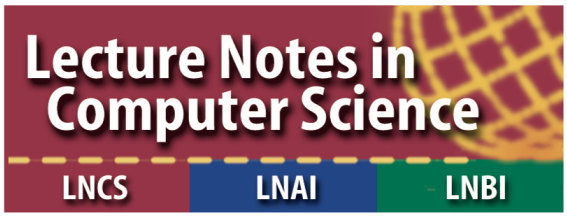
Security in Machine Learning and its Applications (SiMLA 2021)

ACNS 2021



21-24 June 2021 - Kamakura, Japan

(Co-located with ACNS 2021)

Important Dates

- Submission deadline: March 25, 2021 (Anywhere on Earth)

Workshop Background

As the development of computing hardware, algorithms, and more importantly, availability of large volume of data, machine learning technologies have become a increasingly popular. Practical systems have been deployed in various domains, like face recognition, automatic video monitoring, and even auxiliary driving. However, the security implications of machine learning algorithms and systems are still unclear. For example, people still lack deep understanding on adversarial machine learning, one of the unique vulnerability of machine learning systems, and are unable to evaluate the robustness of those machine learning algorithms effectively. The other prominent problem is privacy concerns when applying machine learning algorithms, and as general public are becoming more concerned about their own privacy, more works are definitely desired towards privacy preserving machine learning.

Motivated by this situation, this workshop solicits original contributions on the security and privacy problems of machine learning algorithm and systems, including adversarial learning, algorithm robustness analysis, privacy preserving machine learning, etc. We hope this workshop can bring researchers together to exchange ideas on edge-cutting technologies and brainstorm solutions for urgent problems derived from practical applications.

Topics

Topics of interest include, but not limited, to followings:

- Adversarial Machine Learning
- Robustness Analysis of Machine Learning Algoritms
- Detection and Defense to Training Data set Poison attack
- Privacy Preserving Machine Learning
- Watermarking of Machine Learning Algorithms and Systems
- Attack and defense of face recognition systems
- Attacks and defense of voice recognition and voice commanded systems
- Attacks and defense of machine learning algorithms in program analysis
- Malware identification and analysis
- Spam and phshing email detection
- Vulnerability analysis

Submissions Guidelines

Authors are welcome to submit their papers in following two forms:

- **Full papers** that present relatively mature research results related to security issues of machine learning algorithms, systems, and applications. The paper could be attack, defense, security analysis, surveys, etc. The submissions for this type must follow the original LNCS format (see http://www.springeronline.com/lncs) with a page limit of 18 pages (including references) for the main part (reviewers are not required to read beyond this limit) and 25 pages in total.

- **Short papers** that describe an on-going work and bring some new insights and inspiring ideas related to security issues of meaching learning algorithms, systems, and applications. Short papers will follow the same LNCS format as full paper (http://www.springeronline.com/lncs), but with a page limit of 9 pages (including references).

The submissions must be anonymous, with no author names, affiliations, acknowledgement or obvious references. Once accepted, the papers will appear in the formal proceedings. Authors of accepted papers must guarantee that their paper will be presented at the conference and must make their paper available online. There will be a best paper award.

- **Special Note to Springer LNCS Proceedings**

Authors should consult Springer’s authors’ guidelines and use their proceedings templates, either for LaTeX or for Word, for the preparation of their papers. Springer encourages authors to include their ORCIDs in their papers. In addition, the corresponding author of each paper, acting on behalf of all of the authors of that paper, must complete and sign a Consent-to-Publish form, through which the copyright for their paper is transferred to Springer. The corresponding author signing the copyright form should match the corresponding author marked on the paper. Once the files have been sent to Springer, changes relating to the authorship of the papers cannot be made.

EasyChair System will be used for paper submission.

Please submit your paper via the following link EasyChair System.

Workshop Organizers

Sudipta Chattopadhyay	Singapore University of Technology and Design	Workshop Chair
Sakshi Udeshi	Singapore University of Technology and Design	Web Chair

Program Committee

Dr John Doe	University of Atlantis