Proposal for HOST Hardware Demonstration
Florida Institute for Cybersecurity (FICS) Research, University of Florida

Hardware Hacking Security Education Platform (HaHa SEP):

Enabling Hands-On Applied Research of Hardware Security Theory & Principles

Presenters: Jason Vosatka, Shuo Yang
Authors: Jason Vosatka, Shuo Yang, Dr. Domenic Forte, Dr. Mark Tehranipoor

The domain of Hardware Security and Trust is growing exponentially. It is critical for academic students and security professionals to transform their theoretical understanding of hardware security into an advanced, real-world expertise. Although undergraduate and graduate students study hardware security principles through curriculum at academic universities, our research indicates there is no platform that allows students to further develop the vast learned theory beyond the typical classroom. Additionally, security professionals have the challenge of refining their skillset as existing development platforms perform only a very limited number of fixed experiments. Our novel solution empowers any security researcher to further develop their knowledge and skills by performing research and development of hardware and systems security. This is accomplished through hands-on experimentations with observable and measureable results; thus enabling tech-transfer based research spanning from academic theory to real-world applications of hardware security and trust.

Security researchers using our "Hardware Hacking Security Education Platform (HaHa SEP)" system will develop the expertise required to effectively combat current and emerging threats to hardware and systems security. The HaHa SEP is both educational and flexible as it allows for implementation of a diverse range of hands-on attacks and countermeasures. It is also expandable, which enables researchers to continually develop and refine their security skills as new threats emerge. Furthermore, the HaHa SEP is an easy to understand system and features an FPGA, microcontroller, JTAG interface, Bluetooth wireless technology, EEPROM memory, and also supports user interactivity through pushbuttons, LEDs, as well as an analog and digital sensor suite. The HaHa SEP currently supports over a dozen organized experiments including the following: hardware trojan attacks, hardware-based security primitives (PUFs, RNGs), side-channel attacks, bus snooping attacks, PCB reverse engineering, fault-injection attacks, modchip attacks, buffer-overflow attacks, cryptography attacks, as well as performing security analysis of System-on-Chip (SoC) and Internet-of-Things (IoT) systems.

The main components of the hardware demonstration at IEEE HOST will consist of four HaHa SEPs, two laptops, two oscilloscopes, and two logic analyzers. The audience will be allowed to interact with the demonstrations, perform selected hardware attacks (e.g. triggering a hardware trojan), and witness other hardware vulnerabilities being exploited in real-time. Please refer to Figure 1 for a notional setup of our HaHa SEP hands-on hardware demonstration.

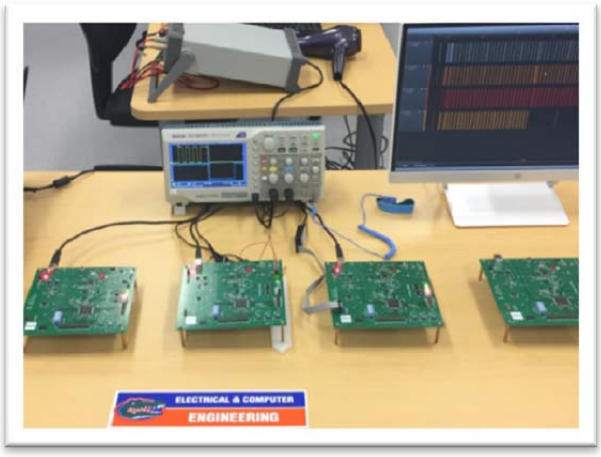

Figure 1: Notional HaHa SEP Hands-On Hardware Demonstration