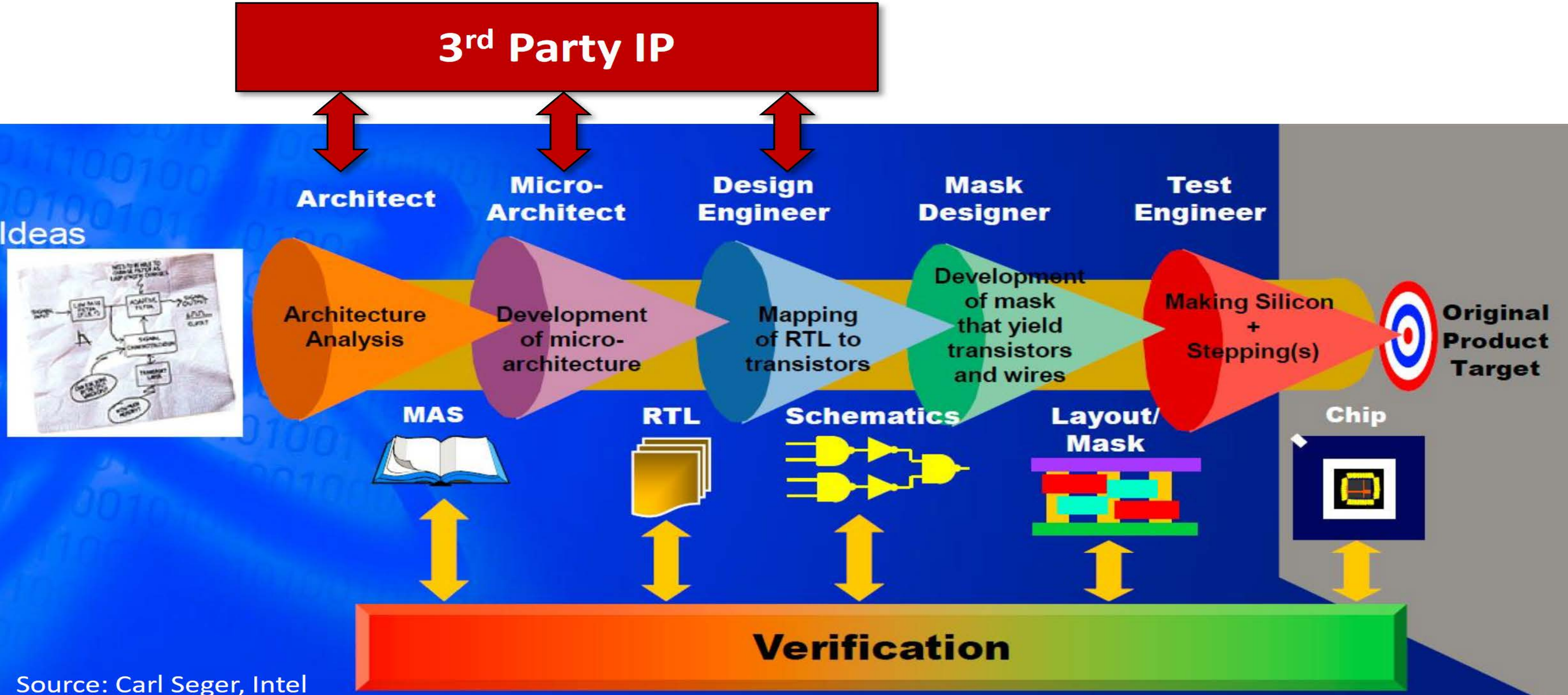
Robert A. Martin
Sr. Secure Software & Technology Prin. Eng.
Trust & Assurance Cyber Technologies Dept.
Cyber Solutions Technical Center

Hardware Assurance and Weakness Collaboration and Sharing (HAWCS)

Trusted and Assured Microelectronics (TAME) Forum
18 Sep, 2019 SSCA Forum

Semiconductor Design & Manufacture



Source: Carl Seger, Intel

Trusted and Assured MicroElectronics (TAME) Forum

TAME Forum’s objective is to provide a bi-annual platform to researchers in academia, and practitioners in industry and government to discuss innovative solutions in the domain of trusted microelectronics in today’s globalized and complex supply chain, discuss grand challenges and identify collaboration opportunities.

TAME Hardware Assured and Weakness Collaboration and Sharing (HAWCS) Forum

TAME Forum Founder: Mark Tehranipoor (University of Florida)

Lead:	Jeremy Bellay (Battelle)
Co-Lead:	Domenic Forte (University of Florida)
Advisor:	Bob Martin (MITRE)
Adviser:	Jon Boyens (NIST)

Members:

Mike Borza, Synopsys
Ron Perez, Intel
Yatin Hoskote, ARM
Sandip Ray, University of Florida
Ioannis Savidis, Drexel University
Fareena Saqib, UNC Charlotte
Jon Graf, Graf Research
Lisa McIlrath, University of Florida
Mark Temmen, US Army
Khalil Maloof, ECI

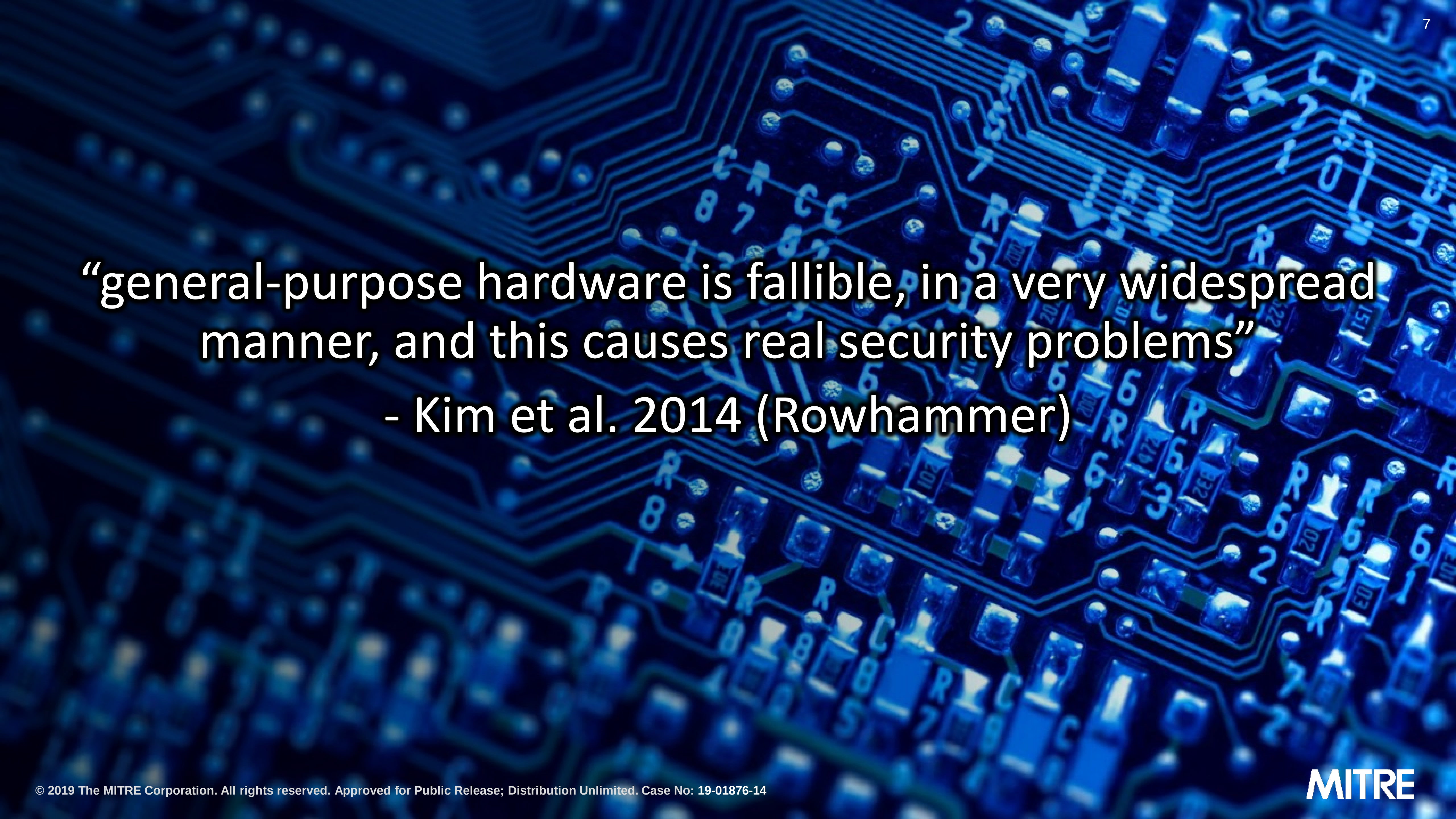
MITRE

HAWCS Working Group Activity

- TAME HAWCS Working Group has met bi-yearly since 2017.
- The final meeting will be December 10, 2019 at the Florida Institute of Cyber Security, University of Florida
- We have weekly meetings where various topics have been discussed:
  - Hardware/software Vulnerability Context/History
  - Hardware Vulnerability Ontologies
  - Hardware Vulnerability Sharing – Risks and Benefits
  - Hardware Vulnerability Scoring
  - Responsible Disclosure
  - Hardware Vulnerability Gaps
- Email the HAWCS Lead <bellayj@battelle.org> to be included in the working group and get access to previous meeting recordings

Overview

- Hardware vulnerability examples – how do hardware vulnerabilities differ from software?
- What descriptive structures are out there?
- What do we want from an ontology?
- What are the current gaps?
- How does scoring differ between software and hardware?
- How about disclosure processes / vulnerability databases?
- What are the future directions for Hardware vulnerability, assurance, and weakness sharing?



“general-purpose hardware is fallible, in a very widespread manner, and this causes real security problems”

- Kim et al. 2014 (Rowhammer)

Types of Hardware Vulnerabilities (i.e., Weaknesses)

- Glitching/Fault Attack (E.g. optical fault injection, 1966)
- Side-Channel Analysis (E.g. Differential Power Analysis,1996)
- Rowhammer (2014)
- Spectre/Meltdown (2017)
- Spoiler (Rowhammer + Spectre, 2018)

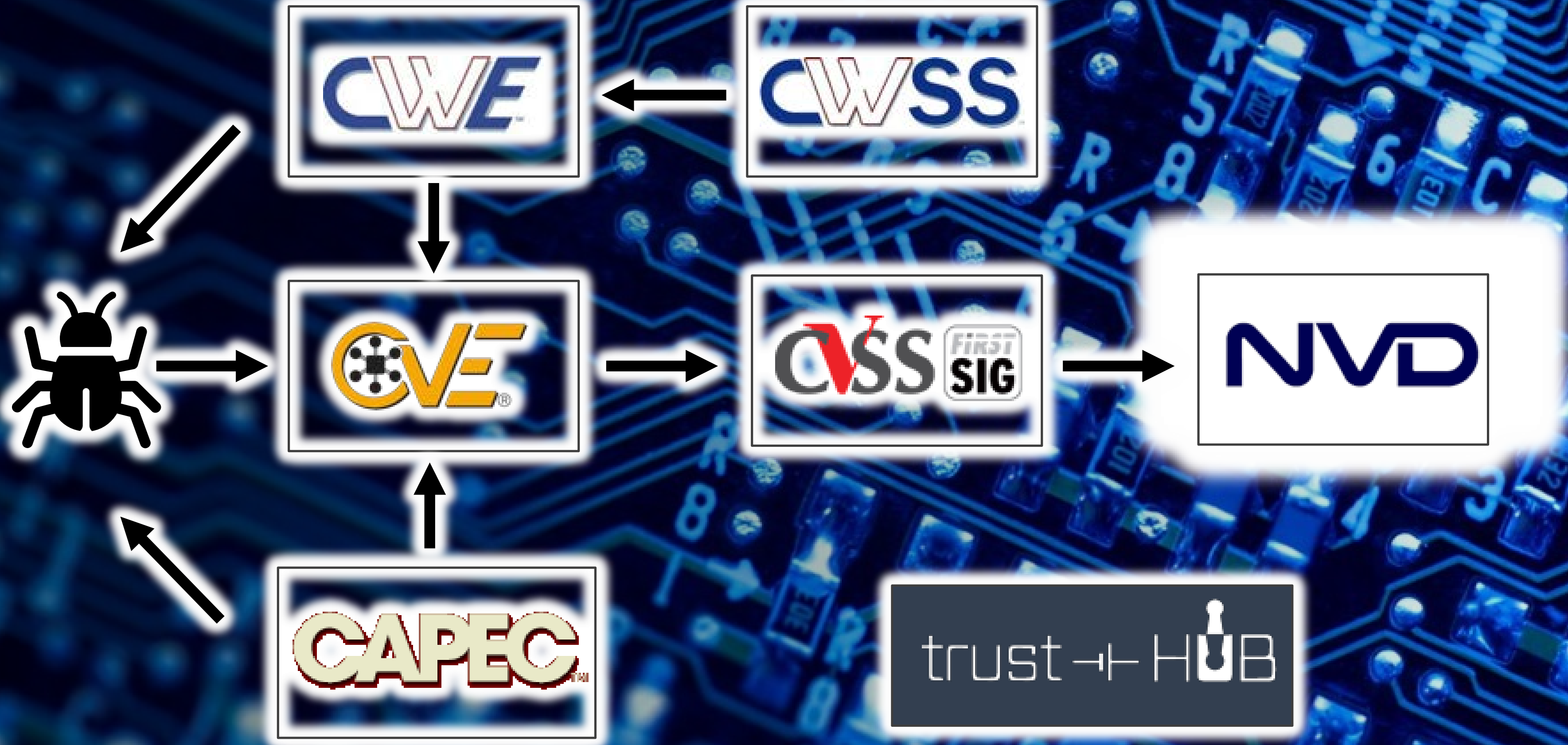
Hardware and Software have Shared but Sometimes Qualitatively Different Security Issues

- Reverse Engineering
- Counterfeits
- Third Party IP Integration and verification
- Complex
- System integration with little visibility in components

Current Security Description Frameworks

- CVE (Common Vulnerabilities and Exposures) - A naming space for identified vulnerabilities
- CWE (Common Weakness Enumeration) - A set of concepts and relations that describe the weaknesses that underly vulnerabilities
- CVSS (Common Vulnerability Scoring System) - A system for scoring the potential impact of a discovered vulnerability
- CWSS (Common Weakness Scoring System) - A system for scoring abstract weakness, primarily for the purpose of security planning
- CAPEC (Common Attack Pattern Enumeration and Classification) - A description framework for attack patterns
- Trust-Hub - Contains taxonomies for hardware vulnerability weaknesses and the other for trojan description as well as examples

Vulnerability and Weakness Monitoring Description Resources



Example: Xilinx SOC Zynq UltraScale+

- UltraScale+ Encrypt Only secure boot mode does not encrypt boot image metadata
- Disclosed 8/12/2019 (Xilinx issue 72588)
- Requires a ROM revision and is unpatchable
- Attackers can only exploit security flaw with physical access to a device, in order to perform a DPA (Differential Power Analysis) attack on the SoCs boot up sequence

How could this be reported using the current infrastructure?

CVE - CVE assigned by discoverer three weeks after disclosure

CVSS - Base score reported (5.5)

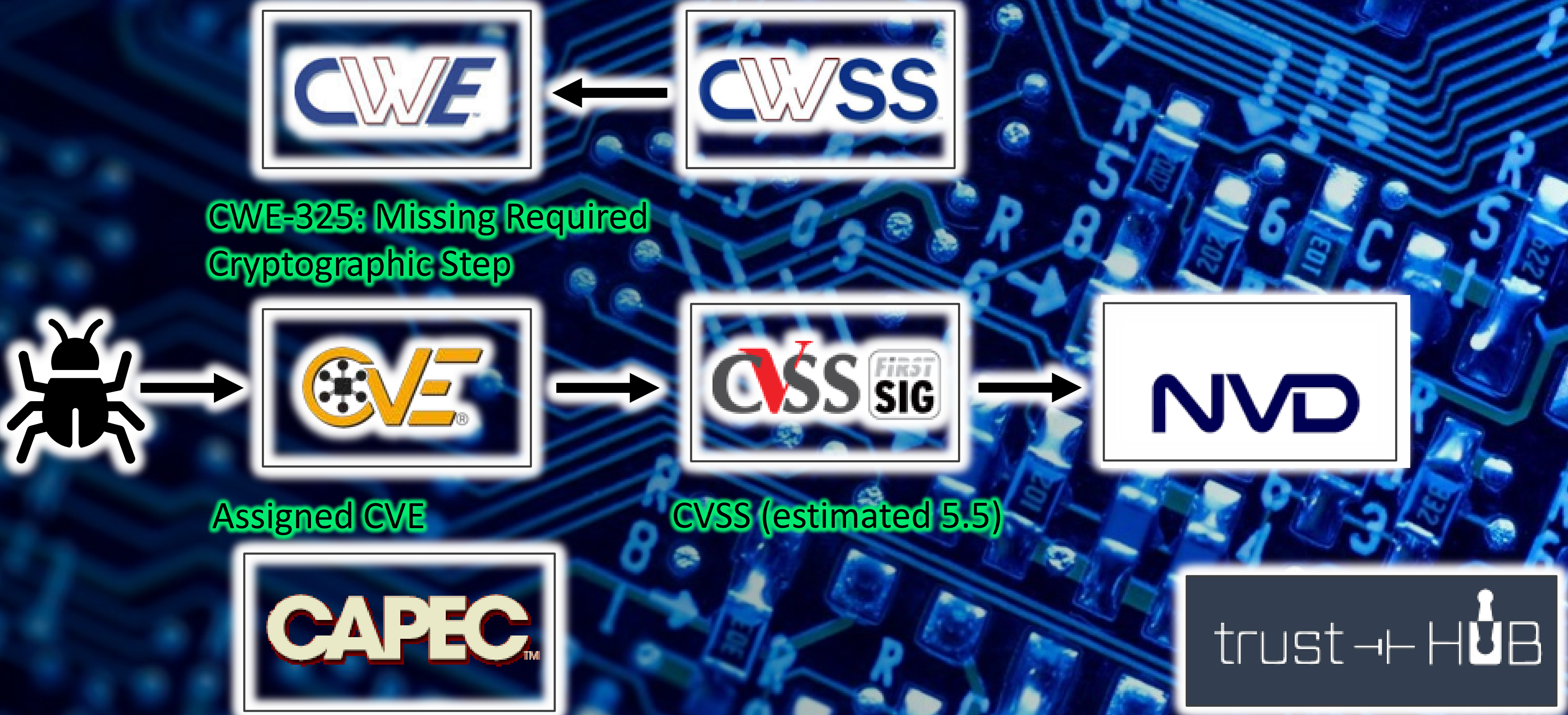
CWE - CWE-325: Missing Required Cryptographic Step

CAPEC - CAPEC-242: Code Injection

CAPEC - CAPEC-622: Electromagnetic Side-Channel Attack (?)

Trust-Hub.org - Current and power measurement node in taxonomy

Vulnerability and Weakness Monitoring Description Resources



CWE-325: Missing Required Cryptographic Step

Assigned CVE

CVSS (estimated 5.5)

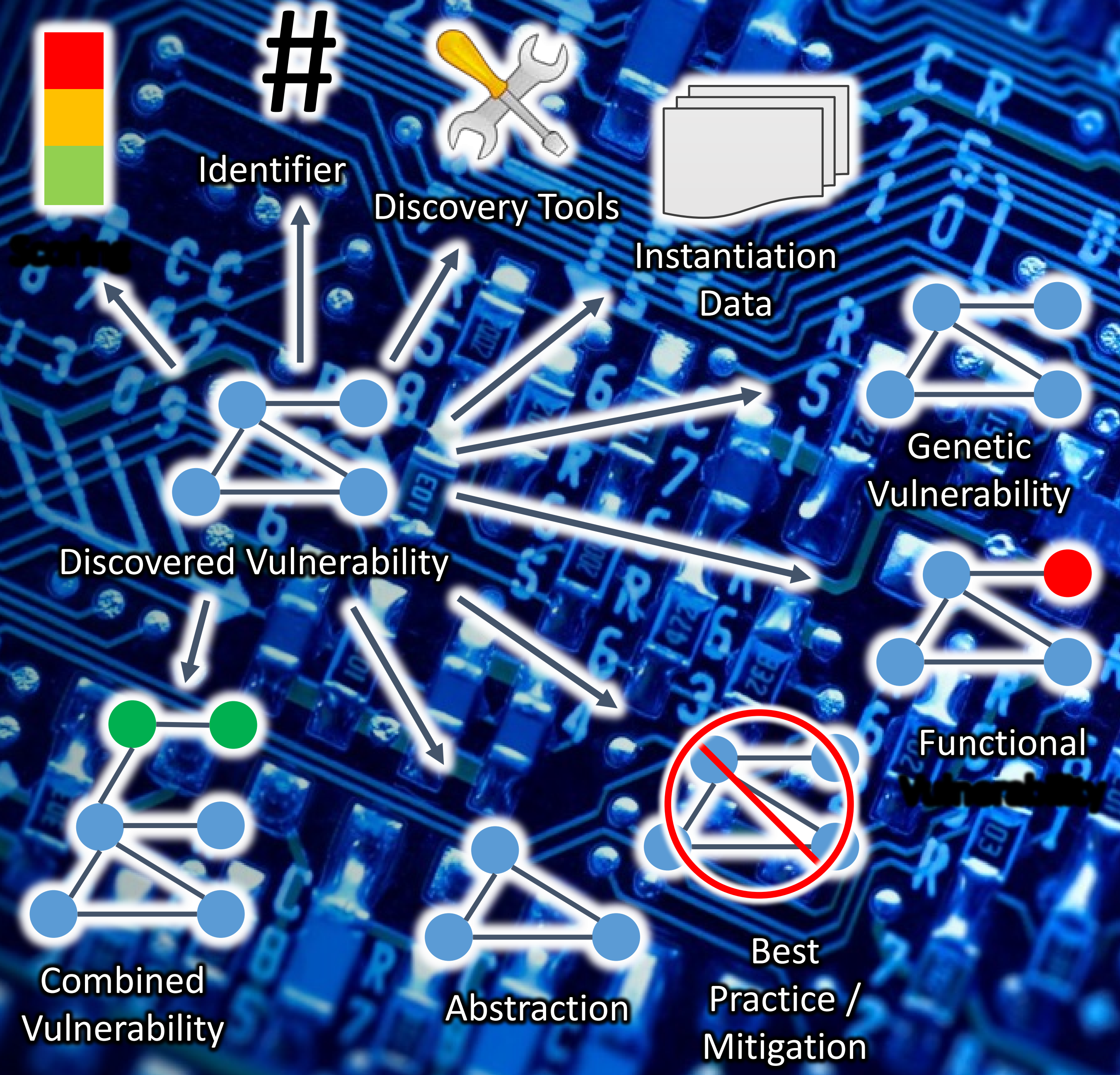
Electromagnetic Side-Channel Attack (?)

Code Injection

Current and power measurement

What do we want from vulnerability/weakness description?

- Can we uniquely identify it?
- Can we describe it and abstract it?
- Where can it be found?
- How could it be accessed?
- What's its impact?
- How can it combine with other vulnerabilities?
- What does it look like functionally?
- How can it be mitigated?
- How can it be prevented?



Current description framework regarding hardware

- CVE appears adequate for vulnerability identification
- CAPEC contains some hardware related attacks and security issues
  - e.g. lacks side-channel
- CWE currently lacks most hardware specific concepts (e.g. SPECTRE)
- Trust-Hub has more a more detailed attack taxonomy but is not integrated with the CVE/CWE environment
- Trust-Hub also has relatively extensive examples of trojans and some vulnerabilities
- CVSS has a hard time scoring non-exploit weaknesses (e.g. reverse engineering)

Do we need something else for hardware?

- Expansion of CVE ecosystem and merging Trust-Hub would expand the concept set substantially
- None of the current description frameworks supports the hardware specific concepts and relations necessary for:
  - Best practices for weakness avoidance
  - Testing regimes for post-design detection
- These are being addressed within manufactures. But (semi) public standards would allow for higher quality products:
  - Across the manufacturers (IOT)
  - Integrated and propagated within a supply chain

How do we score hardware vulnerabilities differently?

- Mitigation – Fundamentally it is assumed that software can be patched, this might not be the case in hardware and mitigations are often only partial
- Effort – Many of the the hardware attack surfaces are necessarily available to an attacker (e.g. power analysis). However the effort required to use such a technique may be prohibitive. Thus quantitative effort estimation is essential.
- Patchability – Vulnerable hardware (especially in physical systems) may be difficult to access to apply a mitigation
- Hardware has an overlapping but different set of threats from software (e.g. remote exploitation, reverse engineering, counterfeiting). These are industry specific and must be addressed to be able to score a vulnerability
- Hardware systems are comprised of deep layered systems most of which is inscrutable to any one party.

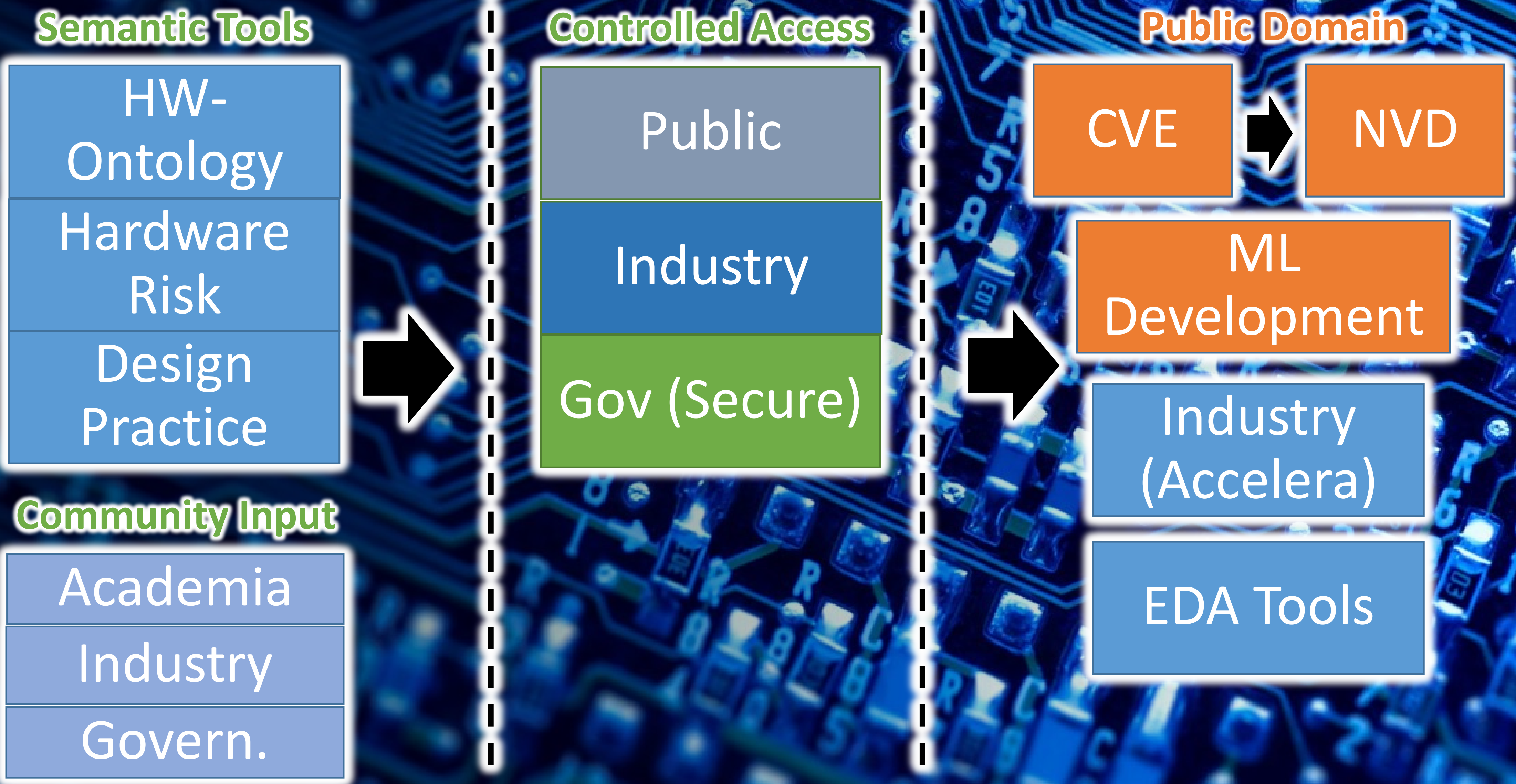
Vulnerability Disclosure

- Hardware vulnerability disclosure has been contentious due the unpatchability of many hardware vulnerabilities.
- Additionally, mitigation can be more complex because the inclusion of Original Equipment Manufacturers (OEMs) in addition to actual hardware vendor and relevant software distributors.
- IOT devices present several challenges for disclosure and mitigation
  - They are often inaccessible
  - Operate in non-standard environments
  - Small value/size may make sophisticated security feature undesirable
  - Only 10% of IOT vendors have a disclosure policy

Public Databases of Hardware Vulnerabilities

- Extending description frameworks to include hardware vulnerabilities will benefit researchers including
  - Open source community
  - Companies and industrial organizations
  - Government researchers in siloed or classified environments
- Extending the description framework will allow for a more integrated approach to the public sharing and characterization of vulnerability

Possible Ecosystem



Semantic Tools

HW-Ontology

Hardware Risk

Design Practice

Community Input

Academia

Industry

Govern.

Controlled Access

Public

Industry

Gov (Secure)

Public Domain

CVE

NVD

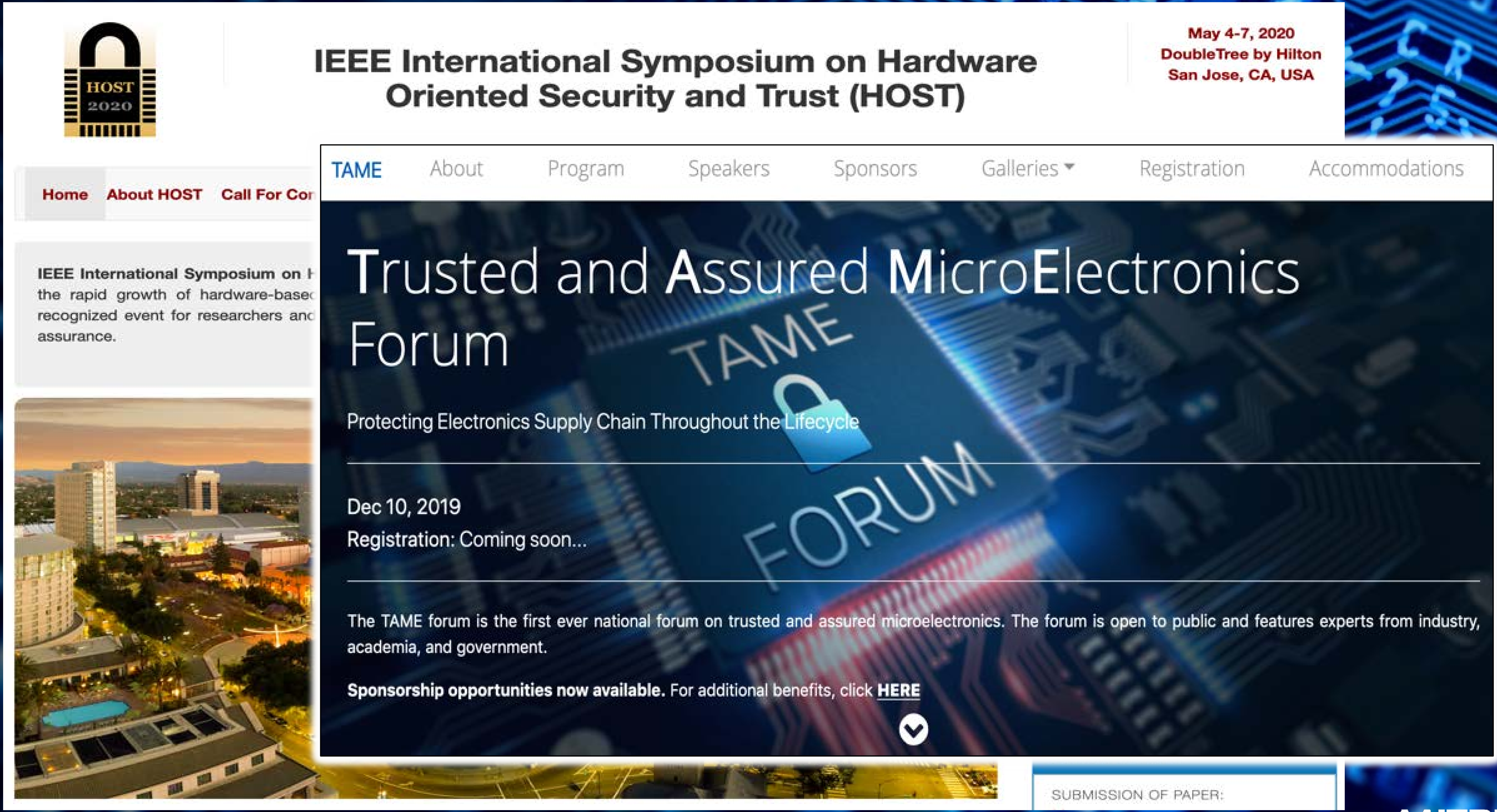
ML Development

Industry (Accelera)

EDA Tools

Resources for Hardware Vulnerability Sharing

- Accellera - A non-profit that includes (among others) designers, manufactures, and EDA tool vendors. They have an established working group for the development of shared database/ontology for the purpose of verifying 3rd part IP.
- TrustHub – A project out the University of Florida to provide a taxonomic structure for vulnerabilities and trojans, as well as example test benches.



IEEE International Symposium on Hardware Oriented Security and Trust (HOST)

May 4-7, 2020
DoubleTree by Hilton
San Jose, CA, USA

IEEE International Symposium on H
the rapid growth of hardware-based
recognized event for researchers and
assurance.

SUBMISSION OF PAPER:

Trusted and Assured MicroElectronics Forum

Protecting Electronics Supply Chain Throughout the Lifecycle

Dec 10, 2019
Registration: Coming soon...

The TAME forum is the first ever national forum on trusted and assured microelectronics. The forum is open to public and features experts from industry, academia, and government.

Sponsorship opportunities now available. For additional benefits, click **HERE**

MITRE