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

Hardware Hacking Security Education Platform (HaHa SEP v2): Enabling Hands-On Applied Research of Hardware Security Theory & Principles

Shuo Yang, Jason Vosatka, and Swarup Bhunia[1]
University of Florida, Gainesville, FL, USA

As the domain of Hardware Security and Trust rapidly grows, the need arises essentially for students and security professionals to practice their academic knowledge of hardware security on real-world security experimental platforms. Although undergraduate and graduate students study hardware security principles through the curriculum at academic universities, our research indicates there is no platform in the market that allows students to further develop the vastly learned theory beyond the typical classroom. Moreover, security professionals have the challenge of finding a platform that can apply their numerous skillsets rather than performing a very limited number of fixed experiments. To address the emerging need of practical hardware security education with well-designed hands-on experiments, we have developed a flexible platform, referred to as, Hardware Hacking Security Education Platform (HaHa SEP), as shown in Figure 1. The board is already being used by students in the hardware security lab course at the University of Florida and by the researchers at Florida Institute for Cybersecurity (FICS).

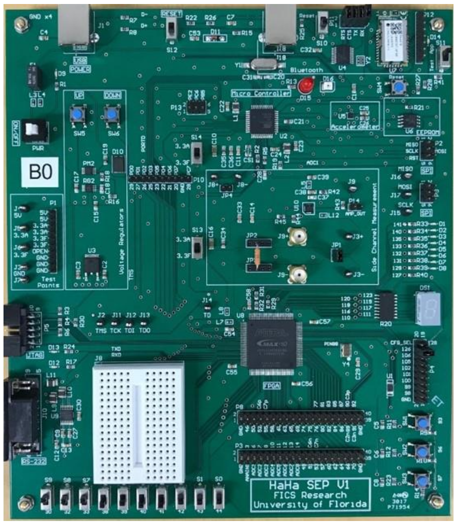

Figure 1: Improved version of HaHa SEP with multiple new features.

HaHa SEP is a platform that allows students and security researchers to develop the expertise required to effectively combat current and emerging threats to hardware and systems security. This year HaHa SEP goes to its 3rd generation which is more powerful and enables more hardware security experiments. The HaHa SEP is educational and flexible as it allows for a diverse range of designed attacks, as well as more expandable experiments that allow researchers to apply it to their own study and refine their security skills as new technics emerge. HaHa SEP keeps its initial attempt to stay as an easy to understand system, but at the same time to include more possible features. It is an only two-layered printed circuit board that features an FPGA, microcontroller, JTAG interface, Bluetooth wireless technology, EEPROM memory, and supports user interactivity through pushbuttons, LEDs, as well as an analog and digital sensor suite. In addition to the original experiments (which include hardware trojan attacks, hardware-based security primitives, side-channel attacks, bus snooping attacks, PCB reverse engineering, buffer-overflow attacks, cryptography attacks, etc.), more new experiments are designed and will be demonstrated. They are JTAG attacks, Bluetooth attacks, Hardware Obfuscation, Fault-injection attacks and Mod chip attacks.

Description of the Experiment:

Fifteen hands-on experiments have been developed on the HaHa SEP platform to comprehensively cover diverse aspects of hardware security. These experiments have been successfully run by numbers of students in the Hardware Security Lab course at the University of Florida for past couple of years. This demonstration of the HaHa SEP v2 platform in HOST 2018 will include some representative experiments, as described below.

- **Bluetooth attack** is an experiment for students and professionals to attack the Bluetooth module of another device through the Bluetooth chip on the HaHa SEP. With the Bluetooth module on the board, one HaHa SEP can communicate with or even control another HaHa SEP and all devices with a Bluetooth module. The users can take the control of another device and make it realize specified behavior through the attack of the Bluetooth module.
- **JTAG attack** allows the users of HaHa SEP to hack the firmware of a chip through the JTAG chain. An FPGA and a microcontroller are included in the same JTAG chain on the HaHa SEP board. The connection can be configured so that they can program each other through the JTAG chain. Thus, the originally prepared firmware in the microcontroller can be tampered with the JTAG attack.
- **Hardware Obfuscation** implements different Hardware Obfuscation techniques for securing hardware intellectual properties against piracy and tampering attacks. Users can apply combinational obfuscation and sequential obfuscation on benchmarks and see how the technic can resist against Brute Force attacks.
- **Fault Injection** attack enables the users of the HaHa SEP to inject a fault into a design so as to compromise the security of the system. The Phase Locked Loop (PLL) in the FPGA can be configured to generate a glitched clock which can lead to a bit fault taken place in an Advanced Encryption Standard (AES) and as a result leak the information of the key that the AES uses.
- **Mod chip attack** is possible due to the flexibility that the HaHa SEP has. It has numerous user-configurable pins and headers. Users can thus modify the board and compromise the security of a key-protected system by modifying the signal bus from a limited key to a full functional key.

Experimental Setup:

1. Four new HaHa SEPs.
2. Two laptops to programming the chips on the HaHa SEPs.
3. Two oscilloscopes to measure the signals from the HaHa SEPs.
4. Two logic analyzers to measure and analyze the signals from the HaHa SEPs.

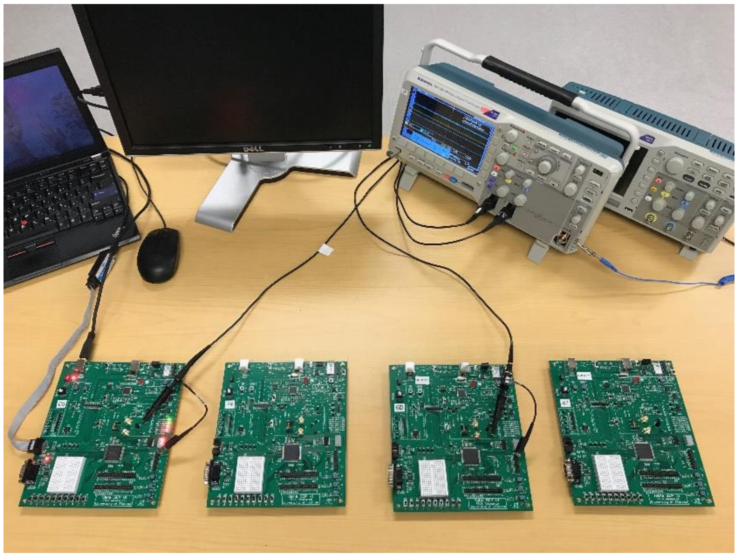

Figure 2: HaHa SEP Hands-on Hardware Security Education and Training Platform Demonstration.