Hardware and Software Techniques for Securing Intelligent Cyber-Physical Systems

Faqih Khalid\(^1\) (Ph.D. Candidate), Muhammad Shafique\(^2\) (Advisor)
\(^1\)Technische Universität Wien (TU Wien), Vienna, Austria
\(^2\)Division of Engineering, New York University Abu Dhabi (NYUAD), Abu Dhabi, UAE

**Problems and Motivation**

- Design a Cost-Effective Secure Intelligent CPS
  - Customized hardware/software solutions at appropriate system layers
  - Adapting to application properties and user requirements

**Hardware-level Techniques**

- Communication-based Runtime HT Detection [MICPRO’20]
  - Extract the Communication Behavior of Trusted IPs
  - Design the PSL Assertion based on the Communication Behavior of the Trusted IP
  - Design Modules to Compute Statistical Parameters during Runtime, i.e., Hurst Exponent, Hop Probability, and Standard Deviation

- Fine-grained Power-profiling-based Runtime HT Detection [TCAD’20]
  - On average, our approach (SIMCom) achieves 99% HT detection accuracy with a 1.5% drop due to process variations (PV) and exhibits less than 1% area overhead and +1% power overhead.

**Software-level Techniques**

- Security Attacks on ML-based Systems [JCNN’20]
  - The proposed attack (FaSec), with appropriate attack parameters values, converges 16x faster and generates the attack image with 20% better imperceptibility than the state-of-the-art decision-based attack. Open-source: https://github.com/FaKldhi/FaDec

- Software-level Defenses for ML-based Systems [IOLTS’19] [D&T’20]
  - On average, QuSecNets increases classification accuracy up to 50%-96% (MNIST) and 10%-50% (CIFAR10). SSCNets increases classification accuracy up to 16%-30% (White-box scenario) and 28% to 48% (Black-box Scenario).

**Selected Publications**


**Overview of Our Methodology**

- Energy-efficient Hardware-level Techniques to Secure a Smart CPS (Access 2021)
- Fast Decision-based Black-box Attack on ML Systems [IOLTS’20]
- Quantization-based Defense Mechanisms [IOLTS’20]

**This Ph.D. is supported in parts by the FFG and the BMVIT, Austria, under the “ICT of the Future” project, iot4CPS. Trustworthy IoT for Cyber-Physical Systems**