August 10, 2022

Intel Names Hardware Security Award Winners

Intel announces the winners of its second annual Hardware Security Academic Award for innovative security research.

SANTA CLARA, Calif.--(BUSINESS WIRE)-- **What's New:** Today, Intel announced the winners of its second annual Intel Hardware Security Academic Award program, aimed at fostering innovative research into solutions, tools and methodologies to address fundamental security challenges and enhance the industry's ability to deliver more secure and trustworthy foundational technologies.

> *"With the exponential growth of data and artificial intelligence (AI) across the compute spectrum, we've also seen increased sophistication and frequency of attacks. As an industry, it is imperative that we aim to protect sensitive datasets across all stages of the lifecycle – at rest, in transit and in use. Intel has a long history of working closely with academic researchers to tackle big challenges through programs like Intel Labs' academic and faculty research grants, the Intel Bug Bounty program, and now through the hardware security award. We value their insights and dedication and, together, we're making progress toward our shared vision of a safe and secure future."*
> - Sridhar Iyengar, vice president of Intel Labs and director of Security and Privacy Research

About the Award Program: The Hardware Security Academic Award program is part of Intel's commitment to collaborate with and foster advancements in the security research community. The award program invites academic researchers to submit a recently published paper demonstrating novel research with a meaningful impact on the hardware security ecosystem, including but not limited to Intel's own products. Anand Rajan, senior director of Emerging Security Lab at Intel Labs, presented this year's awards during a reception in Boston that coincided with the USENIX Security Symposium.

This year's program scope expanded to invite innovations in confidential manufacturing methodologies, tools and capabilities, in support of Intel's IDM 2.0 vision for a trusted and secure supply chain ecosystem. A Test of Time award was also added to the program to honor papers published more than 10 years ago, which have demonstrated a significant and lasting impact in the security field.

For researchers who are interested in submitting a paper for next year's program, the submission window will be announced on the program page.

About the Prizes: A committee at Intel examined the viability, novelty, originality and relevance of all submissions with a focus on demonstrating significant contribution to and impact on the hardware security industry. This year's applicants spanned 34 papers, featuring more than 140 authors from academic and industry backgrounds across 11

countries. One-time awards of $75,000 for first prize and $50,000 for second prize will be granted to the winners' academic institution to be used for further research or curriculum development. In addition to the grant, winning authors will receive access to Intel's virtual pre-production test environment to aid in future research and will be invited to present their work at the invite-only Intel Security Conference (iSecCon) and will be featured on Intel's Cyber Security Inside podcast.

About This Year's Winners:

First place: *"A Formal Approach to Confidentiality Verification in SoCs at the Register Transfer Level"*

In this paper, researchers demonstrate how Unique Program Executing (UPEC) methodology can be used to reason about confidentiality properties of a system-on-chip (SoC). UPEC methodology employs an efficient, induction-based formulation for information flow tracking. While the original UPEC methodology was formulated for micro-architectural side-channel detection for CPUs, this work is demonstrating how to generalize and scale that methodology for confidentiality properties for SoCs. Their formulation works directly on Register Transfer Language (RTL) and has been integrated in one commercial tool backend, thus yielding a first-of-its-kind, practically viable Pre-Si security verification technique.

The winning team included:

- Johannes Müller, Technische Universität Kaiserslautern
- Mohammad R. Fadiheh, Technische Universität Kaiserslautern
- Anna Lena Duque Antón, Technische Universität Kaiserslautern
- Thomas Eisenbarth, Professor, Universität zu Lübeck
- Dominik Stoffel, Apl. Professor, Technische Universität Kaiserslautern
- Wolfgang Kunz, Professor, Technische Universität Kaiserslautern

Second place: *"Nyx: Greybox Hypervisor Fuzzing using Fast Snapshots and Affine Types"*

This research demonstrates how modern hardware features (Intel® Virtualization Technology, extended page tables [EPT], Intel® Processor Trace, and page-modification logging [PML]) can be used to build effective and innovative security validation tools. The research has greatly improved the ability to test critical system software, ranging from embedded x86 firmware, to drivers, hypervisors and future confidential compute stacks. In fact, within Intel's Security Center of Excellence, researchers have already begun to leverage and evolve the technology, and the results have contributed to an even stronger software development lifecycle.

The winning team included:

- Sergej Schumilo, Ruhr-Universität Bochum
- Cornelius Aschermann, Ruhr-Universität Bochum
- Thorsten Holz, Faculty, CISPA Helmholtz Center for Information Security

Test of Time Award: *"AEGIS: Architecture for Tamper-Evident and Tamper-Resistant Processing"*

Published in 2003, this research describes a single-chip secure processor including a

configuration where the underlying system software is untrusted. The proposed architecture incorporated several novel ideas at that time, such as cryptographic measurement and attestation, memory integrity verification and memory encryption. This work helped inspire the broader domain of trustworthy computing and the practical realization of the novel features can be found in a wide range of trusted execution environments (TEEs) deployed across the industry today.

The winning team included:

- G. Edward Suh, Professor, Cornell University, Research Scientist, Meta AI
- Dwaine Clarke, Senior Lecturer, University of the West Indies
- Blaise Gassend, Senior Staff Software Engineer, Waymo
- Marten van Dijk, Professor, Centrum Wiskunde & Informatica, Affiliated Professor, University of Connecticut
- Srinivas Devadas, Webster Professor, Massachusetts Institute of Technology

About Intel

Intel (Nasdaq: INTC) is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better. To learn more about Intel's innovations, go to newsroom.intel.com and intel.com.

No product or component can be absolutely secure.

View source version on businesswire.com:
https://www.businesswire.com/news/home/20220810005757/en/

Jennifer Foss
1-425-765-3485
jennifer.foss@intel.com

Source: Intel