MIT LINCOLN LABORATORY
The Bulletin
News, events, and notices transmitted weekly
December 3, 2021

Technology Office Announces Winners of the FoolMe Hackathon

Awards and Recognition | Lincoln Laboratory

On 29 October, the Technology Office wrapped up the FoolMe Challenge, a hackathon that was part of the Laboratory's ongoing effort to observe trends in the manipulation of information, anticipate the broader implications to national security, and develop mitigation strategies.

Throughout the hackathon, which was held virtually from 15–22 October, each team worked to develop new methods of detecting manipulated images in six datasets that had been modified using different data poisoning techniques. The teams were judged based on the correct identification of manipulated images and the novelty of their problem-solving approach.

The overall winner of the hackathon was team VeritaSerum: Michael Benton, Group 39; Dr. Byung Gu Cho, Group 37; Ashok Kumar, Group 52; Trang Nguyen, Group 52; and Dr. Michael Yee, Group 01.

"While many of the teams approached the challenge by designing several distinct solutions that were tailored to each individual dataset, the overall winning team developed a more general algorithm that worked well across multiple datasets," said Olivia Brown, Artificial Intelligence Technology, Group 01, and an organizer of the event. "They had strong performance, ranking second on the leaderboard, and their approach was determined to be the most creative and generalizable according to a poll of the audience."

The Technology Office's FoolMe Challenge was held virtually from 15–22 October.

VeritaSerum also won the award for best team name, while Kingsfoil won the top of the leaderboard award, and You Can't Fool Me won best perseverance.

"I hope that those who participated in the challenge were able to learn something new, meet people they don't normally get to interact with, and have fun," said Andrea Scouras, Structural and Thermal-Fluids Engineering, Group 74.

Overall, the hackathon has helped the Technology Office identify potential new ways to increase the robustness of the Laboratory's machine learning systems to poisoning attacks.