Università della Svizzera italiana

Advanced Learning and Research Institute ALaRI

High-level Architecture of an IPSec-dedicated System on Chip

Alberto Ferrante
ALaRI,
University of Lugano
E-mail: ferrante@alari.ch

Vincenzo Piuri
DTI,
University of Milano
E-mail: piuri@dti.unimi.it

Outline

IPSec and IPSec Accelerators

Architecture of the Accelerator

Conclusions and Future Work

IPSec

- ✔ Is a suite of protocols
  - ✘ adding security at IP (network) level;
- ✔ makes extensive use of cryptographic functions:
  - ✘ it is resource consuming.

AH, ESP

- ✔ IPSec is mainly composed of two protocols:
  - ✘ Authentication Header (AH);
  - ✘ Encapsulating Security Payload (ESP);
- ✔ both protocols can be used in:
  - ✘ transport mode;
  - ✘ tunnel mode.

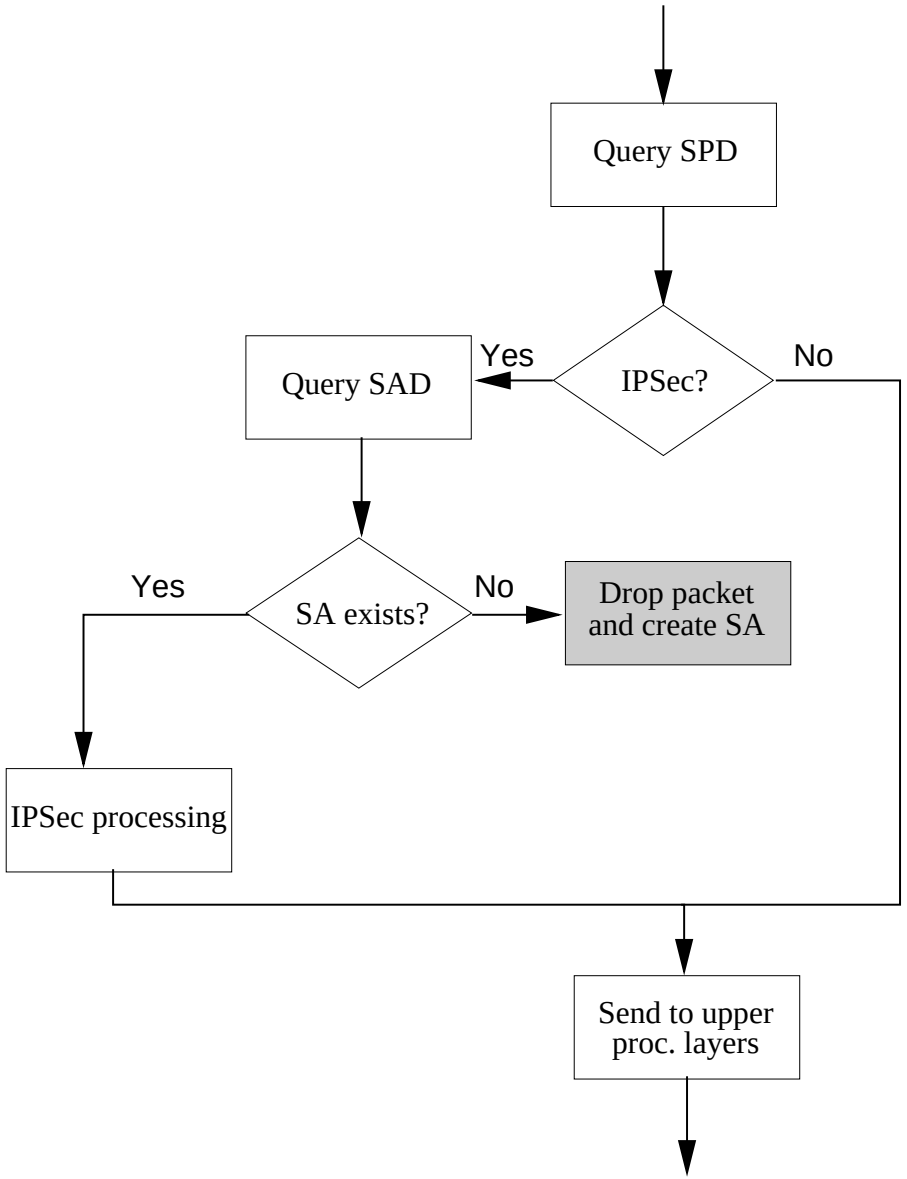
Databases

- ✔ IPSec uses two databases:
  - ✘ the Security Policy Database (SPD);
  - ✘ the Security Association Database (SAD):
    - ✓ the records are the Security Associations (SAs).

Security Associations

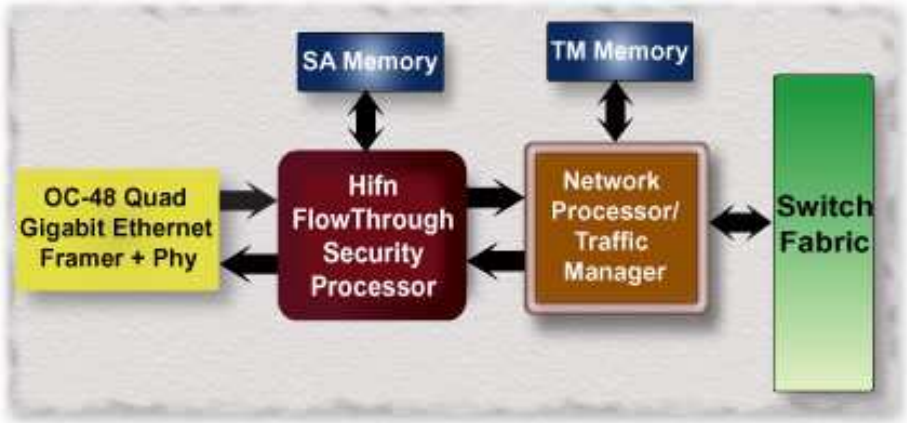
- ✔ Each SA contains:
  - ✘ protocol/algorithms settings;
  - ✘ keys for cryptographic algorithms;
- ✔ SAs are mono-directional:
  - ✘ two SAs need to be created for normal bidirectional communications.

Main IPSec Processing Steps



IPSec Accelerators

- ✔ Required to support high throughput on secure gateways;
- ✔ *flow-through* processors:

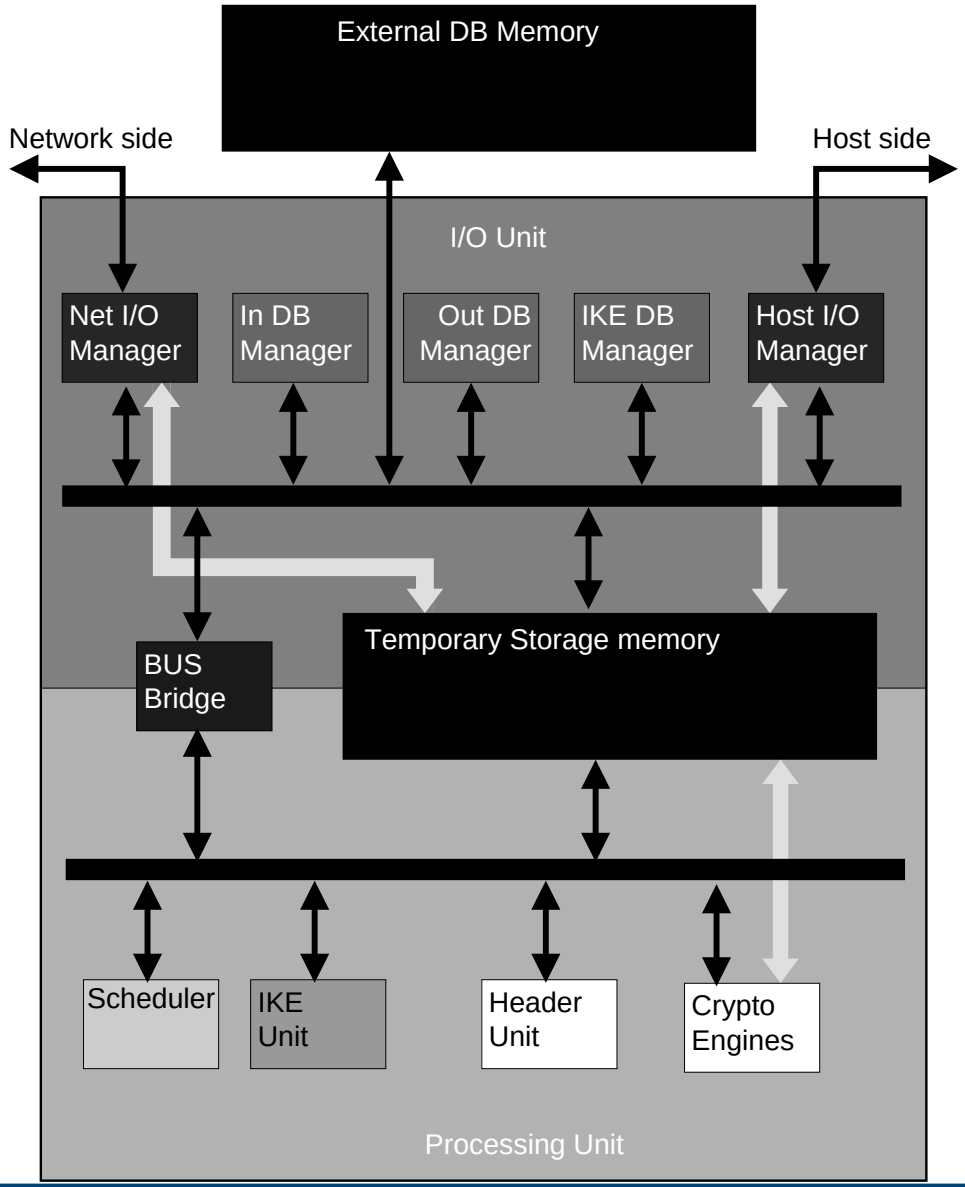


[1]

[1] "Hifn Intelligent Packet Processing III (HIPP III)," Hifn, http://www.hifn.com/technology/HIPP_III.html

The SoC Architecture

- ✔ Two parts:
  - ✘ I/O;
  - ✘ processing;
- ✔ shared memory data communication
- ✔ fast non-shared buses for memory load store;
- ✔ shared control bus.



The I/O Managers

- ✔ Recognize and multicast packet headers to the DB managers (local I/O bus);
- ✔ transfer incoming packets to the memory;
- ✔ transfer outgoing packets from the memory;
- ✔ manage fragmentation.

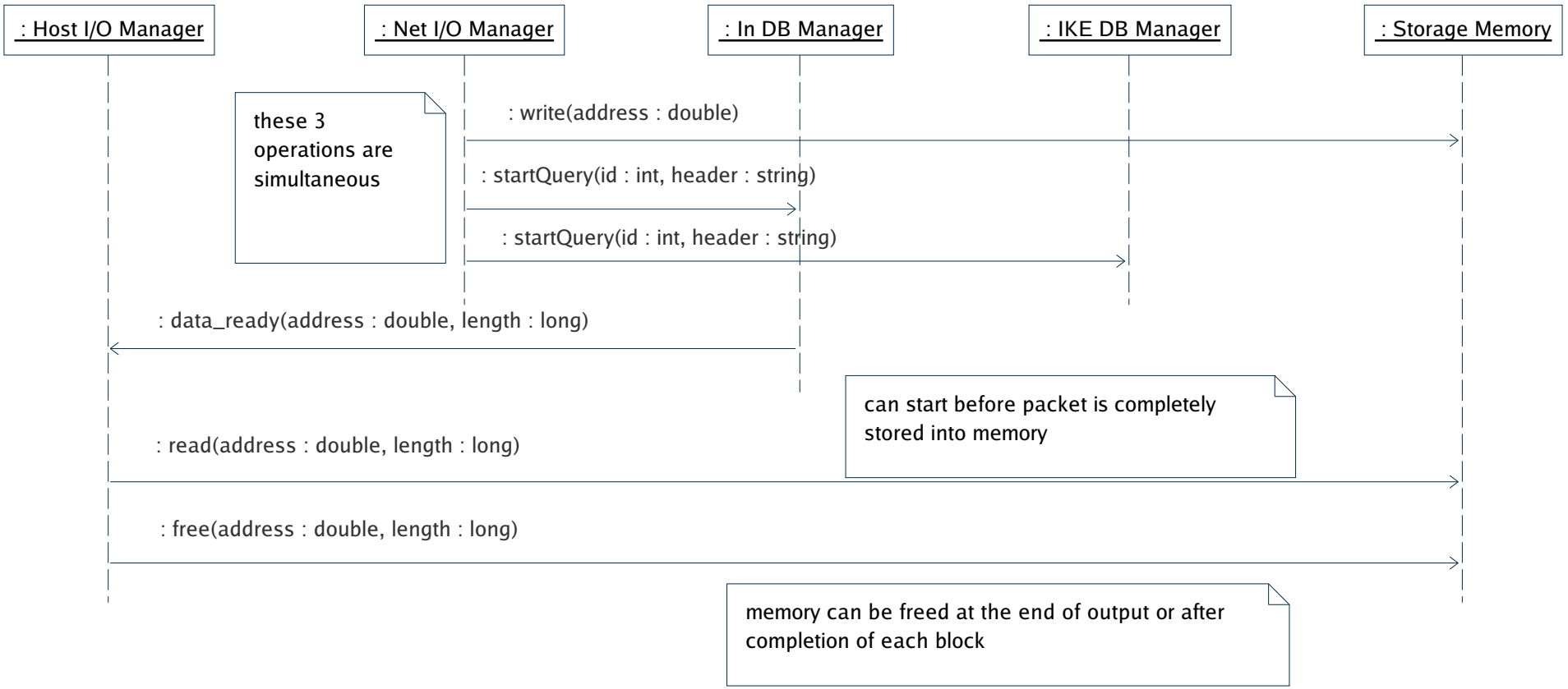
The DB Managers

- ✔ Query the IPSec DBs:
  - ✘ requests multicasted by the I/O Managers;
  - ✘ units autonomously decide if they should process a request or not:
    - ✓ one of the units processes the request;
- ✔ generate commands for the operational units.

The Memory

- ✔ Its efficiency is fundamental;
- ✔ 4 read/write ports;
- ✔ read/write requests
  are decoupled from memory reads/writes:
  - ✘ prefetching and bufering
    on the memory interface.

SoC Behavior for Inbound non-IPSec Packets



Performance

- ✔ The speed is limited by the one of the memory:
  - ✘ memory bandwidth must be 4 times the network one.

Extending the Processing Capabilities

- ✔ We can use multiple processors to increase bandwidth;
- ✔ load balancer to distribute traffic:
  - ✘ use a distributed shared-memory for SAD;
  - ✘ use a centralized memory for SPD;
  - ✘ parallel processing of packets belonging to the same SA is not possible.

Conclusions

We designed a SoC:

- ✔ completely implementing IPSec;
- ✔ efficient.

Future Work

- ✔ Simulate the architecture;
- ✔ tune the architecture;
- ✔ tune the architectural parameters.