin Wang
- **Dates submitted**: v00 on 2024-04-08; v01 on 2024-05-08
- https://datatracker.ietf.org/doc/draft-wang-hybrid-kem-ikev2-frodo/

❑ General Motivation

- The cryptographic agility of PQ migration has been highlighted by many organizations, like NIST, ETSI, BSI. (see talks at ETSI QSC workshop, May of 2024)
- Algorithm diversity is important to support cryptographic agility
- The availability of various PQC algorithms is beneficial to applications
- Generally speaking, post-quantum algorithms are still not mature yet
- Supporting a good size of various algorithms is also good from engineering aspect

IKEv2 with FrodoKEM

❑Concrete Motivation of this draft

- RFC 9370 specifies a framework that supports up to 7 layers of additional KEMs in IEKv2
- [I-D.KR24] by Panos and Gerardo describes how the framework can be run with ML-KEM (Kyber)
- Some applications demanding high security level may need additional PQ KEMs.
- Based on unstructured lattice based KEM, the security of FrodoKEM more conservative, compared to ML-KEM
- **FrodoKEM** is one of three KEMs in the process of ISO standardization

[**I-D.KR24]** Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2)
draft-kampanakis-ml-kem-ikev2-03
https://datatracker.ietf.org/doc/draft-kampanakis-ml-kem-ikev2/

IKEv2 with FrodoKEM: Challenges

- **Communication**: The public key and ciphertext of FrodoKEM is about 10 times of ML-KEM
- Luckily, the IKE Intermediate Exchange supports large message exchange (but less than 2^{16} - 1 = 65,535 Bytes) (RFC 9242, RFC 7383)
- Also, need 8 or 12 OIDs: Most likely, ISO shall go for 8 parameter sets

Algorithms	secret key sk	public key pk	ciphterext ct	shared secret ss
ML-KEM-512	800	1,632	768	32
ML-KEM-768	1,184	2,400	1,088	32
ML-KEM-1024	1,568	3,168	1,568	32
FrodoKEM-640	19,888	9,616	9,752	16
FrodoKEM-976	31,296	15,632	15,792	24
FrodoKEM-1344	43,088	21,520	21,696	32

Table 1: Size (in bytes) of keys and ciphertexts of ML-KEM and FrodoKEM

IKEv2 with FrodoKEM: An example

```
Initiator                    Responder
-------------------------------------------------------------------
HDR(IKE_SA_INIT), SAi1(.. ADDKE*...), --->
KEi(Curve25519), Ni, N(IKEV2_FRAG_SUPPORTED),
N(INTERMEDIATE_EXCHANGE_SUPPORTED)
    Proposal #1
    Transform ECR (ID = ENCR_AES_GCM_16,
                   256-bit key)
    Transform PRF (ID = PRF_HMAC_SHA2_512)
    Transform KE (ID = Curve25519)
    Transform ADDKE1 (ID = TBD36)
    Transform ADDKE1 (ID = TBD37)
    Transform ADDKE1 (ID = NONE)
    Transform ADDKE2 (ID = TBD43)
    Transform ADDKE2 (ID = TBD45)
    Transform ADDKE2 (ID = NONE)
    Transform ADDKE3 (ID = TBD49)
    Transform ADDKE3 (ID = NONE)
                                                <--- HDR(IKE_SA_INIT), SAr1(.. ADDKE*...),
                                                     KEr(Curve25519), Nr, N(IKEV2_FRAG_SUPPORTED)
                                                     N(INTERMEDIATE_EXCHANGE_SUPPORTED)
                                                     Proposal #1
                                                       Transform ECR (ID = ENCR_AES_GCM_16,
                                                                      256-bit key)
                                                       Transform PRF (ID = PRF_HMAC_SHA2_512)
                                                       Transform KE (ID = Curve25519)
                                                       Transform ADDKE1 (ID = TBD36)
                                                       Transform ADDKE2 (ID = TBD43)
                                                       Transform ADDKE3 (ID = NONE)
HDR(IKE_INTERMEDIATE), SK {KEi(1)(TBD36)} -->
                        <--- HDR(IKE_INTERMEDIATE), SK {KEr(1)(TBD36)}
HDR(IKE_INTERMEDIATE), SK {KEi(2)(TBD43)} -->
                        <--- HDR(IKE_INTERMEDIATE), SK {KEr(2)(TBD43)}

HDR(IKE_AUTH), SK{ IDi, AUTH, SAi2, TSi, TSr } --->
                           <--- HDR(IKE_AUTH), SK{IDr, AUTH, SAr2,TSi, TSr}
```

IKEv2 with FrodoKEM: Comments

Comments by Leonie Bruckert, 15 May 2024

I really appreciate the intention to use FrodoKEM in IKEv2. However, I do not understand why the draft describes the combination of FrodoKEM and ML-KEM instead of just FrodoKEM. I think draft-kampanakis-ml-kem-ikev2 gives us all necessary information how to use ML-KEM in IKEv2. In my opinion, an analogue draft describing the use of FrodoKEM in IKEv2 including assignment of IDs would be very helpful. I do not see the need to describe combinations of KEMs. If we do this, we will soon have large number of drafts describing every possible combination of KEMs.

Feedback on 23 May 2024

Yes, I am happy to remove ML-KEM in this draft, if other experts also think that the combination of ECDH+ ML-KEM+FrodoKEM is not necessary to be described here.

IKEv2 with FrodoKEM

Further Actions

- To add the details about fragmentation of PK and CT
- To align with ISO for acquiring its PQC KEM standardization progress?
- By IPSECME, PQUIP or CFRG?

Invitations

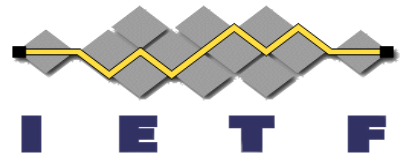
- Welcome to give your kind Suggestions and comments
- If you are interested in this work, welcome to let us know
- Wang.guilin@Huawei.com

Thanks!

Presentations

• Delete info, SA TS Payloads opt, Anti replay notification, Child PFS info	Paul Wouters
• ESP Echo Protocol	Jen Linkova
• Encrypted ESP Ping	Antony Antony
• Beet mode	Antony Antony
• Multiple sequence counters	Steffen Klassert
• WESPv2	Steffen Klassert
• Diet-ESP	Daniel Migault
• FrodoKEM in IKEv2	Wang Guilin
• **PQC Auth**	**Valery Smyslov**

Signature Authentication in the IKEv2 using PQC

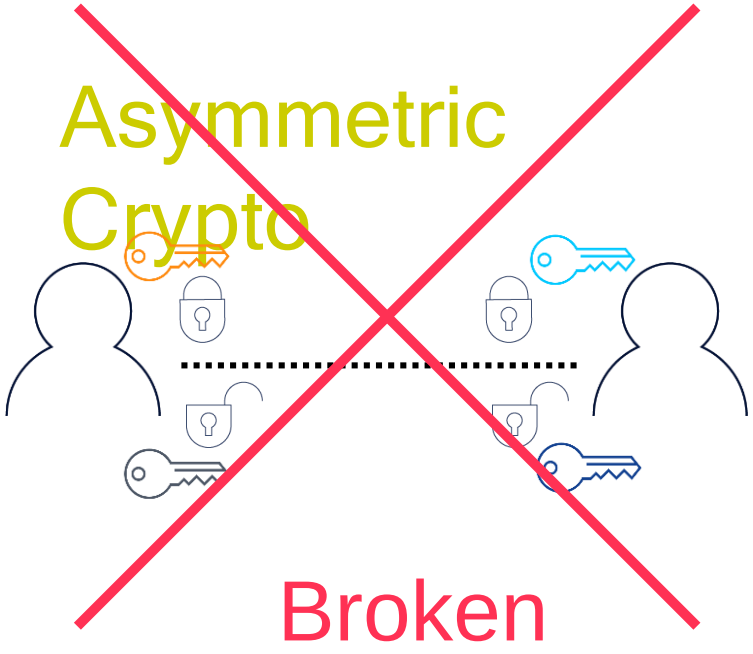


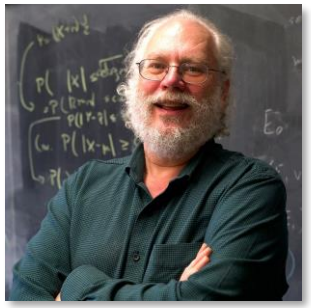
draft-reddy-ipsecme-ikev2-pqc-auth

Tirumaleswar Reddy, **Valery Smyslov**, Scott Fluhrer

IETF 120, Vancouver

Impact of Quantum Computers in Cryptography





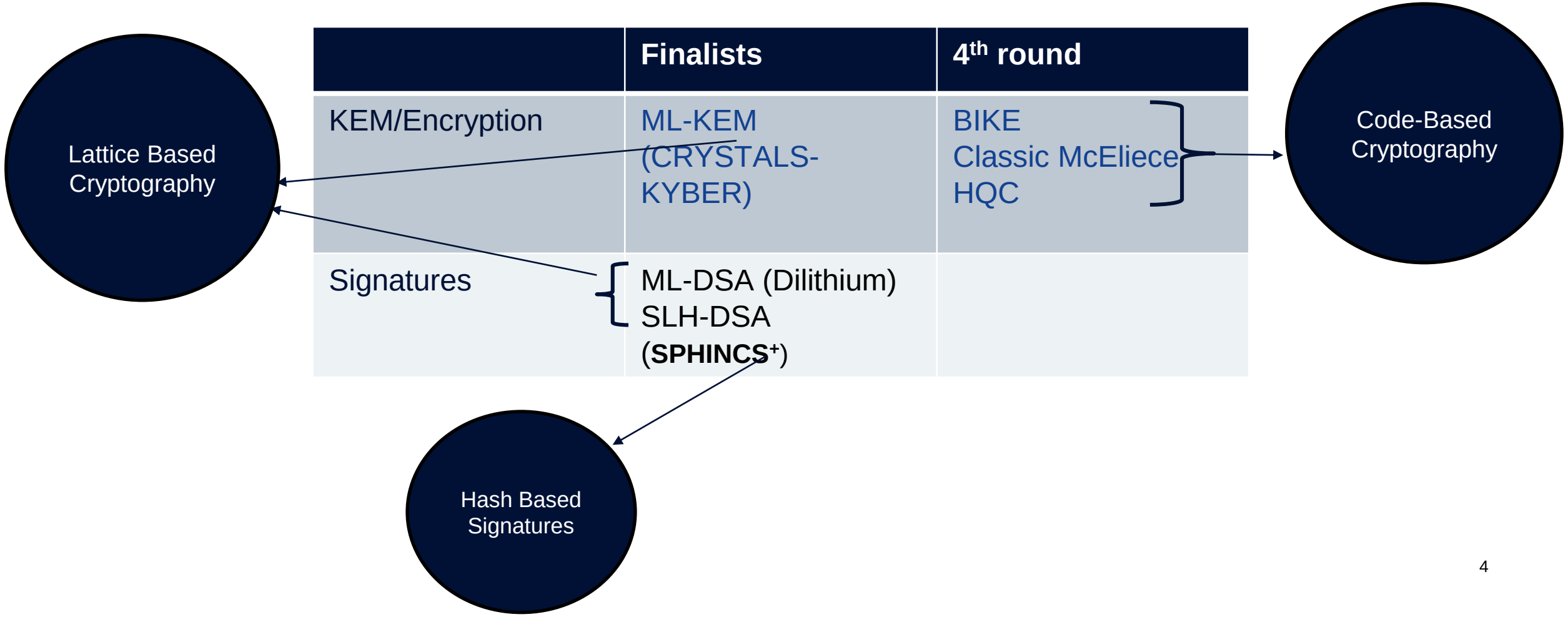
Peter Shor

Algorithm for prime factorization of large integers

PQC Auth in IKEv2

- IKEv2 relies on traditional algorithms vulnerable to quantum attacks, like RSA and ECDSA.
- Introduce PQC signatures for authentication in IKEv2.
  - Enhance security against potential future cryptographically relevant quantum computer attack that could break current asymmetric cryptographic algorithms.

NIST Candidates Selected for Standardization



	Finalists	4th round
KEM/Encryption	ML-KEM (CRYSTALS-KYBER)	BIKE Classic McEliece HQC
Signatures	ML-DSA (Dilithium) SLH-DSA (**SPHINCS+**)	

ML-DSA in IKEv2

- ML-DSA in X.509 certificates is defined in https://datatracker.ietf.org/doc/draft-ietf-lamps-dilithium-certificates/
- ML-DSA algorithm in IKEv2 at three PQ security levels:
  - ML-DSA-44:
    - PQ Security Level: 2
    - AES/SHA Hardness: Comparable to SHA-256/SHA3-256 (collision search)
  - ML-DSA-65 :
    - PQ Security Level: 3
    - AES/SHA Hardness: Comparable to AES-192 (exhaustive key recovery)
  - ML-DSA-87 :
    - PQ Security Level: 5
    - AES/SHA Hardness: Comparable to AES-256 (exhaustive key recovery)
- ML-DSA can be used in both deterministic and randomized signing mode.

SLH-DSA in IKEv2

- SLH-DSA in X.509 certificates is defined in https://datatracker.ietf.org/doc/draft-ietf-lamps-cms-sphincs-plus/
- SLH-DSA algorithm in IKEv2 at three security levels.
  - It includes the small (S) or fast (F) versions of the algorithm
  - Use of either SHA-256 or SHAKE256 as the hash function.
- SLH-DSA algorithm in IKEv2 at three security levels:
  - SLH-DSA-128{S,F}-{SHA2,SHAKE}
  - SLH-DSA-192{S,F}-{SHA2,SHAKE}
  - SLH-DSA-256{S,F}-{SHA2,SHAKE}
- SLH-DSA can be used in both deterministic and randomized signing mode.

Signaling support for PQC signatures

- The initiator could indicate in the Certificate Request payload that it trusts a CA certificate signed by an ML-DSA or SLH-DSA key.
- Leverage ipsecme-ikev2-auth-announce that allows peers to announce their supported authentication methods.

Next Steps

- Comments and suggestions are welcome
- Consider for WG adoption

Open Discussion

- Other points of interest?