HACS 2022 Overview

Gilles Barthe, Karthik Bhargavan, Diane Hosfelt, Ben Laurie, Trevor Perrin, Peter Schwabe

Introduction

The importance and complexity of cryptographic software makes it an ideal application for formal and high-assurance verification. The Workshop on High Assurance Crypto Software ("HACS") was launched in 2016 to drive this convergence forward. As a yearly event, we've been bringing the world's best cryptographic developers together with top experts in formal verification and high-assurance methodologies. The goal is to foster collaborations towards making cryptographic software flawless.

Earlier HACS workshops launched many collaborations and gave participants a greater understanding of the tool and technology ecosystems that are taking shape (for more details on projects that have been incubated at HACS, please see https://hacs-workshop.org).

In 2021 we faced the challenge of an unprecedented pandemic, which prompted us to take the event virtual, but allowed us to be more experimental and inclusive. We advanced our core focus areas while also expanding to consider a broader range of topics:

- Testing, formal verification, and generation of crypto code (with an increased focus on post-quantum crypto). This has been a core topic area in all prior HACS events. Work at HACS 2021 focused on assessing progress made and work remaining to be done.

- Formal verification and generation of security proofs for cryptographic algorithms and protocols, with the goal of having machine-checked proofs.

- Secure distributed computation, including zero-knowledge topics such as Schnorr, SNARKs/STARKs, bulletproofs, anonymous credentials, pairing-friendly curves, and multiparty computation, with particular focus on languages, tools and formal methods.

- Hardware/software interfaces, including instruction set architectures (e.g., crypto extensions for RISC-V, and secure enclaves) and microarchitectural attacks such as Spectre and variants, as well as formal modeling of these attacks and associated countermeasures.

- Developer usability, i.e. understanding how tools for formal verification can improve to be accessible and productively usable for software developers who do not have a strong background in formal methods.

For 2022, we hope to build on the momentum we created in 2021 and consolidate these areas as core topics of HACS, by bringing many of the discussions started in 2021 into the more concentrated setting of an in-person workshop.

The Plan for HACS 2022

Our goal is for HACS 2022 to be a two-day physical event in Amsterdam, on January 13-14, with an optional hack day on January 15. This would directly follow the Real World Crypto 2022 workshop, which is currently scheduled for January 10-12 in Amsterdam. The event will once again be co-organized and facilitated by Allen Gunn of Aspiration.

We will evaluate the pandemic situation in early November and determine if it is safe to hold an in-person event or if we must postpone to a virtual event during the spring. Full vaccination and masks will be required for participation in any in-person event.

We will build on the success of the past HACS events--in particular, we expect to reinvite many of the attendees from 2021's virtual HACS to carry forward last year's discussions in person. Considering that previous workshops served to make introductions and start a number of projects, we will continue adjusting the process to drive collaboration toward concrete outcomes:

- We expect a significant number of attendees to have ongoing projects and concrete goals in mind. The organizers will spend significant time before the event discussing what these are and arranging workshop sessions to advance concrete objectives.

- Last year, we introduced a number of new topic areas that we would like to continue broadening into. We started a number of new discussions that will likely be even more productive in an in-person setting.

- Over the years, the HACS Workshop has grown dramatically, and 2021 was three times as large as the first workshop. Historically HACS participation has been by invitation, but in order to broaden inclusion, diversity, and participation as we grow, we are planning to implement a formal "requests for participation" process to encourage inquiries from interested practitioners.

HACS events to date have already produced significant outcomes in driving the convergence of cryptographic software and formal and high assurance verification. We are excited about the potential for the 2022 event to continue this trajectory while also moving in new and compelling directions.