NIST CHIPS Metrology R&D Program: Pre-Workshop Data Collection and Mapping Exercise

The goal of this exercise is to align NIST CHIPS Metrology R&D project briefs to the program's 10 priority Focus Areas. In addition, this exercise provides an opportunity for technical leads to describe how additional resources (budget for federal staff, associates, external contracts, and equipment) might enable these projects to more effectively support CHIPS Act mandates.

Response data will be used as an input for an internal NIST CHIPS Metrology R&D program workshop scheduled for March 2023 to support future project planning activities. Respondents will be invited to this workshop to discuss their project briefs with other NIST researchers working in similar fields.

This exercise is divided into multiple sections. Submitting a response will automatically advance users to the next appropriate section:

- **Project Background & Mapping:** In this section, you will align your project to the NIST CHIPS Metrology R&D Program's 10 priority Focus Areas.
- **Current State Baseline (for current projects only):** In this section, you will describe how your project would support CHIPS Act mandates as currently planned and funded.
- **Additional CHIPS Resources (for current projects only):** In this section, you will identify how your project could more effectively support CHIPS Act mandates with additional funding and resources.
- **New Project Proposals (for new project proposals only):** In this section, you will estimate resource requirements for your new project proposal and describe how it could support CHIPS Act mandates.

Technical leads should submit one (1) response per project. Please submit response(s) by COB February 24, 2023.

NIST staff may direct questions regarding the March 2023 Metrology R&D Program workshop to Rachel Pollitt (rpollitt@corneralliance.com), Sarah Jasper (sjasper@corneralliance.com), or Marc Leh (mleh@corneralliance.com).

Email address is required.

Email Address
irena.bojanova@nist.gov

Name
Irena Bojanova

Please Select Your OU

☐610 NCNR

☐630 MML

☐670 CTL

☐680 PML

☐730 EL

☒770 ITL

Please Select Your Division

☐610 NCNR

☐640 Office of Reference Materials

☐641 Office of Data and Informatics

☐642 Materials Science and Engineering Division

☐643 Materials Measurement Science Division

☐644 Biosystems and Biomaterials Division

☐645 Biomolecular Measurement Division

☐646 Chemical Sciences Division

☐647 Applied Chemicals and Materials Division

☐671 Public Safety Communications Research Division

☐672 RF Technology Division

☐673 Wireless Networks Division

☐674 Smart Connected Systems Division

☐675 Spectrum Technology and Research Division

☐681 Microsystems and Nanotechnology Division

☐682 Radiation Physics Division

☐683 Nanoscale Device Characterization Division

☐684 Quantum Measurement Division

☐685 Sensor Science Division

☐686 Applied Physics Division

☐687 Quantum Electromagnetics Division

☐688 Time and Frequency Division

☐689 Quantum Physics Division

☐731 Materials and Structural Systems Division

☐732 Building Energy and Environment Division

☐733 Fire Research Division

☐734 Systems Integration Division

☐735 Intelligent Systems Division

☐771 Applied and Computational Mathematics Division

☐773 Computer Security Division

☐774 Information Access Division

☒775 Software and Systems Division

☐776 Statistical Engineering Division

☐777 Applied Cybersecurity Division

☐N/A

Project Title

Ontology of Firmware Bugs and Weaknesses &
Repository of Formally Described Firmware Security Vulnerabilities

Project Status

☒New Project

Cluster 1 (Automation, Virtualization, and Security) Focus Area Mapping

Please select the priority Focus Area(s) that align with your project. Select all that apply. For the definitions of the 10 priority Focus Areas, please review the document attached in the email containing the link to this data collection and mapping exercise.

☐Advanced Metrology for Supply Chain Trust and Assurance

☒Verification and Validation of Advanced Models

☐Advanced Modeling for Next-Generation Manufacturing Processes

☒Standards for Automation, Virtualization, and Security

☐Interoperability Standards for Equipment and Software

Cluster 2 (Metrology for Next Generation Microelectronics) Focus Area Mapping

Please select the priority Focus Area(s) that align with your project. Select all that apply. For the definitions of the 10 priority Focus Areas, please review the document attached in the email containing the link to this data collection and mapping exercise.

☐Metrology for Advanced Materials and Devices

☐Metrology for Nanostructured Materials Characterization

☐Advanced Measurement Services

☐Advanced Metrology for 3D Structures and Devices

☐Materials Characterization Metrology for Advanced Packaging

Section 2: New Project Proposals

Please answer the following questions based on your <u>new</u> proposed project's estimated resource requirements.

Estimated Resources Required

Describe the estimated resources required for your new project proposal. Please quantify the estimated resources required, to the best of your ability, across the following categories:

- **Federal Staff**
- **Associates**
- **Other Objects (budget for federal staff, associates, external contracts, and equipment)**
- **TOTAL Budget**

TOTAL Budget: $3.5M

$700K/year for 5 years

- Federal Staff: one senior computer scientist, PhD – $300K
- Associates: two computer scientists/physicists/electrical engineers, PhDs – $120K
- Other Objects: one contractor (PhD), conferences, travel – $280K

Estimated Timeline

Provide the estimated start and end dates for your new project proposal **(mm/yy - mm/yy).** Please provide your best effort to determine the timeline for the proposed project or key project outputs.

10/01/2023-09/31/2028

Measurement Need

What is the measurement need associated with this new project proposal?

Chips' die area dedicated to firmware is becoming increasingly significant, both for chips and systems on chip (SoC). The firmware comprises sets of computer instructions (code) that provide the low-level control for a device hardware. Common reasons for updating firmware include not only adding features, but also increasingly – fixing bugs (code defects and code specification defects). Such defects in firmware may lead to security vulnerabilities and failures that are commonly used to attack cyberspace and the critical infrastructure. The first essential step towards preventing such attacks, logically, is to first secure the chips and SoCs firmware – identify bugs and weaknesses, detect vulnerabilities and develop defenses against new exploits. However, the mainstream efforts so far have been primarily on securing the high-level OSs software, which is becoming a huge problem. For example, a wrong data type could cause a casting or calculation error, resulting in a value that is inconsistent with the size of a buffer, leading to a pointer repositioning overbound, which would allow reads of data that should not be read – aka buffer overflow. A chip single event upset (SEU), such as silent data corruption

(SDC), could also result in a wrong value, causing a chain of firmware weaknesses that underlie a security vulnerability.

The creation of modern firmware security tools needs structured taxonomies of firmware bugs/weaknesses and detailed, unambiguous descriptions of observed vulnerabilities initiated by chip firmware weaknesses. The focus is on both code and specification defects. The resulting errors from such defects may propagate through firmware security faults, including in embedded systems, and possibly resurface and propagate through security faults in high-level OSs, leading to severe final errors and security failures. The repository of formally described firmware security vulnerabilities will allow in-depth understanding and formal analysis of the weaknesses underlying firmware vulnerabilities to improve bug fixing and mitigation at chip provisioning (testing and validation) and integration into OEM products, and during post deployment maintenance.

NIST Approach/Solution

What are the anticipated major milestones for this new project proposal?

We will create a formal classification system of firmware security bugs and weaknesses and a dataset of formally described firmware security vulnerabilities. For that, we use the NIST Bugs Framework (BF) approach and methodology and will create tools for automated document curation and vulnerability descriptions generation.

To find and fix bugs that trigger security vulnerabilities or to be able to reason over mitigation techniques, we need to first clearly understand all the chained underlying weaknesses that lead to an observed security failure. BF's approach and methodology assures this and allows the creation of appropriate tools (including use of AI based methods) would also allow the creation of a dataset of vulnerabilities descriptions for use in AI/ML research. The BF's structured formal approach of specifying security vulnerabilities is key to the integration of this work into the chip's highly structured and formal design process.

Stage I: We will first create firmware bugs taxonomies. In more details, we will:

- Analyze firmware bugs, weaknesses, and vulnerabilities related repositories and literature.
- Perform brainstorming sessions to create firmware bug models.
- Perform brainstorming sessions to create taxonomies, formal language, and ontology for firmware bugs/weaknesses/vulnerabilities.
- Create a public searchable online repository (and API) with firmware bugs/weaknesses taxonomies.

Stage II: We will then create AI-related tools for retrieving bugs, weaknesses, and vulnerability related terms and structured information from all over the Internet. These tasks are impossible to do manually. Their automation would be achievable only via the developed in Stage I firmware taxonomies and ontology. In more details, we will:

- Create tools for mapping identified entries to operations and other entities of our ontology.
- Create/use a tool to generate a Gazetteer for our firmware taxonomies.
- Create a tool to generate lists of easy to describe firmware vulnerabilities with the taxonomies based on multiple techniques including mining of unstructured information and possibly the actual buggy code.
- Create a tool for generation of matrices of all meaningful cause-consequence (fault-operation-error) transitions for our taxonomies. The eventual combined matrix would comprise the transition paths of all theoretically possible security vulnerabilities allowing awareness about future vulnerabilities, as well as backtracking from an observable security failure to its possible root cause bugs that need to be fixed.
- Create a tool for generation of formal firmware vulnerability descriptions.
- Generate and curate formal firmware vulnerability descriptions for use in AI and ML.
- Create a public searchable online repository (and API) with formal vulnerability descriptions.

Deliverables and Impact

What are the expected deliverables and impact for this new project proposal?

- Data and operations flow models for identified phases of execution in which chips-related security bugs and weaknesses happen.
- Structured, complete, orthogonal classification system (and its taxonomies) that is also language and technology independent.
- A formal language for clearly describing chips-related vulnerabilities, triggered by firmware code or specification defects. Such a vulnerability description will be a "defect – error/fault–…–error/fault–final error" chain, leading to a security failure.
- A formal LL1 grammar in BNF form and an ontology corresponding to the taxonomies and the BF vulnerability model.
- Several database tools supporting the previously listed deliverables.
- A dataset of labeled vulnerabilities descriptions for use by firmware security tools and other AI-based projects related to chips security vulnerabilities and failures.
- Several AI-based tools supporting the creation of the dataset.

Security vulnerabilities lead to failures that are commonly used to attack cyberspace and the critical infrastructure. Securing the embedded systems firmware is the first essential step towards preventing such attacks.

The formal classification system of firmware security bugs and weaknesses and the database of formally described firmware security vulnerabilities will benefit wide areas of government, industry, and academia projects related to security vulnerabilities. The developed taxonomies, formal language, and ontology will help improve the firmware testing tools and their bug

reports, and facilitate the implementation of automatic bugs finding and fixing. The taxonomies will enable detailed, unambiguous reporting from firmware code analyzers. The large datasets of correct, meaningful formally described known vulnerabilities will enable the creation/training of ML and AI models for bug finding and vulnerability detection in chip firmware. Clear descriptions of firmware-initiated security vulnerabilities will help also improve and extend the public vulnerability repositories). Finally, the created bug models and vulnerabilities dataset would allow academics to teach better about firmware bugs and weaknesses and conduct formal research about vulnerabilities and security failures initiated from chips and SoCs.

New Industry or OA Collaborations

Describe collaboration opportunities you expect for this new project proposal.

We expect strong involvement from INMETRO (Brazil's NMI), University of Missouri, Carnegie Mellon, RIT, and JHU APL. We will participate at planned workshops related to the CHIPS initiative and as the project work progresses, we will extend our collaborations with other industry, government, and academia entities appropriately.

The Primary Investigator (PI) is the NIST security researcher, who created the Bugs Framework (BF) approach and methodology. She collaborated with the DARPA SSITH (System Security Integration Through Hardware) team on identifying firmware security weaknesses related to their hardware vulnerability classes, and currently collaborates with the NIST NVD and Vuntology teams, and the CISA KEV team.

added from the online form:
New NIST Collaborations

Indicate how this project could collaborate with other NIST entities or staff. Please list the name and division of each team member, if applicable.

The development of this project would benefit from collaboration with:
- the CSD Vuntology team, lead by David Waltermire
- the CSD NVD team, lead by Tanya Brewer
- the ACD Chips team, lead by Nelson Hastings