HCSS 2020 Call for Presentations

The Twentieth Annual

High Confidence Software and Systems (HCSS) Conference

CALL FOR PRESENTATIONS AND POSTERS

INTRODUCTION

The twentieth annual High Confidence Software and Systems (HCSS) Conference will be held May 5-7, 2020 at the Historic Inns of Annapolis in Annapolis, Maryland. We solicit proposals to present talks at the conference and to participate in the poster session.

BACKGROUND

Our security, safety, privacy, and well-being increasingly depend upon the correctness, reliability, resilience, and integrity of software-intensive systems of all kinds, including cyber-physical systems (CPS). These systems must be capable of interacting correctly, safely, and securely with humans, with diverse other systems, and with the physical world even as they operate in changing, difficult-to-predict, and possibly malicious environments. New foundations in science, technology, and methodologies continue to be needed. Moreover, these methods and tools have to be transitioned into mainstream use to build and assure these systems--and to move towards more effective models for acceptance and certification.

CONFERENCE SCOPE, GOALS, AND VISION

The High Confidence Software and Systems (HCSS) Conference draws together researchers, practitioners, and management leaders from government, universities, non-profits, and industry. The conference provides a forum for dialogue centered upon the development of scientific foundations for the assured engineering of software-intensive complex computing systems and the transition of science into practice. The technical emphasis of the HCSS conference is on mathematically-based tools and techniques, scientific foundations supporting evidence creation, systems assurance, and security. The HCSS vision is one of engaging and growing a community--including researchers and skilled practitioners--that is focused around the creation of dependable systems that are capable, efficient, and responsive; that can work in dangerous or inaccessible environments; that can support large-scale, distributed coordination; that augment
human capabilities; that can advance the mission of national security; and that enhance quality of life, safety, and security.

CONFERENCE THEMES

We invite submissions on any topic related to high-confidence software and systems that align with the conference scope and goals listed above. In addition, the 2020 HCSS Conference will highlight the following themes:

Formal Methods at Scale
Despite the increasing power of formal methods, most hardware and software systems are not formally verified. Recent advances in industrial applications of formal methods, however, suggest that this may be changing. We solicit research and experience reports related to the problem of scaling up formal methods tools and broadening their use, especially for systems of industrial scale. Increasing the scalability and automation of the tools themselves is of interest, as is reducing the investment or expertise needed to use them. Real-world experiences with integrating formal tools into engineering workflows may highlight other relevant issues.

Example topics include:

- case studies of successful applications of formal methods to large systems
- scaling formal tools, especially with respect to quantifiable metrics
- putting formal tools into the hands of rank-and-file engineers (e.g., by reducing the expertise or effort needed to use them)
- approaches that enable a "pay as you go" process in which up-front investment is reduced
- applications of AI / machine learning to increase automation and scale

Architecture-level Formal Methods for New and Existing Systems
Technical architecture comprises commitments to systems' structure and internal interfaces, global invariants and other internal properties, and, for components, constraints on visibility of design elements. These commitments, well crafted, enhance system characteristics including quality outcomes, evolution and adaptation, and decoupling of development processes for system components. This motivates modeling and analysis at the level of technical architecture as a way to assess potential outcomes regarding these characteristics. Architecture-level Formal Methods, including diverse kinds of modeling and analysis, can thus be used on their own to strengthen confidence in the design and configuration of systems. They can also be used to facilitate verification that implementations are consistent with various architectural commitments, ensuring that the intended architecture-level properties are respected by the implementation. These approaches allow the development of (new) high-assurance systems to be coupled with validated architectures, with assurance linked down to the implementation. The need for high-assurance is, of course, not confined to newly built systems. Critical software systems that have already been deployed may
face new requirements to accomplish "retrofits" that deliver higher levels of assurance. This often requires analysis of as-built architecture and gradual transitions to improved architectures that address emerging assurance needs. We solicit descriptions of approaches and tools for architecture-level formal methods, and experience on using such approaches to new and retrofitted systems.

Example topics include:

- formal approaches for the modeling and analysis of system architecture elements
- formal approaches for linking architecture-level models to implementations
- experience in retrofitting existing deployed software into more assured systems through architecture-driven processes

**Human/Machine Cognitive Security**

We find ourselves in the midst of an era of social-information warfare, for which we are presently ill-prepared to mount an effective defense. Both the technological and the human dimensions of cognitive security need to be addressed to secure and support cognitive activities (e.g. decision-making, analytic judgements) in cyber contexts. This theme explores applications of formal methods that could mitigate the effects of both bad information and bad judgements that may lead to vulnerabilities and exploits (note that bad judgements may result either from natural cognitive biases or from explicit adversarial manipulation). We solicit descriptions of technology and experience reports in support of cognitive security and supporting human/machine interaction.

Example topics include:

- Rigorous characterization of cognitive models and the associated impact of such formalization on the nature of emerging vulnerabilities and exploits.
- The role of formal methods in realizing cognitive limitations and bias, as well as their practical use to discover and describe emerging vulnerabilities and exploits.
- The use of automated reasoning technologies within the domain of cognitive security.
- The effectiveness of formal methods in detecting and mitigating individual and group-level cognitive biases.
- Case studies that examine what constitutes an effective relationship between humans and machine automation, through the sharing of mental states and context with regard to correctly capturing and communicating hidden or implied artifacts (such as cognitive or machine state artifacts).
- Assessments quantifying the effectiveness of a human-machine team, considering the characteristics of efficient interaction between the two as teammates.

**CONFERENCE PRESENTATIONS**

The conference program features invited speakers, panel discussions, poster presentations, and a technical track of contributed talks.

*Technical Track Presentations*
The technical track features two kinds of talks:

* **Experience reports.** These talks inform participants about how emerging HCSS and CPS techniques play out in real-world applications, focusing especially on lessons learned and insights gained. Although experience reports do not have to be highly technical, they should emphasize substantive and comprehensive reflection, building on data and direct experience. Experience reports focus on topics such as transitioning science into practice, architecture and requirements, use of advanced languages and tools, evaluation and assessment, team practice and tooling, supply-chain issues, etc.

* **Technical talks.** These talks highlight state-of-the-art techniques and methods for high-confidence software systems with an emphasis on how those techniques and methods can be used in practice. Presenters of these talks should strive to make their material accessible to the broader HCSS community even as they discuss deep technical results in areas as diverse as concurrency analysis, hybrid reasoning approaches, theorem proving, separation logic, analysis, synthesis, analytics, various modeling techniques, etc.

If you are interested in offering a talk—or nominating someone else to be invited to do so—please upload an abstract of one page or less for your proposed talk, or a one paragraph description of your nominee’s proposed talk, by **Friday, January 10, 2020** to [https://cps-vo.org/hcss20/presentation/cfp](https://cps-vo.org/hcss20/presentation/cfp). Abstracts and nomination paragraphs should clearly indicate why the talk would be relevant to HCSS and which, if any, conference themes the talk would address. Notifications of accepted presentations will be made by **Friday, February 14, 2020**.

**POSTER PRESENTATIONS**

If you are interested in participating in the poster session, please upload an abstract of your proposed poster theme with title by **Friday, January 10, 2020** to [https://cps-vo.org/hcss20/poster/cfp](https://cps-vo.org/hcss20/poster/cfp). Abstracts should clearly indicate why the poster is relevant to HCSS and which, if any, of this year’s themes the poster would address. Notifications of accepted posters will be made by **Friday, February 14, 2020**.

The conference organizers will print posters free of charge if design content is electronically submitted by **Monday, April 17, 2020**. After April 17, poster session participants will be responsible for the printing and delivery of their own posters. Content designs of accepted posters can be submitted electronically in PDF format. The conference organizers will provide easels, foam boards, and tacks for all poster displays. Poster session participants should contact the conference organizers in advance if additional materials or props are desired.

**ADDITIONAL INFORMATION**
Further instructions for electronically submitting print-ready abstracts, final slide presentations, and print-ready posters will be provided in the acceptance notification messages. Abstracts of accepted presentations and posters will be printed in the 2020 HCSS Conference proceedings.

**IMPORTANT DATES**

**Presentations:**
- Abstracts Due: January 10, 2020 **January 24, 2020**
- Notification of Decisions: February 14, 2020
- Print-Ready Abstracts Due: April 6, 2020
- Slides Due: May 4, 2020

**Posters:**
- Abstracts Due: January 10, 2020 **January 24, 2020**
- Notification of Decisions: February 14, 2020
- Print-Ready Abstracts Due: April 6, 2020
- Print-Ready Posters Due: April 17, 2020

**HCSS Conference: May 5-7, 2020**

**PLANNING COMMITTEE**

**Co-Chairs**
- June Andronick, CSIRO's Data61 and UNSW
- Eric Smith, Kestrel Institute

**Steering Group**
- Perry Alexander, University of Kansas
- Kathleen Fisher, Tufts University
- John Hatcliff, Kansas State University
- John Launchbury, Galois, Inc.
- Stephen Magill, Muse Dev and Galois, Inc.
- Brad Martin, National Security Agency
- Ray Richards, DARPA
- Bill Scherlis, DARPA
- Sean Weaver, National Security Agency
- Matt Wilding, Collins Aerospace

**Organizers**
- Katie Dey, Vanderbilt University
- Anne Dyson, Cyber Pack Ventures
- Amy Karns, Vanderbilt University