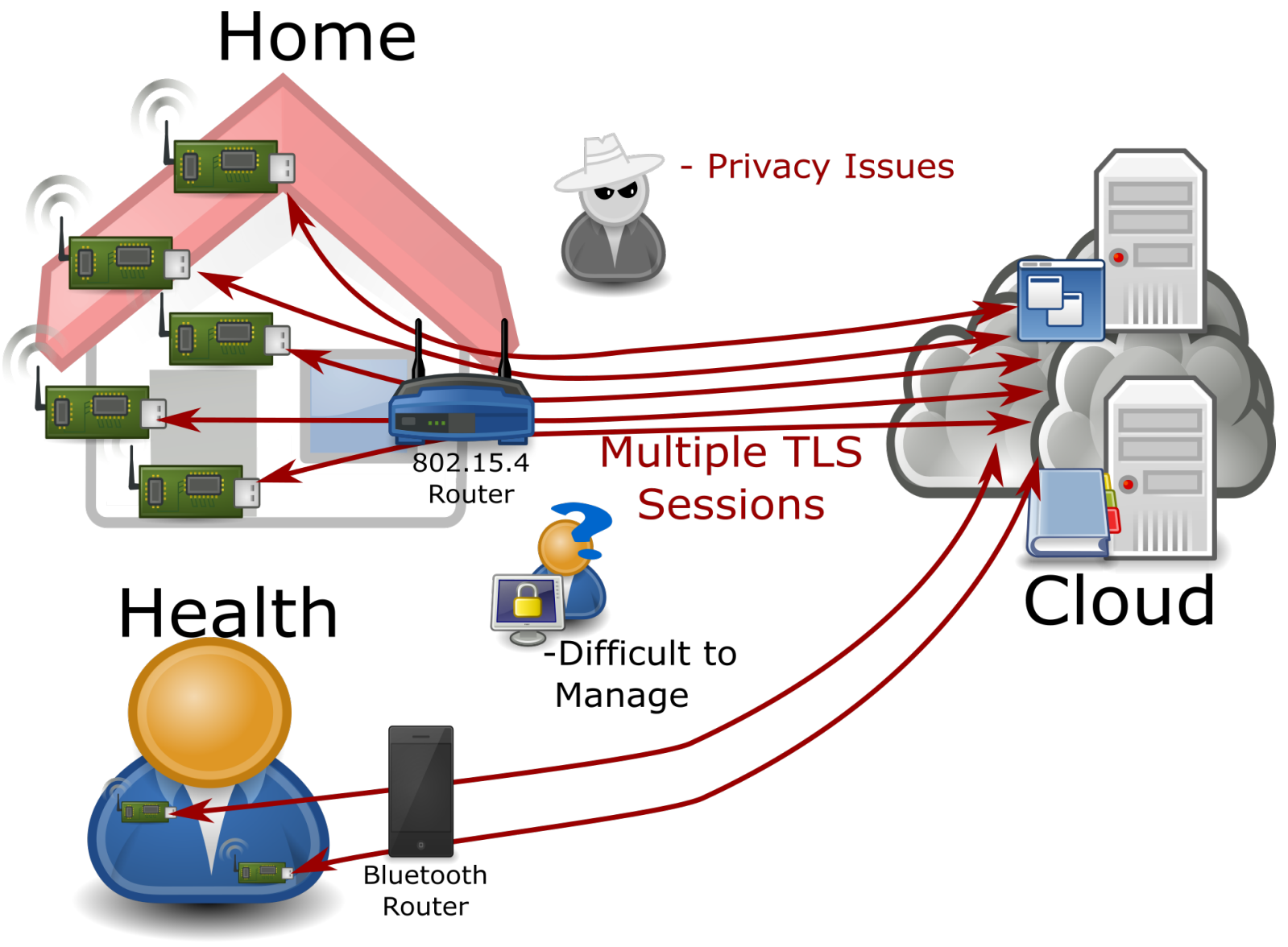
Minimal ESP

draft-mglt-lwig-minimal-esp-02.txt

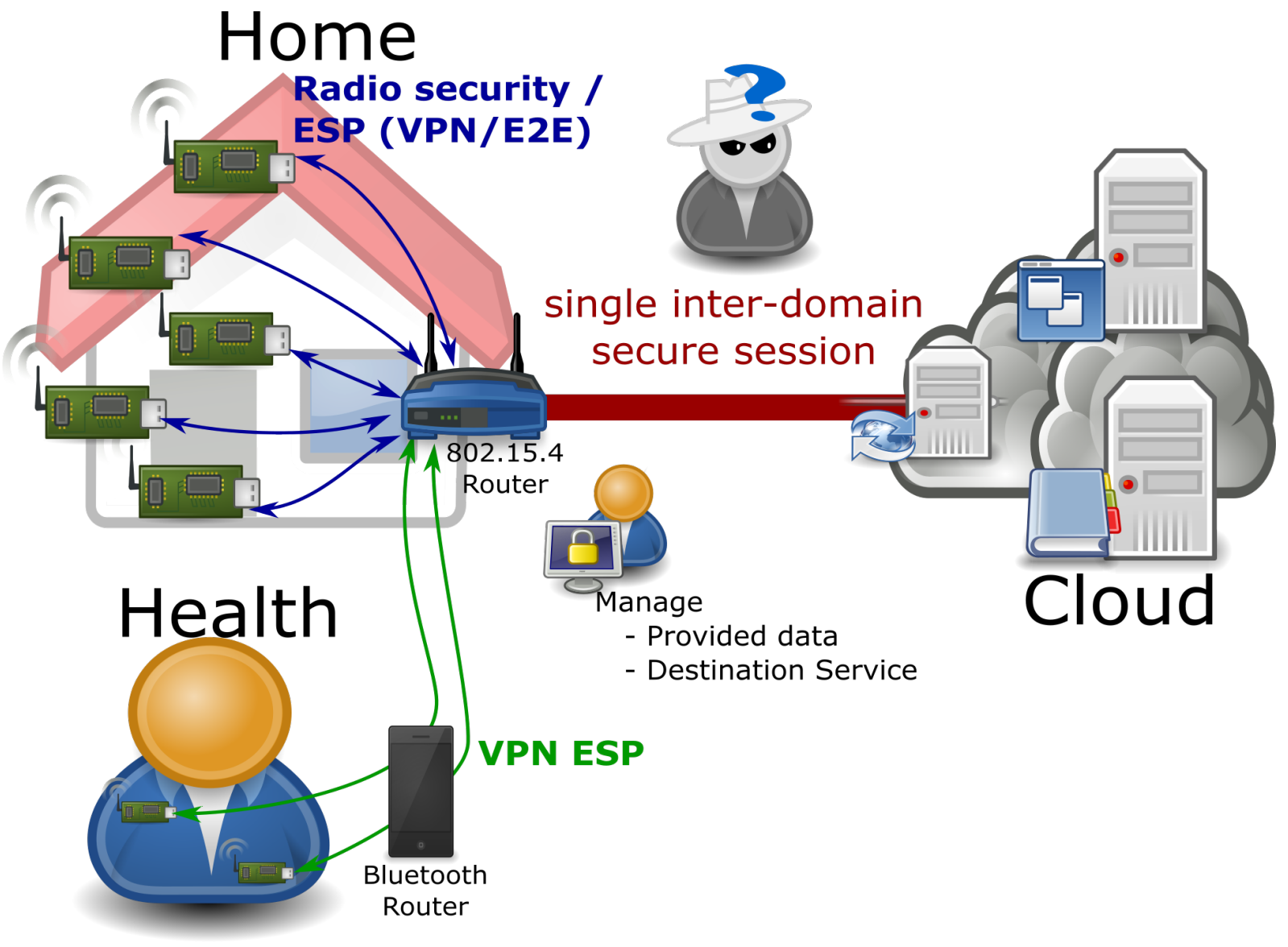
D. Migault, T. Guggemos

22/07/2016- IETF96- Berlin

Motivation - E2E Security



Motivation - Domain Security



ESP Features

There are significant scenarios that shows:

- IPsec/ESP complements (D)TLS/DICE

IPsec/ESP got significant features that justify to have ESP for IoT, e.g:

- Domain Security
- Multicast Security

Security & Privacy :

- Secures the transport layer
- Avoids disclosure of the application (port)/ sensor involved (IP)

ESP Features

Flexibility:

- ESP is independent of key exchange protocols
  - IKEv2 (We already have Minimal IKEv2 [RFC7815])
  - DEX
  - GDOI [RFC6407] (Multicast)
  - Other (3GPP)

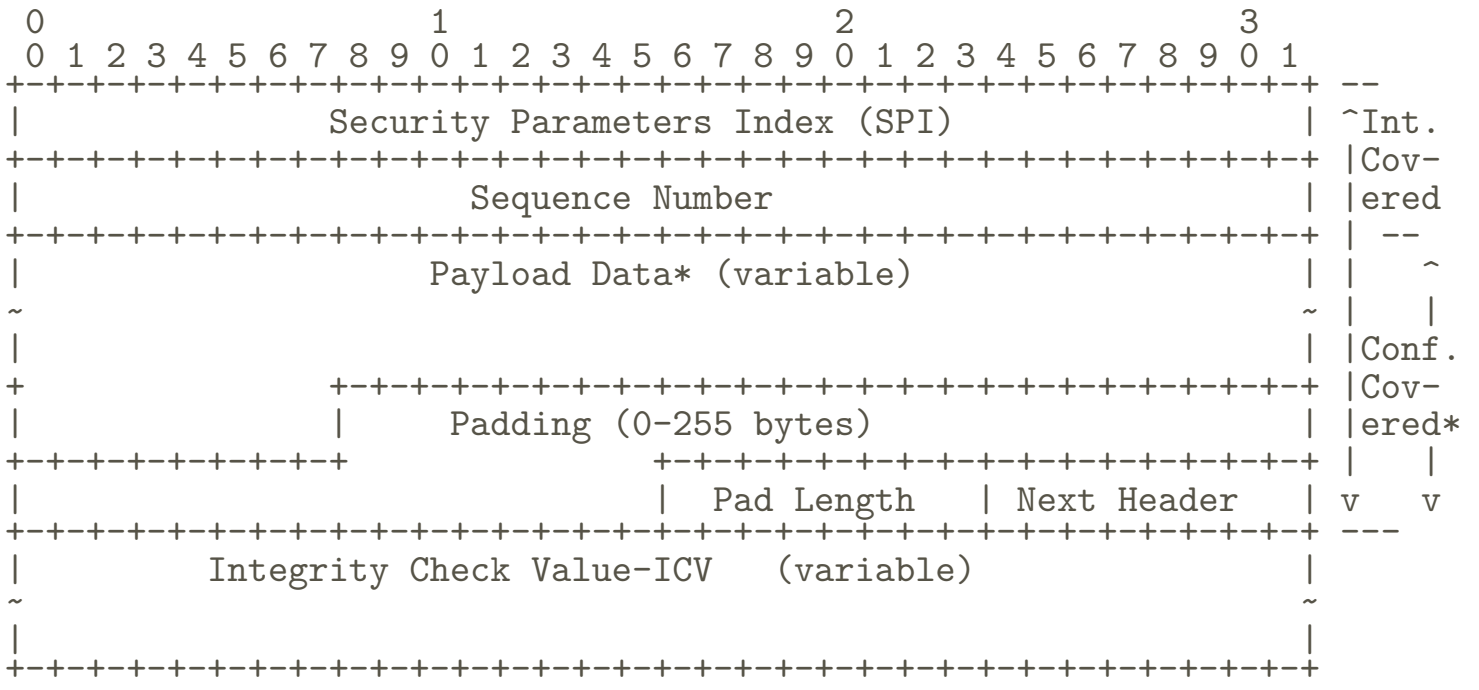
Goals of Minimal ESP

Implement IPsec/ESP [RFC4303] in small homenet devices and IoT

The document provides guidances on implementation experience:

- Remain IPsec/ESP [RFC4303] fully compatible
- How to build all IPsec/ESP fields
- Which crypto-suites to implement [RFC7321bis]

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) [Mandatory 32 bits]:

- To avoid maintaining a counter: time may be used

Padding [variable] / Pad Length [Mandatory 8 bits]:

- Address the 32 bit IPv4 Header and 64 bit IPv6 Header alignment
- May be part of the encryption (AES-CBC 128 bit block size)
- May not be part of IPsec/ESP:
  - Set Padding to Zero instead of random, counters...
- Document impact of fixed size data on Padding

Next Header (NH) [Mandatory 8 bits]:

Next

- 6Lo WG agreed on having IPsec ESP to the IoT toolbox.
- IPsecME WG adresses IoT requirements in its updated charter
  - Implicit-IV
  - Cipher supports [RFC7321bis]
- We already have Minimal IKEv2 [RFC7815]

$\Rightarrow$ We would like this document to be accepted as a document WG document.

Thank you for your attention

Encryption / Authentication

Encryption:

- Prefer algorithm benefiting from hardware acceleration (e.g. AES-NI)
- Prefer AES-CTR to AES-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)
- (MAY) Prefer AES-CBC to AES-CTR:
  - For full interoperability AES-CBC is mandatory

Authentication:

- Use algorithm which re-use 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)