



2015 USENIX Summit on Gaming, Games, and Gamification in Security Education

Sponsored by USENIX, the Advanced Computing Systems Association

August 11, 2015, Washington, D.C.

3GSE '15 will be co-located with the 24th USENIX Security Symposium (USENIX Security '15) and take place on Tuesday, August 11, 2015.

Important Dates

- Paper submissions due: **Tuesday, May 5, 2015, 11:59 p.m. PDT**
- Notification to authors: **Tuesday, June 9, 2015**
- Final, camera-ready deadline for applicable submissions: **Tuesday, July 7, 2015**
- Short talk abstracts due: **Tuesday, June 30, 2015, 11:59 p.m. PDT**
- Short talk acceptance notifications: **Tuesday, July 7, 2015**

Workshop Organizers

Program Co-Chairs

Mark Gondree, *Naval Postgraduate School*
Zachary N J Peterson, *Cal Poly, San Luis Obispo*

Program Committee

Peter Chapman, *Carnegie Mellon University*
Julian Cohen, *Flatiron Health*
Tamara Denning, *University of Utah*
Portia Pusey, *National CyberWatch Center*
Adam Shostack

Overview

The 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE), to be co-located with USENIX Security, is designed to bring together educators and game designers working in the growing field of digital games, non-digital games, pervasive games, gamification, contests, and competitions for computer security education. The summit will attempt to represent, through invited talks, paper presentations, panels, and tutorials, a variety of approaches and issues related to using games for security education.

Building upon the success of last year's inaugural 3GSE Summit, this year's mission is to continue to build a broad, interdisciplinary community interested in answering critical, open questions, including:

- What makes a good security game?
- How can games be used to draw students to computer science?
- How do we meaningfully evaluate security games?
- How does one build a game playable by populations with different backgrounds, skill levels, and cultural experiences?

The year's summit welcomes paper submissions on the use of games or game-like approaches to computer security education in any setting (K-12, undergraduate, graduate, non-traditional students, professional development, and the general public). Security education goals may include developing or maturing specific knowledge, skills and abilities (KSAs), or improving awareness of issues in the cyber domain (e.g. cyber literacy, online citizenship). 3GSE is intended to be a venue for educators, designers, and evaluators to collaborate,

to share knowledge, to improve existing practice, to critically review state-of-the-art, and to validate or refute widely held beliefs.

Format

3GSE is intended to be a venue for informal collaboration and community-building. The program will consist of a keynote speaker, paper sessions for both accepted and invited papers discussing new approaches or technologies and reporting on actual experiences while allowing time for follow-on discussion, and a panel discussion and sessions exploring some of the more popular and controversial issues in gaming in security. All sessions are intended to stimulate group discussion and impact future work. We also encourage attendees to participate in the "lightning talk" session, where they are encouraged to bring attention to new results, to present a short video demo of technologies, to distribute games, or to make announcements of interest to the 3GSE community (new events, projects, funding opportunities, venues, etc).

Topics

Specific topics of interest include, but are not limited to:

- **Games**—Experiences with the integration of games for security education and awareness (in the workplace, in the classroom, in extra-curricular programs); any audience may be considered, but especially interesting are CS-major audiences, non-major audiences, K-12 audiences and technically inexperienced adult learners.
- **Gamification**—How do we leverage gamification to meet our pedagogical goals? Experience reports in asynchronous courses, distance learning, and MOOCs are especially welcome.
- **Competitions and CTFs**—How can we maximize the pedagogical value of capture the flag exercises? How do we make competitions easier to design, deploy, and replay while maintaining their appeal and pedagogical quality? How do we design competitions for players with different learning styles and social backgrounds? Can we rigorously investigate issues of practical significance in these games (e.g., approaches to detect cheating, to scoring, to bracket design, to event timing, to gameplay duration, pedagogical evaluation) to arrive at best practices?
- **Outreach**—How can game-based approaches serve to engage populations underrepresented in computer science? What approaches seem most promising, either validated in CS pilot programs or by other fields?
- **Play**—Can we enhance lessons and activities for security education by making these "playful" and/or by leveraging games? When does playfulness succeed, and when does it fail / distract/ lead to misunderstandings?
- **Design**—How can various design elements (e.g., storytelling, narrative, game balance, game flow) serve or inform security

education? How can we ease the “design burden” by leveraging existing capabilities or novel collaborations?

- **Measurement and Methodology**—How do we evaluate games from an educational perspective? What data do we need? How do we collect and analyze the data we need? What approaches from other fields are most useful to validating security games?

Short Talks

This year, 3GSE is introducing a “short talk” submission option. These 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.

Short talk presentations are five minutes in duration with an additional five minutes for discussion. If you would like to present a short talk at the event, please email a talk abstract to 3gse15talks@usenix.org. Short talk abstracts are due June 30th, 2015, and acceptance notifications will be sent July 7th, 2015.

Paper Submission

This year’s paper submission process is open to all. Submissions must be 6–8 pages long including tables, figures, and references. 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.

Submission need not be anonymized. Submissions must be in PDF and must be submitted via the Web submission form, which will be available soon on the 3GSE ’15 Call for Papers Web site.

All accepted papers 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 at www.usenix.org/submissionpolicy for details. Questions? Contact your program co-chairs, 3gse15chairs@usenix.org, or the USENIX office, submissionpolicy@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 3GSE ’15 Web site; rejected submissions will be permanently treated as confidential.

