draft-mglt-ipsecme-diet-esp-04

IPsecME WG @ IETF 99
21.07.2017

Daniel Migault, Tobias Guggemos, Carsten Bormann

Motivation / History of Diet-ESP

→ Support for Diet-ESP in 6Lo at IETF 96 in Berlin

→ Asked to move to ipsecme

→ Re-design of Diet-ESP:

- changed Diet-ESP to ESP Header Compression (EHC)
- replaces ROHC by one similar to SCHC (LWPAN WG)
  - defines EHC Rules, coordinated by and EHC Strategy
  - Diet-ESP as one of these strategy

→ Implementations:

- Contiki
- Python
- RIOT and Linux (ongoing work)

→ Publication:

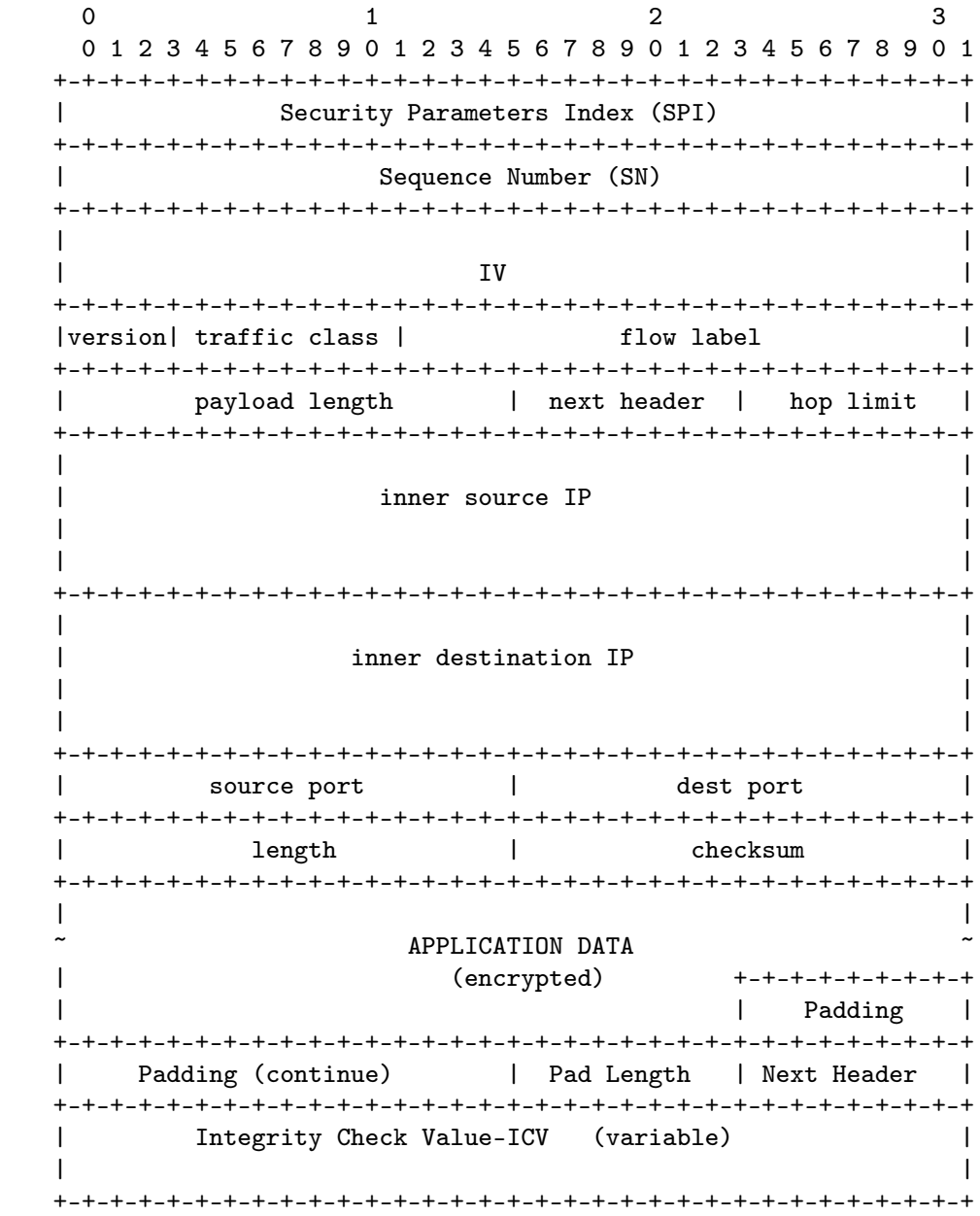
Migault, Guggemos et. al:
Diet-ESP: IP-Layer Security for IoT
IOS Press, Journal of Computer Security, May 2017
`https://www.researchgate.net/publication/316348221`

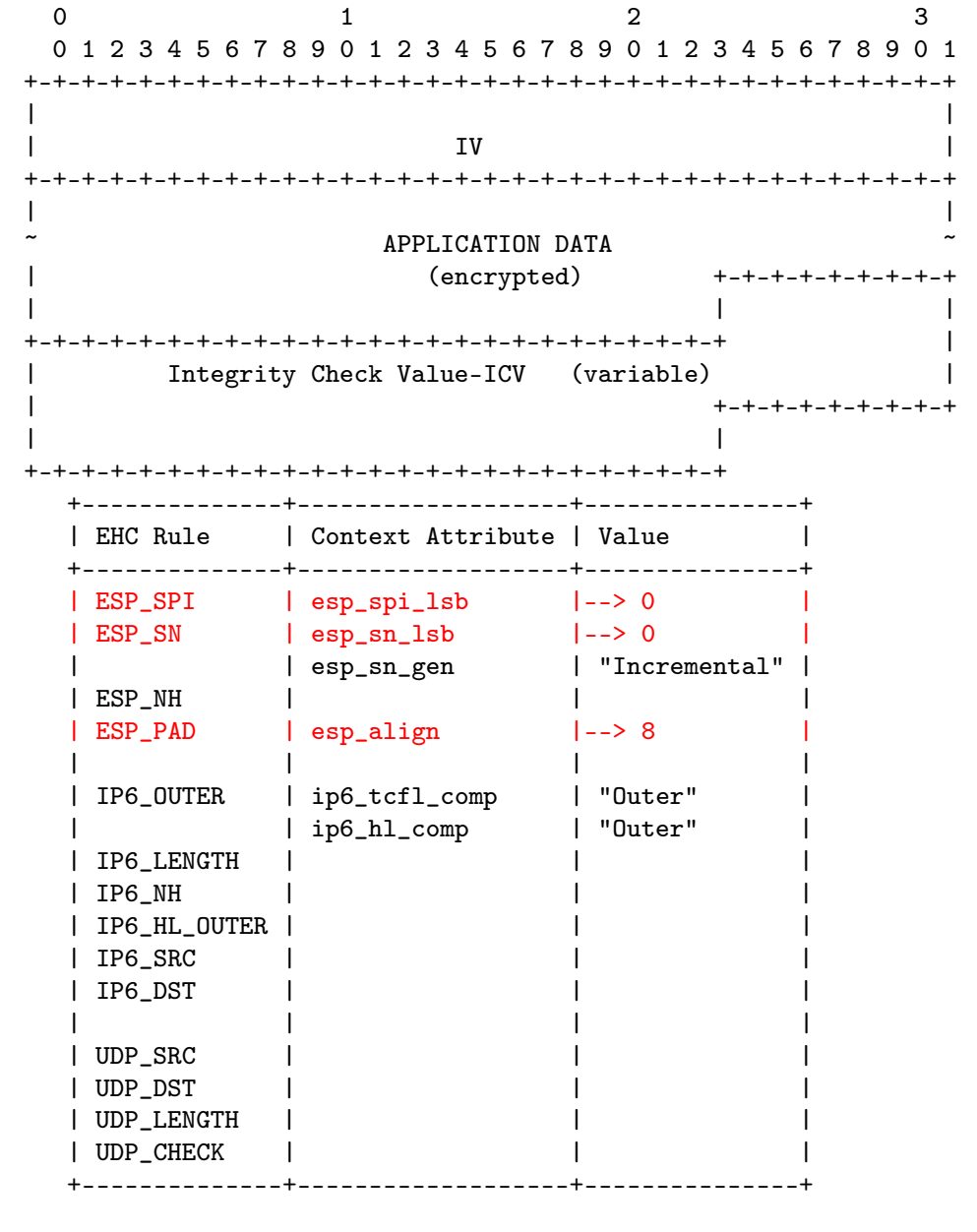
EHC Rules and Actions

EHC Rule	Field	Action	Parameters
EHC_RULE_NAME	f1	a1	p1_1, ... p1_n
	...		
	fm	am	pm_1, ... pm_n

Function	Compression	Decompression
send-value	No	No
elided	Not send	Get from EHC Context
lsb(_lsb_size)	Sent LSB	Get from EHC Context
lower	Not send	Get from lower layer
checksum	Not send	Compute checksum.
padding(_align)	Compute padding	Get padding

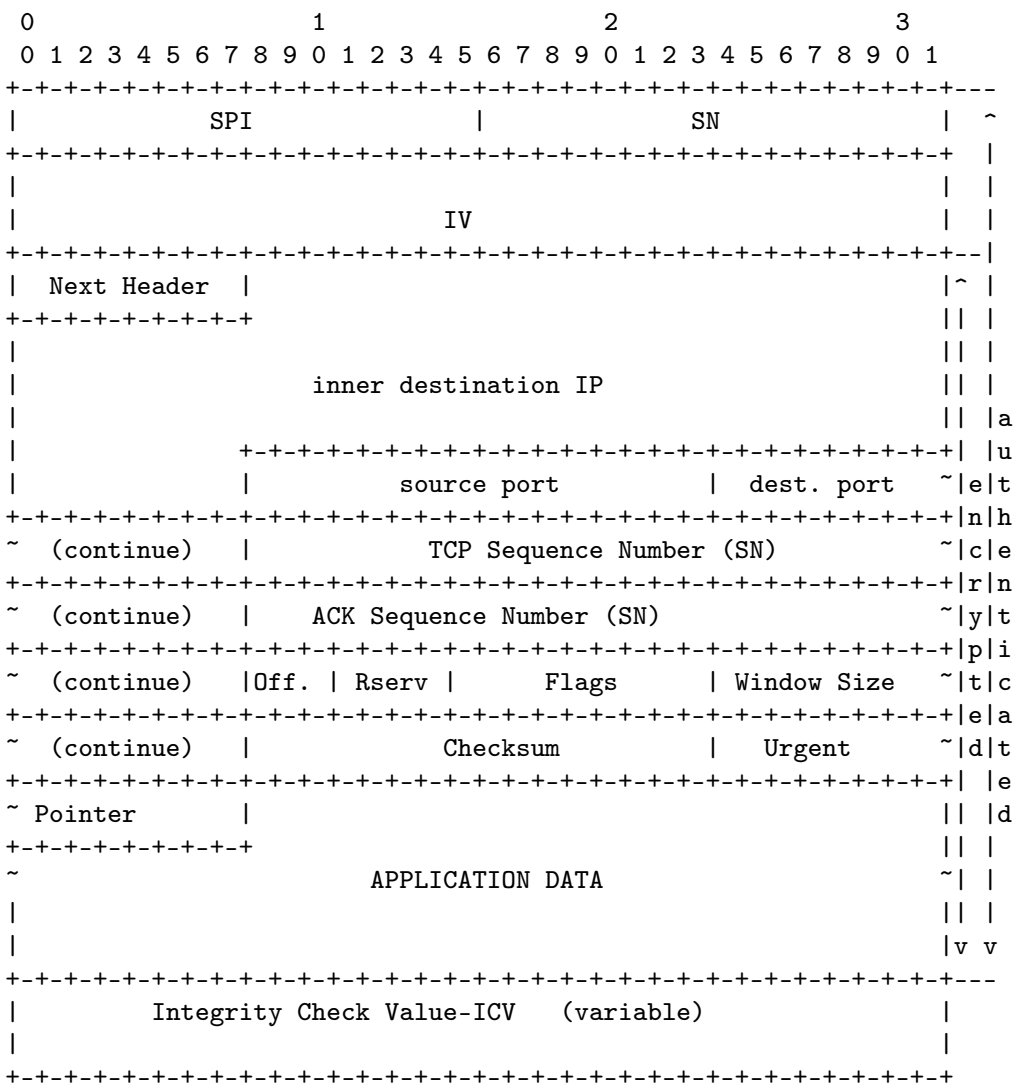
Example: Scenario IoT VPN (68 bytes saving)





EHC Rule	Context Attribute	Value
ESP_SPI	esp_spi_lsb	--> 0
ESP_SN	esp_sn_lsb	--> 0
	esp_sn_gen	"Incremental"
ESP_NH		
ESP_PAD	esp_align	--> 8
IP6_OUTER	ip6_tcfl_comp	"Outer"
	ip6_hl_comp	"Outer"
IP6_LENGTH		
IP6_NH		
IP6_HL_OUTER		
IP6_SRC		
IP6_DST		
UDP_SRC		
UDP_DST		
UDP_LENGTH		
UDP_CHECK		

Example 2: Traditional VPN (32 bytes saving)



EHC Rule	Context Attribute	Value
ESP_SPI	esp_spi_lsb	2
ESP_SN	esp_sn_lsb	2
	esp_sn_gen	"Incremental"
ESP_NH		
ESP_PAD	esp_align	8
IP6_OUTER	ip6_tcfl_comp	"Outer"
IP6_LENGTH		
IP6_HL_OUTER	ip6_hl_comp	"Outer"
IP6_SRC		

Questions

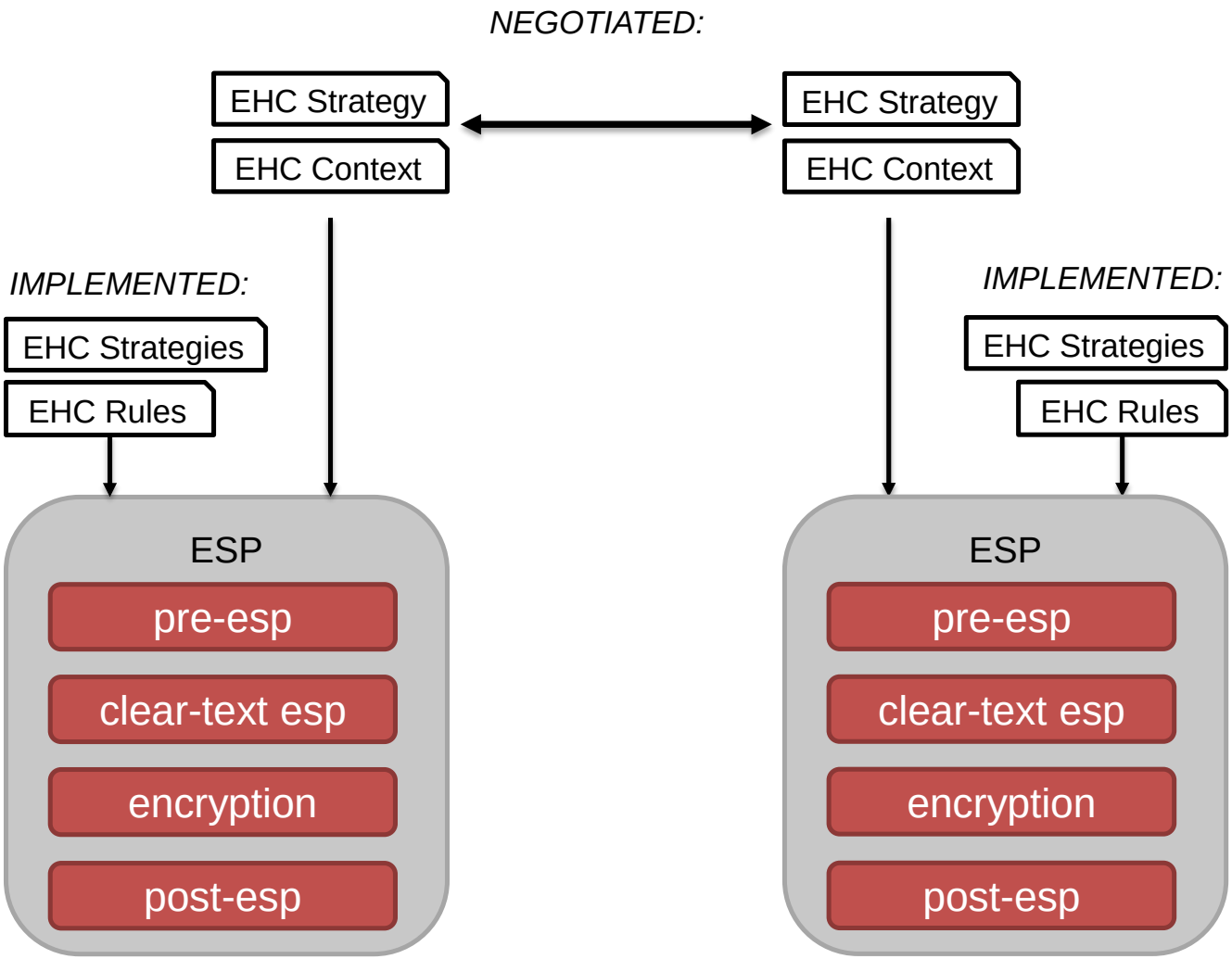
→ Better compression vs. complexity?

→ How to move forward?

Backup Slides

Backup

EHC design


NEGOTIATED:
EHC Strategy
EHC Context
EHC Strategy
EHC Context
IMPLEMENTED:
EHC Strategies
EHC Rules
IMPLEMENTED:
EHC Strategies
EHC Rules
ESP
pre-esp
clear-text esp
encryption
post-esp
ESP
pre-esp
clear-text esp
encryption
post-esp

Field Classification and compression

- Each field of ESP, IPv4, IPv6, TCP, UDP, UDP-Lite is classified using the ROHC classifiers
- Each of this fields is compressed using the related EHC Action
  - STATIC-DEF, STATIC-KNOWN $\rightarrow$ elided or lsb()
    - e.g. SPI, IP-addresses, ports, etc.
  - PATTERN $\rightarrow$ lsb()
    - e.g. Seq/Ack Numbers
  - INFERRED $\rightarrow$ lower()
    - e.g. packet size