

Preface

The Conference on Applied Machine Learning in Information Security (CAMLIS) is a venue that gathers researchers and practitioners to discuss applied and fundamental research on machine learning in information security. We invited paper and/or extended abstract submissions on the direct application or adaptation of statistics, machine learning, deep learning, and data science to infosec relevant areas. We particularly encouraged submissions that include analytic and/or predictive themes.

The 2021 iteration of CAMLIS was held as a two-day event on November 4-5, 2021 in Arlington, Virginia at the Sands Capital Management. Overall, 16 were accepted as full talks and six were accepted as lightning talks. Accepted full talks had presentations of 20 minutes and lightning talks had presentations of 10 minutes each. Four of the 16 accepted full talks have a combination of authors (i.e., have an author team that includes an academic and industry entity and/or independent researcher).

- Eight of the 16 full papers are from industry. Top contributors are Two Six Technologies (three papers), Mandiant (two papers), Sophos (two papers). MITRE, Booz Allen Hamilton, DEFCON AI Village, Duo, Arraya, CEMPRA, Royal Bank of Canada also all made contributions.
- Four of the 16 accepted full papers are strictly from academia (RIT, Weight State, Imperial College London, and University College Dublin). Other contributing academic institutions (that partnered with industry) include the University of Maryland Baltimore County, Stony Brook, University of New Haven.
- With regards to lightning talks, contributors were either industry, academia, or independent researcher – no accepted lighting talk had a combination. Top contributors for lighting talks were Mandiant (two), Sophos (one), Duo (one). Academic institutions contributing lightning talks included RIT, Manchester Metro University, Cranfield University, and University of East Anglia
- All acceptances considered Mandiant had the most (four), followed by Sophos (three), Duo (two), Imperial College (two), and RIT (two).

Full talks were grouped into one of the following themes: (1) Malware Analysis, (2) Adversarial AI, (3) Netflow Analysis, Anomaly Detection, and Vulnerability Management, or (4) AI-enabled Incident Report Analytics. Rounding out the program were two excellent keynote addresses. The first was from Katie Nickels from Red Canary and SANS Institute, and the second was from Dr. Nicolas Papernot from the University of Toronto. CAMLIS has a mix of academic and industry participation, and of the accepted talks 9 were accepted as papers for the proceedings.

We wish to thank all of the program committee members, reviewers, authors, and local arrangers for their contributions to CAMLIS 2021. We also gratefully acknowledge the support of our sponsors, including Amazon, Microsoft, Elastic, Mandiant, Booz Allen Hamilton, and Sands Capital.

Edward Raff, Hyrum Anderson, and Sagar Samtani