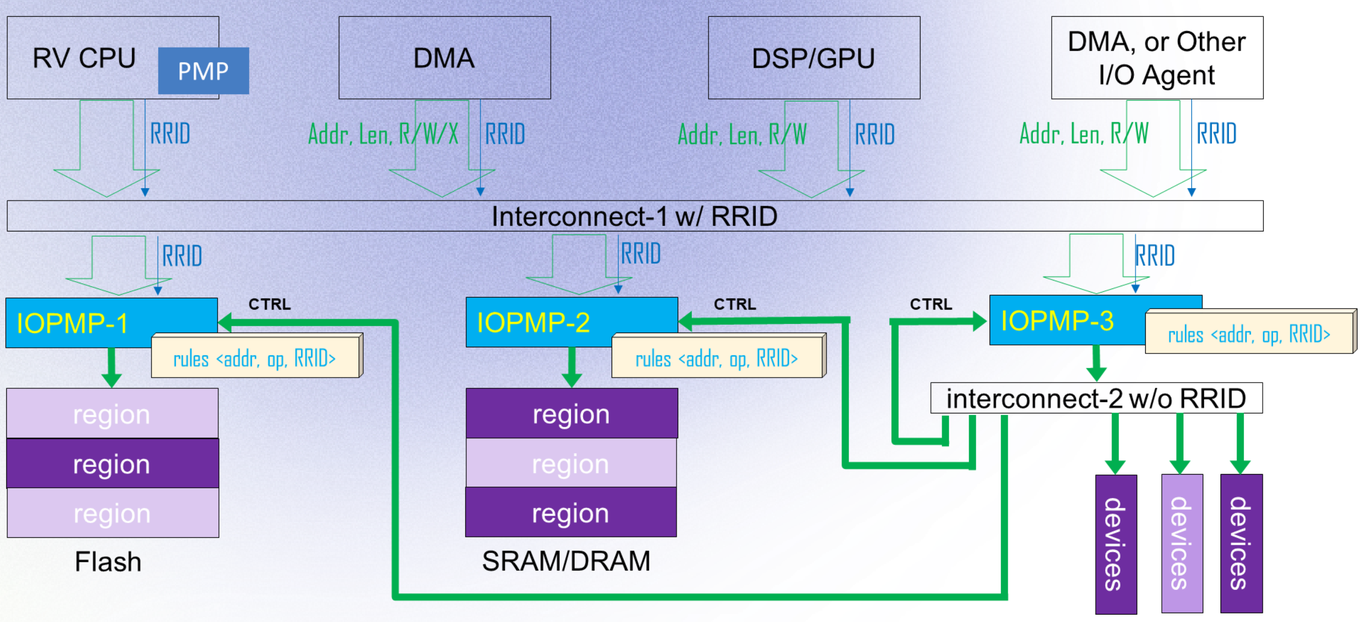
Deep Insight into IOPMP: Priority and Non-Priority Rules

Paul Shan-Chyun Ku
Andes Technology



IOPMP Secure Platform

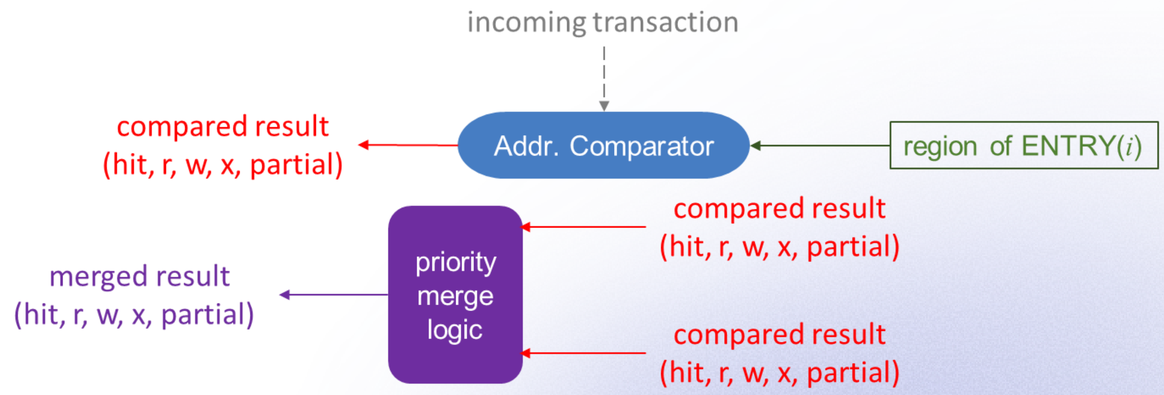
•The IOPMP is a hardware component that safeguards data by denying unauthorized access from I/O agents. It operates by checking each access against user-defined rules and reacts to unauthorized access by responding to the bus matrix, triggering an interrupt, or generating a violation report.

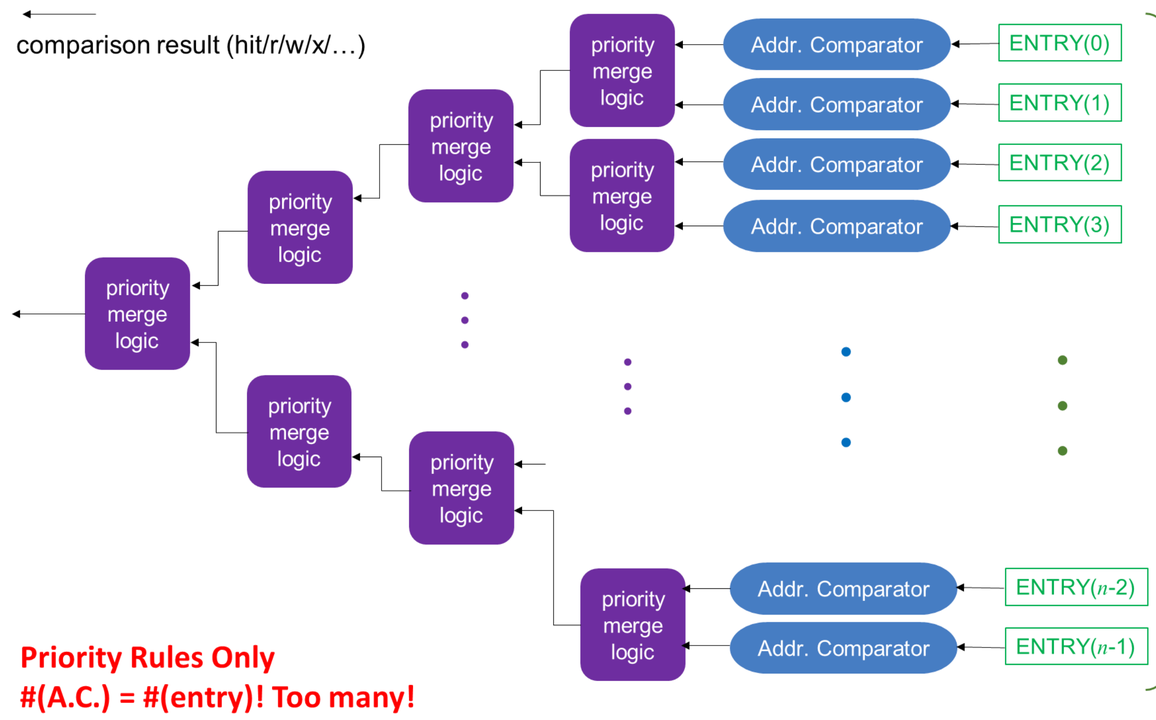
•Without access checks, the malicious can access everywhere by manipulating DMA-capable devices.

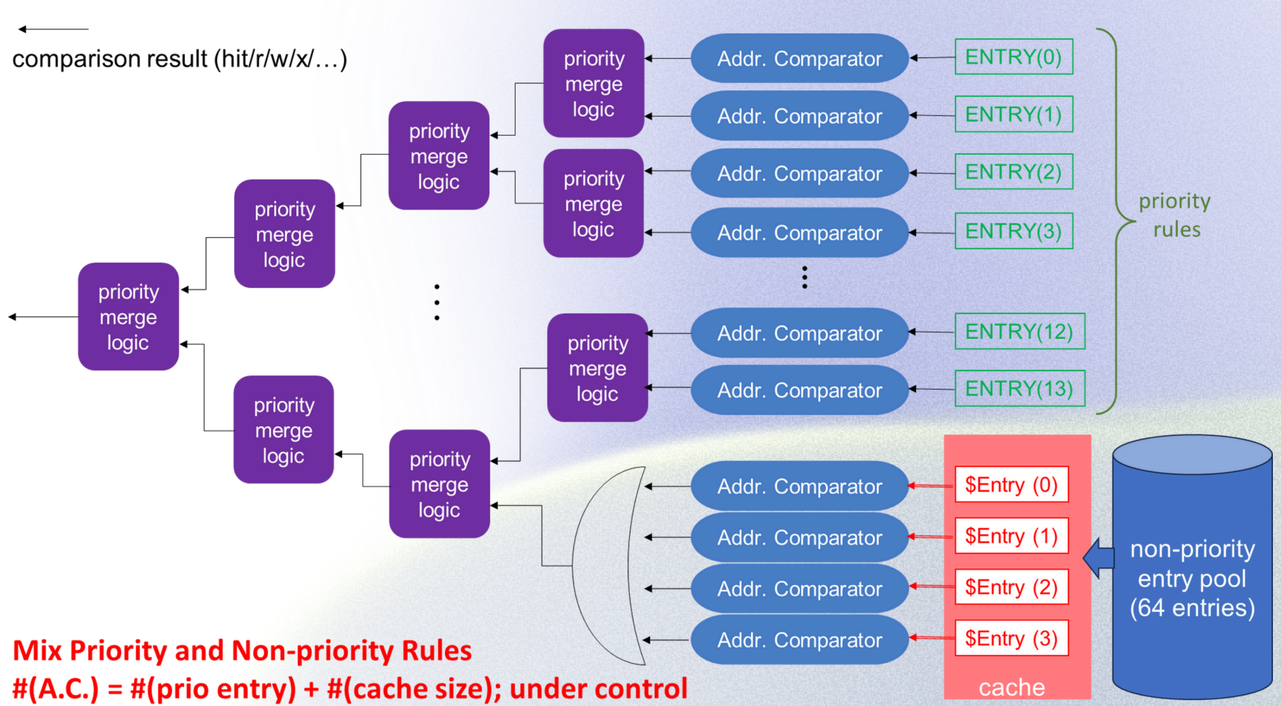
Scalability Challenge

- Rules increase when systems scale:
  - Address-Comparator and Priority-Merge-Logics increase linearly as rules increase
  - Size, power consumption, and check latency increases corresponding

The key components in an IOPMP increase as #(rule)







Priority and Non-priority Rules

	Priority Rule	Non-priority Rule
Permission	The matching rule having the highest priority decides	The rule granting enough permission grants
Violation condition	The matching rule having the highest priority denies	No matching rule granting enough permission
Overwrite	Lower indexed rules can overwrite higher indexed rules	No overwrite
Security strength	Higher: locked rules having highest priority cannot be breached. HW ensures.	Lower: a compromised rule can compromise the whole IOPMP.
Cacheability	Hardly: not sure if a cached rule is overwritten for a transaction.	The rules can be cached with a high locality.
Scalability	Lower: #(AC and PML)=#(rule)	Higher: #(AC and PML)=#(cache size)

Visit Andes' website for more info

Remarks

- Cache locality is excellent since
  - A stream of accesses from a DMA typically falls in a single IOPMP region
- Minimize the cache contention by
  - Letting cache size = max number of concurrent access streams
- Mixing priority and non-priority rules so that
  - Balancing security and scalability
  - Optimizing amortized throughput
- Enables SRAM/ROM use for rules storage