BUD17-306
ODP IPsec Offload Panel
LNG ODP Development Team
Participants

Application Perspective
- Petri Savolainen, Nokia
- Bogdan Pricope, Enea

Implementer Perspective
- Bala Manoharan, Cavium
- Nikhil Agarwal, NXP

Moderator
- Bill Fischofer, Linaro
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 Offload Goals - Offload Processing
Application Perspective
Application level entities

- Security Policy Database (SPD-I, SPD-O, SPD-S)
- Security Association Database (inbound, outbound)
- Cache inbound (optional) meant for multicast traffic
- Cache outbound
- Custom key management (interaction) support
Asynchronous processing

**Inbound processing**
- `odp_thread` processing loop
  - Packet
  - `odp_ipsec_in_enq()`
  - unicast
  - Cache inbound SA search
  - `odp_thread` processing loop
  - Async event
  - Process result
  - SAD check
  - Process next header

**Outbound processing**
- Packet processing
  - Packet
  - Cache outbound
  - `odp_ipsec_out_enq()`
  - not found
  - SPD
  - Key mgmt
  - found, protect
  - `odp_thread` processing loop
  - Async event
  - Process result
  - Encrypted packet
  - Send packet
Implementation Perspective
IPSEC LOOKASIDE API offerings

- Complete IPSEC state machine in ODP(HW)
- Pushing IPSEC tunnel headers in HW.
- Expose HW accelerators via common ODP APIs.
- IPSEC bottlenecks are offloaded in HW for performance including:
  - Sequence number update
  - Random IV
  - Anti replay checks
  - ICV checksum
  - Crypto operations
Implementation Domain vs Application Domain

1. Check IPSEC result
   - Event type?
     - IPSEC_EVENT
       - No
         - ODP_schedule
       - Yes
         - Policy lookup
2. Route Lookup
   - ESP or AH?
     - No
       - IPSEC_IN_ENQ
     - Yes
       - IPSEC_OUT_ENQ
3. Policy lookup
   - IPSEC needed?
     - No
       - ODP_PKTIO_ENQ
     - Yes
       - Enqueue to crypto engine
         - HW crypto Engine with protocol assist
6. Enqueue to crypto engine
   - Pktio-IN
   - HW crypto Engine with protocol assist
   - Pktio-Out
IMIX Traffic Performance Comparison

- Linux
- OFP IPSEC App
- ODP IPSEC app
- Cipher Line Rate (20Gbps)
Work in Progress:
ODP Inline offload APIs
Implementation Domain vs Application Domain

- IPSEC_EVENT
  - Event type?
  - Packet
  - ODP_schedule

- Check IPSEC result
  - Route Lookup

- ODP_PKTIO_ENQ
  - Policy lookup

- HW crypto Engine with protocol assist
  - Yes
  - IPSEC needed?
    - Yes
      - Pktio-Out
    - No
      - No
  - ESP or AH?
    - Yes
      - SA Lookup
      - HW crypto Engine with protocol assist
    - No
      - Pktio-IN
IPSEC INLINE API proposals

- Packets received directly by IPsec offload engine
- SPI based lookup for inbound traffic
- Classification rules run on Decrypted IPsec packets before sending to application
- Packets can be transmitted directly through PKTIO after encryption
- Packets could also be sent through Traffic Manager queues for transmission
IMIX Traffic Performance Comparison
Thank You

#BUD17

For further information: www.linaro.org
BUD17 keynotes and videos on: connect.linaro.org