

# Call for Papers

## IEEE Cybersecurity Development (SecDev) 2016



New Conference on Security Innovation in Design and Development

Nov 3-4, 2016

Submissions due: Jun 24, 2016

Boston, MA

SecDev is distinguished by its focus on how to “build security in” (and not simply discover the absence of security). Its goal is to encourage and disseminate ideas for secure system development among both academia and industry. Developers have valuable experiences and ideas that can inform academic research, and researchers have concepts, studies, and even code and tools that could benefit developers. We anticipate that attendees from academic conferences like IEEE S&P, USENIX Security, PLDI, FSE, ISSTA, SOUPS, and many others could contribute ideas to SecDev, as could attendees of industrial conferences like AppSec, RSA, Black Hat, and Shmoocon.

Papers have the option of appearing in the conference’s formal proceedings, or not. SecDev is also interested in tutorials on processes, frameworks, languages, and tools. The goal is to propose useful and thought provoking ideas, and to share knowledge on the art and science of secure system development.

SecDev is interested in work that has a demonstrated connection to building systems that are more secure. It is not enough to show that an existing system, however prominent, is insecure. Nor is it enough to propose a new cryptosystem or formal security model with nice mathematical properties but no concrete exploration of how it would be used to build systems more securely. Instead, papers should be about (as a few examples) how a development library, tool, or process can produce systems resilient against certain attacks; how a formal foundation could underpin a language, tool, or testing strategy that can help produce stronger systems; and experience, designs, or applications showing how cryptography can be used effectively to secure systems.

#### Areas of interest include (but are not limited to):

- Security engineering processes, from requirements to maintenance
- Dynamic/static analysis and runtime approaches towards application security
- Programming languages and frameworks supporting security
- Testing strategies to ensure security
- Explorations of formal verification and other high-assurance methods for security
- Code reviews, red teams, and other human-centered assurance
- Security-focused system (HW/SW/architecture) designs
- Human-centered design for systems security
- Distributed systems design and implementation for security

Submit your papers at <https://secdev16.hotcrp.com/>

Submissions may be one of three categories:

- **(Up to) 5-page papers.** These must be well-argued and worthy of publication and citation, on the topics above. They may present new work or ideas, or draw substantially from the authors’ previously published results. Authors of accepted papers will present their work at the conference. The page count does not include bibliographic references.
- **One-page abstracts.** Abstracts will be reviewed lightly and all accepted abstracts will be published on the SecDev 2016 web page. Authors of accepted abstracts will be invited to give a talk during a “5-minute madness” session at the conference.
- **Tutorial proposals.** Tutorials should aim to be 90 minutes long. Preference will be given to tutorials that are hands-on. Proposals should be 1 page and cover (a) the topic; (b) a summary of the tutorial format with possible pointers to relevant materials; (c) the expected audience and expected learning outcomes; (d) prior tutorials or talks on similar topics by the authors (and audience size), if any.

We are seeking broad representation in the program, and may take this into account when reviewing multiple submissions from the same authors. We prefer experienced presenters, and each submission must indicate on the submission site which co-author will present the paper at the meeting.

A good SecDev paper may resemble an elaborated vision statement, a grant proposal, or a mini-keynote summarizing prior work and directions. We are not interested in complete works that manage to fit in a few pages; rather we want bigger ideas (previously published or not) that will lead to a stimulating, thoughtful, and perhaps (gently) provocative discussion. A good SecDev tutorial will introduce interested practitioners and researchers to technologies (e.g., languages, tools, frameworks) that show promise in aiding the development of secure systems.

**General Chair:** Robert Cunningham, MIT Lincoln Laboratory

**Program Chair:** Michael Hicks, University of Maryland

**Tutorial Chair:** Stelios Sidiroglou-Douskos, MIT

This call for papers is inspired by SNAPL (<http://snapl.org/2015/cfp.html>).

Questions about submissions? Email [secdev16-pcchairs@ieee.org](mailto:secdev16-pcchairs@ieee.org).

Questions about tutorials? Email [secdev16-tutorials@ieee.org](mailto:secdev16-tutorials@ieee.org).