Call for Papers: Intel Hardware Security Academic Award

The Intel Hardware Security Academic Award recognizes advancements in solutions, tools, and methodologies which enhance the industry's ability to deliver more secure and trustworthy foundational technologies. The program rewards the authors of two recently published papers that contain outstanding novel research with a meaningful impact on the hardware security ecosystem and industry, including Intel's products.

We are pleased to share the 2022 award guidelines and invite researchers to submit their work by June 5, 2022. We will grant two research awards in the amounts of $75,000 (first prize) and $50,000 (second prize). Awards will be paid to the lead author's university in the form of a research gift per the guidance below. In addition to the grant, winners will receive access to Intel's virtual pre-production test environment, with 12 months of access to aid in research. Winners will also be featured on Intel's Cyber Security Inside podcast and receive an exclusive invitation to present their work at an Intel Security conference. Conference participation is limited to two presenters for each award.

New this year, we also will present a Test of Time award to a paper published at least 10 years ago which has demonstrated significant and lasting impact in the field. The winning paper will be selected by the Hardware Security Academic Award Program Committee.

Research Focus Areas

While all recently published (January 1, 2021, to December 31, 2021) papers demonstrating innovative research into architecture, design, development, and validation that advance product security are welcome, the following focus areas are highly encouraged:

- Innovations in scalable, automated tools and methodologies for hardware design and verification that are effective in addressing common security weaknesses, significantly improving product quality and assurance efficiency.
- Emerging usages, threat analysis, systemic mitigations, and security enhancements that strengthen cloud-to-edge computing, accelerant, and communication solutions.
- Architectural, micro-architecture, and circuit innovations that improve resiliency and reliability of silicon and electronics against transient faults.
- Innovations in "Confidential Manufacturing" methodologies, tools and capabilities to support Intel's IDM 2.0 vision, offering assurance, transparency and a trusted supply chain to the ecosystem.
- Groundbreaking advancements in foundational security capabilities, including next generation cryptographic techniques, safety-critical systems verification and resilience against adversarial behavior.
- Use of analytics and machine learning to improve product security capabilities and robustness.

Who Qualifies

Any full time, tenured or tenure track (or equivalent) faculty member involved in research may make a submission. Intel will not, however, consider submissions by individuals residing in, or affiliated with, an academic institution located in a U.S. Government embargoed country. Intel also will not consider submissions by individuals on a U.S. Government sanctions list, including individuals affiliated with academic institutions on a U.S. Government sanctions list. Intel employees and immediate family members are ineligible to participate.

What Qualifies / Submission Format

All submissions must reflect only completed research which was first published or presented publicly between January 1, 2021, and December 31, 2021, and that has the potential to be disruptive to product security in the areas outlined above. All submissions must be made using the EasyChair CFP submission system ("EasyChair") and include the following information:

- Short description (no more than 400 words) of:
  - Research focus and techniques
  - Brief summary of current state-of-the-art
  - Novel contribution
  - Potential impact to the industry, ecosystem, and Intel's products and technologies
  - Prior and future relevant work, if applicable
  - Alignment with the above-listed "focus categories"
- Details on:
  - Prior awards and recognition of the research
  - Accepted conference (the paper needs to have been accepted, peer-reviewed and published or presented publicly between January 1, 2021, and December 31, 2021)
- Full paper (*camera-ready* in PDF format, as submitted and accepted to a conference or journal following peer review).
- Curriculum vitae of applicable authors.
- Affiliation and organization details including relevant tax/gift information and administrative contacts for the submitter's academic institution.

Awardees will be selected by the Intel Hardware Security Academic Award Program Committee. The committee will examine, among other factors, the viability, novelty, originality, and relevance of the submissions with a focus on demonstrating significant contribution and impact on the hardware security ecosystem and Intel products. The committee retains full discretion on selection of the award winners, and the awardees will be required to sign an award acceptance letter.

Notifications are expected in July 2022, and the awards are expected to be presented at a ceremony with Intel engineers and executives during an industry security conference in August 2022.

How the Award Is Gifted

One-time awards of $75,000 (first prize) and $50,000 (second prize) payable to the awardee's academic institution to be used at the discretion of the awardee's university for research or curriculum development support (class material, conferences sponsorship, travel expenses, computer lab infrastructure, web site development, textbooks, etc.). For winning papers with authors

from multiple institutions, the award will be granted to the university of the first named academic author.

Deadline

All submissions must be fully submitted via the EasyChair system by June 5, 2022, at 11:59 PM PT, in order to be considered.

Additional Terms, Notices, and Disclaimers

Intel's decisions will be final in all matters relating to this program, including whether or not to grant an award and the interpretation of these additional terms, notices, and disclaimers and the guidelines above (collectively, "Terms and Conditions"). By making a submission, applicants affirm that they have read and agree to the Terms and Conditions.

- Awards must comply with applicable U.S. and international laws, regulations, and policies.
- Intel is authorized to evaluate submissions, to consult with outside experts, in evaluating submissions, and to grant or deny awards using criteria determined by Intel to be appropriate and at Intel's sole discretion. Intel's decisions will be final in all matters relating to this program, and applicants agree not to challenge any such decisions.
- Implementation and management of this program and associated awards is subject to change at any time without notice to applicants or awardees and is at the complete discretion of Intel.
- Awardees are responsible for confirming that acceptance of any awards will not be in violation of any university policy regarding such awards and that acceptance of any award is not in exchange for promotion or influence regarding any of Intel's commercial activities, products, services, or the adoption of Intel-related standards.
- Neither Intel nor the applicant is obligated to enter into a business transaction as a result of the submission. Intel is under no obligation to review or consider any submission.
- Any information collected as part of this award will be used for the administration of the program. This may include sharing of any submitted information within Intel (and contractors) for purposes of selecting awardees, planning visits, public relations (with prior approval), or other purposes reasonably related to the program. Any information collected is also subject to Intel's privacy policy found at www.intel.com/privacy.
- Awards granted in connection with this program will be subject to terms and conditions contained in the research gift agreement (or, in some cases, other mechanisms) pursuant to which the award funding will be provided. Applicants understand and acknowledge that they will need to agree to these terms and conditions to receive an award.