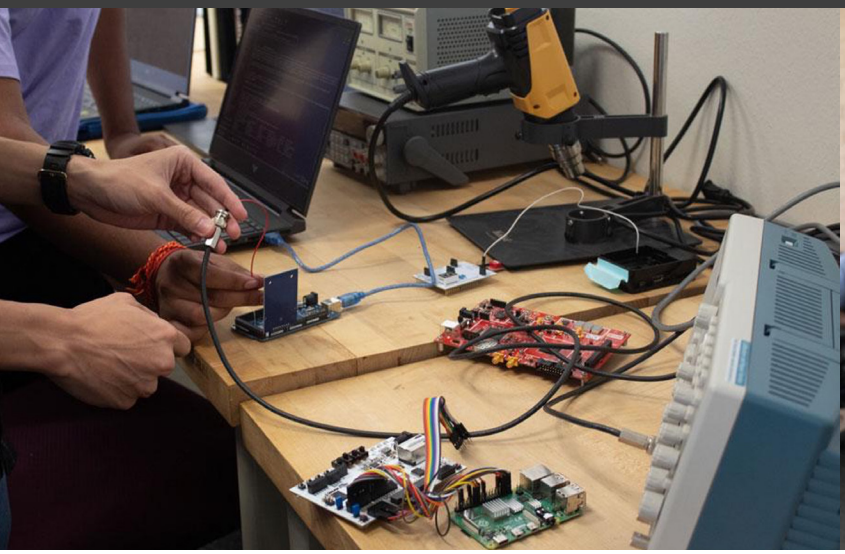
HANDS-ON HARDWARE SECURITY: ATTACK & DEFENSE



The hardware security lab is designed to provide an immersive, hands-on experience with real-world threats and defenses. You will conduct practical experiments on physical devices and obtain critical insights into hardware vulnerabilities. By working directly with real hardware platforms, you will develop the expertise needed to analyze vulnerabilities, execute attacks, and implement defenses. This lab serves as a crucial foundation for those seeking to specialize in hardware security, equipping them with job-ready skills sought after in semiconductor design, embedded systems, and electronic design automation industries.

WHAT YOU'LL LEARN

Fault Injection Attacks

- Inject transient faults into electronic systems without direct electrical contact.
- Perform attacks by generating rapidly changing magnetic fields near the target hardware, inducing unintended currents that alter its behavior.
- Equipment includes NewAE-CW520 ChipSHOUTER Kit, an electromagnetic fault injection platform.
- Attack targets include STM32F303K8T6 microcontroller and CW 522 Ballistic Gel SRAM.

Side-Channel Attacks

- Extract secret keys from encryption algorithms through unintended information leaks.
- Equipment includes NewAE-SCAPACK-L1 ChipWhisperer Kit, an integrated hardware platform to perform side-channel attacks.

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

Texas A&M Engineering Experiment Station

Hacking Embedded Systems

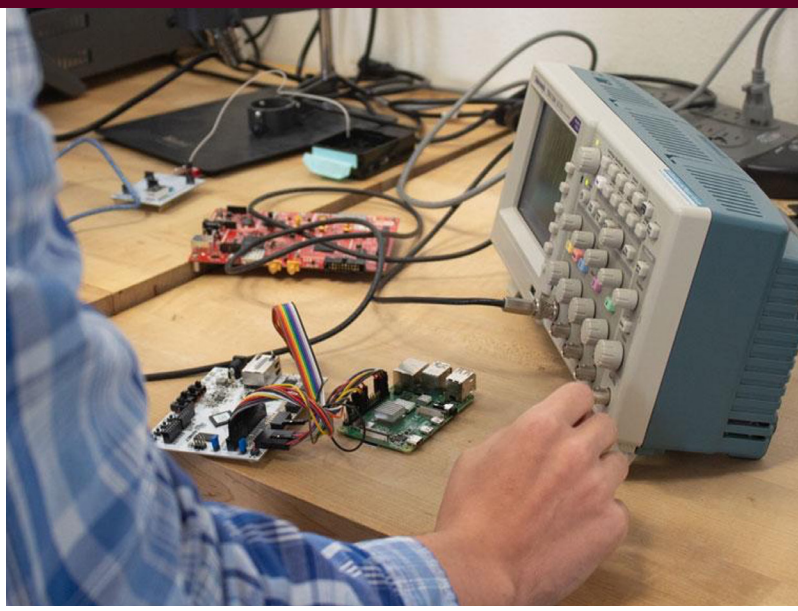
- Exploit a real-world embedded system by bypassing password authentication.
- Perform a buffer overflow attack to overwrite critical memory regions and hijack execution flow.
- Use ARM-based RPi as the target for hands-on exploitation.
- Reverse engineer the program executable using the GDB debugger.
- Corrupt the stack, manipulate return addresses, and execute arbitrary code on the RPi.

Exploiting Hardware Vulnerabilities

- Develop exploit programs to leak secret flags.
- Use FPGA development boards for hands-on exploitation.
- Understand software-exploitable hardware vulnerabilities.
- Hack real-world RISC-V system-on-chip designs emulated on FPGAs.

Hardware PenTesting

- Build hardware fuzzers to verify hardware.
- Use FPGA development boards and RPi for security testing.
- Generate programs for security verification of processors to verify RISC-V processors.
- Analyze and capture the activity in FPGA-emulated processors to guide intelligent smart security testing.



Why Join?

- Gain hands-on experience with real-world attack and defense scenarios.
- Develop high-demand technical skills for careers in security, embedded systems, semiconductor, and EDA industries.
- Gain expertise in securing hardware systems against emerging cyber threats.

Location

- Wisenbaker Engineering Building 102, a state-of-the-art research facility dedicated to analyzing, exploiting, and mitigating hardware vulnerabilities.
- Open to academic, non-profit, national labs, and industry researchers.
- Secure and Trustworthy Hardware (SETH) Lab **seth.engr.tamu.edu**
- Department of Electrical and Computer Engineering **engineering.tamu.edu/electrical**

Prepare for a future in hardware security!

TEXAS A&M UNIVERSITY
Department of Electrical & Computer Engineering

Texas A&M Engineering Experiment Station

engineering.tamu.edu/electrical | **seth.engr.tamu.edu**