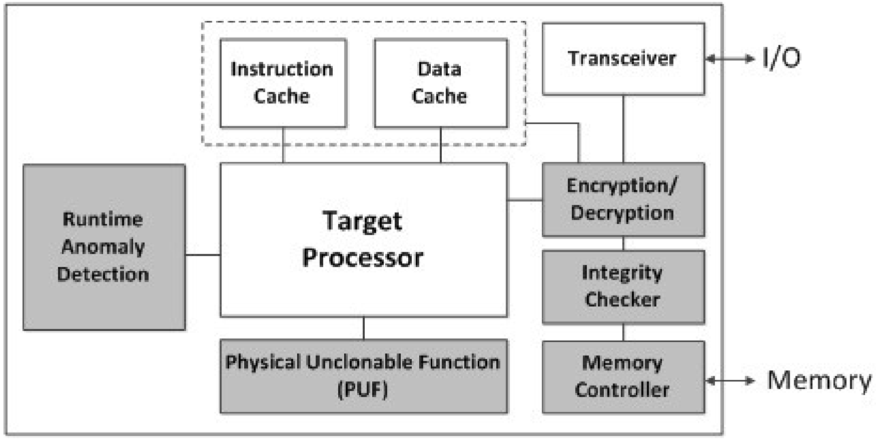
DEFEND: Design for Security

This research aims to address the question on how to design energy and resource efficient embedded processors that can still meet speed constraints and at the same time, withstand malicious cyber-attacks. We aim to develop a novel design-for-security methodology, called DEFEND, that is capable of systematically transforming insecure programmable computing environment by auto-generating a secure wrapper to meet user-specified design constraints and security levels. A major challenge is to effectively explore security-performance-area trade-off.

In order to provide for secure execution, we propose to employ hardware-aided runtime anomaly detection to leverage on the number of advantages hardware assisted mechanisms offer over software solutions. Hardware solutions cannot be easily bypassed by the attacker and are immutable and the inherent parallelism of hardware provides for high-speed detection of attacks. Computation intensive security countermeasures can be achieved in an energy-efficient way. Lastly, reconfigurable computing techniques using FPGAs facilitate security updates while providing for the performance advantages of hardware. Secure communication through lightweight encryption and authentication schemes provide countermeasures against data/identity thefts. However, the underlying security primitives for these schemes can still be compromised through side-channel attacks. Hence, it is necessary to design security primitives that are also resilient to implementation attacks. Finally, secure storage using memory encryption and authentication scheme are necessary for protecting integrity attacks on the storage contents.



Principal Investigator	Asst. Prof. Lam Siew Kei *(SCSE)*
Student	Ms. Saru Vig
School/Department	School of Computer Science and Engineering