# ScAINet '20: 2020 USENIX Security and AI Networking Summit

## August 10, 2020, Boston, MA, USA

*Sponsored by USENIX, the Advanced Computing Systems Association*

The 2020 USENIX Security and AI Networking Summit (ScAINet '20) will be co-located with the 29th USENIX Security Symposium and will take place August 10, 2020, at the Boston Marriott Copley Place in Boston, MA, USA.

## Important Dates

- Submissions due: Friday, April 10, 2020, 8:59 pm PDT
- Notification to submitters: Friday, June 5, 2020

## Summit Organizers

### Program Co-Chairs

Richard Harang, *Sophos*
Carmela Troncoso, *École Polytechnique Fédérale de Lausanne (EPFL)*

### Program Committee

Sadia Afroz, Avast
Battista Biggio, University of Cagliari
Nicholas Carlini, Google
Lorenzo Cavallaro, King's College London
Tudor Dumitras, University of Maryland
Kassem Fawaz, University of Wisconsin—Madison
Seda Gurses, Technische Universität Delft
Ariel Herbert-Voss, OpenAI
Luca Melis, Amazon
Anita Nikolich, Illinois Institute of Technology
John Seymour, Salesforce
Shruti Topli, Microsoft Research
Cody Wild
Aleatha Wood, Humu
Ben Zhao, The University of Chicago

### Steering Committee

Hyrum Anderson, *Endgame*
David Freeman, *Facebook*
Andrew Gardner, *Symantec*
Rachel Greenstadt, *New York University*
Casey Henderson, *USENIX Association*
Wenke Lee, *Georgia Institute of Technology*
Prateek Mittal, *Princeton University*
Aleatha Parker-Wood, *Humu*

## ScAINet: At the Frontier of AI, ML, and Cybersecurity

ScAINet is a single-track summit of cutting edge and thought inspiring talks covering a wide range of topics at the intersection of ML/AI, security, and privacy. The format will be similar to Enigma, but with a focus on security and AI. Our goal is to explore the emerging landscape of machine learning security and privacy applications and implications. We take a broad view of the field, with an eye to anticipating the risks and benefits of these technologies—including externalities such as privacy risks, disparate impact, latent biases; and offensive uses of machine learning, including traditional 'red teaming', construction of intentionally biased models, and the exploitation of biases and flaws in machine learning algorithms for malicious effect. We expect to build a rich and vibrant community which brings academia and industry together under the same roof to build on successes and address the challenges. We view diversity as a critical enabler for this goal and actively work to ensure that the ScAINet community encourages and welcomes participation from all employment statuses and sectors, racial and ethnic backgrounds, nationalities, and genders.

ScAINet is committed to fostering an open, collaborative, and respectful environment. ScAINet and USENIX are also dedicated to open science and open conversations, and will make all talk media freely available on the USENIX website. For more information, view the USENIX Event Code of Conduct and USENIX Event Guidelines for Speakers at www.usenix.org/conferences/coc.

## Call for Speakers

We solicit proposals for original talks. All talks will be 25 minutes long, followed by 5 minutes for Q&A. The program committee will select presentations that illuminate big ideas and problems, that clearly describe the state of the art, that pose novel problems or challenges, and that enrich or provoke important discussion. Ideal talks will address significant problems or advances within the intersection of machine learning and security, and contain sufficient technical depth to enable deep discussion while still being accessible to a broad audience. Our expected attendees include, but are not limited to, researchers from industry and academia, data scientists, engineers, security-oriented managers, and security analysts.

Our program features a diversity of topics and perspectives. We're interested in talks that cover new insights into popular topics (e.g., malicious artifact detection, differential privacy, fraud, and fake account detection) as well as emerging or more niche areas (e.g., representation learning for security data, economic analysis of the threat landscape, new applications of privacy-enhancing technologies to machine learning, adversarial machine learning for user protection, automated analysis and reverse engineering). We welcome talks that share pragmatic approaches and those that explain high-risk research. For examples of previous topics, please see the ScAINet '19 program at www.usenix.org/conference/scainet19/conference-program.

ScAINet emphasizes presentation quality, so we are looking for great explainers: those who can describe complex topics and convey their excitement while maintaining the integrity of science.

## Submission Guidelines

To submit a talk, please prepare the following information and submit it to the ScAINet '20 submission system linked from the Call for Participation web page. Both presenters and organizers may withdraw or decline proposals for any reason, even after initial acceptance. Speakers must submit their own proposals; third-party submissions, even if authorized, will be rejected.

### Speaker Information

- Speaker Name
- Speaker Title and Company/Affiliation (if applicable)
- Speaker pronouns or preferred form of address
- Speaker Email Address
- Speaker Bio
- Link to a video of a previous talk (must not be on the same topic; links to private/unlisted videos okay)
- [OPTIONAL] Social networking handle(s)
- [OPTIONAL] Homepage

If accepted, we will ask you to supply the following additional info:

- A high resolution headshot

Single-speaker talks tend to be higher quality and are thus strongly preferred. If you wish to submit a talk given by multiple speakers, please make this clear in your submission, and make the case for why more than one speaker will make for a better talk as well as how multiple speakers will fit within the 25-minute limit.

### Presentation Information

- Talk Title
- Presentation Summary. Please submit in a widely readable format, such as PDF or plain text. Please include (1) the core idea, (2) why it matters, and (3) a brief summary of prior work either by yourself or in the field. The approximate total length of the presentation summary should be 1–2 pages. We encourage participants to use the following format:
  - An abstract of the talk. We will use this to understand technical merit and, if selected, for promotional purposes.
  - A single main takeaway point for the talk.
  - An outline for the talk.
- Are you currently submitting this topic to any other conferences held prior to ScAINet? Or has a version of this presentation been given or accepted to any other venue or conference? If so, explain how this submission is different from your prior work.

### Questions?

Please contact scainet20chairs@usenix.org.