P4 2022 Workshop
May 24-26th

Line Rate IPSec on a PNA-compliant Packet Processing Pipeline

Sameer Kittur

Overview

- IPSec edge use cases
- High Performance IPSec: The Building Blocks
- Portable NIC Architecture (PNA)
- Pensando’s Programmable P4 Achitecture
- P4-16 and Cryptography Engine Extern Support
- Packet flows
- Control-plane interface
- Network Security

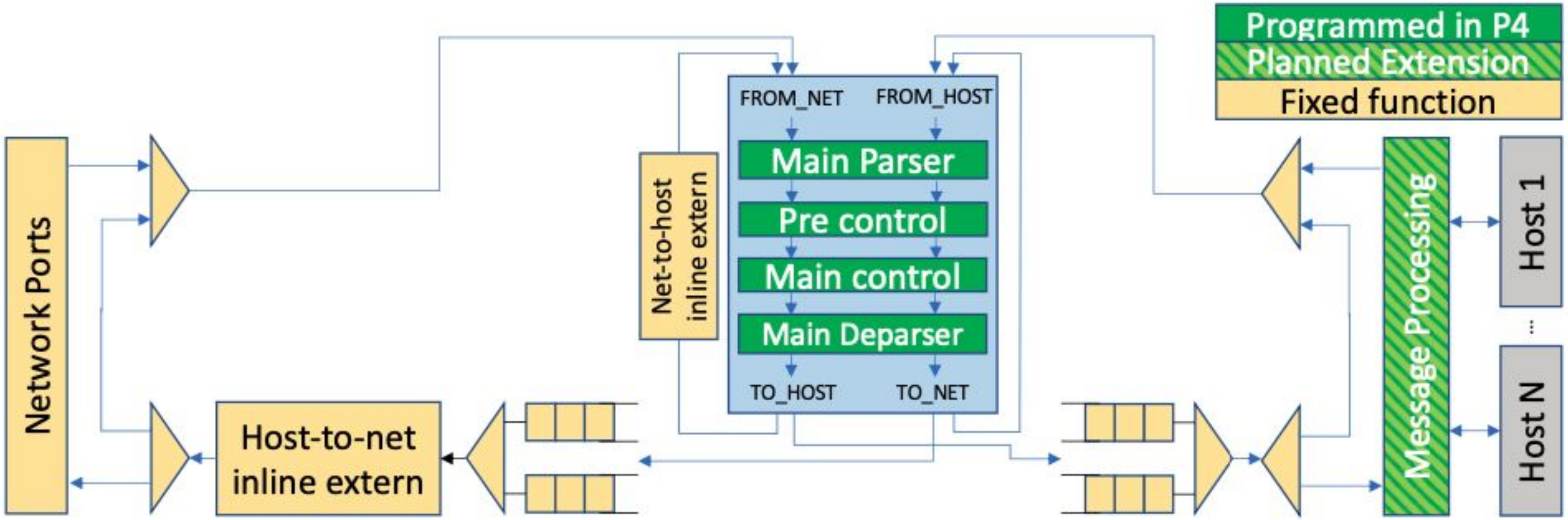
IPSec Edge Use Cases

- IPSec: one of the de facto network security protocol in massively distributed environments
- Traditionally used in VPN gateways, lately being integrated into gateway solutions to secure multi-cloud deployments
- SDN services in the substrate secured at every server in large cloud infrastructure providers
- Servers with P4 based IPUs/DPUs enable network encryption services transparently within an enterprise

High Performance IPSec: The Building Blocks

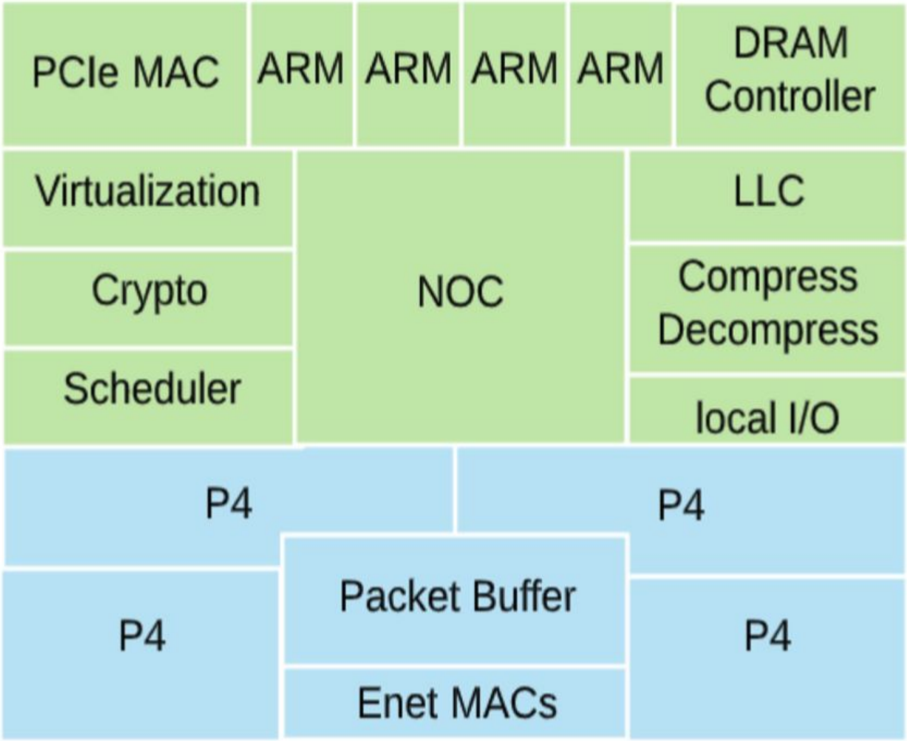
- High performance P4 based packet processing pipeline on an edge device
    - Flexibility to cater to varied use cases
    - Programmed with a high level language (P4-16) enables easy maintenance and feature additions
- High performance configurable cryptographic engine interfaced to the P4 pipeline
    - Support for an array of capabilities including different key sizes, programmable header/payload offsets and sizes etc.
    - Configurable via P4 pipeline

Portable NIC Architecture



Reference: https://p4.org/p4-spec/docs/PNA.html

Pensando’s Programmable P4 Architecture



PCIe MAC

ARM

ARM

ARM

ARM

DRAM Controller

Virtualization

Crypto

Scheduler

NOC

LLC

Compress Decompress

local I/O

P4

P4

P4

Packet Buffer

Enet MACs

P4

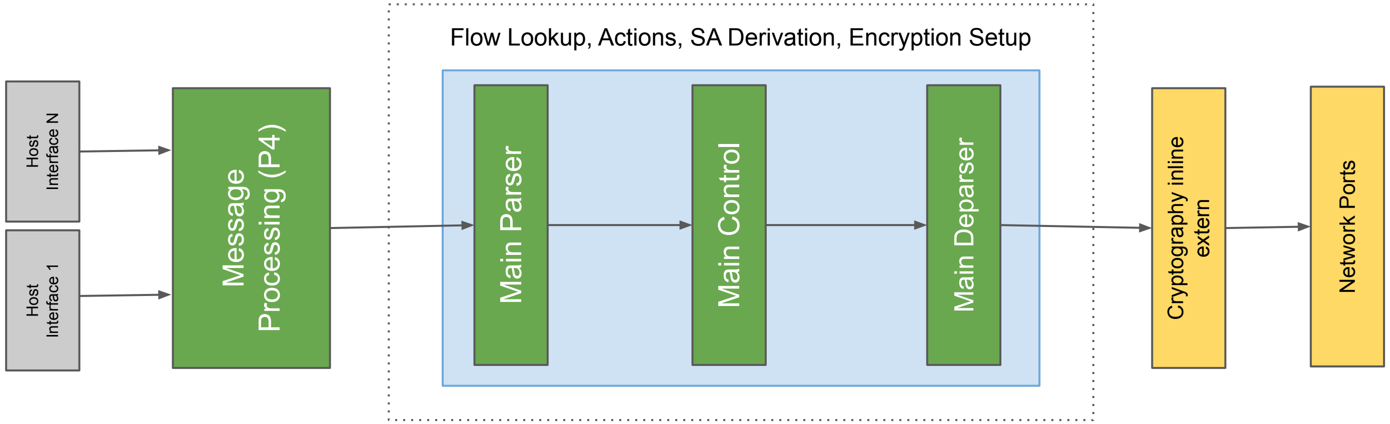
- Four different pipelines in the Programmable P4 subsystem
- Two of the pipelines support high speed packet processing
- The other two P4 pipelines support the message passing/DMA interface towards the host and the Arm cores
- High performance configurable cryptographic offload in the packet processing path

P4-16 and Cryptography Engine Extern Support

- *Pre Control / Main Control* sets up intrinsic header via *Main Deparser*
- Cryptographic extern encrypts/decrypts the payload and associates the output and authentication results with the packet
- Decryption and Authentication results available to *Main Parser* via intrinsic header

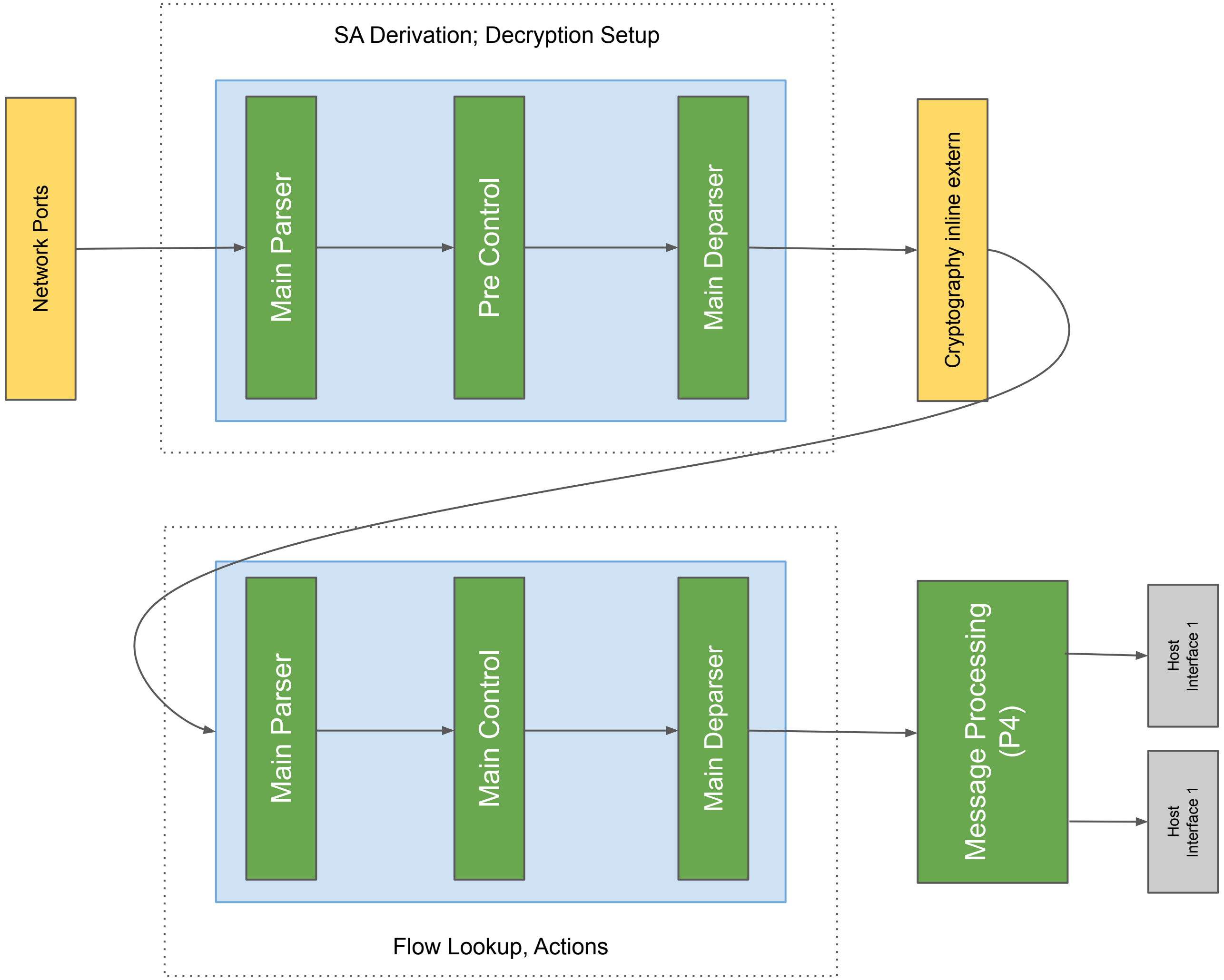
```
hdr.crypto_intr_hdr.op = IPSEC_OP_ENCRYPT;

// 96b IV
hdr.crypto_intr_hdr.iv[127:96] = salt;
hdr.crypto_intr_hdr.iv[95:32] = hdr.esp.iv;

// Key
hdr.crypto_intr_hdr.key = key;
hdr.crypto_intr_hdr.key_size = key_size;

// Header and payload information
hdr.crypto_intr_hdr.hdr_len = (bit<14>)aad_len;
hdr.crypto_intr_hdr.hdr_offset = (bit<14>)aad_offset;
hdr.crypto_intr_hdr.total_len = total_len;

// Request deparser to emit the intrinsic header
hdr.crypto_intr_hdr.setValid();

// Specify that this packet contains the crypto engine
header and subjected to the IPSec extern
intr_p4.crypto_hdr = TRUE;
```

Packet Flow - Host to Network



- Packet data packetized from host by the message Processing P4 pipeline; relayed to Packet Processing P4 pipeline
- *Main Control* looks up the flow tuples and determines if a packet needs to be encrypted
- The Security Association (SA) for the flow is derived from the lookup
- *Main Control* sets up intrinsic header for encryption at the cryptography extern engine
- Post encryption, packet forwarded to the host or to a port/uplink

Packet Flow - Network to Host



- IPSec packet parsed by *Main Parser* and SA derived by *Pre Control*
- *Pre Control* sets up intrinsic header for decryption at the cryptography extern block
- Post decryption, *Main Control* looks up flow tuples for associated actions
- Decrypted packet forwarded to the host

PNA based IPSec implementation: Control Plane Interface

- Table entry APIs generated by P4-16 compiler tools
- Control-plane use APIs to update tables based on results of policy evaluation
- IPSec control-plane use the generated APIs to update Security Associations
    - IKE or other non-standard session key negotiations

PNA Based IPSec implementation: Network Security

- Traditional fixed function IPSec engines are functionally limited
- P4 pipeline and a programmable cryptographic extern provides flexibility and performance
- IPSec encryption options at different layers: overlay packet vs. underlay packet
- Encryption/decryption with any type of preceding encapsulation headers
    - VXLAN, Geneve etc.
- Highly extensible and configurable
- Incorporate changes made to the protocol standards via programmability support
- Other network security protocols (DTLS) and custom/non-standard protocol implementations
- Wire speed encryption/decryption

Thank You

https://pensando.io/

https://p4.org/p4-spec/docs/PNA.html