Mitigating the Threat of a Malicious Network-on-Chip

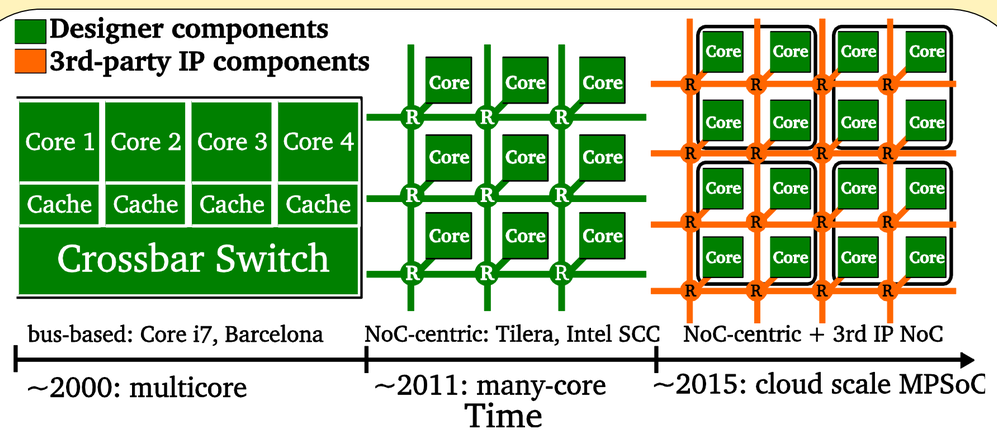
PIs: Koushik Chakraborty, Sanghamitra Roy, Utah State University

http://bridgelab.usu.edu/

Emerging Challenges in Trustworthy Computing

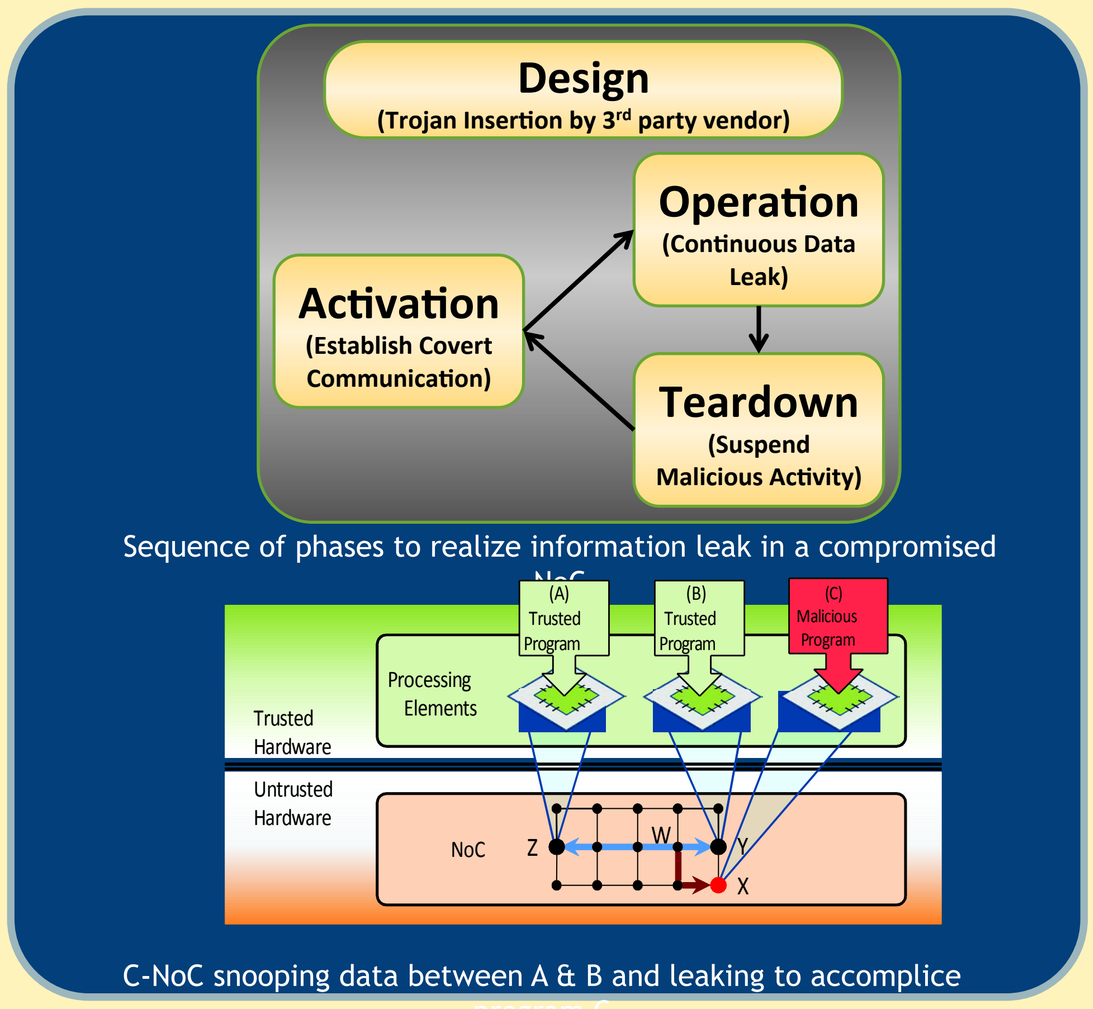
The objective of this project is to uncover the threat of a compromised Network-on-Chip and the range of possible attacks.

- Multicore server processor evolution.
- Transition from bus-based crossbars to on-chip Network for inter-core communication.
- Increased emphasis on employing third party IP blocks to reduce cost.
- Increased vulnerability of MPSoC to malicious third party NoC IP.



Cloud Chips Design Evolution

Threat Overview



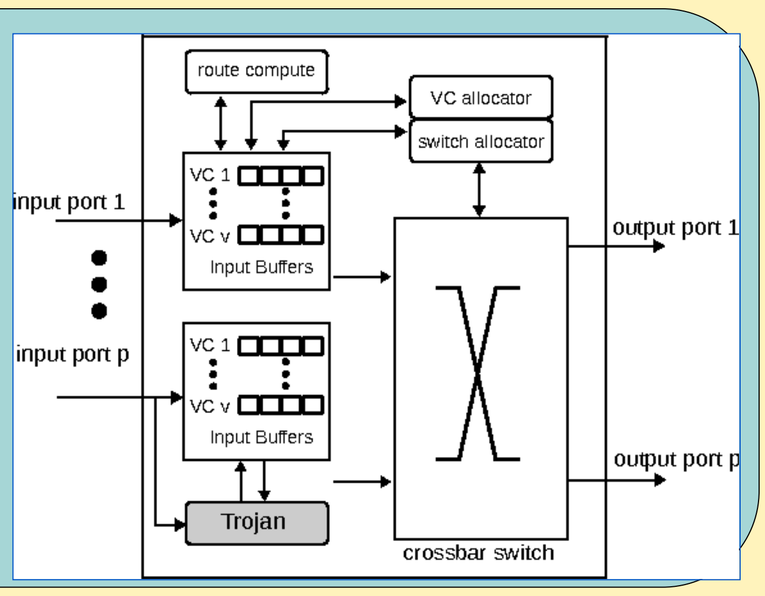
Sequence of phases to realize information leak in a compromised NoC

C-NoC snooping data between A & B and leaking to accomplice program C

Approach

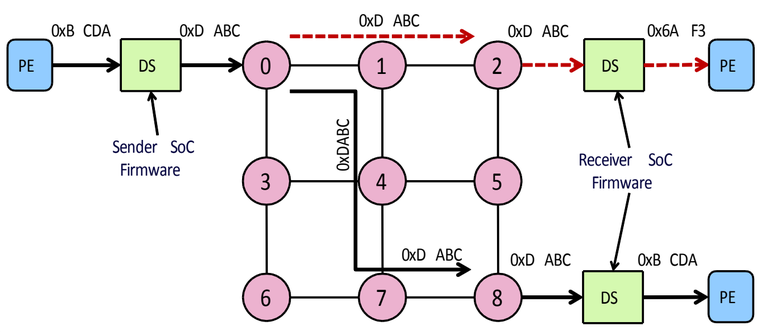
1. Detailed design of novel threat model stemming from Compromised NoC.
2. Holistic layered security mechanism to counter compromised communication platform.
3. Analysis of design solutions for power, area and performance overheads.

Metric	Overhead
Area(μm^2)	4.62%
Power(mw)	0.28%



Three-Layer Security

DATA SCRAMBLING – Data scrambled in SoC firmware before injection.

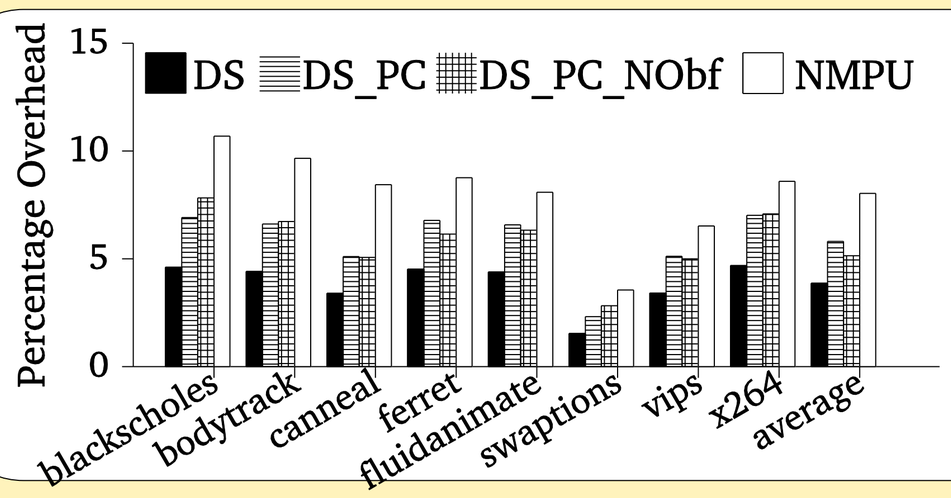


PACKET CERTIFICATION - Authentication using translated identifier tag

- Firmware creates lookup table with 16-bit, node based unique identifier
- Source: Each data packet embeds encrypted tag containing *translated identifier of destination node*.
- Destination: SoC firmware authenticates certificate before forwarding data to PE

NODE OBFUSCATION - Dynamically hides communication nodes in NoC

- Routine seamless migration of running application to different node.
- Periodically decouples source-destination of a given communication.



Products from this project

- Publications: DAC-14, NOCS-15, DAC-16
- 1 Patent Filed

Interested in meeting the PIs? Attach post-it note below!