In Hardware We Trust?

ENRICHING THE WORLD with HARDWARE SECURITY RESEARCH

Jason M. Fung, Intel
Jeyavijayan (JV) Rajendran, Texas A&M University
Ahmad-Reza Sadeghi, TU Darmstadt

Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands might be claimed as the property of others. © Intel Corporation
Jason M. Fung
Director, Academia Research Engagement
Offensive Security Research
Intel Product Assurance and Security

Jeyavijayan (JV) Rajendran
Assistant Professor
Electrical & Computer Engineering Dept.
Texas A&M University

Ahmad-Reza Sadeghi
Professor
Computer Science Department
TU Darmstadt
We create world-changing technology that enriches the lives of every person on earth
Appreciate the Big Picture
Big Picture: The Hardware Security Challenges

Emerging threat landscapes

RV1 – Identify emerging threats on area X and characterize attack feasibility
RV2 – Research and propose architectural mitigations
RV3 – Identify methodology to detect associated vulnerabilities
Big Picture: The Hardware Security Challenges

Emerging threat landscapes

Increasing window of risk exposure

Over 160K vulnerabilities have been documented between 1999 to 2019

Over half were reported in the last 5 years

REFERENCE: Silicon as Code, the Cybersecurity Vulnerability Paradox, and the Transparency Requirements for a 21st Century Processor Vendor, Frank Dickson, IDC Signature White Paper
Big Picture: The Hardware Security Challenges

Emerging threat landscapes
Increasing window of risk exposure
Security requirements continue to evolve after product launch
Big Picture: The Hardware Security Challenges

- Emerging threat landscapes
- Increasing window of risk exposure
- Security requirements continue to evolve after product launch
- Disproportionate expectations on product security vs. functionality
Big Picture: The Hardware Security Challenges

- Emerging threat landscapes
- Increasing window of risk exposure
- Security requirements continue to evolve after product launch
- Disproportionate expectations on product security vs. functionality
- Robust In-field update infrastructure still uncommon
Dive Deep to the Fundamentals

Technology enriches people’s lives when it is secure

Hardware security is harder than it seems

Challenges take industry and academia working together to address

Where should we start?
Dive Deep: Common Hardware Weaknesses

- General Circuit & Logic Design Concerns
- Privilege Separation & Access Control
- Debug & Test
- Power, Clock & Reset
- Security Flow
- Security Primitives & Cryptography
- Manufacturing & Life Cycle Management
Deep Dive: How can Security Research Help?

SYSTEMIC MITIGATIONS
SECURITY-AWARE DESIGN AUTOMATION
DETECTION AUTOMATION
REMEDICATION AUTOMATION
Research Thrust: Systemic Mitigations

Robust building blocks and timely security intelligence for hardware designers

- Fault-resilient electronics and circuits
- Future-proof security primitives
- Robust in-field update capability
- Privacy-preserving telemetry
Research Thrust: Security-Aware Design Automation

How would a smart Electronic Design Automation framework supporting secure-by-construction look like?

Offer INSIGHTS ... not just DATA ... WHEN and WHERE needed
Research Thrust: Auto Detection & Remediation

What does it take for an Intelligent Assistant to work like a seasoned security researcher?

- Review & enumerate early concerns
- Verify in the most optimized & effective manner
- Recommend mitigation options
- Learn & address similar issues proactively
Collaborate Passionately & Genuinely

SHARE

MENTOR

INSPIRE
Collaborate: Hardware Common Weakness Enumeration (CWE)

REFERENCE: https://cwe.mitre.org/

Semiconductor Research Corporation (SRC) Industry Led e-Seminar, January 2021
Collaborate: Hardware CWE

CWE 4.0 released with HW CWE

CAPEC/CWE Advisory Board formed with 15 institutions as founding members

HW CWE Special Interest Group formed with 20+ institutions meeting monthly
Collaborate: Building a Diverse Community


Princeton-Intel Research Experience for Undergraduates (REU) Program

Princeton University’s Department of Electrical Engineering, in partnership with Intel, invites rising college juniors to apply to participate in a research experience program focused on computer security. We seek students interested in research (although experience is not required) and welcome applicants from all majors but with a preference for students majoring in computer/electrical engineering and computer science.

Students chosen for the program will spend the summer of 2021 at Princeton University conducting computer security research under the guidance and mentorship of a Princeton faculty member with active mentoring from researchers at Intel.

The program is especially interested in qualified candidates who can contribute to the diversity and excellence of our academic community and STEM fields as a whole. Women and other historically underrepresented groups in STEM disciplines are strongly encouraged to apply. Applicants must demonstrate an interest in STEM-related disciplines and curiosity about research.

DATES:
Apply: November 1, 2020-January 22, 2021.
Summer Research Experience for Undergraduates Program: June 2021-August 2021.

ELIGIBILITY:
U.S. citizens and permanent residents
Rising juniors in summer 2021 with good academic standing
All STEM majors welcome; Computer/Electrical Engineering and Computer Science majors preferred

Collaborate: HACK@HARD Hardware CTF

REFERENCE: https://hackathard.com/