Understanding and Mitigating the Threat of a Malicious Network-on-Chip

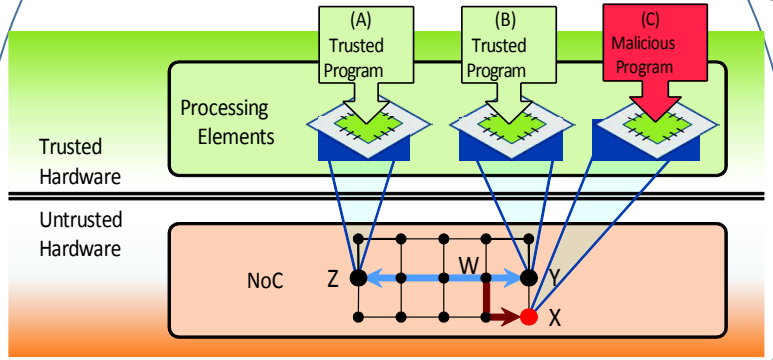
COLLEGE of ENGINEERING
UtahStateUniversity

Challenge:

- Multicore evolution-- Increased emphasis on employing third party IP blocks to reduce cost.
- Increased vulnerability of MPSoCs to malicious third party NoC IP..

Solution:

- Detailed design of novel threat model stemming from Compromised NoC.
- Holistic layered security mechanism to counter compromised communication platform.



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

Scientific Impact:

- Uncovering a potent threat from a compromised NoC.
- Demonstrate increased security vulnerabilities from growing use of third party IP blocks.

Broader Impact:

- Boost the MPSoC platforms by playing a central role in their security enhancement. Co-I actively involved with the Center for Women and Gender (CWG) group and the Society of Women Engineers (SWE). The Co-I holds sessions at Engineering Extravaganza.

Project info (1421068, Utah State University, PI: Koushik Chakraborty, Koushik.Chakraborty@usu.edu, Co-PI: Sanghamitra Roy, Sanghamitra.roy@usu.edu)