Chip Multi Processors, System On a Chip, and Multi-socket Protections

Chapter 7

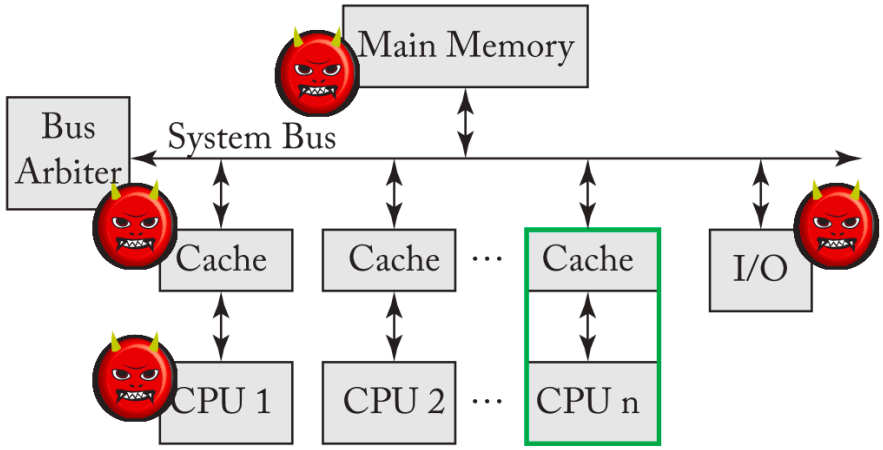
[1] J. Szefer, “Principles of secure processor architecture design,” *Synth. Lect. Comput. Archit.*, vol. 13, no. 3, pp. 1–173, 2018.

Security Challenges on Multiprocessors

- Multi-socket Multiprocessors required off-chip communication between cores
  - Susceptible to similar attacks of memory (e.g., probing, physical interchange with rogue chips, …)
  - Require solutions (in the processor design) to guarantee system **confidentiality**, **integrity** and **authenticity**
- Chip Multiprocessors (CMP)
  - Less susceptible but (in Systems-on-a-chip or SoC) might include many IPs (accelerators, ASICs,..)
  - Certain IP can be malicious

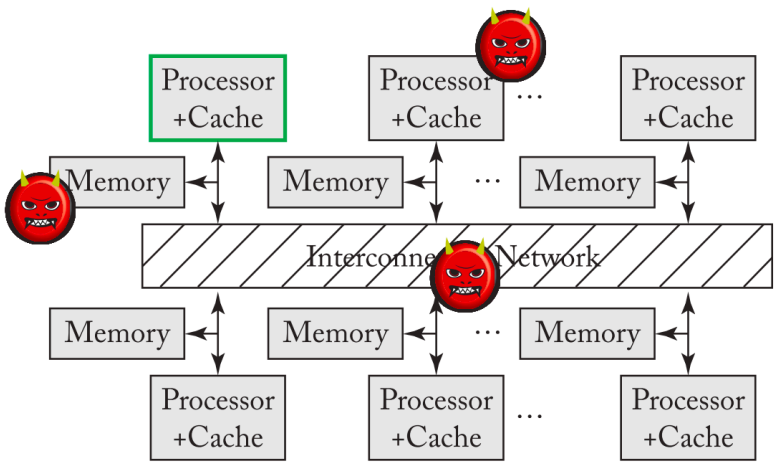
UMA Threat Model

- Confidentiality and Integrity
  - Communications
    - Counter mode AES (pregen. a counter encryption and *xor* with actual data)
    - Challenge to track the counters (pair origin destiny → higher storage reque., shared counter → increases protocol complexity)
    - For integrity use MAC
      - Can be combined: AES Galois Counter Mode (AES GCM)
    - **Easy to deploy mechanism: bus is shared**
  - Memory
    - Same as uniprocessor
- Access Patter Protection
  - SMT can be a problem
  - Independent ORAM per hardware context
- Key Management
  - Each processor will have their own key
  - Need some form of "coordination" in measurement. Public key cryptography might be too costly



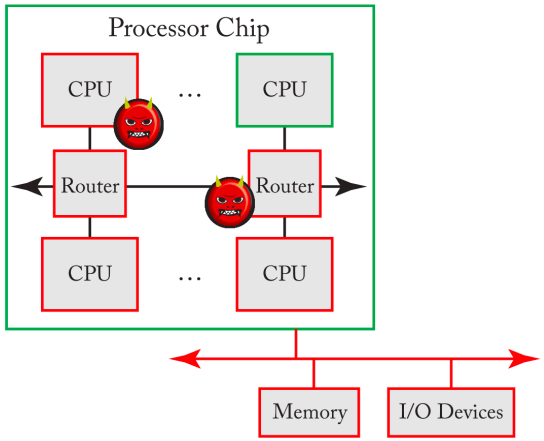
NUMA Threat Model

- None of the processors have a global vision of what is happening in the system
- Confidentiality and Integrity
  - Processor-to-processor comms AES or AES GCM
  - Need to be accommodate within the coherency protocol (prohibitive to cypher and decipher all messages)
  - AES might be too Slow ?(0.25 per cycle)
- Access Pattern Protection
  - Easier to obfuscate
- Key Management
  - Similar to UMA (perhaps a bit easier)



Threat Model for CMP + SoC (MPSoCs)

- Usually many IP inside a single chip: increased risk of having a malicious component (both in the supply chain and manufacture process)
- Processors or Accelerators can tamper with memory
- Routers can tamper packets (i.e., tamper memory)
- NoC wires are more easily detectable to external probing (i.e., packets can be accessed or modified)



Communication Protection Mechanisms

- Packets are broken down into flits->phits
- Phits should move fast (1-cycle from router to router): no room for encryption
  - Optimized (big) AES 4bytes/cycle, lightweight cyphers 1 byte/cycle while phits are 4bytes
- Solutions
  - Combine network coding into the cyphering strategy
  - Injection time

3D Integration Considerations

- Higher integration make less easy to access to the wires
  - Might need to change the threat model