IEEE Security Development Conference (SecDev) 2018
Call for Papers

Sponsored by the IEEE Computer Society Technical Committee on Security and Privacy

September 30–October 2, 2018 at the Hyatt Regency, Cambridge, MA

Overview

SecDev is a venue for presenting ideas, research, and experience about how to develop secure systems.

SecDev is distinguished by its focus on the theory, techniques, and tools for how to “build security in” to computing systems, and not simply discover the absence of security. Its goal is to encourage and disseminate ideas for secure system development among academia, industry, and government. 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. Great SecDev contributions could come from attendees of industrial conferences like AppSec, RSA, Black Hat, and Shmoocon; from attendees of academic conferences like IEEE S&P, IEEE CSF, USENIX Security, PLDI, FSE, ISSTA, SOUPS, and others; and from newcomers.

SecDev solicits four types of contributions. First, SecDev is a forum for novel research papers that present innovations, experience-based insights, or a vision about how to “build security in” to existing and new computing systems. Position papers with exceptional visions will also be considered. Second, SecDev seeks Best Practices (BP) papers that provide an in-depth clarification and integration of solutions on a major security area. The paper needs to provide new perspectives and insights, although it could draw upon prior work. Third, SecDev seeks hands-on and interactive tutorials on processes, frameworks, languages, and tools for building security in. The goal is to share knowledge on the art and science of secure systems development. Fourth, SecDev seeks abstracts from practitioners to share their practical experiences and challenges in security development.

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

- Security engineering processes, from requirements to maintenance
- Security-focused system designs (HW/SW/architecture)
- Distributed systems design and implementation for security
- Human-centered design for systems security
- Tools and methodology for secure code development
- Programming languages, development tools, and ecosystems supporting security
- Risk management and testing strategies to improve security

- Static program analysis for software security
- Dynamic analysis and runtime approaches for software security
- Explorations of formal verification and other high-assurance methods for security
- Automation of programming, deployment, and maintenance tasks for security
- Code reviews, red teams, and other human-centered assurance
- Security assistance for software developers and security analysts

What makes SecDev different from other conferences?

SecDev is interested in work that can demonstrate a practical 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 with no concrete experience of how it would be used to build systems more securely. Examples of topics that are in scope include: how a development library, tool, or process can produce systems resilient to certain attacks; how a formal foundation can underpin a language, tool, or testing strategy that improves security; techniques that drastically improve the scalability of security solutions for practical deployment; and experience, designs, or applications showing how to apply cryptographic techniques effectively to secure systems.

SecDev provides an integrated forum for researchers and practitioners to share their experiences. It aims at bridging the gap between constructive security research and the practice and enabling real-world impact in the long run.

Submission Details
Papers must be submitted using the two-column IEEE Proceedings style:
http://www.ieee.org/conferences_events/conferences/publishing/templates.html.

Submissions must be one of the four categories:

- **Research papers**, up to 8 pages. These must be well-argued and worthy of publication and citation, on the topics above. The research papers must present new work or ideas. Position papers with exceptional visions will also be considered. Authors of accepted papers will present their work at the conference (likely in a 30-minute slot) and their papers will appear in the conference's formal IEEE proceedings.

- **Best Practices (BP) papers**, up to 10 pages. Suitable papers are those that provide an integration and clarification of ideas on an established, major research area, support or challenge long-held beliefs in such an area with compelling evidence, or present a convincing, comprehensive new taxonomy of some aspect of secure development. Such a paper would be marked with the prefix "**BP:**" in the title, and would need to provide new insights, although it could draw upon prior work. Authors of accepted papers will present their work at the conference (likely in a 30-minute slot) and their papers will appear in the conference's formal IEEE proceedings.

- **Tutorial proposals**. Tutorials should aim to be either 90 minutes or 180 minutes long. We strongly encourage tutorials to have hands-on components and audience interactions. We do not recommend simply slide presentations. Tutorial proposals should be 2 pages 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. Accepted tutorials may provide an abstract that will appear in the conference's formal IEEE proceedings. Tutorials will occur on the first day of the conference and will be included as part of the conference registration. Note that if an accepted tutorial requires special materials or environments for the hands-on participation, we expect the authors to provide necessary preparation instructions for the attendees.

- **Practitioners session abstracts**, up to one page. The abstracts will be lightly reviewed. We strongly encourage practitioners from the industry and government to submit, to share their security experiences and insights, challenges and obstacles encountered. Authors of accepted abstracts will be invited to give a short talk during the practitioners sessions at the conference. The abstracts will be included in the conference's IEEE proceedings.

We are devoted to 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.

SecDev also seeks poster submissions. The 1-page poster abstracts will be included in the conference's IEEE proceedings. More details will be on the Call For Poster page.

If you have any questions submissions, send an email to secdev18-pc@ieee.org.

Important Dates

Paper and tutorial submission:	March 5, 2018
Paper and tutorial notification:	May 15, 2018
Practitioners session abstract submission:	July 20, 2018
Practitioners session notification:	August 10, 2018
Camera-ready versions due:	August 17, 2018
Conference:	Sept. 30 - Oct. 2, 2018

2018 IEEE SecDev Program Committee

Research Program Committee

Daphne Yao, Virginia Tech (Co-chair)
Stephen Chong, Harvard University (Co-chair)
Yasemin Acar, Leibniz University Hannover
George Baah, MIT Lincoln Laboratory
Nataliia Bielova, INRIA
Haipeng Cai, Washington State University
Ran Canetti, Boston University and Tel Aviv University
Sarah Chmielewski, MIT Lincoln Laboratory
Haixin Duan, Tsinghua University
Michael Emmi, SRI International
Lori Flynn, Carnegie Mellon University
Michael Franz, University of California, Irvine
Dan Geer, In-Q-Tel
Ronghui Gu, Columbia University
Joshua Guttman, Worcester Polytechnic Institute
Bill Harris, Georgia Tech
Michael Hicks, University of Maryland
Trent Jaeger, Penn State University
Christoph Kern, Google
Shriram Krishnamurthi, Brown University
Morley Mao, University of Michigan
Na Meng, Virginia Tech
Toby Murray, University of Melbourne
Divya Muthukumaran, Imperial College, London
Hamed Okhravi, MIT Lincoln Laboratory
Xinming Ou, University of South Florida
Frank Piessens, KU Leuven, Belgium
Raymond Richards, DARPA
Patrick Schaumont, Virginia Tech
Kent Seamons, Brigham Young University
Kostya Serebryany, Google
Sean Smith, Dartmouth College
Deian Stefan, University of California, San Diego
Sal Stolfo, Columbia University
Jun Sun, Singapore University of Technology and Design
Gang Tan, Penn State University
Tao Wei, Baidu X-Lab
Heng Yin, UC Riverside
Danfeng Zhang, Penn State University

Xiangyu Zhang, Purdue University

Practitioners Session Program Committee

Richard Chow, Intel Labs (Co-chair)
Andy Chou, ex-Coverity (Co-chair)
Lydia Chen, IBM Zurich
Jin-Hee Cho, Army Research Laboratory
John Criswell, University of Rochester
Bill Horne, Intertrust Technologies
James Imanian, PricewaterhouseCoopers
Jason Li, Intelligent Automation
Zhou Li, RSA Laboratories
Francesco Logozzo, Facebook
Leigh Metcalf, Carnegie Mellon University
Thomas Moyer, University of North Carolina at Charlotte
Nick Multari, Pacific Northwest National Laboratory
Raj Rajagopalan, Honeywell
Kevin Roundy, Symantec Research Labs
Christian Skalka, University of Vermont
Xiaokui Shu, IBM Research
Jason Syverson, Siege Technologies
Chris Wysopal, Veracode
Tao Xie, University of Illinois at Urbana Champaign

Poster Session Committee

Bogdan Copos, SRI International (Chair)
Hussain Almohri, Kuwait University
Lotfi ben Othmane, Iowa State University
Madhusudan Singh, Yonsei University
Shiyi Wei, UT Dallas