DISTINGUISHED WEBINAR SERIES IN ARTIFICIAL INTELLIGENCE AND CYBER SECURITY

Revealing the gap between Research and Practice in Adversarial Machine Learning

Featuring Giovanni Apruzzese, Ph.D., Assistant Professor, University of Liechtenstein

Abstract

This talk is an extended version of the presentation of a paper I co-authored---presented at the First IEEE Conference on Secure and Trustworthy Machine Learning (IEEE SaTML) on February 2023. Specifically, the talk focuses on the interplay between "practical" cybersecurity, and the research area known as "adversarial machine learning". Despite ML being increasingly deployed in our world, practitioners still seem not to care about the security of ML. The talk will hence shed light on the root causes underpinning the disconnection between research and practice in this context. After providing (new) evidence about the lack of attacks ("in the wild") conforming to the threats portrayed in research papers, I will discuss two (original) case studies from the real world, explaining the difficulties that real attackers must face but which are often neglected by scientific literature. Then, I will showcase some "inconsistencies" that affect the terminology adopted in recent research, which can be detrimental for future endeavors. Finally, I will present some recommendations---jointly written by researchers and practitioners---that can help bridging the gap between research and practice in the context of adversarial ML. Alongside all these findings, however, the talk will also tell the "backstory" that led to the writing and publication of our paper, since it will be particularly inspirational for "young" researchers.

Biography:

Giovanni Apruzzese is an Assistant Professor within the Hilti Chair of Data and Application Security at the University of Liechtenstein since 2022 and was previously a PostDoc at the same institution since 2020. He received the PhD Degree and the Master's Degree in Computer Engineering (summa cum laude) in 2020 and 2016 respectively at the Department of Engineering "Enzo Ferrari", University of Modena and Reggio Emilia, Italy. In 2019 he spent 6 months as a Visiting Researcher at Dartmouth College (Hanover, NH, USA) under the supervision of Prof. V.S. Subrahmanian. His research interests involve all aspects of big data security analytics with a focus on "practical" machine learning, and his main expertise lies in the analysis of Network Intrusions, Phishing, and Adversarial Attacks. He is also intrigued by the offensive capabilities of artificial intelligence.

.

DATE:
Thursday, March 30th, 2023

TIME:
11-11:45 a.m. CST

LOCATION:
Virtual

Registration LINK:
Get Webinar LINK via Email

The **Distinguished Speaker Webinar Series** is aimed to advance the state-of-the-art concepts and methods in artificial intelligence and cyber security areas. The series is jointly hosted by the Center for Cyber Security Research (C2SR), the Artificial Intelligence Research (AIR) Initiative, and the School of Electrical Engineering and Computer Science (SEECS) at the University of North Dakota College of Engineering & Mines with support from University of Minnesota, North Dakota State University, University of Miami, Texas A&M Kingsville, University of Connecticut and West Virginia University.

For inquires please contact UND.C2SR@und.edu

C2SR CENTER FOR CYBER SECURITY RESEARCH · AIR Initiative · UND UNIVERSITY OF NORTH DAKOTA COLLEGE OF ENGINEERING & MINES · UNIVERSITY OF MINNESOTA · UNIVERSITY OF MIAMI · University of Connecticut · NDSU NORTH DAKOTA STATE UNIVERSITY · TEXAS A&M UNIVERSITY KINGSVILLE · WestVirginiaUniversity.