Semiconductor Research Corporation

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

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

REMEDIATION 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

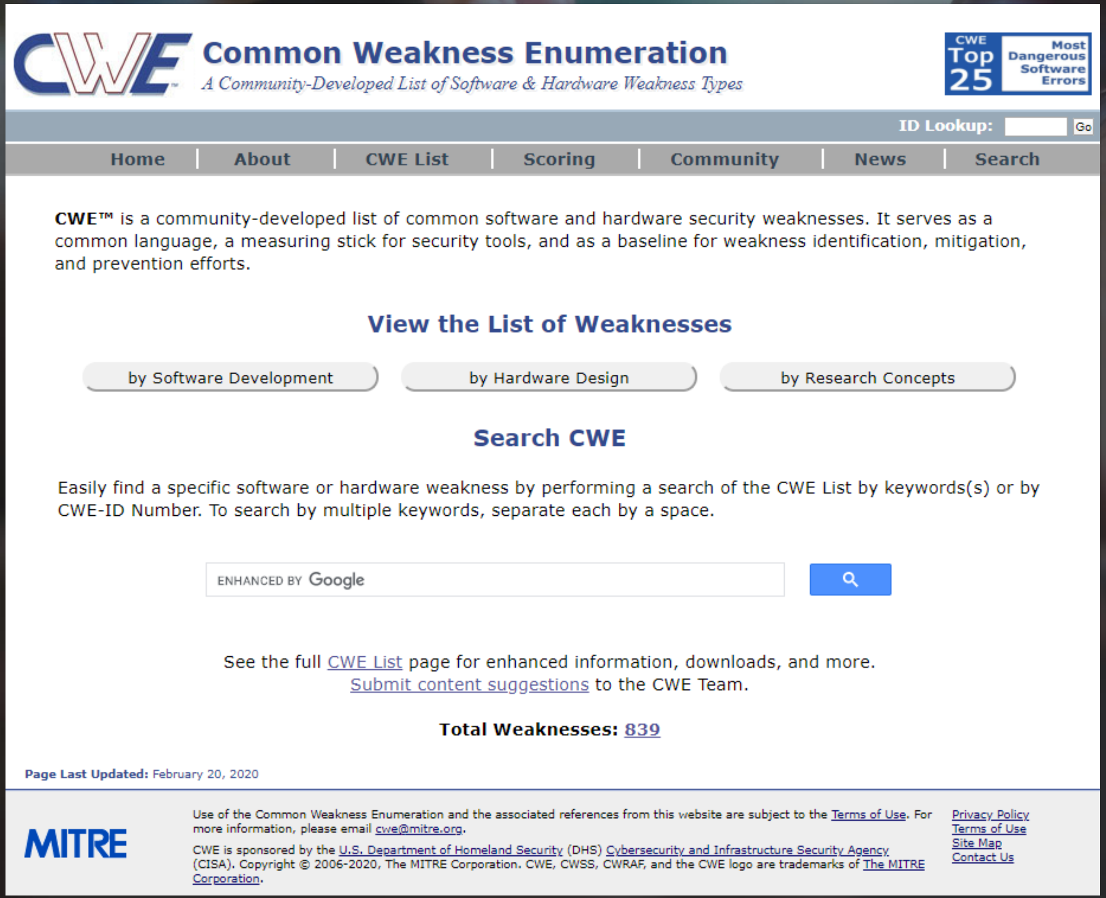
Collaborate Passionately & Genuinely

SHARE

MENTOR

INSPIRE

Collaborate: Hardware Common Weakness Enumeration (CWE)



CWE Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types

CWE Top 25 Most Dangerous Software Errors

ID Lookup: Go

Home | About | CWE List | Scoring | Community | News | Search

CWE™ is a community-developed list of common software and hardware security weaknesses. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

View the List of Weaknesses

by Software Development | by Hardware Design | by Research Concepts

Search CWE

Easily find a specific software or hardware weakness by performing a search of the CWE List by keywords(s) or by CWE-ID Number. To search by multiple keywords, separate each by a space.

ENHANCED BY Google

See the full CWE List page for enhanced information, downloads, and more.
Submit content suggestions to the CWE Team.

Total Weaknesses: 839

Page Last Updated: February 20, 2020

MITRE

Use of the Common Weakness Enumeration and the associated references from this website are subject to the Terms of Use. For more information, please email cwe@mitre.org.

CWE is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 2006-2020, The MITRE Corporation. CWE, CWSS, CWRAF, and the CWE logo are trademarks of The MITRE Corporation.

Privacy Policy
Terms of Use
Site Map
Contact Us

1194 - Hardware Design

- Manufacturing and Life Cycle Management Concerns - *(1195)*
  - Semiconductor Defects in Hardware Logic with Security-Sensitive Implications - *(1248)*
  - Improper Scrubbing of Sensitive Data from Decommissioned Device - *(1266)*
  - Product Released in Non-Release Configuration - *(1269)*
  - Device Unlock Credential Sharing - *(1273)*
  - Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques - *(1278)*
  - Unprotected Confidential Information on Device is Accessible by OSAT Vendors - *(1297)*
- Security Flow Issues - *(1196)*
  - DMA Device Enabled Too Early in Boot Phase - *(1190)*
  - Power-On of Untrusted Execution Core Before Enabling Fabric Access Control - *(1193)*
  - Hardware Logic with Insecure De-Synchronization between Control and Data Channels - *(1264)*
  - Insufficient Protections on the Volatile Memory Containing Boot Code - *(1274)*
  - Mutable Attestation or Measurement Reporting Data - *(1283)*
  - Missing Ability to Patch ROM Code - *(1310)*
  - Missing Immutable Root of Trust in Hardware - *(1326)*
  - Security Version Number Mutable to Older Versions - *(1328)*
- Integration Issues - *(1197)*
  - Hardware Child Block Incorrectly Connected to Parent System - *(1276)*
- Privilege Separation and Access Control Issues - *(1198)*
  - Incorrect Default Permissions - *(276)*
  - Unintended Proxy or Intermediary ('Confused Deputy') - *(441)*
  - Improper Isolation of Shared Resources on System-on-a-Chip (SoC) - *(1189)*
  - System-on-Chip (SoC) Using Components without Unique, Immutable Identifiers - *(1192)*
  - Insufficient Granularity of Access Control - *(1220)*
  - Inclusion of Undocumented Features or Chicken Bits - *(1242)*
  - Improper Handling of Overlap Between Protected Memory Ranges - *(1260)*
  - Register Interface Allows Software Access to Sensitive Data or Security Settings - *(1262)*
  - Policy Uses Obsolete Encoding - *(1267)*
  - Policy Privileges are not Assigned Consistently Between Control and Data Agents - *(1268)*
  - Access Control Check Implemented After Asset is Accessed - *(1280)*
  - Insecure Security Identifier Mechanism - *(1294)*
    - Improper Restriction of Security Token Assignment - *(1259)*
    - Generation of Incorrect Security Tokens - *(1270)*
    - Incorrect Decoding of Security Identifiers - *(1290)*
    - Incorrect Conversion of Security Identifiers - *(1292)*
  - Missing Protection Mechanism for Alternate Hardware Interface - *(1299)*
  - Missing Security Identifier - *(1302)*
  - Non-Transparent Sharing of Microarchitectural Resources - *(1303)*
  - Missing Write Protection for Parametric Data Values - *(1314)*
  - Missing Support for Security Features in On-chip Fabrics or Buses - *(1318)*
  - Unauthorized Error Injection Can Degrade Hardware Redundancy - *(1334)*
- General Circuit and Logic Design Concerns - *(1199)*
  - Failure to Disable Reserved Bits - *(1209)*
  - Incorrect Register Defaults or Module Parameters - *(1221)*

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

Collaborate: Hardware CWE

FEB'20 — **CWE 4.0** released with HW CWE

AUG'20 — **CAPEC/CWE Advisory Board** formed with 15 institutions as founding members

OCT'20 — **HW CWE Special Interest Group** formed with 20+ institutions meeting monthly

Collaborate: Building a Diverse Community

REFERENCE: http://bit.ly/Princeton-IntelREU

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

Decisions by:
January 31, 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

Application Link: http://bit.ly/Princeton-IntelREU

PRINCETON
School of Engineering and Applied Science

Collaborate: HACK@HARD Hardware CTF

DESIGN AUTOMATION CONFERENCE
FROM CHIPS TO SYSTEMS – LEARN TODAY, CREATE TOMORROW

29TH USENIX SECURITY SYMPOSIUM

TECHNISCHE UNIVERSITÄT DARMSTADT

intel

TEXAS A&M UNIVERSITY

REFERENCE: https://hackathard.com/