

# 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

NGI 2007, 23/05/2007 A. Ferrante – High-level Architecture of an IPSec-dedicated System on Chip – 1 / 17



# Outline

IPSec and IPSec Accelerators

Architecture of the Accelerator

Conclusions and Future Work IPSec and IPSec Accelerators Architecture of the Accelerator Conclusions and Future Work



# IPSec

IPSec and IPSec Accelerators

IPSec

AH, ESP

Databases

Security

Associations

Main IPSec

Processing Steps

**IPSec** Accelerators

Architecture of the Accelerator

Conclusions and Future Work

#### Is a suite of protocols

★ adding security at IP (network) level;

 makes extensive use of cryptographic functions:

**×** it is resource consuming.



# AH, ESP

IPSec and IPSec Accelerators

AH, ESP

**IPSec** 

Databases

Security

Associations

Main IPSec

Processing Steps IPSec Accelerators

Architecture of the Accelerator

Conclusions and Future Work ✓ IPSec is mainly composed of two protocols:

- ✗ Authentication Header (AH);
- **×** Encapsulating Security Payload (ESP);
- ✓ both protocols can be used in:
  - **x** transport mode;
  - **×** tunnel mode.



#### Databases

IPSec and IPSec Accelerators

IPSec

AH, ESP

Databases

Security

Associations

Main IPSec

**Processing Steps** 

**IPSec Accelerators** 

Architecture of the Accelerator

Conclusions and Future Work ✓ IPSec uses two databases:

**x** the Security Policy Database (SPD); **x** the Security Association Database (SAD):

✓ the records are the Security Associations (SAs).

# Security Associations

IPSec and IPSec Accelerators

Advanced

and Resear

Learning

Institute ALaRI

IPSec

Università

della Svizzera

italiana

AH, ESP

Databases

Security

Associations

Main IPSec

Processing Steps

**IPSec Accelerators** 

Architecture of the Accelerator

Conclusions and Future Work Each SA contains:

- x protocol/algorithms settings;
- **x** keys for cryptographic algorithms;
- ✓ SAs are mono-directional:
  - two SAs need to be created for normal bidirectional communications.

#### Main IPSec Processing Steps

Università

della Svizzera italiana Advanced 👘

Learning and Research Institute ALaRI



NGI 2007, 23/05/2007 A. Ferrante – High-level Architecture of an IPSec-dedicated System on Chip – 7 / 17



### **IPSec Accelerators**

IPSec and IPSec Accelerators IPSec AH, ESP Databases Security Associations Main IPSec Processing Steps IPSec Accelerators Architecture of the

/

Accelerator Conclusions and

Future Work

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

NGI 2007, 23/05/2007 A. Ferrante – High-level Architecture of an IPSec-dedicated System on Chip – 8 / 17



# The SoC Architecture

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





# The I/O Managers

IPSec and IPSec Accelerators

Architecture of the

Accelerator The SoC

Architecture

The I/O Managers

The DB Managers

The Memory SoC Behavior for Inbound non-IPSec Packets

Performance Extending the Processing

Capabilities

Conclusions and Future Work  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

IPSec and IPSec Accelerators

- Architecture of the Accelerator
- The SoC
- Architecture
- The I/O Managers
- The DB Managers
- The Memory SoC Behavior for Inbound non-IPSec Packets
- Performance Extending the
- Processing
- Capabilities
- Conclusions and Future Work

## • Query the IPSec DBs:

- $\pmb{\times}$  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



- Architecture of the
- Accelerator The SoC
- Architecture
- The I/O Managers
- The DB Managers

#### The Memory

- SoC Behavior for Inbound non-IPSec Packets
- Performance Extending the Processing Capabilities
- Conclusions and Future Work

- 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



NGI 2007, 23/05/2007 A. Ferrante – High-level Architecture of an IPSec-dedicated System on Chip – 13 / 17



#### Performance

IPSec and IPSec		
Accelerators		

- Architecture of the
- Accelerator
- The SoC
- Architecture
- The I/O Managers
- The DB Managers
- The Memory
- SoC Behavior for Inbound non-IPSec Packets

#### Performance

Extending the Processing Capabilities

Conclusions and Future Work The speed is limited by the one of the memory:**x** memory bandwidth must be 4 times the network one.

# **Extending the Processing Capabilities**

**IPSec and IPSec** ✓ We can use multiple processors Accelerators Architecture of the to increase bandwidth; Accelerator The SoC load balancer to distribute traffic: Architecture The I/O Managers The DB Managers use a distributed shared-memory for SAD; X The Memory SoC Behavior for use a centralized memory for SPD; X Inbound non-IPSec Packets parallel processing X Performance Extending the of packets belonging to the same SA Processing Capabilities is not possible. Conclusions and Future Work

Università

della Svizzera

italiana

Advanced

and Resear

Learning

Institute ALaRI



### Conclusions

/

/

IPSec an	d IPSec
Accelerat	ors

Advanced

Learning and Research Institute ALaRI

Architecture of the Accelerator

Conclusions and Future Work

Conclusions

Future Work

We designed a SoC:

completely implementing IPSec; efficient.



# **Future Work**

IPSec and IPSec Accelerators

Architecture of the Accelerator

Conclusions and Future Work

Conclusions

Future Work

Simulate the architecture;

- ✓ tune the architecture;
- ✓ tune the architectural parameters.

NGI 2007, 23/05/2007 A. Ferrante – High-level Architecture of an IPSec-dedicated System on Chip – 17 / 17