DPDK IPSEC: A SCALABLE HIGH PERFORMANCE LIBRARY FOR YOUR IPSEC APPLICATION

LEGAL DISCLAIMER

- NO LICENSE (EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE) TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT.
- INTEL DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, AS WELL AS ANY WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE IN TRADE.
- THIS DOCUMENT CONTAINS INFORMATION ON PRODUCTS, SERVICES AND/OR PROCESSES IN DEVELOPMENT. ALL INFORMATION PROVIDED HERE IS SUBJECT TO CHANGE WITHOUT NOTICE. CONTACT YOUR INTEL REPRESENTATIVE TO OBTAIN THE LATEST FORECAST, SCHEDULE, SPECIFICATIONS AND ROADMAPS.
- THE PRODUCTS AND SERVICES DESCRIBED MAY CONTAIN DEFECTS OR ERRORS KNOWN AS ERRATA WHICH MAY CAUSE DEVIATIONS FROM PUBLISHED SPECIFICATIONS. CURRENT CHARACTERIZED ERRATA ARE AVAILABLE ON REQUEST.
- COPIES OF DOCUMENTS WHICH HAVE AN ORDER NUMBER AND ARE REFERENCED IN THIS DOCUMENT MAY BE OBTAINED BY CALLING 1-800-548-4725 OR BY VISITING: HTTP://WWW.INTEL.COM/DESIGN/LITERATURE.HTM
- INTEL AND THE INTEL LOGO ARE TRADEMARKS OF INTEL CORPORATION IN THE U.S. AND/OR OTHER COUNTRIES.
- *OTHER NAMES AND BRANDS MAY BE CLAIMED AS THE PROPERTY OF OTHERS.
-
- INTEL'S COMPILERS MAY OR MAY NOT OPTIMIZE TO THE SAME DEGREE FOR NON-INTEL MICROPROCESSORS FOR OPTIMIZATIONS THAT ARE NOT UNIQUE TO INTEL MICROPROCESSORS. THESE OPTIMIZATIONS INCLUDE SSE2, SSE3, AND SSSE3 INSTRUCTION SETS AND OTHER OPTIMIZATIONS. INTEL DOES NOT GUARANTEE THE AVAILABILITY, FUNCTIONALITY, OR EFFECTIVENESS OF ANY OPTIMIZATION ON MICROPROCESSORS NOT MANUFACTURED BY INTEL. MICROPROCESSOR-DEPENDENT OPTIMIZATIONS IN THIS PRODUCT ARE INTENDED FOR USE WITH INTEL MICROPROCESSORS. CERTAIN OPTIMIZATIONS NOT SPECIFIC TO INTEL MICROARCHITECTURE ARE RESERVED FOR INTEL MICROPROCESSORS. PLEASE REFER TO THE APPLICABLE PRODUCT USER AND REFERENCE GUIDES FOR MORE INFORMATION REGARDING THE SPECIFIC INSTRUCTION SETS COVERED BY THIS NOTICE. NOTICE REVISION #20110804
- TESTS DOCUMENT PERFORMANCE OF COMPONENTS ON A PARTICULAR TEST, IN SPECIFIC SYSTEMS. DIFFERENCES IN HARDWARE, SOFTWARE, OR CONFIGURATION WILL AFFECT ACTUAL PERFORMANCE. CONSULT OTHER SOURCES OF INFORMATION TO EVALUATE PERFORMANCE AS YOU CONSIDER YOUR PURCHASE. FOR MORE COMPLETE INFORMATION ABOUT PERFORMANCE AND BENCHMARK RESULTS, VISIT WWW.INTEL.COM/BENCHMARKS TEST AND SYSTEM CONFIGURATIONS: ESTIMATES ARE BASED ON INTERNAL INTEL ANALYSIS USING AT LEAST DATA PLANE DEVELOPMENT KIT IPSEC SAMPLE APPLICATION ON INTEL(R) XEON(R) GOLD 6142 CPU @ 2.60GHZ WITH AT LEAST USING INTEL(R) COMMUNICATIONS CHIPSET(S) 8955.
- NO COMPUTER SYSTEM CAN BE TOTALLY SECURE

AGENDA

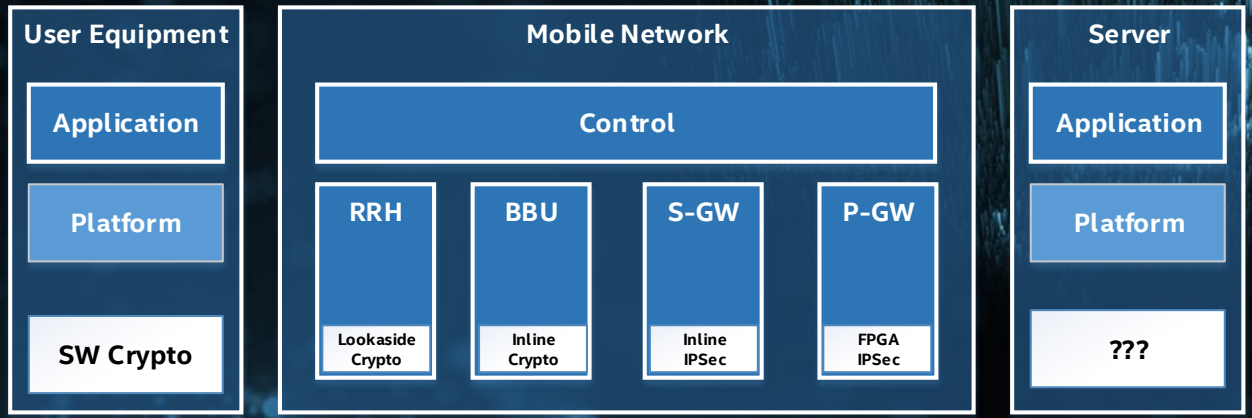
- Motivation
- DPDK and rte_cryptodev brief introduction
- DPDK rte_ipsec deep-dive
- Performance
- Current status and future work

MOTIVATION

Network traffic has to be secured.
IPSec as the popular secure network protocol, is still a very heavy task for modern system.

Large scale network systems, such as 5G Network infrastructure, are likely contained heterogeneous hardware, including crypto/IPSec workload Acceleration methods.

From Cloud Native point of view, we expect the network nodes running same software. Is this possible for IPSec application?



WHAT IS DPDK?

Data Plane Development Kit, includes a set of libraries and user-space device drivers
Accelerates workload on generic computer (Network, Crypto, Compression, Virtualization, and many more)

Data I/O abstraction

Standard API to access hardware from different vendors. **Accelerated**

DumbNIC/SmartNIC, Lookaside/inline Crypto, BBDev, Virtio, AF-XDP, and FPGA ready

How?

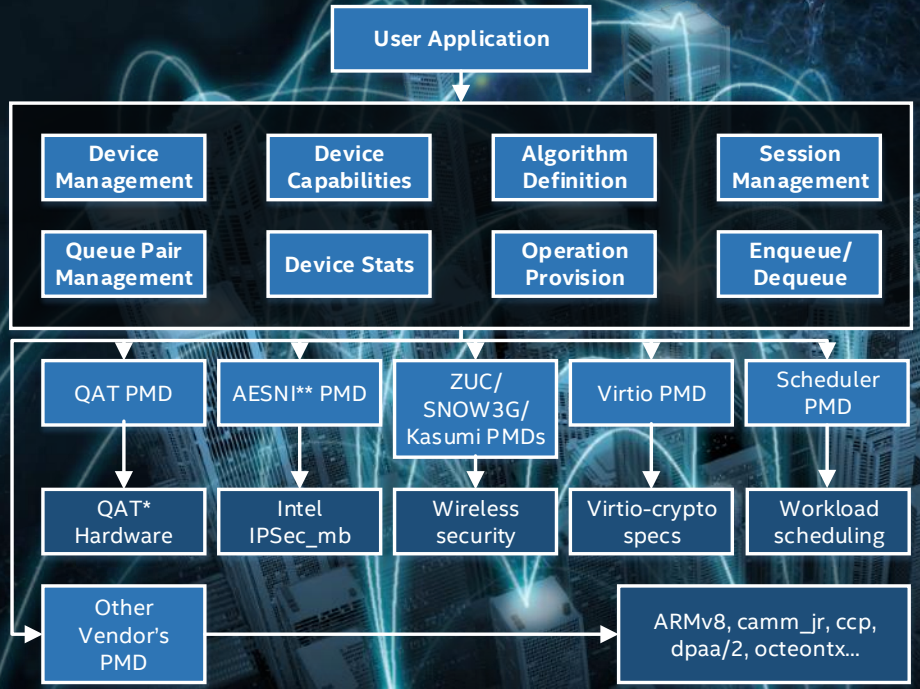
Polling, working in bursts, core affinity, memory/buffer management,
PCI utilization, use of vector instructions.

DPDK RTE_CRYPTODEV BRIEF

CRYPTO FRAMEWORK FOR PROCESSING SYMMETRIC AND ASYMMETRIC CRYPTO WORKLOADS IN DPDK.

Target SW and Lookaside crypto accelerator

- Wide range of SW and HW PMDs
- Standard API supports all PMDs
- Multi-queues for multi-thread sharing



WHAT'S LEFT? OH, IPSEC!

We now have tools we need to access different HW for acceleration.

BUT all IPSec solutions need:

- SA management
- Transport/Tunnel header assembly/strip
- SAD/SPD
- A crypto load-balancer
- Native support of current and future HW/SW acceleration methods

We propose DPDK Rte_ipsec library for community to address common IPSec challenges

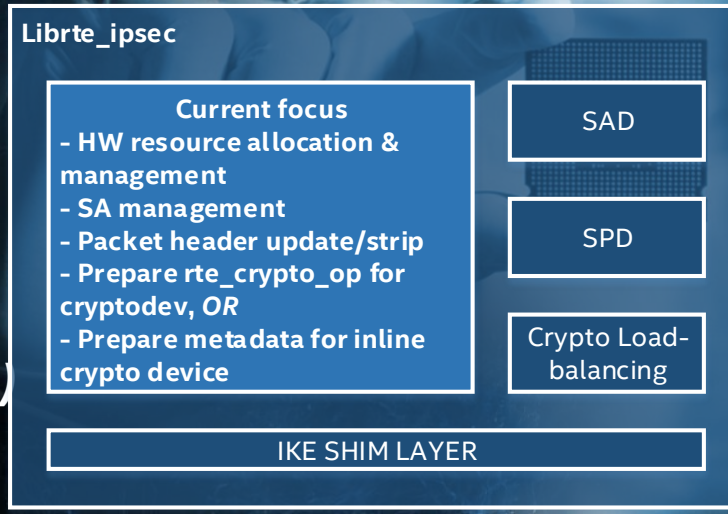
RTE_IPSEC: A LIBRARY TO ADDRESS IPSEC CHALLENGES

A modular library built around a core functionality of data-path processing and SA management.

Optional modules:

- *Scalable and performant SAD and SPD*
- *Crypto load-balancing (host, lookaside, inline)*
- *Integration point for IKE clients*

Automatically handle HW accelerator allocation and resource usage.

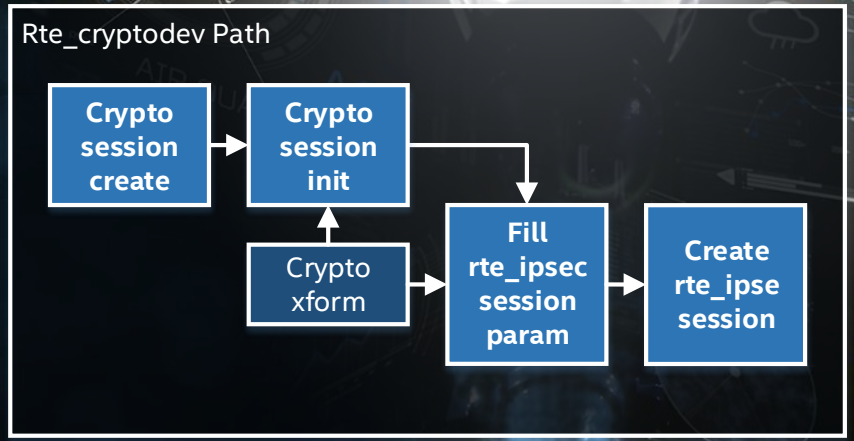


RTE_IPSEC SESSION CREATION

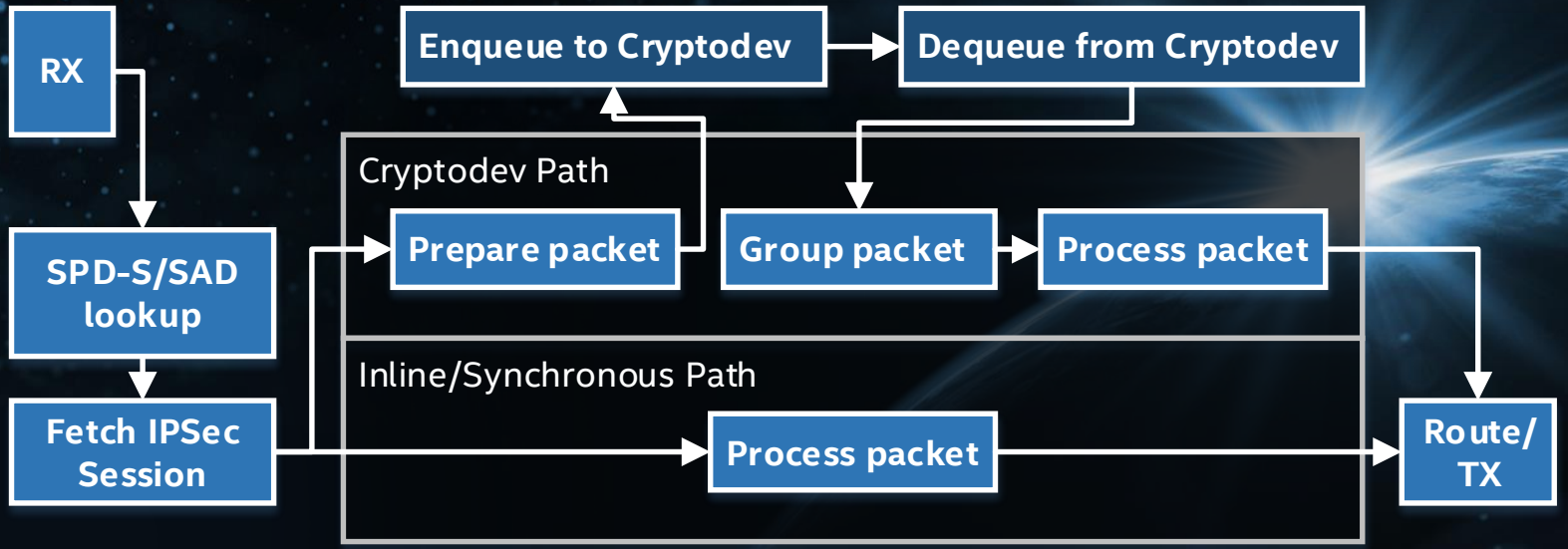
Different paths for rte_cryptodev to create crypto/security session (automatable).

After the session is created, same code path is used to create ipsec session.

Same crypto transform (xform) is reused.

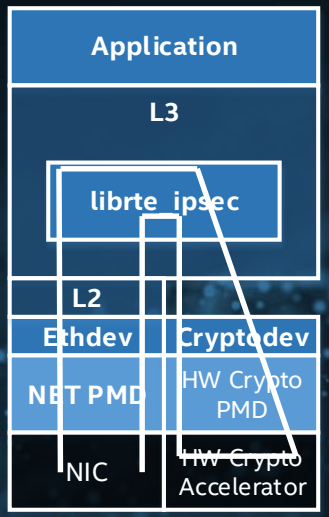


RTE_IPSEC DATA PATH

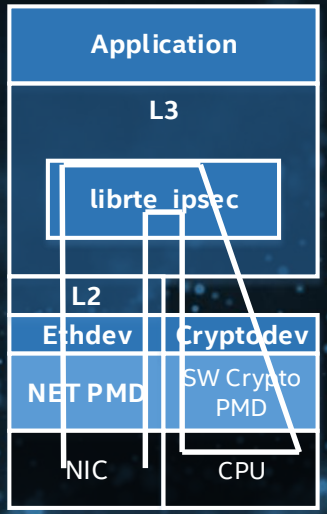


MULTIPLE IPSEC PROCESSING MODES

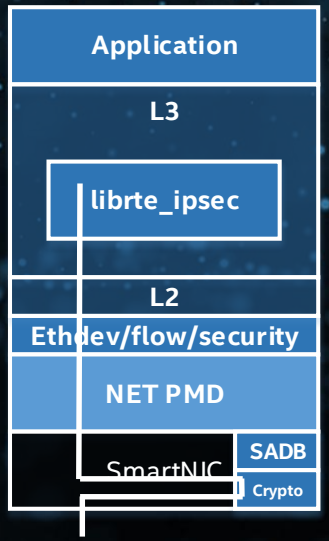
Lookaside HW Crypto Processing



Host based SW Crypto Processing



I/O based inline Crypto Processing



CURRENT ACTIVITY

Transport/Tunnel ESP, IPv4 and IPv6
Supported cipher algorithms: **AES-CBC-128/256, AES-CTR-128, 3DES-CBC, NULL**
Supported authentication algorithms: **HMAC-SHA1/SHA256, NULL**
Supported AEAD algorithms: **AES-GCM-128**
ESN and anti-replay
Multi-segment packets support (DPDK 19.08)
Header reconstruction (DPDK 19.11)
SW/HW lookaside/HW inline crypto accelerator support

Potential Community additions:
SADB/SPDB
NAT
Crypto-load-balancing
IKE client SHIM layer
Integration into VPP, OVS, and other open source projects


THANK YOU