CT Advanced Computing Center (CACC) Security Seminar Series 2024

Speaker: Caleb Manicke - University of Connecticut
Date: December 11, 2024
Time: 11:15 12:30pm
Location: ITE 336
Meeting Link : https://uconn-cmr.webex.com/uconn-cmr/j.php?MTID=m4d36ddf4d36edd727aa04331cdb7d7f6
Meeting number (access code): 2633 368 4613
Meeting password: MqmJMizs533

Busting the Paper Ballot: Voting Meets Adversarial Machine Learning [In-person]

We show the security risk associated with using machine learning systems in the application of United States election systems. Counting votes in a paper ballot involves a binary classifier that decides whether a \emph{mark} does or does not appear on a \emph{bubble} associated to an alternative in a contest on the ballot. We show that classification techniques like support vector machines, basic convolutional neural networks, ResNets, and transformers are vulnerable to input manipulation, commonly referred to as adversarial examples, both in the virtual and physical world where they are printed and scanned. Adversarial examples are challenging to produce in the physical domain but remain a viable attack vector that can change the outcome of election races with small margins of victory.

CACC UCONN