Framework to Integrate Post-Quantum Key Exchanges into IKEv2

C. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer,
D. van Geest, Z. Zhang, O. Garcia-Morchon

IETF 101

Agenda

- Quick Recap on Version 00
- Design Criteria
- Version 01
- Questions for the WG

Recap on Version 00

- Performs a post-quantum key exchange in parallel with Diffie-Hellman key exchange in IKE_SA_INIT.

```
Initiator                                    Responder
--------------------------------------------------------------------------------
HDR, SAi1, KEi, [ QSKEi,]
      Ni                                -->
                                        <--  HDR, SAr1, KEr, [ QSKEr,]
                                                   Nr, [CERTREQ]
```

- Requires a new transform type and a new payload type.
- Relies on RFC 8229 (TCP encapsulation) to deal with fragmentation.
- Feedback receives:
  - Don’t introduce a new transform type
  - Need to handle fragmentation over UDP

Design Criteria

1. Need for PQ key-exchange
2. Hybrid key-exchange
3. Focus on quantum-resistant confidentiality
4. Limit the amount of data exchanged
5. Future proof
6. Efficient negotiation of hybrid algorithms
7. Supports for fragmentation
8. Backward compatibility and interoperability
9. FIPS compliance

Version 01 - Backward Compatibility

- Backward compatibility and interoperability issues when handling unknown transform types
  - Potential issues in handling unknown payload (not notification payload)
- Need to meet the following points:
  - No new transform types, unless we know the peer supports it
  - No new payload type, unless we know the peer supports it
  - Okay to introduce a new notification payload

Version 01 - Backward Compatibility (cont’d)

- Use KE payload to negotiate hybrid key exchange algorithms
  - New value is assigned for `Diffie-Hellman Group Num` field, which denotes a hybrid group
  - The `Key Exchange Data` field does not contain DH or PQ public value, but proposed PQ algorithms and the associated policy.
- Two-phase approach

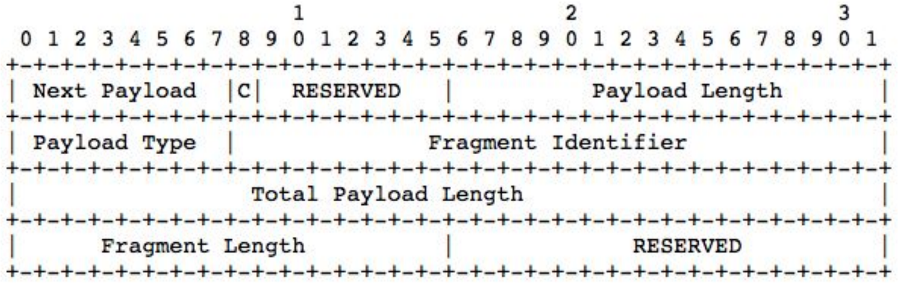
```
Initiator                                            Responder
-------------------------------------------------------------
        <-- First round (hybrid group negotiation) -->

     <-- Second round (hybrid quantum-safe key exchange) -->
```

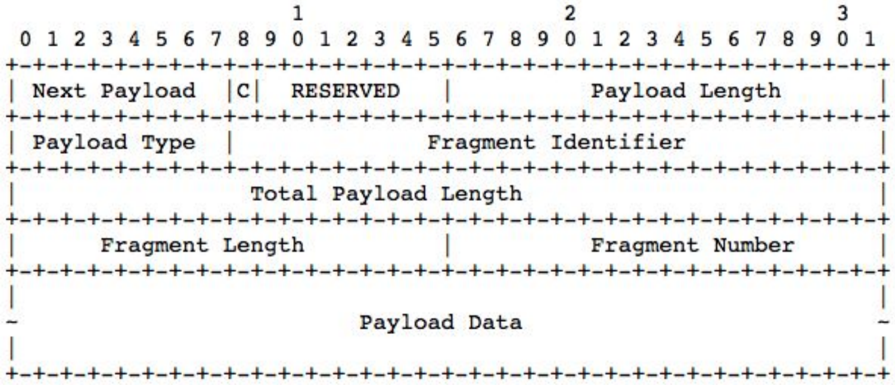
- Multiple KE payloads to carry hybrid key exchange public values.

Version 01 - Fragmentation

- Public key and ciphertext size of PQ cipher is large
  - More than one PQ cipher may be exchanged
- Our approach is to fragment individual payloads, rather than the entire IKE packet
- FRAG_POINTER and FRAG_BODY payloads



```
                     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 Payload  |C|  RESERVED   |         Payload Length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Payload Type  |              Fragment Identifier              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Total Payload Length                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Fragment Length        |           RESERVED              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



```
                     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 Payload  |C|  RESERVED   |         Payload Length        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Payload Type  |              Fragment Identifier              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Total Payload Length                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Fragment Length        |         Fragment Number         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                        Payload Data                           ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

FRAG_POINTER **FRAG_BODY**

Version 01 - Downgrade Attack Prevention

- In RFC 7296, the full set of group proposal is always resent in subsequent IKE_SA_INIT if responder chooses a different DH group
- Keep the same principle in this draft
    - The full set of proposal is sent via Notify payload in the second round of IKE_SA_INIT message pair
- A number of ways to check for downgrade attack
    - Allocate states
    - Relies on IKE_AUTH
    - COOKIE

Questions to WG - Design Criteria

1. Need for PQ key-exchange
2. Hybrid key-exchange
3. Focus on quantum-resistant confidentiality
4. Limit the amount of data exchanged
5. Future proof
6. Efficient negotiation of hybrid algorithms
7. Supports for fragmentation
8. Backward compatibility and interoperability
9. FIPS compliance

Questions to WG - Dealing with Fragmentation

```
Initiator                                                  Responder
------------------------------------------------------------------------------------------------------------
HDR(IKE_SA_INIT, MID=0), SAi1, KEi, Ni,    -->
    N(IKEV2_FRAG_SUPPORTED), N(PRE_AUTH_SUPPORTED)
                                                           HDR(IKE_SA_INIT, MID=0), SAr1, KEr, Nr,
                                           <--                     N(IKEV2_FRAG_SUPPORTED), N(PRE_AUTH_NEEDED), [CERTREQ]


HDR(PRE_AUTH, MID=1),                      -->
    SKF(NextPld=PLD1, Frag#=1, TotalFrags=m){...}
                                           •••
HDR(PRE_AUTH, MID=1),                      -->
    SKF(NextPld=0, Frag#=m, TotalFrags=m){...}

                                           <--      HDR(PRE_AUTH, MID=1),
                                                       SKF(NextPld=PLD1, Frag#=1, TotalFrags=m){...}
                                           •••
                                           <--      HDR(PRE_AUTH, MID=1),
                                                       SKF(NextPld=0, Frag#=2, TotalFrags=m){...}


                                       IKE_AUTH stage
```

Thank You