SFO17-406: IPsec Full Offload Support in OpenDataPlane

Bill Fischofer
Credits

The work described in this session represents the collaborative contribution of the LNG ODP team, particularly:

Petri Savolainen, Nokia
Dmitry Eremin-Solenikov, Cavium
Bala Manoharan, Cavium
Nikhil Agarwal, NXP

Plus inputs from Member Engineers and the ODP Community at large.
IPsec Background

- Standard means of creating cryptographically secure communication channels over the Internet, also provides data authentication services
- Operates at Layer 3
- Common use in telecom to provide secure tunnels for VPNs, backhaul links, etc.
- Defined by IETF RFCs (4301, 4302, 4303, 6040, 7619, 7296, etc., etc.)
IPsec - Authentication Header (AH)

**Transport Mode**

- IP Hdr
- Payload
- Authenticated

**Tunnel Mode**

- IP Hdr
- AH Hdr
- Payload
- Authenticated
IPsec - Encapsulating Security Protocol (ESP)

Transport Mode

- IP Hdr
- Payload
- ESP Hdr
- ESP Trailer
- ESP Auth
- Encrypted
- Authenticated

Tunnel Mode

- IP Hdr
- Payload
- ESP Hdr
- ESP Trailer
- ESP Auth
- Encrypted
- Authenticated
Security Association (SA)

- One per direction (RX, TX) for an IPsec flow
- Contains keying and other material needed to encrypt, decrypt, and authenticate packets
- Key negotiation done via a separate protocol - Internet Key Exchange (IKE)
- Packets identify which SA they belong to via the Security Parameter Index (SPI) field in IPsec headers
Why is IPsec of Interest to ODP?

- Encryption is slow in software
- IPsec relies heavily on encryption
- Many SoCs offer hardware support for IPsec
- ...but each differ in how such support is accessed
- This is exactly the type of problem ODP is designed to address!
ODP IPsec APIs

Capabilities
- odp_ipsec_capability()
- odp_ipsec_cipher_capability()
- odp_ipsec_auth_capability()

Global Configuration
- odp_ipsec_config_init()
- odp_ipsec_config()

SA Creation and Management
- odp_ipsec_sa_param_init()
- odp_ipsec_sa_create()
- odp_ipsec_sa_disable()
- odp_ipsec_sa_destroy()
- odp_ipsec_sa_mtu_update()
- odp_ipsec_sa_context()
- odp_ipsec_sa_to_u64()

Inbound Processing
- odp_ipsec_in()
- odp_ipsec_in_enq()

Outbound Processing
- odp_ipsec_out()
- odp_ipsec_out_enq()
- odp_ipsec_out_inline()

Event Types / Subtypes
- ODP_EVENT_PACKET_IPSEC
- ODP_EVENT_IPSEC_STATUS

Event Processing
- odp_ipsec_packet_from_event()
- odp_ipsec_packet_to_event()
- odp_ipsec_result()
- odp_ipsec_status()
IPsec Lookaside Processing in ODP

Synchronous:
- `odp_ipsec_in()` for decrypt
- `odp_ipsec_out()` for encrypt

Asynchronous:
- `odp_ipsec_in_enq()` for decrypt
- `odp_ipsec_out_enq()` for encrypt
IPsec Inline Processing in ODP

Inline Encrypt:

```
inline_encrypt
```

Inline Decrypt is Implicit
Not Part of ODP IPsec Support

IKE (Internet Key Exchange)
- Control plane function
- Use strongSwan or similar packages - https://strongswan.org/

Time-based SA expirations
- Application responsibility
- ODP provides byte/packet soft and hard expiration support

Inline Output via Traffic Manager
- May be added in the future
- For now, use lookaside-mode processing if this is needed
Performance Results - IMIX Traffic
IMIX Traffic Performance Comparison

![Bar chart showing traffic performance comparison across different cores and applications.]
Thank You

OpenDataPlane.org
Thank You

#SFO17
SFO17 keynotes and videos on: connect.linaro.org
For further information: www.linaro.org