September 21, 2022

HACS 2023 Overview

Gilles Barthe, Karthik Bhargavan, Sofía Celi, Deirdre Conolly,
Allen Gunn, Diane Hosfelt, Ben Laurie, Trevor Perrin, Peter Schwabe, Cathie Yun

Introduction

Since 2016, the workshop on High Assurance Crypto Software has been bringing together cryptographic developers, cryptographers, and high-assurance experts to improve the quality of cryptographic software.

HACS has helped connect many participants into networks and communities where best practices are fostered and exchanged, and where computer-aided tools are finding users (see https://hacs-workshop.org).

Yet as we look to the future, this progress must confront two looming challenges:

- First, cryptography in many applications is evolving past the simple goal of transmitting hidden data towards more complex goals based on *computing on* hidden data (e.g. zero-knowledge proofs, MPC, homomorphic encryption, etc.)

- Second, the threat of quantum computing is forcing cryptographers and software developers into new mathematical realms where risks and capabilities are still poorly understood; and forcing complex migrations on deployed systems.

Based on this, the HACS organizers see the following themes for the 2023 workshop:

- **Consolidate and accelerate best practices:** What are the best tools and practices from the current generation of cryptographic software? How can we spread this knowledge and accelerate tool deployment?

- **Orient to face new challenges:** How can we adapt existing practices and tools (and create new ones!) to face the challenges posed by complex and post-quantum cryptosystems. Interpreting challenges as opportunities, we see the potential for fresh thinking and new projects across the spectrum from design, analysis, and specification of algorithms; to implementation, testing, and deployment.

Concretely, HACS 2023 will focus on the following areas:

- **Correctness and security of crypto code**, including formal generation and verification with an emphasis on tool usability; as well as informal techniques (testing, fuzzing, and code review).

- **Computer-aided and verified proofs of security** for cryptographic algorithms and protocols, with a focus on usability by cryptographers who are not formal methods experts.

- **Secure distributed computation**, including zero-knowledge proofs, threshold and multi-party computation, and homomorphic encryption. We will emphasize compilers, connections and interoperation between these domains, improving community and developer practices, and tooling in distributed settings.

- **Post-quantum cryptography**, including implementation correctness, security proofs, redesigning protocols for PQC, and new algorithms and requirements.

- **Security at the hardware/software interface** - in particular, tools and techniques for developing software that remains secure in complex threat environments (e.g. software-based side channel and fault attacks, speculative execution, and secure enclaves).

The Plan for HACS 2023

HACS 2023 will be a two-day physical event in Tokyo, Japan, on March 30 and 31, with an optional hack day on April 1st. This will be directly after the Real World Crypto 2023 workshop, which is scheduled for March 27, 28 and 29 in Tokyo. The event will once again be co-organized and facilitated by Allen Gunn of Aspiration.

We will build on the success of the past HACS events - in particular, we expect to reinvite many of the attendees from HACS 2022 to carry forward their discussions. We expect many attendees will have ongoing projects and concrete goals in mind. The organizers will spend significant time before the event discussing these goals with attendees and arranging workshop sessions to advance concrete objectives.

Over the years, the HACS Workshop has grown substantially; the 2022 edition had around 100 participants and was about twice as large as the first workshop, and we are aiming for 100-150 participants for HACS 2023.

Historically HACS participation has been by invitation. We will continue this for 2023, but to broaden inclusion, diversity, and participation we will be expanding our organizing team to bring in fresh perspectives and connections (welcome Cathie, Deirdre, and Sofia!); advertising the event and our self-nomination process more widely; and providing travel grants for early-career or under-represented attendees (funds permitting).

HACS to date has catalyzed significant advances in the convergence of cryptographic software with formal and high-assurance verification. We are excited for the 2023 event to consolidate these gains and launch new efforts towards new challenges.