Announcement and Call for Papers

www.usenix.org/ase18/cfp

ASE '18: 2018 USENIX Advances in Security Education Workshop

August 13, 2018, Baltimore, MD, USA

Sponsored by USENIX, the Advanced Computing Systems Association

The 2018 USENIX Workshop on Advances in Security Education (ASE '18) will be held on Monday, August 13, 2018, in conjunction with the 27th USENIX Security Symposium in Baltimore, MD, USA.

Important Dates

- Full Papers and Demo video submissions due: **Tuesday, May 8, 2018, 11:59 p.m. PDT (no extensions)**
- Notification to paper authors: **Thursday, June 7, 2018**
- Lightning Talk abstracts due: **Wednesday, June 27, 2018, 11:59 p.m. PDT**
- Final paper files due: **Thursday, July 5, 2018**
- Notification about Lightning Talks: **Thursday, July 5, 2018**

Workshop Organizers

Program Co-Chairs

Wu-chang Feng, *Portland State University*
Ashley Podhradsky, *Dakota State University*

Program Committee

Adam Aviv, *US Naval Academy*
Abe Bagilli, *University of New Haven*
Matt Bishop, *UC Davis*
Rakesh Bobba, *Oregon State University*
Glencora Borradaile, *Oregon State University*
Tom Chothia, *University of Birmingham*
Dave Dampier, *University of Texas at Austin*
Melissa Dark, *Purdue*
Kevin Du, *Syracuse University*
Márk Félegyházi, *Budapest University of Technology and Economics CrySyS Lab*
Wai Yi Feng, *University of Cambridge*
Nathan Fisk, *University of South Florida*
Mark Gondree, *Sonoma State University*
Andreas Haggman, *Royal Holloway University of London*
Cynthia Irvine, *Naval Postgraduate School*
Jelena Mirkovic, *University of Southern California Information Sciences Institute*
Zachary N J Peterson, *Cal Poly, San Luis Obispo*
Z. Cliffe Schreuders, *Leeds Beckett University*
Ambareen Siraj, *Tennessee Tech University*
Josh Stroschein, *Dakota State University*

Steering Committee

Adam Aviv, *US Naval Academy*
Matt Bishop, *UC Davis*
Melissa Dark, *Purdue*
Mark Gondree, *Sonoma State University*
Zachary N J Peterson, *Cal Poly, San Luis Obispo*

Overview

The 2018 USENIX Advances in Security Education Workshop (ASE '18) is co-located with the 27th USENIX Security Symposium, and intended to be a venue for cutting-edge research, best practices, and experimental curricula in computer security education.

The workshop welcomes a broad range of paper and demo submissions on the subject of computer security education in any setting (K–12, undergraduate, graduate, non-traditional students, professional development, and the general public) with a diversity of goals, including developing or maturing specific knowledge, skills and abilities (KSAs), or improving awareness of issues in the cyber domain (e.g., cyber literacy, online citizenship). ASE is intended to be a venue for educators, designers, and evaluators to collaborate, share knowledge, improve existing practices, critically review state-of-the-art, and validate or refute widely held beliefs.

Format

ASE is intended to be a venue for informal collaboration and community building. The current program includes:

- A keynote address.
- Sessions for Full Papers: authors accompany these with presentations at the workshop, with time for follow-up discussion.
- Sessions for Demos: authors accompany these with "live lessons" at the workshop, demonstrating a successful or innovative lesson, activity, exercise or tool. Authors are encouraged to share any data sets or files with the ASE community.
- A session for Lightning Talks and community announcements.
- A panel discussion, exploring popular and/or controversial issues in security education.

Rev. 05/14/18

All sessions are intended to stimulate group discussion and impact future work. We encourage attendees to participate in lightning talks, where they can bring attention to new results, distribute materials, or make announcements of interest to the education community (new events, projects, funding opportunities, venues, etc.).

Topics

The core mission of ASE is to disseminate cutting-edge, practitioner-oriented, computer security education research. Specific topics of interest include, but are not limited to:

- Novel pedagogical approaches and experimental curricula
- Outreach and mentorship of groups underrepresented in security
- Education technology research in a security education context
- Tools and techniques for measurement, evaluation, and assessment
- Frameworks and infrastructures supporting education
- Experiences with standards, certifications, and accreditation
- Security games and competitions
- Extramural and extracurricular education programs
- Experience with alternative teaching modalities for computer security, including: MOOCs, flipped classrooms, peer-instruction and inquiry-based instruction, and distance learning
- Security education geared toward non-technical audiences

Full Papers

Full paper submissions should be no more than 8 pages long (excluding references). Full Papers are expected to follow style and format of a typical academic workshop paper for the computer science field, featuring an abstract, introduction, related work, conclusion and references. As a workshop paper, these may highlight early work, in-progress work, lessons-learned, position papers, or program summaries; however, full papers are intended do at least one of the following: highlight some technical solution of merit to the education community, feature some analysis or survey work of value to the education community, or employ some assessment based on community-accepted practices for the scholarship of teaching and learning.

Each Full Paper will be accompanied by a presentation delivered at the workshop by one of the paper's authors (approximately 20–25 minutes in duration).

Demos

We are excited to provide educators with a venue to demonstrate an exercise, problem set, activity, or tool at the workshop. A demo submission should include (i) a link to a demo video submission, (ii) an abstract, and optionally (iii) supplemental materials. Your abstract should be 1–2 pages long, follow the format of all paper submissions, and highlight your work while providing commentary on its value to the security community. Your Demo video submission should feature the tool, technique or curricular materials that will be showcased at the workshop; it should demonstrate the style and tone of the presenter for the demo session. Demo video submissions should be between 3–5 minutes, and accessible via a public link provided during submission. Supplemental materials may include lesson plans (e.g., featuring learning objectives and related materials to help educators reproduce the lesson) or technical descriptions. Supplemental materials for lessons, in particular, may consider paralleling the format of SIGCSE Nifty submissions (http://nifty.stanford.edu/). All supplemental materials should be accessible to reviewers at the time of submission and throughout the review period.

Accepted demo submissions will have a "live lesson" delivered at the workshop by one of the authors (approximately 25–30 minutes in duration with 5 additional minutes for Q&A), but extra time may be afforded during breaks or after sessions for continued exploration. Potential "live lessons" include scaffolded exercises, abbreviated lessons, tool demonstrations, or classroom activities (engaging the workshop audience, either as students or fellow practitioners). They may include a short video of a classroom practice, a live demo of an instructional technique, an interactive exercise with the workshop attendees, a technology demonstration, etc.

Lightning Talks

Lightning Talks highlight fresh ideas, unique perspectives, valuable experiences, and emerging trends in computer security education. Short talks are five-minute presentations on work and ideas not ready or suitable for peer-reviewed publication, but worth sharing to jump-start discussion among and solicit feedback from attendees.

Lightning Talk presentations are five minutes in duration with an additional five minutes for discussion. If you would like to present a Lightning Talk at the event, please email an abstract to ase18chairs@usenix.org. There are no length or content requirements for the talk abstract, but a few sentences describing what you'd like to do or announce, informally, is appropriate.

Paper Submissions

For all submissions, text should be formatted in two columns on 8.5" x 11" paper using 10-point type on 12-point leading ("single-spaced"), with the text block being no more than 6.5" x 9" deep. Text outside the 6.5" x 9" block will be ignored. Submissions need not be anonymized. Submissions must be in PDF and must be submitted via the web submission form linked from the Call for Papers website, www.usenix.org/conference/ase18/call-for-papers.

All accepted submissions will be available online to registered attendees before the workshop. If your paper should not be published prior to the event, please notify production@usenix.org. The papers will be available online to everyone beginning on the day of the workshop. At least one author from every accepted paper must attend the workshop and present.

Simultaneous submission of the same work to multiple venues, submission of previously published work, or plagiarism constitutes dishonesty or fraud. USENIX, like other scientific and technical conferences and journals, prohibits these practices and may take action against authors who have committed them. See the USENIX Conference Submissions Policy for details. Questions? Contact your program co-chairs, ase18chairs@usenix.org, or the USENIX office, submissions-policy@usenix.org.

Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the USENIX ASE '18 website; rejected submissions will be permanently treated as confidential.