STARSS: Small: Automatic Synthesis of Verifiably Secure Hardware Accelerators

CNS-1618275; PIs: **Zhiru Zhang and G. Edward Suh**
Computer Systems Lab (CSL), School of Electrical and Computer Engineering, Cornell University

Challenges

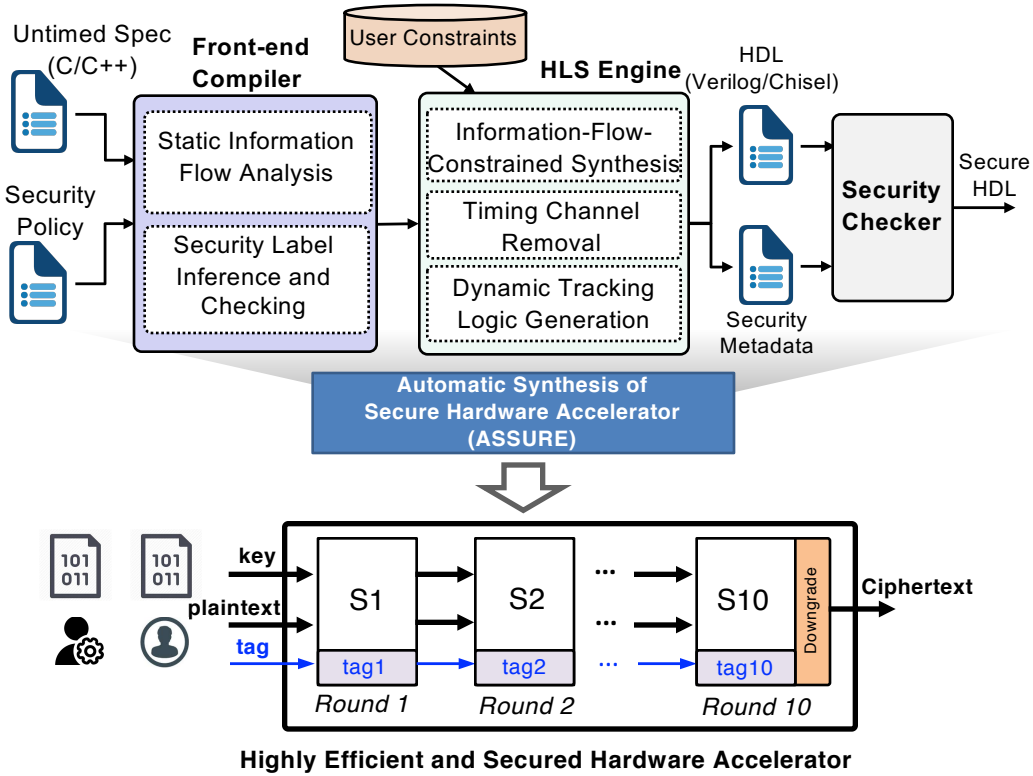
- **Context**: Modern systems are increasingly heterogeneous, integrating a broad range of special-purpose hardware accelerators for performance and energy efficiency
- **Problem:** Hardware specialization introduces daunting design complexity and a host of new security challenges that have not been adequately explored

Proposed Solution

- **Proposal:** A novel design automation framework called ASSURE to automatically synthesizing verifiably secure hardware accelerators from high-level programs
- **ASSURE high-level synthesis (HLS)**: Generating efficient accelerators that ensure no information leaks through either explicit information flows or timing side channels; scheduling algorithms (FPGA'18, DAC'19), HLS framework (ICCAD'18).
- **ASSURE security checker:** Verifying that the desired security properties of the synthesized accelerators are guaranteed through a formally defined type checks; Attacks on CNN (DAC'18), AES case study (DAC'19).

Scientific Impact

- **Enabling new advances** in design and design automation for secure accelerator-rich system-on-chips
- **Setting new directions** in interdisciplinary research between security, EDA, and programming languages – the first attempt that offers automatic timing-sensitive information flow guarantees by HLS and type systems



Broader Impact

- **Impact on Society:** Ensuring strong and verifiable information control for future system-on-chips, which are expected to be widely used from small embedded devices to servers in data centers
- **Education and Outreach:** (1) Integration of hardware security topics into the computer engineering curriculum (2) High-school outreach efforts through a week-long summer program for URM students