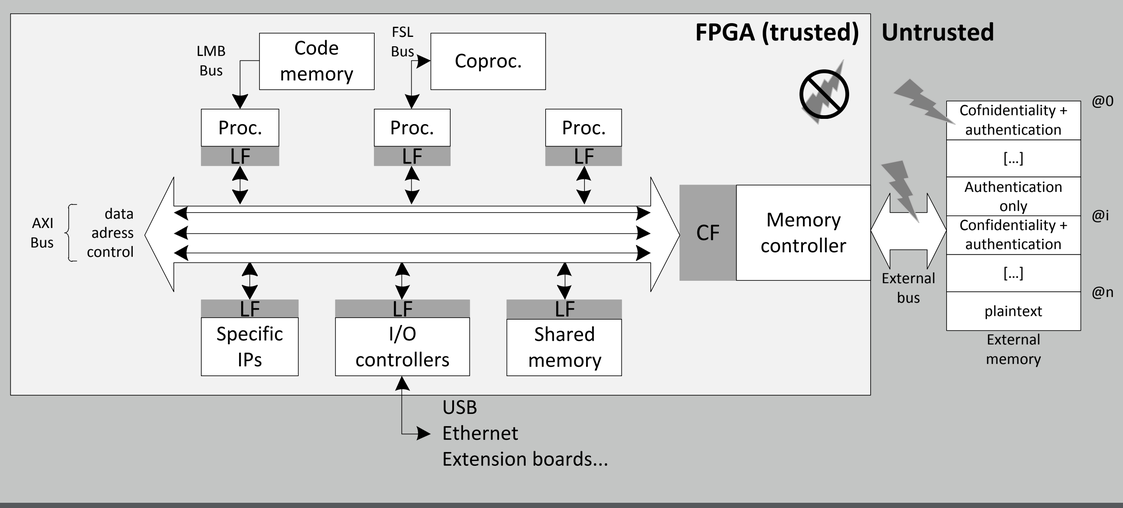
Lightweight reconfiguration security services for AXI-base MPSoCs

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

†Laboratory Lab-STICC, University of South Brittany, Lorient, France
‡Laboratory LIRMM, University of Montpellier, Montpellier, France

Firewall-enhanced multiprocessor architecture

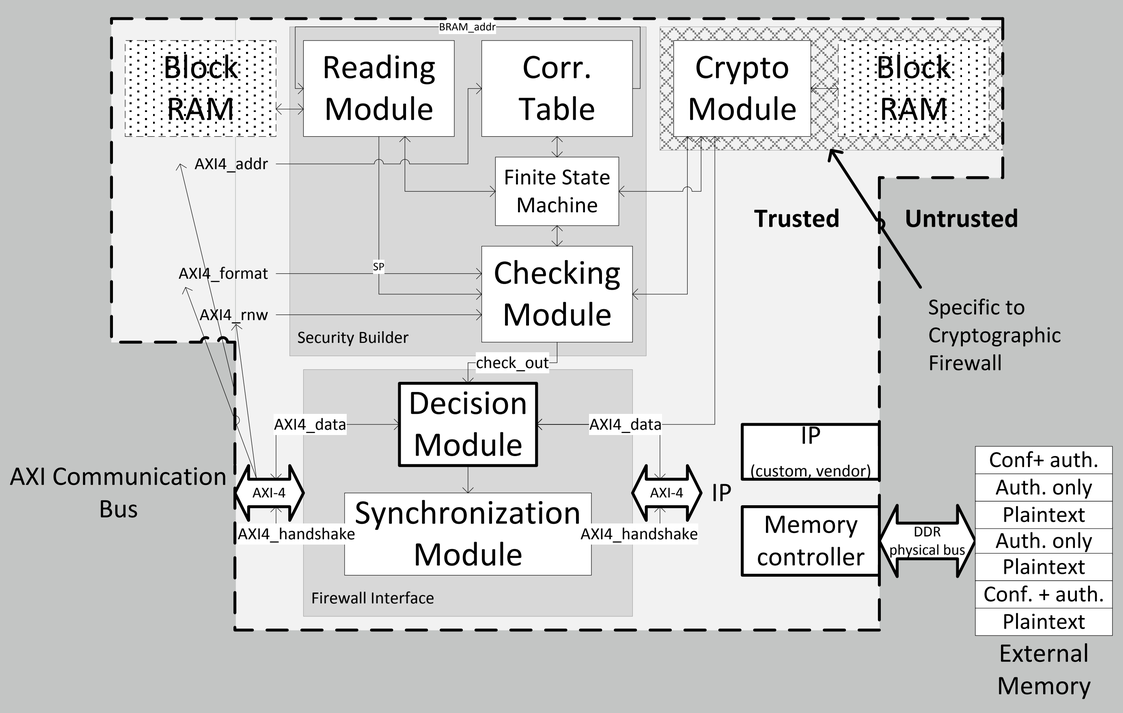
Hardware firewalls embedded in each IP interface.



Security update requirements

- **Area consumption:** mechanisms for security updates must not take too much area.
- **Reactivity:** in case of an attack, a news security policy must be set as soon as possible without suspending the system features.
- **Evolution:** security parameters can be set to an higher or a lower level of severity depending on the presence of attacks.
- **Adaptivity:** Flexible cryptography for the external memory.

Firewall structure



- **Firewall Interface:** communication purposes between the IP and the system bus.
- **Security Builder:** extraction and verification of security policies.
- Security policies stored in a Block RAM.

.

Several security levels

In a **mixed situation**, transactions between 2 IPs can contain several security levels: some parts can be accessed in read and write while others are in write only. In some cases, access rights associated with the current transaction are uniform: the whole address space is in a particular mode (read-only, write-only, read/write or no access). For critical IPs, a **read-only mode** can be set to save confidential parameters before blocking the system. When an error is detected, a **quarantine/error mode** is set in order to isolate the IP currently attacked from any transaction: in this case, no read or write is allowed but security enhancements simulate a successful transaction. The most critical security level is the **system reboot**: when too many attacks happen in the security-enhanced MPSoC, the system is rebooted with the initial bitstream and the intial securiy configuration.

Update flows

- **Non-critical IPs:** Initial situation ⇒ Read-only ⇒ Error/quarantine ⇒ System reboot.
- **Critical IPs:** Initial situation ⇒ Error/quarantine ⇒ System reboot..

Current features

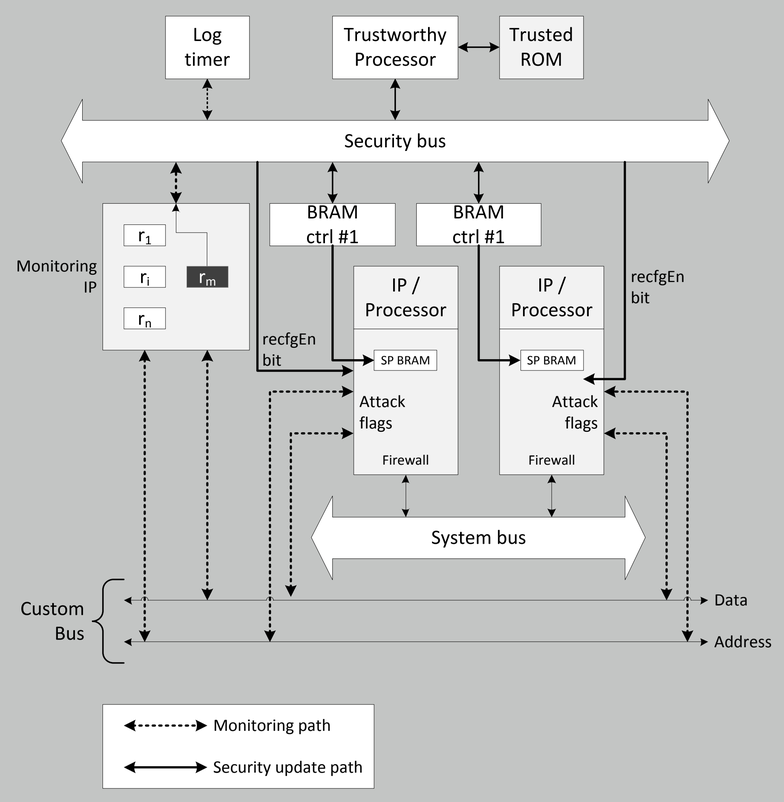
- Low-latency runtime protection for communications and memories.
- Cryptographic services for external memories (confidentiality and authentication).
- Monitoring of access rights, transactions formats and memory mapping using security policies.

Related work

- Pascal Cotret, Jérémie Crenne, Guy Gogniat, Jean-Philippe Diguet. *Bus-based MPSoC security through communication protection : A latency-efficient alternative.* FCCM 2012.
  ⇒ Protection and monitoring of communications and memories in a bus-based multiprocessor architecture.
- Joel Coburn, Srivaths Ravi, Anand Raghunathan, Srimat Chakradhar. *SECA: Security-Enhanced Communication Architecture.* CASES 2005.
  ⇒ Centralized security enhancements for a bus-based MPSoC without security update features.
- Leandro Fiorin, Slobodan Lukovic, Gianluca Palermo. *Implementation of a Reconfigurable Data Protection Module for NoC-based MPSoCs.* RAW 2008.
  ⇒ Distributed and adaptive security interfaces for a NoC-based system.

Reconfiguration requirements

When an attack event is detected, security policies must be updated to keep a safe execution environment.



- Attacks monitoring through the *Monitoring IP*.
- Block RAM update of security and cryptographic parameters by the *Trustworthy processor*.
- Security-related events in a log file using timestamps from the *Log timer* and attack/reconfiguration signals.

Results

	Slices	Regs	LUTs	BRAMs
Unprot. solution	5,446	7,195	8,354	32
Firewalls w/o recfg	7,302 (+34.08%)	9,848 (+36.87%)	12,215 (+46.22%)	51 (+37.25%)
Adapt. prot.	7,442 (+36.65%)	9,913 (+37.78%)	12,405 (+48.49%)	51 (+37.25%)

Conclusion

Trade-off between Fiorin and Coburn solutions.

	Coburn	Fiorin	This work
Area over a processor	6.20%	25%	11.41%
Adaptivity ?	No	Yes	Yes

Fiorin's based on a buffer-like mechanism (*shadow memory*) makes the area higher than this work.