Protecting communications in bus-based MPSoCs using hardware firewalls

Pascal Cotret, Jérémie Crenne,
Guy Gogniat, Jean-Philippe Diguet

University of South Brittany, Lorient (France)

CryptArchi'11, June 17th, Bochüm (Germany)

Context

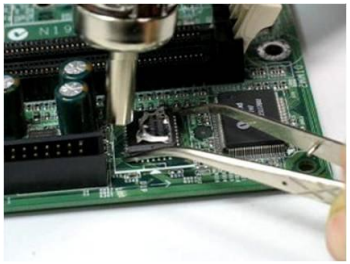
When embedded systems are jeopardized…

Remote software attacks

Worm, virus, Trojan horse

Reversible proximity-based attacks

Fault injection



Promity-based Hardware attacks

Power or EM analysis

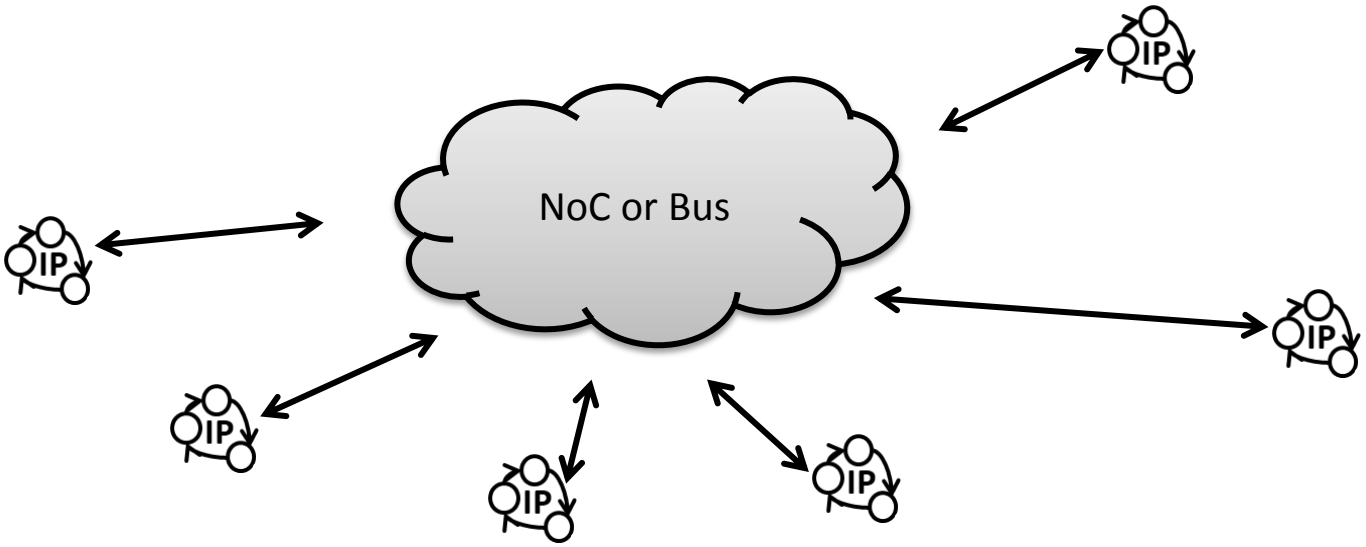
- The more elements (processors or IPs) there are in a MPSoC, the more security flaws are introduced.
- Attacker's goals:
  - Processor hijacking.
  - Extraction of secret information.
  - Denial of service.

Outline

1) Related work
2) Hardware firewalls
3) Case study
4) Results analysis
5) Conclusion and perspectives

Related work

- NoC-based systems (1).
  - DPU : security-enhanced network interfaces.
- Bus-based systems (2).
  - SECA : secure interfaces + global security processing module.

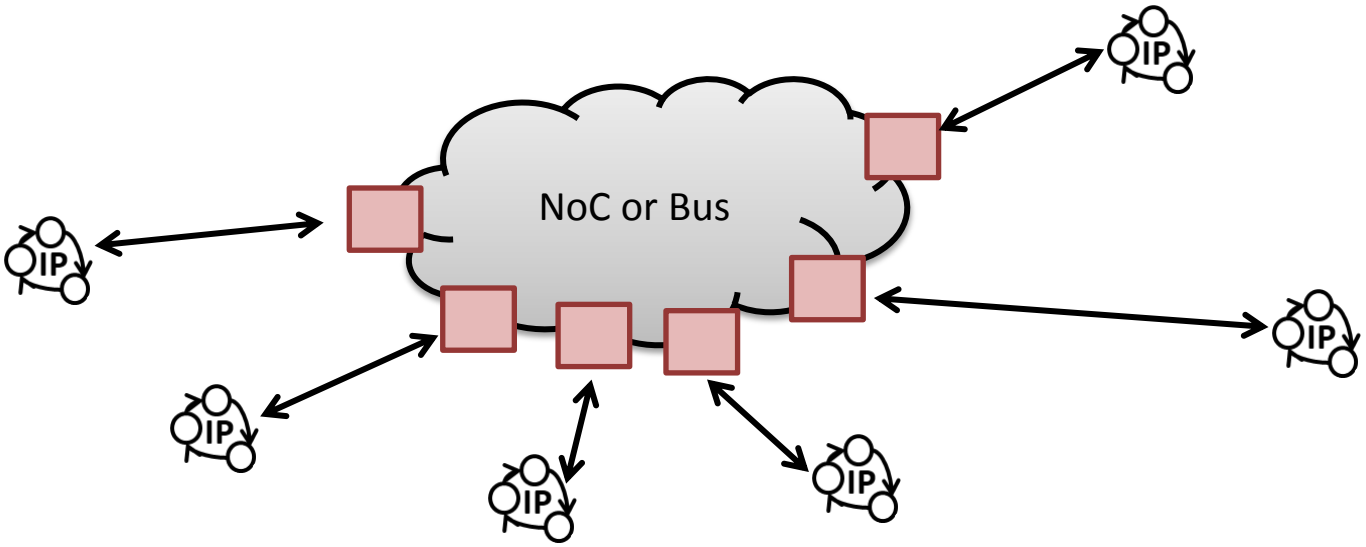


[1] Fiorin, L., Palermo, G., Lukovic, S., and Silvano, C. 2007. A data protection unit for NoC-based architectures. In *Proceedings of the 5th IEEE/ACM international Conference on Hardware/Software Codesign and System Synthesis* (Salzburg, Austria, September 30 - October 03, 2007).

[2] Coburn, J., Ravi, S., Raghunathan, A., and Chakradhar, S. 2005. SECA: security-enhanced communication architecture. In *Proceedings of the 2005 international Conference on Compilers, Architectures and Synthesis For Embedded Systems* (San Francisco, California, USA, September 24 - 27, 2005).

Related work

- NoC-based systems (1).
  - DPU : security-enhanced network interfaces.
- Bus-based systems (2).
  - SECA : secure interfaces + global security processing module.



[1] Fiorin, L., Palermo, G., Lukovic, S., and Silvano, C. 2007. A data protection unit for NoC-based architectures. In *Proceedings of the 5th IEEE/ACM international Conference on Hardware/Software Codesign and System Synthesis* (Salzburg, Austria, September 30 - October 03, 2007).

[2] Coburn, J., Ravi, S., Raghunathan, A., and Chakradhar, S. 2005. SECA: security-enhanced communication architecture. In *Proceedings of the 2005 international Conference on Compilers, Architectures and Synthesis For Embedded Systems* (San Francisco, California, USA, September 24 - 27, 2005).

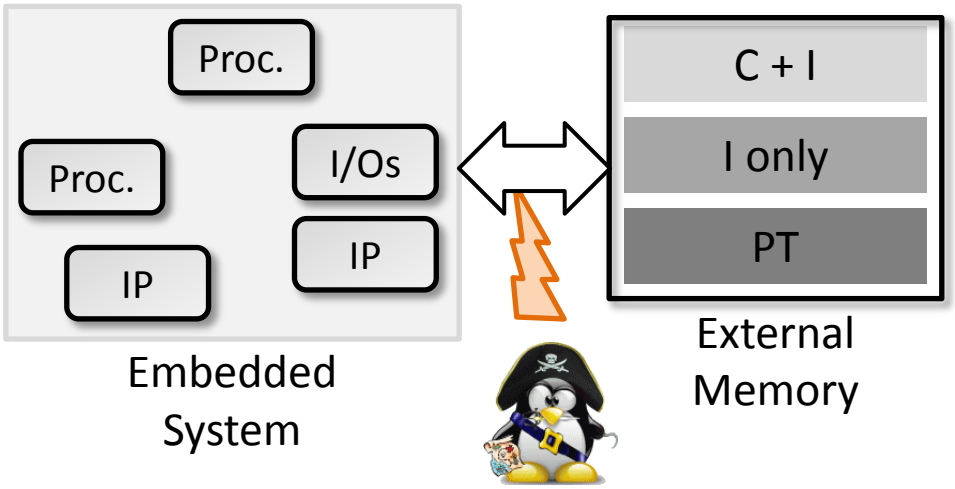
Related work

	SECA [1]	Fiorin [2]	Our objectives
Area overhead	6.6 %	~21%	-
Latency overhead	< 1 %	N/A	Main goal
Memory occupancy	N/A	N/A	-
Cryptographic services	No	No	Yes
Granularity	IP level	IP level	IP multi-level Can be enhanced to thread level (software)
Threat model coverage	Wide range of soft. attacks	Mainly buffer overflow	Wide range of soft. attacks
Comm. link	AMBA (ARM)	NoC	AXI (ARM)

[1] Coburn, J., Ravi, S., Raghunathan, A., and Chakradhar, S. 2005. SECA: security-enhanced communication architecture. In *Proceedings of the 2005 international Conference on Compilers, Architectures and Synthesis For Embedded Systems* (San Francisco, California, USA, September 24 - 27, 2005).

[2] Fiorin, L., Palermo, G., Lukovic, S., and Silvano, C. 2007. A data protection unit for NoC-based architectures. In *Proceedings of the 5th IEEE/ACM international Conference on Hardware/Software Codesign and System Synthesis* (Salzburg, Austria, September 30 - October 03, 2007).

Threat model

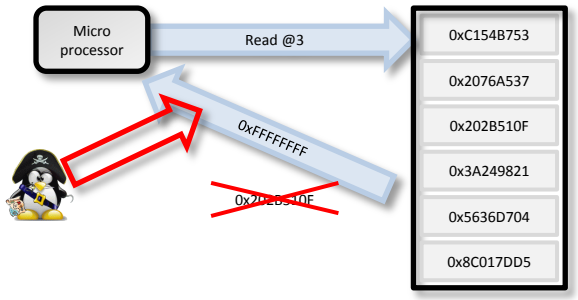


External bus attacks:

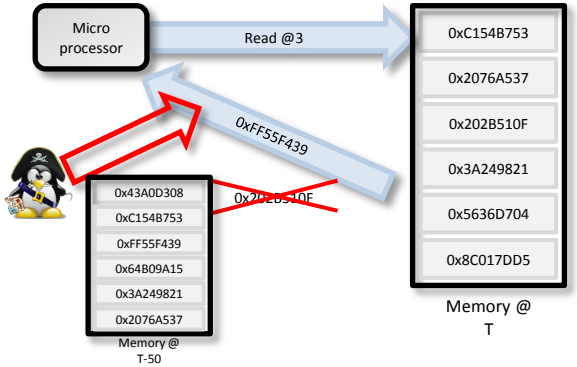
Attacker can modify the memory bus.

It leads to misbehavior (or failure !) of the overall system.

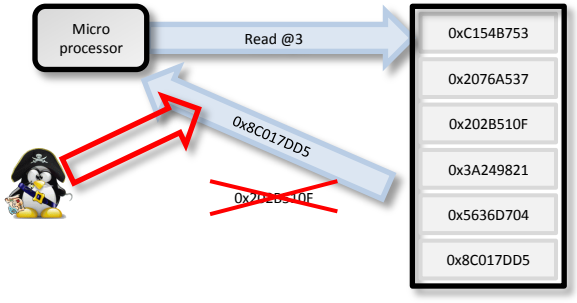
Spoofing



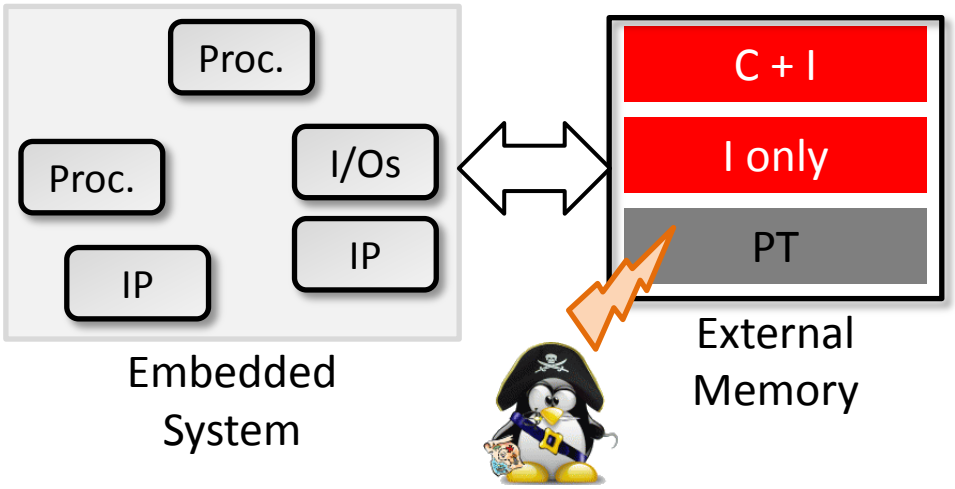
Replay



Relocation

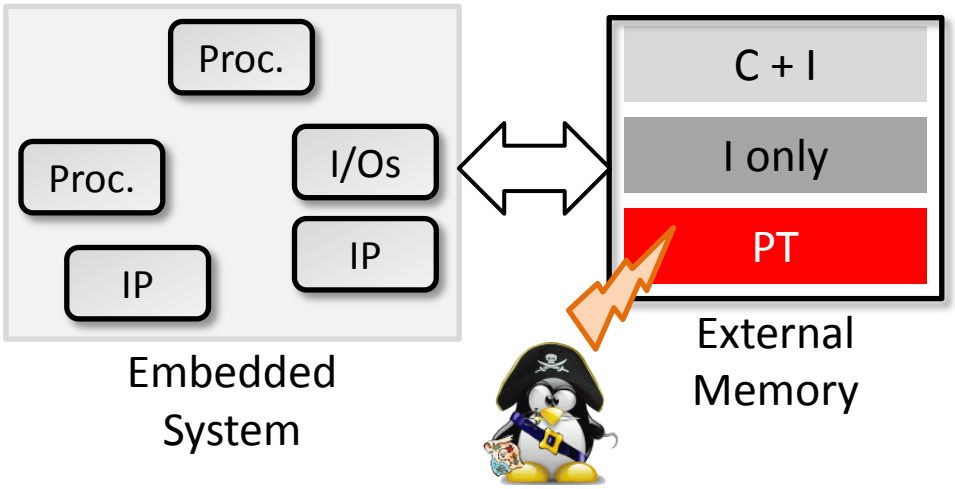


Threat model



“Confidentiality+Integrity” and “Integrity only” modes do not need additional protection.

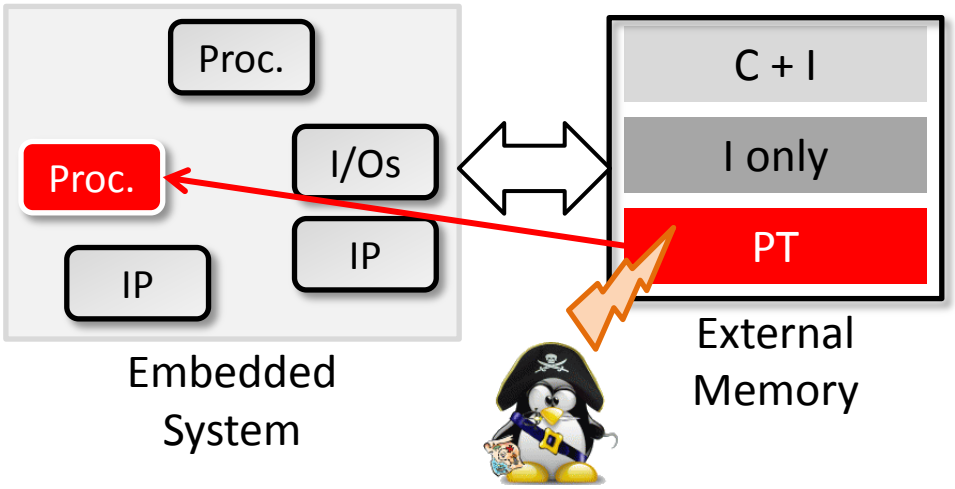
Threat model



“Confidentiality+Integrity” and “Integrity only” modes do not need additional protection.

“Plaintext” mode is more critical: PT memory section could be code or data of a processor…

Threat model



Modifying External Memory leads to:

- Extraction of secret information.
- Processor hijacking.
- Denial of service within the embedded system.

“Confidentiality+Integrity” and “Integrity only” modes do not need additional protection.

“Plaintext” mode is more critical: PT memory section could be code or data of a processor…

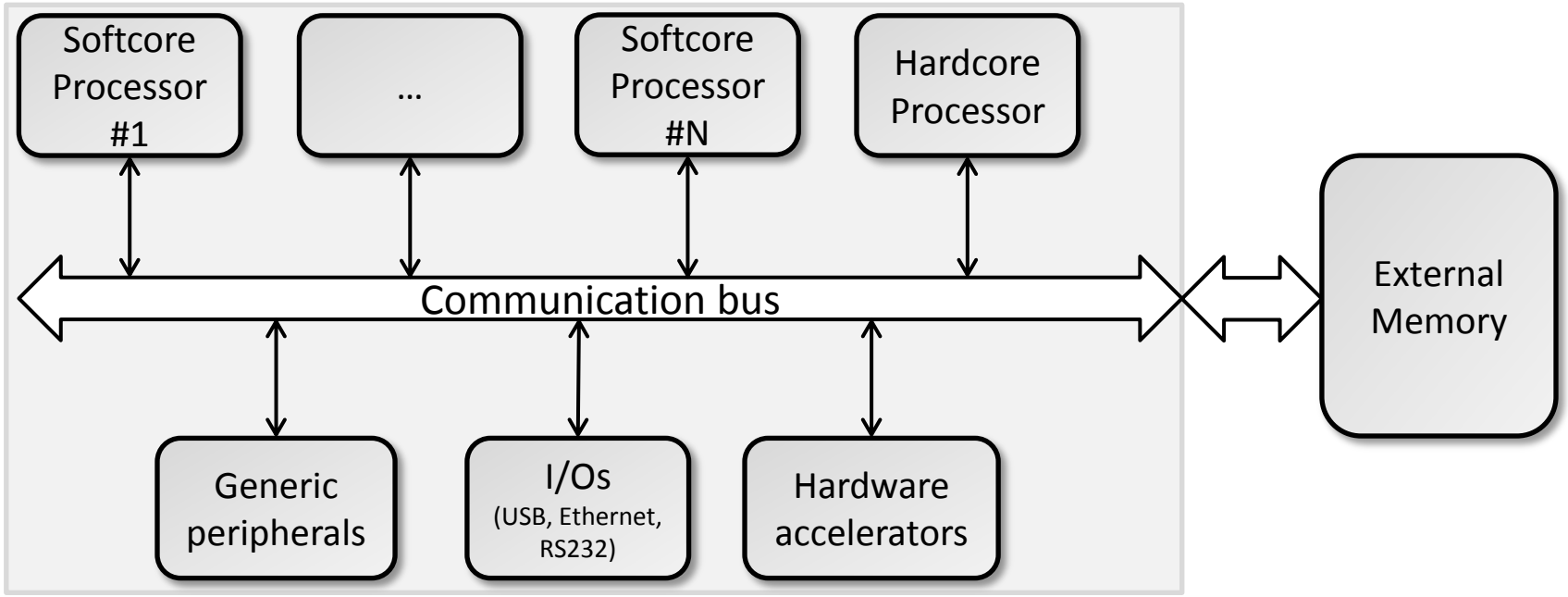
Outline

1) Related work
2) Hardware firewalls
3) Case study
4) Results analysis
5) Conclusion and perspectives

Outline

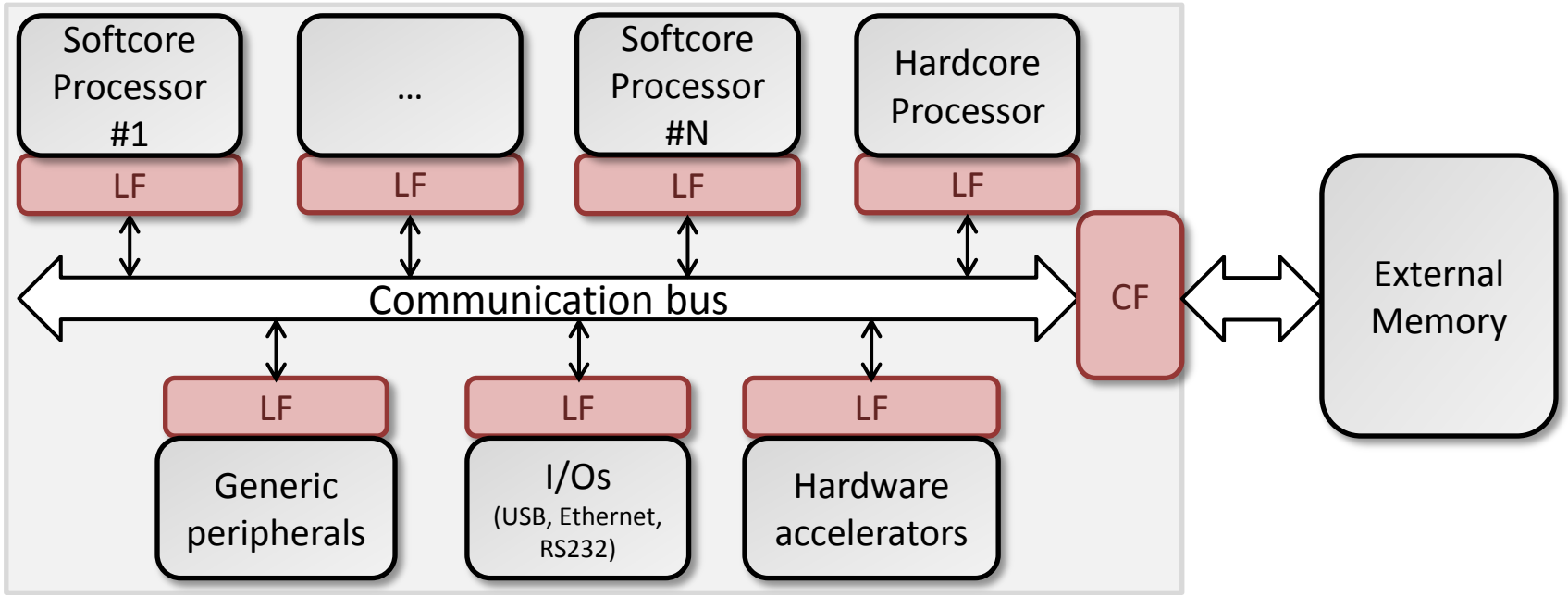
1) Related work
2) Hardware firewalls
3) Case study
4) Results analysis
5) Conclusion and perspectives

Overview of our solution



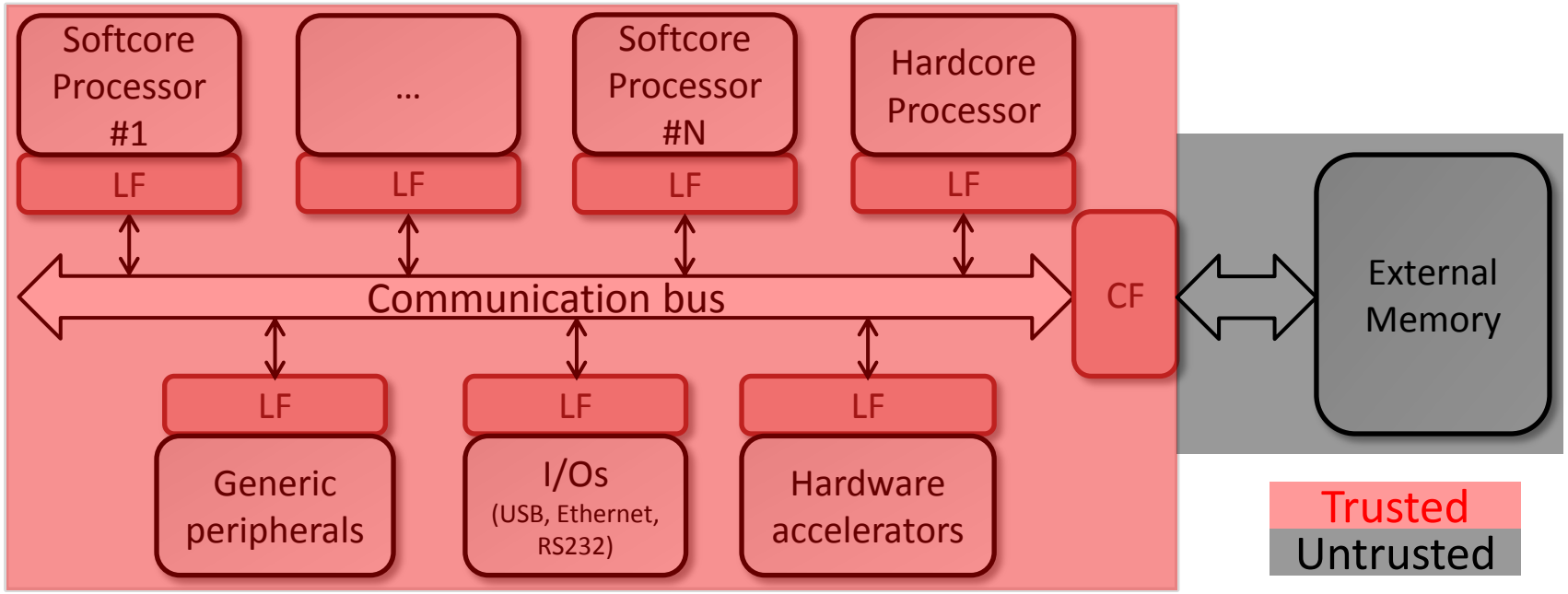
Firewalls are inserted at each interface between an IP and the communication bus. These security-enhanced components will help keeping safe critical data and executing the main application in a trusted environment.

Overview of our solution



Firewalls are inserted at each interface between an IP and the communication bus. These security-enhanced components will help keeping safe critical data and executing the main application in a trusted environment.

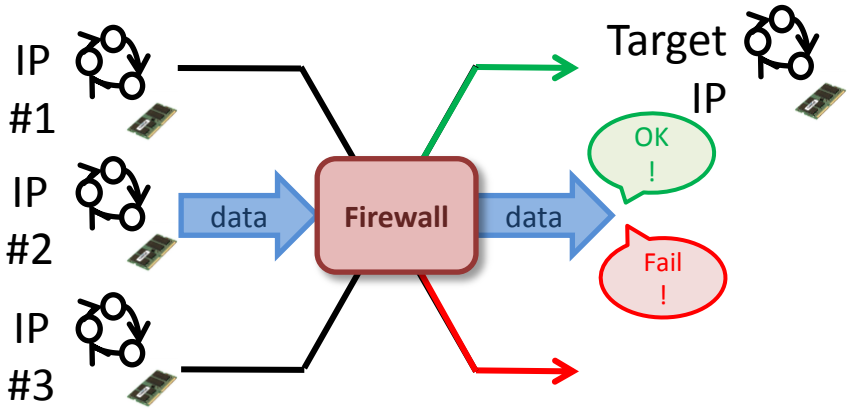
Overview of our solution



Firewalls are inserted at each interface between an IP and the communication bus. These security-enhanced components will help keeping safe critical data and executing the main application in a trusted environment.

Security policies

A firewall is able to manage traffic on the communication bus by applying rules defined in security policies. A firewall can contain a large set of security policies. Each IP of the architecture may have different rights to access a given firewall (and its target IP).

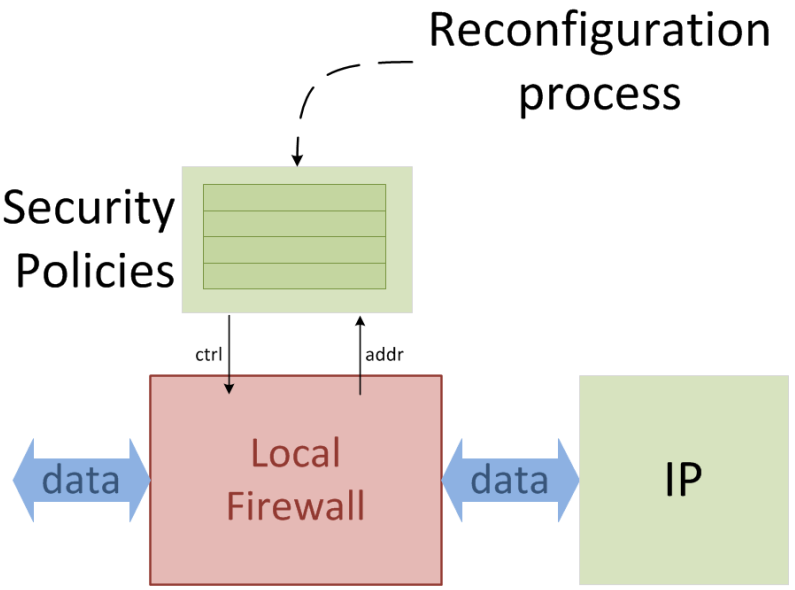


- Read/Write rules.
- Allowed data format.
- Critical parameter values (optional).

- Specific to the external memory:
  - Confidentiality.
  - Integrity.

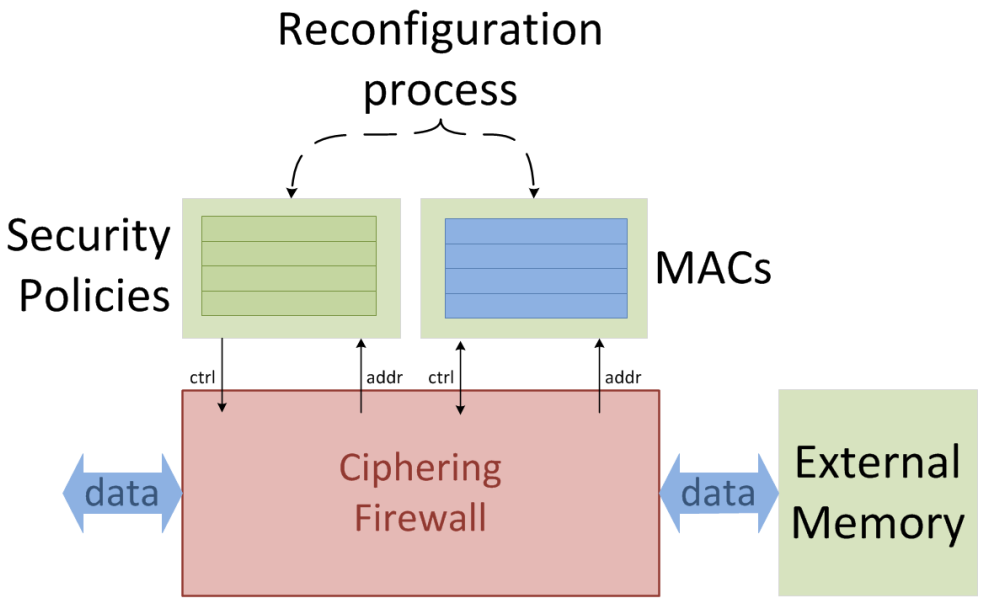
Local Firewall overview

- Manages traffic within the embedded system communication architecture.
- Interface between communication bus and IP.
- Security policies stored in on-chip trusted memory.
- Reconfigurable security policies (through dedicated circuitry, supposed secure).

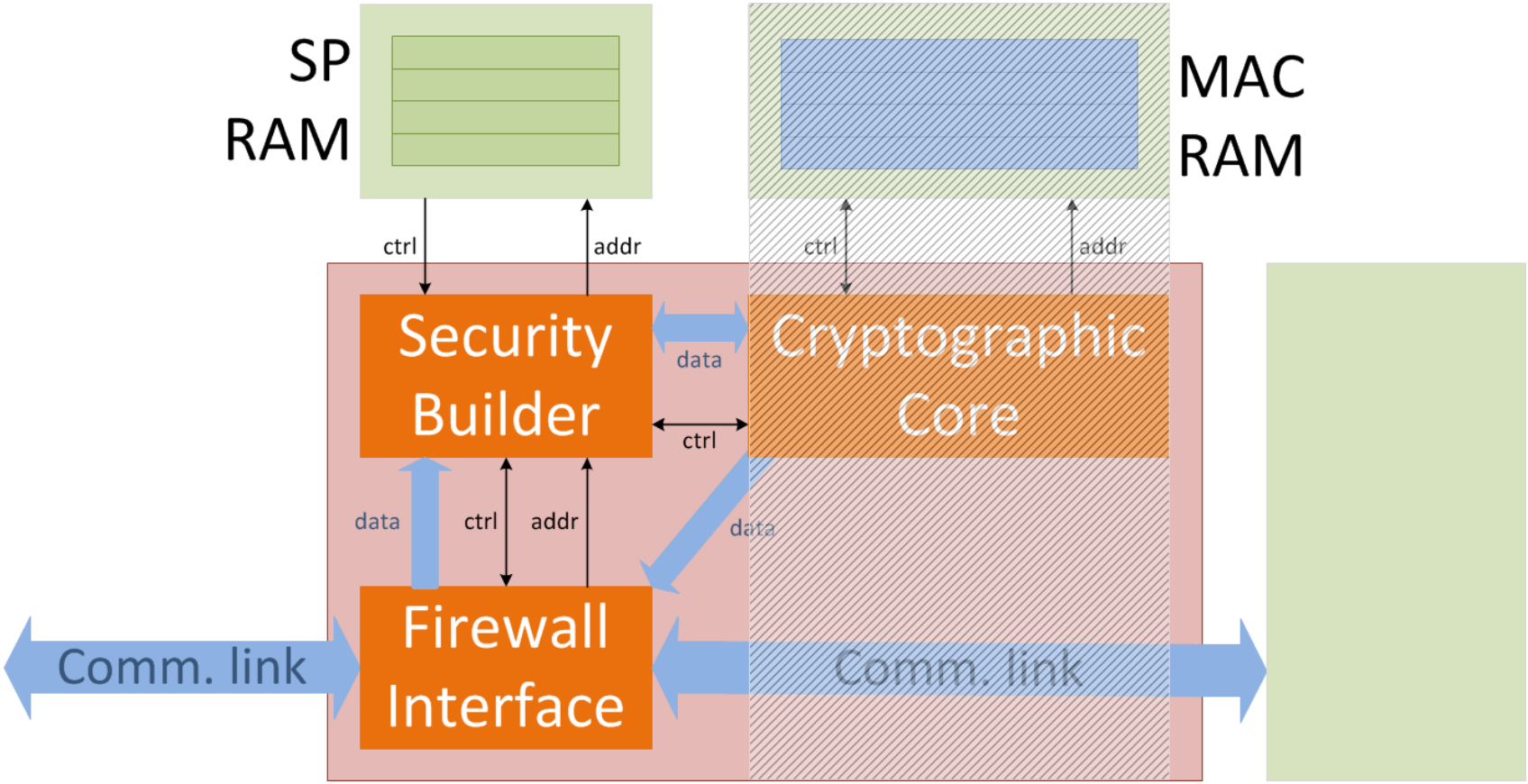


Ciphering Firewall overview

- Interface between the embedded system and the external memory interface.
- MACs and security policies are stored in on-chip trusted memory.
- Reconfigurable security policies (through dedicated circuitry, supposed secure).



Hardware overview of firewalls

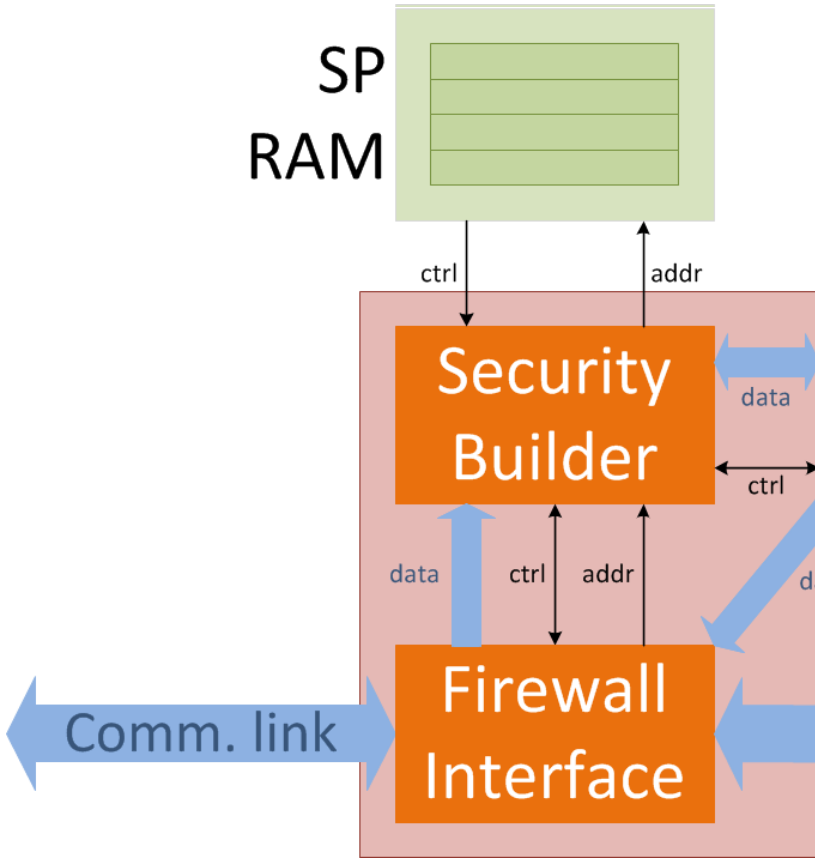


- CF additional logic is represented by the hatched area.
- Full hardware design.
- RAMs are implemented using FPGA block RAMs.

Security Builder and Firewall Interface

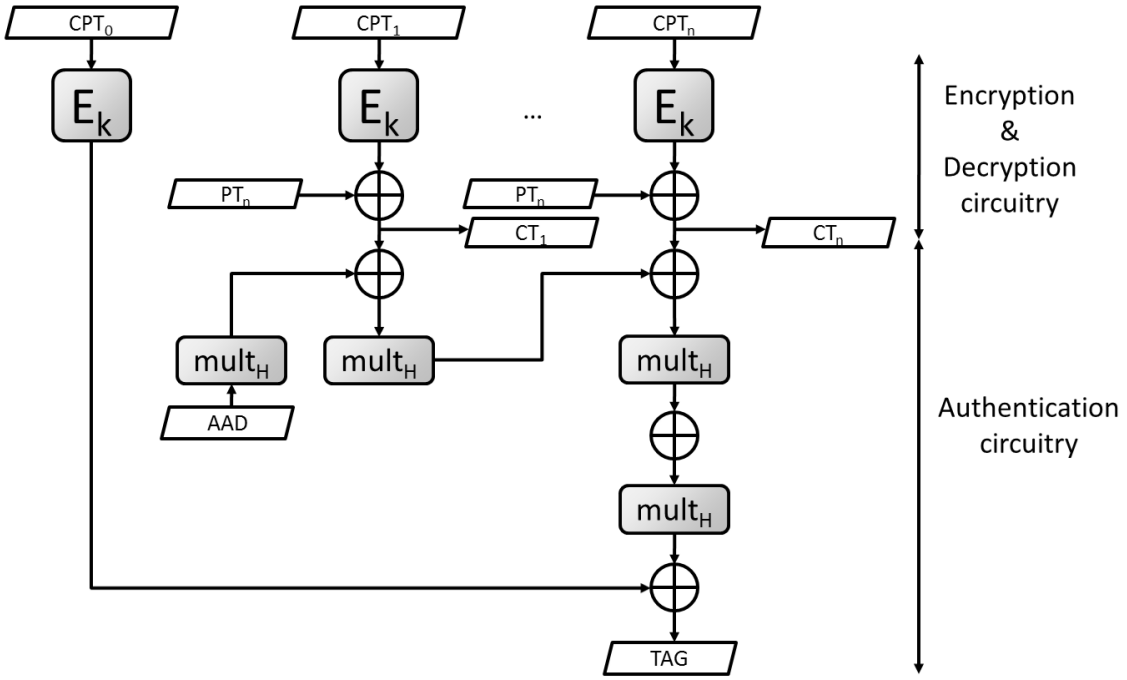
- Firewall Interface:
  - Temporary data storage.
  - Synchronization.
  - Communication with the external world.

- Security Builder:
  - Reading Security Policies.
  - Checking parameters.
  - Transmitting to Cryptographic Core.



Cryptographic Core

- Based on AES-GCM standard.
- Provides authentication and confidentiality in a single core.
- MACs are stored in trusted on-chip memories.



- Ciphered data available in 10 clock cycles.
- Authentication needs 2 additional cycles.

McGrew, D. 2004. "The Galois/Counter mode of operation (GCM)." *http://siswg.net/docs/gcm_spec.pdf*.

Outline

1) Related work
2) Hardware firewalls
3) Case study
4) Results analysis
5) Conclusion and perspectives

Outline

1) Related work

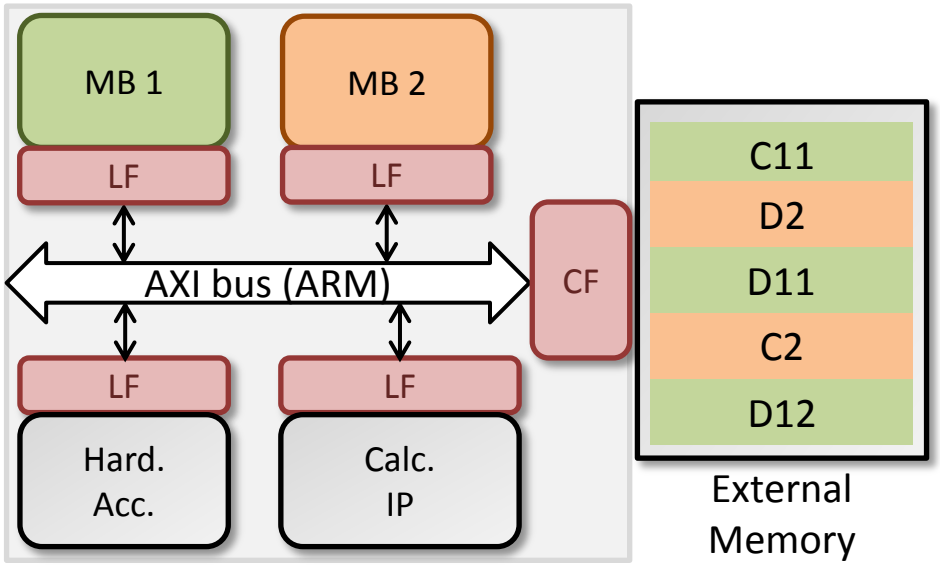
2) Hardware firewalls

3) Case study

4) Results analysis

5) Conclusion and perspectives

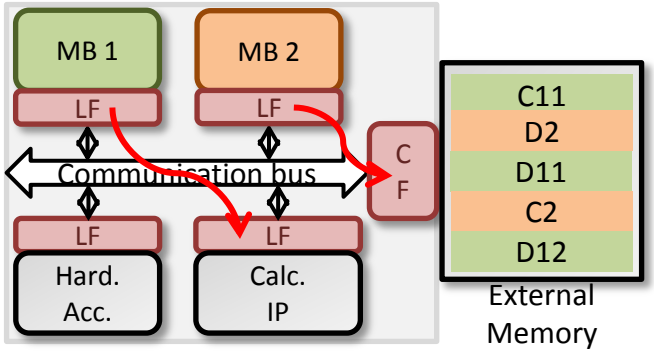
Case study



- Processors.
- Hardware accelerators.
- Specific access rules.
- Memory protection:
  - C11 + D11: confidentiality + integrity.
  - D12: integrity only.
  - D2 + C2: plaintext.
- Hard. Acc:
  - MB1: Read/Write access.
  - MB2: Write access.
- Calc. IP:
  - MB2: Read/Write access.
  - MB1: no access.

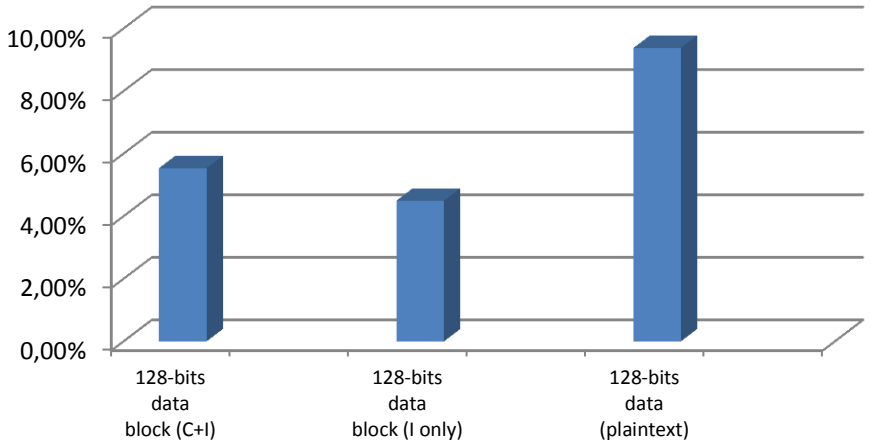
- Representative of a generic embedded system.
- Implementation on XC6VLX240T Virtex-6 FPGA with Xilinx 13.1 ISE tools.
- Latency, memory occupancy and area.

Results - Latency

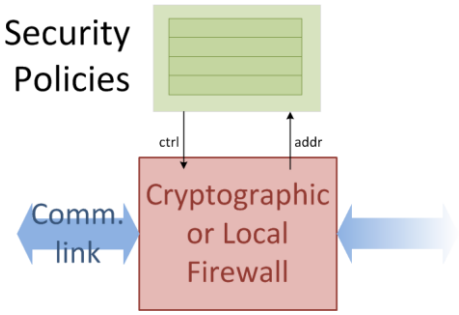


- Overheads for 128-bits wide data blocks.
- 5 cycles for Local Firewall.
- Number of cycles for Cryptographic Firewall depends on protection type (C+I, I or PT).
- Crypto-related features are part of the context established in our case study.

Latency overheads for LF-CF scenarios



Memory occupancy

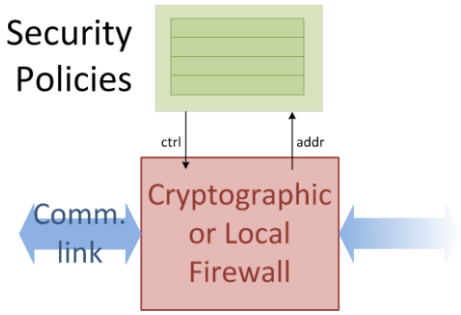


Reminder: Each firewall (Local or Crypto) has its own trusted on-chip memory containing its security policies.

Results are compared with the overall capacity of the Xilinx ML605 FPGA board (15 Mb).

SP RAM needed for:	Size (# of bits)
MB1	204
MB2	170
Hard. Acc.	68
Calc. IP	586
Ext. Mem.	68
Total	1096
Percentage (%) (/total BRAMs)	7,32 %

Memory occupancy



Reminder: Each firewall (Local or Crypto) has its own trusted on-chip memory containing its security policies.

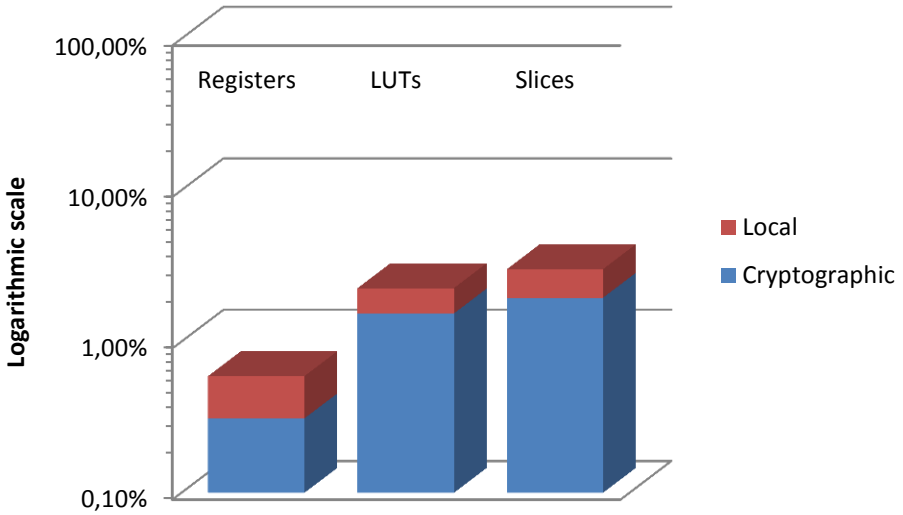
Results are compared with the overall capacity of the Xilinx ML605 FPGA board (15 Mb).

SP RAM needed for:	Size (# of bits)
MB1	204
MB2	170
Hard. Acc.	68
Calc. IP	586
Ext. Mem.	68
Total	1096
Percentage (%) (/total BRAMs)	7,32 %

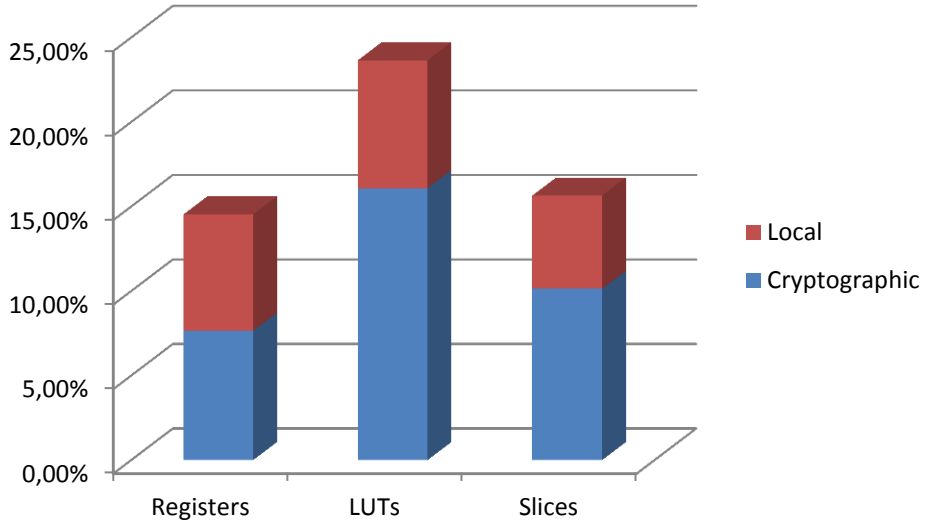
Bottleneck: MACs, which are also stored on-chip, are not taken into account… (compromise with latency).

Results - Area

Board occupancy



Overhead for the case study



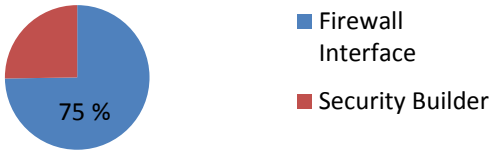
- Local + Cryptographic contributions.

- 4 Local Firewalls + 1 Cryptographic Firewall.

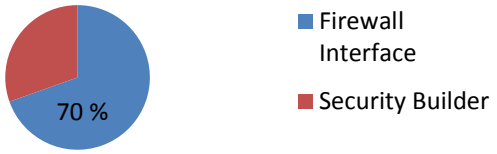
Results – Area

- What is the overhead due to ?

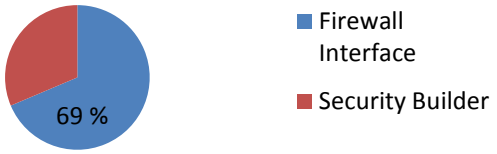
Local Firewall (registers)



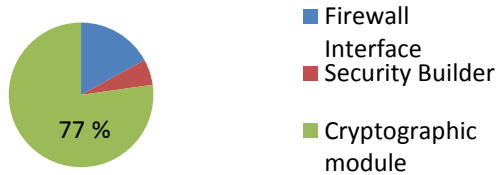
Local Firewall (LUTs)



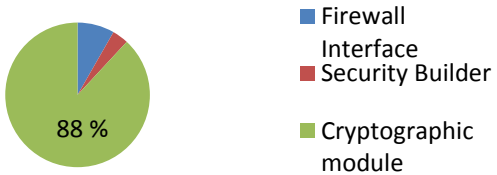
Local Firewall (slices)



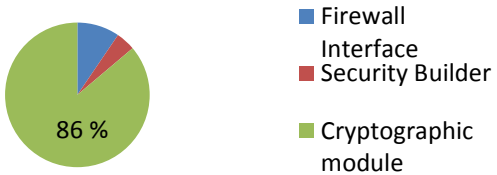
Cryptographic Firewall (registers)



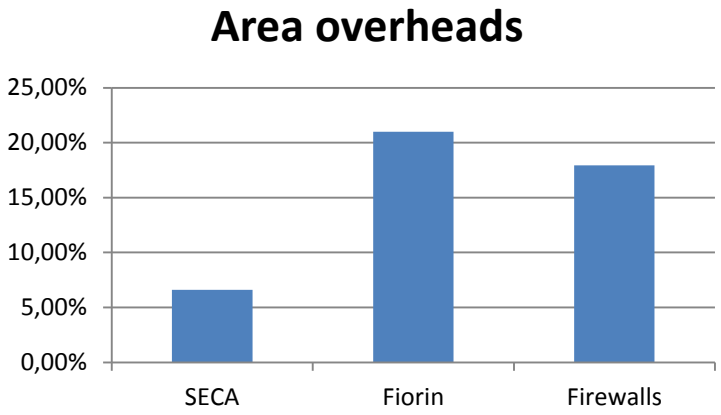
Cryptographic Firewall (LUTs)

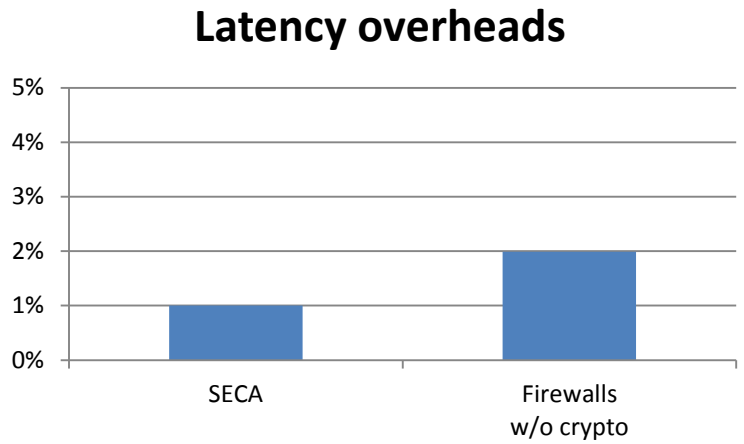


Cryptographic Firewall (slices)



Comparison with existing solutions



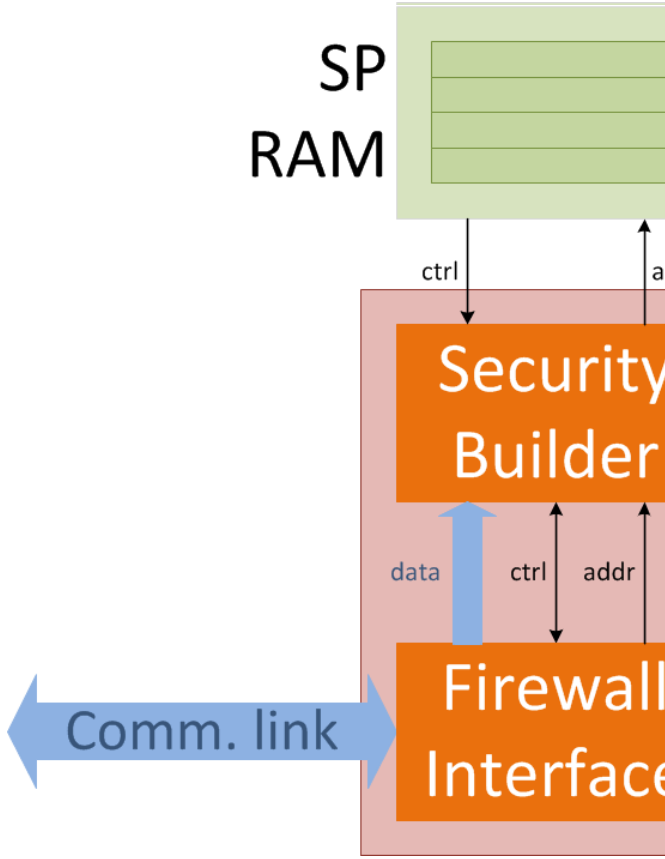


Area overhead should be put into perspective according to the overall size of the embedded system. Local Firewall area is low compared to CF one. Cryptographic Core is the “heaviest” block in terms of area: it does not matter how large is the MPSoC, there will be only only Cryptographic Firewall (one per DDR chip).

Does it fit specified requirements ?

- Reduced area overhead (for this case study).
- Low latency.
- Bottleneck : memory occupancy.

- Flexible security policies.
- Based on AXI protocol, an ARM standard.



Conclusion and perspectives

- Efficient solution in terms of area and latency overheads.

- Multi-level security-enhanced communications.
- Full hardware solution, no modification of the communication protocol.
- Extension to NoC-based architectures ?

- Ability to reconfigure security services (dynamically ?).
- Extension to threat-granularity security enhancements.

Protecting communications in bus-based MPSoCs using hardware firewalls

Pascal Cotret, Jérémie Crenne,
Guy Gogniat, Jean-Philippe Diguet

University of South Brittany, Lorient (France)

CryptArchi'11, June 17th, Bochüm (Germany)