SAND2019-8021D

The Center for Cyber Defenders

Expanding computer security knowledge

Hardware Trojan Demo

Jonathan Cruz, University of Florida and Julian Tuminaro, Carnegie Mellon University

Project Mentors: Ray Finch, 5847; Eric Hokanson, 5847; Vivian Kammler, 5845

Problem Statement:

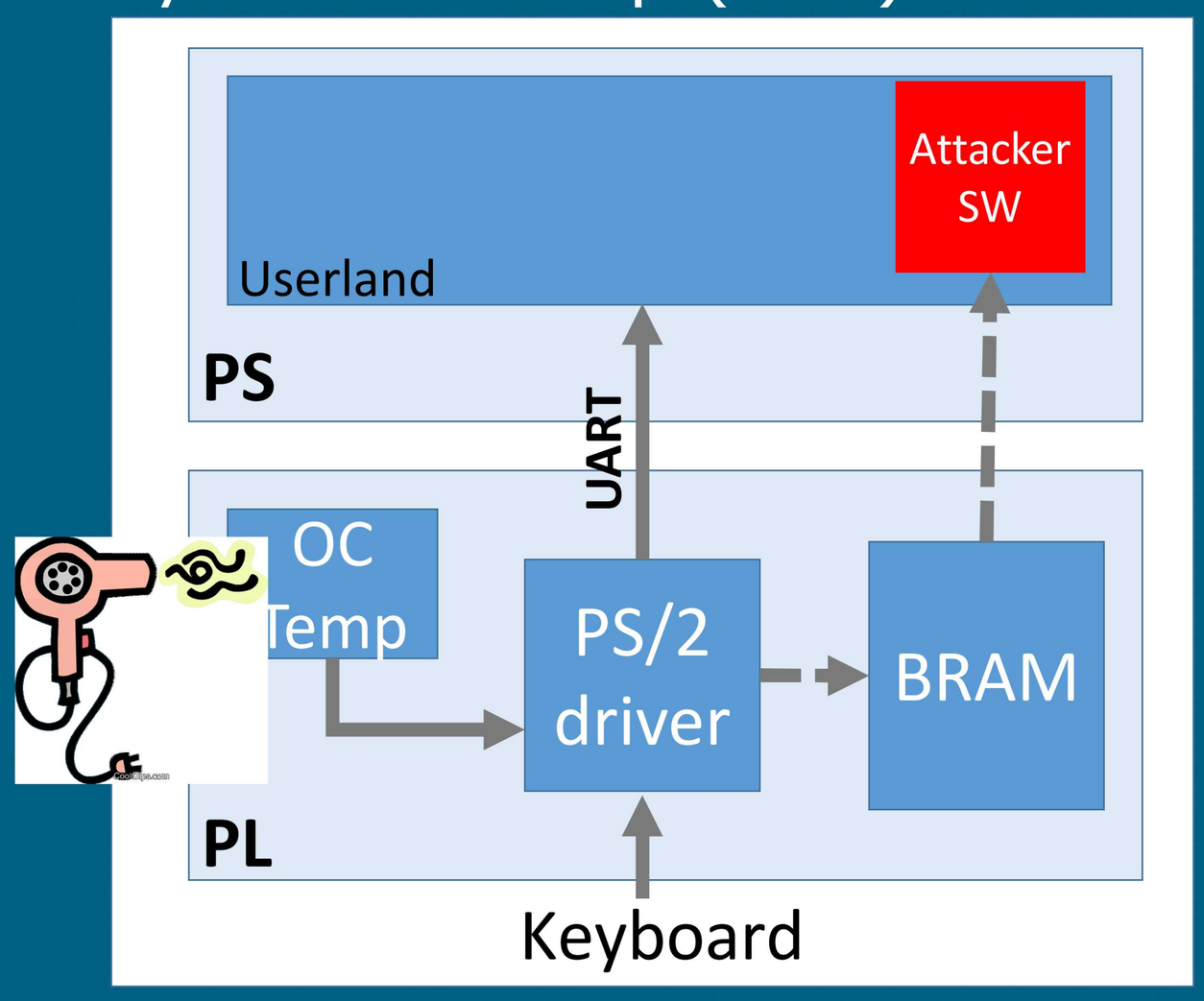
- Globalization of semiconductor supply-chain introduces security concerns for domestic entities.
- Hardware Trojans are hard-to-activate and hard-to-detect malicious circuitry that can be inserted by untrusted parties and cause unwanted functionality.

Objectives and Approach:

- Create demonstration of Hardware Trojans that can exist in 3rd –party IP.
- Demo 1: Malicious hardware (~8% area) PS/2 driver that logs key presses in block RAM (BRAM) of FPGA upon activation.
  - Use on chip (OC) temperature sensor to trigger Trojan once threshold temperature is reached.
- Demo 2: Hardware Trojan that logs key presses. Upon activation, can inject key strokes.

Results:

- Demo 1: Design implemented using Zybo Board with Zynq7000 System on Chip (SoC).



Demo 1 block diagram

- Demo 2: Design implemented using USB Master Board with PIC18F67J10 Flash Chip and VNC1L USB Host Controller.

Impact and Benefits:

- Logging implemented solely in hardware – no amount of software protection will help (yet).
- Showcase problems and solutions being addressed at Sandia for hardware security.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.