# INTEL REQUEST FOR PROPOSALS (RFP)

## SUBJECT

Targeted academic research on computer and communications security. This includes specific security research questions and the corresponding validation and prototyping with Intel technologies.

We call for proposals of targeted research projects (max US$100K per year for up to three years). The funds can be distributed among up to two principal investigators and teams, usually at a single organization.

## KEY DATES

**Proposal Submission deadline (PIs): August 14, 2017 at Midnight PST**

## OVERVIEW

Intel's Corporate Research Council (CRC) invites proposals from academic researchers to innovate and develop new capabilities in the area of secure computing. Intel expects the research results will impact the development of edge and cloud architectures for diverse application domains by the year 2022. A key goal is to dramatically increase the security and privacy of Intel systems, procedures, and services.

We call for proposals that target one of the following research vectors:

- **RV1: FPGA Security**
- **RV2: Resilience against Side Channels**
- **RV3: Machine Learning and Threat Detection**
- **RV4: Adversarial Machine Learning**
- **RV5: Machine Learning for Product Security Verification**

Below is an expansion on each of these research vectors to provide an illustration of the type of problem and areas of investigation that are of interest.

# RESEARCH VECTORS IN DETAIL

## RV1: FPGA SECURITY

### BACKGROUND

To date, FPGA security has been primarily focused on IP protection, i.e., ensuring that user designs (bitstreams) are secure from compromise when deployed into hostile environments across end markets ranging from communications through consumer to industrial and military. Most visibly, vendors have responded with bitstream encryption and authentication capabilities combined with fault-tolerance techniques to secure designs in field. An assumption underlying previous FPGA security efforts is that the implemented design originates from a single entity. Emerging trends point towards usage models where multiple, mutually distrusting, entities co-exist on a single FPGA. For example, an FPGA in an automotive setting may host applications from multiple stakeholders or an FPGA deployed in a cloud setting may have its resources exposed to multiple cloud users or tenants. In such multi-tenant usages, tenants and the platform owner may be mutually distrusting, bringing new security threats into scope.

### RESEARCH QUESTION

Proposals on RV1 can address issues from, but not limited to, the following list:

- What are the security threats deriving from the multi-tenant usage model? What are the mitigations?
- Intersection of safety and security. Fail-safe strategies in the presence of a malicious adversary.
- Secure multi-tenant resource sharing. How can FPGA resources, e.g. host and network interfaces be securely shared?
- Secure multi-tenant bitstream re-location. Can we achieve efficient relocation at the bitstream level in a secure manner?
- Security-aware FPGA design methodologies, flows and toolchains. Validation tools to detect malicious configurations.

## RV2: RESILIENCE AGAINST SIDE CHANNELS

### BACKGROUND

Side-channel attack (SCA) is one of the non/semi-invasive methods to break the security of a computing system by exploiting the information leaked from the physical devices. With cloud usage, emerging Trusted Execution Environments (TEE) like SGX and exposed edge-devices in IoT, side-channels have re-emerged as a prominent attack vector, exploiting both software as well as hardware signals and potentially fusing different side-channels in a single attack. While there is a

long history of attacks and mitigation targeted at implementations of particular crypto algorithms, there are still numerous open challenges. For the wider domain of potentially vulnerable applications, we need principled approaches to understand and mitigate attacks for more general classes of algorithms with low-overhead (semi-)automated mitigation strategies.

### RESEARCH QUESTION

Proposals on RV2 can address issues from, but not limited to, the following list:

- Root cause analysis and cost-effective mitigation of electromagnetic emanation (EM) side-channels
- Secure composition of mitigation for different side-channels and other security defense measures such as ALSR.
- Automated side-channel mitigation tools
- Protect keys/embedded secrets against optical probing attacks while they reside in register-file/memory or are transmitted over on-chip buses

## RV3: MACHINE LEARNING AND THREAT DETECTION

### BACKGROUND

Currently, threat detection through algorithms based on a collection of signatures (often created by security ISVs) are still popular, but can be easily bypassed. Threat detection through machine learning techniques, such as analyzing dynamic behavior patterns, is gaining popularity. In particular, one direction that deserves more exploration is developing effective algorithms for dynamic analysis of data that is collected from the hardware or even based in the hardware.

### RESEARCH QUESTION

Proposals on RV3 can address issues from, but not limited to, the following list:

- New waves of machine learning algorithms for effective threat detection, without knowledge of threat signatures, for malicious or anomalous behaviors
- State-of-the-art machine learning algorithms for threat detection using low-level trace data collected from existing hardware
- New machine learning hardware algorithms to detect malicious or anomalous activity, for instance, using data from on-die hardware monitors

The target metrics for this research vector include the following:

- Improved machine learning resiliency and robustness against techniques for threat evasion or bypassing analytics
- Improved accuracy and false positive rates of threat detection through use of data from hardware

- Effective validation of the new algorithms via theoretical explanation, experimental design, feature ranking, and security interpretation

## RV4: ADVERSARIAL MACHINE LEARNING

### BACKGROUND

Machine learning algorithms themselves are vulnerable to attack in order to subvert the output of the algorithms. Attacks on ML algorithms have been demonstrated not only for malware detection, but also fields such as signal processing and computer vision. Developing resilient ML algorithms to enhance security for the autonomous systems of the future is critical.

### RESEARCH QUESTION

Proposals on RV4 can address issues from, but not limited to, the following list:

- Adversarial machine learning for autonomous systems
- Adversarial machine learning for vision

The target metrics for this research vector include the following:

- Effective defense mechanisms for ML used in computer vision and autonomous systems
- Theoretical basis for effectiveness of ML defense mechanisms

## RV5: MACHINE LEARNING FOR PRODUCT SECURITY VERIFICATION

### BACKGROUND

Fuzzing, dynamic analysis, static analysis, and formal methods are a few automated or semi-automated techniques commonly employed to identify security vulnerabilities during software and hardware product development. Yet, these methodologies are limited in their own ways, and manual source code reviews of software (e.g., C, assembly) and hardware description language (e.g., Verilog, VHDL) by highly-skilled security professionals is still essential to bridge the gaps.

In addition, new attack vectors, hacking techniques and vulnerabilities are reported daily by external researchers through widely scattered information channels and sources (e.g., papers, reports, CWEs, blogs, articles, forum conversations). There is no efficient way for security

researchers to scale and track all of them. Digesting the information to generate appropriate action takes even more effort. At the same time, security professionals are expected to constantly keep their tools and capabilities up-to-date and expand their coverage and effectiveness, in order to stay ahead of these emerging classes of security vulnerabilities. For example, static code analysis tools identify vulnerabilities via pattern matching. Security professionals need to translate learning from a new attack vector into new rules to ensure checkers can now catch the new breeds of vulnerabilities reported.

We are looking for novel techniques to leverage machine learning (ML) to improve the depth, coverage and accuracy of product security analysis when source code is available (i.e. white-box security analysis). Such capability would allow software and hardware companies to build products with higher security robustness. It might also serve as a "neutral middle-man" or Product Verification as a Service (PVaaS) to enable integrators to assess the security robustness of third party libraries/components without gaining full access to the source code and the associated intellectual property.

### RESEARCH QUESTION

Proposals on RV5 can address issues from, but not limited to, the following list:

- ML to catch known vulnerabilities
  - Vulnerability Classes: Focus on where existing verification techniques fall short
  - Targets: Software, Hardware
  - Domains: Security, Privacy, Functional-safety
- ML to self-learn to catch newly published vulnerabilities
  - ML to monitor online articles/reports/blogs for new attacks
  - ML to digest reports, extract attack patterns and generate actionable recommendations to improve detection capability
  - ML to update appropriate tool chains to extend detection coverage
- ML to fix vulnerabilities
  - ML to generate self-tests to confirm if vulnerabilities are properly fixed
  - ML to come up with a proper fix for vulnerable code

## EVALUATION CRITERIA

Each proposal will be evaluated on the merit and relevance of the specific proposal as it relates to the program rather than against other proposals for research in the same general area, since no common work statement exists. Final selections will be based not only on individual proposal merit but also on the importance of funding a balanced project portfolio.

In order of importance, the evaluation criteria for this solicitation are as follows:

1. **Potential contribution and relevance to Intel Corporation**: We have a high interest to demonstrate the relevance and leadership of Intel platforms for continuous edge learning and intelligence applications. As such proposals that will contribute to broaden

continuous edge learning and intelligence capabilities (algorithms, edge/cloud partitioning, hardware extensions, and software environments) targeted at Intel platforms and/or architectures will have higher prospects to be accepted.

2. **Potential gains and innovative technical objectives and approach**: The field of continuous learning is moving fast and the gains and discovery of new innovations is at tremendous speedy path. The ability to demonstrate new usages as well as new algorithms or approaches is of high importance for anyone willing to lead this domain.
3. **Qualifications of participating researchers**, including interdisciplinary collaborations: Since this topic requires investigating algorithms, architectures and systems, it would be valuable for participating researchers to highlight their deep expertise area as well as collaborations across disciplines as required.
4. **Potential for co-funding and follow-on funding**: the extent to which Intel's financial investment will be leveraged, either immediately or prospectively. Cost-sharing is not required although it is encouraged.
5. **Cost effectiveness and cost realism**: The extent to which the proposed work is both feasible and impactful within the proposed resource levels.

## PROPOSAL FORMAT

Please note that Intel is unable to receive proposals under an obligation of confidentiality. All proposals submitted should therefore include only public information. Also, Intel reserves the right to share the proposals with potential industry partners who may have an interest in co-funding this program.

The proposal overall should not exceed 1 cover page (Each response should comprise the following sections:

- **Cover page (1 page)**. Title of proposal, name(s) of author(s), contact information, name of university, funds requested, the amount of cost share (if any), and an executive summary and innovative claims that summarize the new ideas being discussed in the detailed proposal, state how these ideas compare to the current state-of-the-art, and describe the potential capacity gains which could be achieved if the research is successful.

- **Detailed technical proposal including rationale, approach, and innovative claims (maximum 2 pages)**.

    - **Research Plan:** Proposals should address key issues along one or more of topics identified in the above research vectors. Proposals need to clearly articulate their research ideas, estimate the potential capacity gains which they expect to achieve if their ideas are successful and describe the rationale and/or assumptions for the estimates, and clearly articulate what is new as compared to current state-of-the-art. Also, proposals should clearly separate the responses for each research vector so that each vector can be selected in isolation should the need arise.

- **Comparison with other ongoing research.** Indicate the advantages, and disadvantages of the proposed effort relative to other key known efforts and the state of the art.
- **Demonstration and experimentation plan.** Describe your infrastructure and plans to demonstrate your ideas in an experimental setup, either with a hardware testbed, software emulation, or other.

- **Organizational Remarks (maximum 1 page):**
  - **Statement of work, schedule, milestones, deliverables**. Outline the scope of the effort including tasks to be performed, schedule, milestones, deliverables, and success criteria. It is understood that this is an exploratory research effort and schedules/deliverables reflect intentions rather than a firm commitment. However, it will be important for proposals to clearly focus on generating tangible results in a timely manner. In particular, a clear research hypothesis and research plan should be articulated, and some results should be generated by the end of the first year to provide some confidence in the initial hypothesis and motivation for continued focus and funding. Demonstrations at key intervals are desirable.
  - **Proposal team**. Summarize the members of the program team, their qualifications, and their level of participation in the project.
  - **Co-funding availability and/or plans. Y**ou may document other ongoing research efforts where synergies and collaboration opportunities are expected. You may provide information on cost-sharing commitments (if any) or plans (if any) for leveraging Intel's potential contribution to secure co-funding.
  - **Cost volume**. Cost summary that documents the expected resources, expenses, overhead, and equipment in USD.
- **Citations (unlimited).**

## ELIGIBILITY

Non-profit Academic research institutions (worldwide) are eligible to submit proposals.

## PROGRAM SCOPE AND FUNDING

The program seeks targeted research proposals. Each proposal should select and focus on a single research vector. The envisioned duration is 3 years, renewable annually contingent on progress. Awards will be made based on the overall best value to Intel. Intel reserves the right to make awards to some, all, or none of the proposals received. Additionally, Intel reserves the right to accept proposals in their entirety or to select only portions of proposals for award. We will not

necessary fund a proposal for each of the research vectors, but rather pick the highest value proposals.

## INTELLECTUAL PROPERTY

This solicitation affords proposers the choice of submitting proposals for the award of a grant, a sponsored research agreement, or other agreement as appropriate. Intel reserves the right to negotiate the final choice of agreement.

The final award terms are expected to follow one or the other of two high-level intellectual property (IP) approaches. Either: (1) Intel and the university will jointly agree that IP developed under a grant will be placed in the public domain, including offering software under an open source license, or (2) Intel and the university will negotiate a sponsored research agreement with more specific IP terms, which, at a minimum, will require the university to grant Intel and other sponsors (if any) a non-exclusive royalty free license to foreground IP.

## CONFIDENTIAL INFORMATION

Please note that Intel is unable to receive proposals under an obligation of confidentiality. Proposals should therefore include only public information. Also, Intel reserves the right to share the proposals with potential industry partners who may have an interest in co-funding this program.

## POINT OF CONTACT FOR INQUIRIES AND SUBMISSIONS

This RFP is administered by the Intel Lab's University Research Office (URO). Please complete the cover sheet at the end of this RFP and include with your proposal. Proposal submissions (and related inquiries) should be directed to: Richard Chow, Academic Research Director, (richard.chow@intel.com).

**Intel Corporate Research Council/ University Research Office (URO)**

**GRANT PROPOSAL COVERSHEET & PRIVACY POLICY NOTICE**

Intel is committed to respecting your privacy. The information you provide will be used and retained for processing and funding your grant/gift, for Intel's audit purposes, and for grant-related correspondence. For more information regarding Intel's personal information handling practices, please visit www.Intel.com/Privacy.

☐ **(For grants other than conference sponsorships)** Check here to certify that you are not engaged in prior agreements (e.g. government contracts) that constraint your ability to negotiate mutually agreeable intellectual property terms for this grant

☐ **(For grants other than conference sponsorships)** Check here to notify us that you are engaged in prior agreements (e.g. government contracts) that constrain your ability to negotiate mutually agreeable intellectual property terms for this grant

☐ Check here to opt in for occasional URO updates - announcements or newsletters

| **Proposal Title:** | | | |
|---|---|---|---|
| | | | |
| **University Name / Receiving Organization** | | **Department/Discipline** | |
| | | | |
| **Representative Authorized To Conduct Grant Administration** | | **Principal Investigator Information** | |
| **Contact Name** | | **PI Name** | |
| **Mailing Address** | | **Mailing Address** | |
| **Phone #** | | **Phone #** | |
| **Fax #** | | **Fax #** | |
| **E-Mail Address** | | **E-Mail Address** | |
| | | **Project /PI URL** | |
| | | **Co-Investigator/Students** | |
| **Amount of Cash Requested** | | | |
| **Additional Comments:** | | | |