Minimal ESP

draft-mglt-lwig-minimal-esp-00.txt

D. Migault, T. Guggemos

25/02/2014- IETF89- London

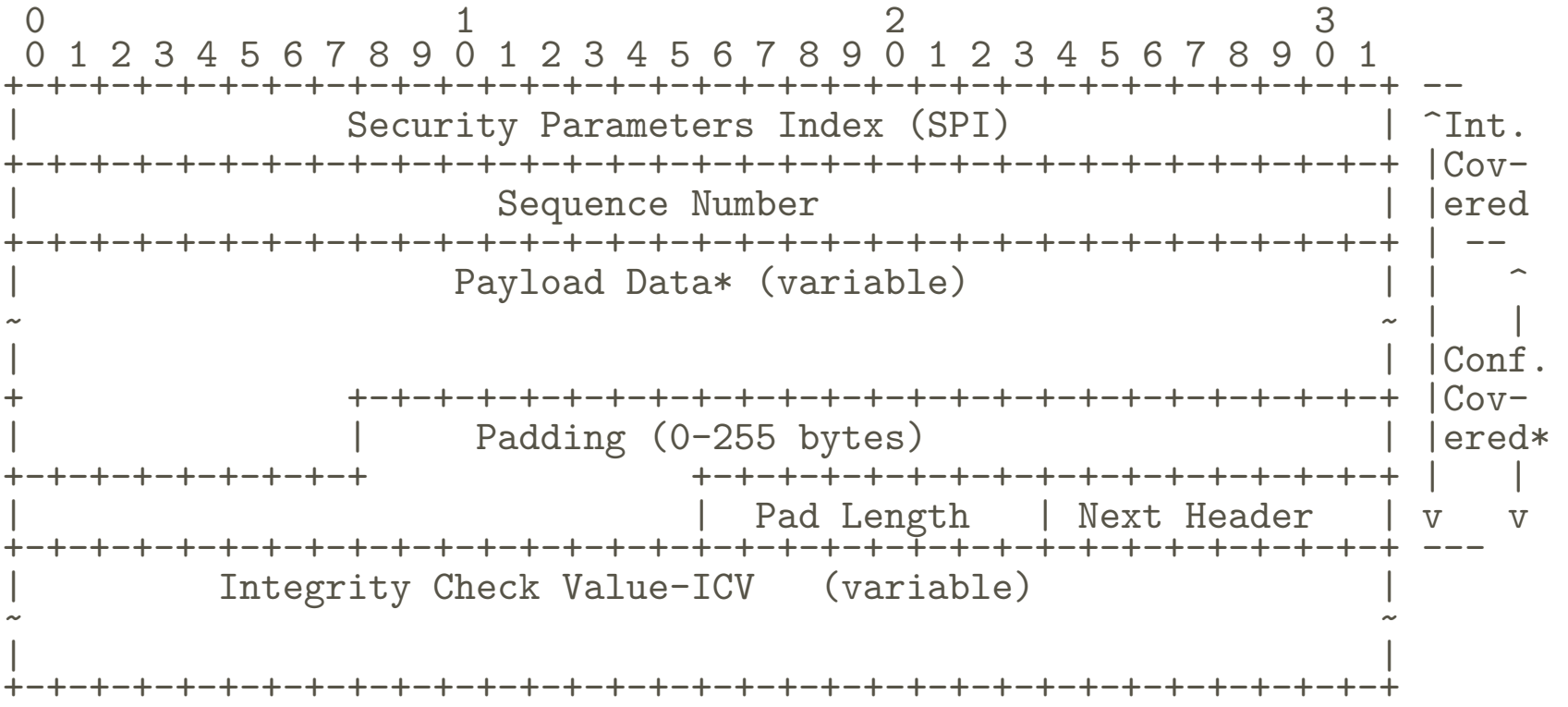
Minimal ESP

ESP [RFC4303] is and IPsec protocol.

Our Goals are to:

- Remove unnecessary parameters/options (there none for ESP)
- Provide guidance that simplifies ESP implementation
  - Choice of algorithm to reduce the sent payload
  - Choice of algorithms that can be used both for encryption and authentication and reduce the code
  - Choice for values to reduce computation
- Remain standard compliant for interoperability

IPsec / ESP


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
Security Parameters Index (SPI)
Sequence Number
Payload Data* (variable)
Padding (0-255 bytes)
Pad Length
Next Header
Integrity Check Value-ICV (variable)
^Int.
|Cov-
|ered
Conf.
Cov-
ered*

ESP Parameters

Security Parameters Index (SPI):

- Mandatory 32 bits
- For single connection device: predefined random / IPv4 / MAC / IPv6

Sequence Number (SN): The IoT context the sender MAY know if the Anti-Replay protection is enabled or disabled:

- Mandatory 32 bits
- If you KNOW the receiver do not implement SN, then fix it to zero.
  - RFC4303 ask the sender increments SN
  - Can we make this simplification?

ESP Parameters

Padding / Pad Length

- Mandatory 8 bits for Pad Length
- Padding is useless sent data on the wire.
- Use CTR mode in stead of CBC
  - CTR has no block size, CBC got block size (128 for AES)
- Clever alignment by the application
  - Ex: fix size application payload...
  - Reduces/prevent Padding
  - Padding / Pad Length are fixed for one cipher

ESP Parameters

Next Header (NH):

- Mandatory 8 bits
- Transport Layer protocol is specified in:
  - The packet
  - Eventually in the SA (Traffic Selector)
- For specific configurations:
  - Sender does not have to calculate the field
  - Receiver can ignore the Next Header field and read it from the SAD

Encryption / Authentication

Encryption:

- Prefer algorithm benefiting from hardware acceleration (e.g. AES-NI)
- Prefer CTR to CBC
  - Reduced Padding (no block size for AES-CTR, 128 bit block size for AES-CBC)
  - Reduced IV (8 bytes for AES-CTR vs 16 for AES-CBC)

Authentication:

- Use algorithm which reuse cipher implementation
  - e.g. HMAC-AES-XCBC instead of SHA1
  - Reduce required ROM space for cipher algorithm
  - Enables benefit of hardware acceleration (e.g. AES-NI)

Thank you for your attention

Looking for a PhD
tobias.guggemos@gmail.com