Partnership and Proactive Cybersecurity Training (PACT)

PI: Salim Hariri, PhD
Co-PI: Tamal Bose, PhD and Gregory Ditzler, PhD
Coordinator: Nancy Emptage
Graduate Assistant Mentors: Alex Berian, Srishti Gupta, and Shalaka Satam
Sponsors: U.S. Department of Energy (DoE) and University of Arizona Graduate College

Asha Anderson

Computer Science at Howard University

Mentored by Dr. Salim Hariri and Ms. Shalaka Satam
(Electrical and Computer Engineering)

Intrusion Detection System Project

ABSTRACT: The quality level of technology increases annually as our civilization works to improve our way of living. Computers become prone to an ample number of cyber-attacks that could potentially harm the user and their productivity on their device. The creation of Intrusion detection systems and Intrusion Prevention systems are to decrease the volume of cyber-attacks by increasing cyber security within our computers. This project demonstrates how intrusion detection systems and Intrusion prevention systems work, as well as how they benefit computer users by analyzing network traffic and sending signals when abnormal behavior is detected. The goal of this paper is to explain how IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems) provide an extra layer of protection against various cyber-attacks. Finally, I will discuss how I used SNORT to combat and identify cyber-attacks like Ransomware attacks and Password Cracking attacks.

Emily Cawley

Computer Science, Information Science & eSociety at

University of Arizona

Mentored by Dr. Tamal Bose, and Mr. Alex Berian (Electrical and Computer Engineering)

Partner: Kelly Morgan

Blind Equalization for Nullifying Adversarial Filters

ABSTRACT: The Partnership for Proactive Cybersecurity Research and Training (PACT) provides students with research opportunities in the field of cybersecurity. The Wireless Cybersecurity research team investigated the use of neural networks to classify radio modulation signals. Regarding neural networks, the team also investigated the creation of adversarial attacks on radio signal data and their ability to both fool neural networks and increase neural network accuracy. Finally, the team explored the use of blind equalization in rendering the Gradient Ascent Filter (GAF) obsolete, achieved through construction of multiple blind equalization filters adjusted to a wide range of different radio modulation schemes.

Megan Herzog

Computer Science, Statistics, and Data Science at University of Arizona

Mentored by Dr. Gregory Ditzler and Ms. Srishti Gupta (Electrical and Computer Engineering)

Partner: Joe Liang

Analyzing Adversarial Attacks on Tabular Data

ABSTRACT: Machine Learning is a relatively new field in the area of technology, yet the growing need for data mining and automation has resulted in its explosive popularity and usage in the past decade. Applications of machine learning are everywhere, from fields that have existed for a while such as spam detection to emergent areas including self-driving cars or virtual assistants. Due to the increasing reliance on artificial intelligence, we need to understand which adversarial attacks have the greatest impact on a classifier's performance. In addition, while the majority of attacks are designed for images, many applications such as finance and cyber security require tabular data, a field with limited existing research. Thus, in this work, we explore the transferability of attacks on tabular data by observing the impact under the lens of performance parameters like Kullback–Leibler (KL) divergence, Area Under the Receiver Operating Characteristics (AUC)score, and accuracy of a classifier.

Joe Liang

Electrical and Computer Engineering at University of Arizona

Mentored by Dr. Gregory Ditzler and Ms. Srishti Gupta (Electrical and Computer Engineering)

Partner: Megan Herzog

Analyzing Adversarial Attacks on Tabular Data

ABSTRACT: Machine Learning is a relatively new field in the area of technology, yet the growing need for data mining and automation has resulted in its explosive popularity and usage in the past decade. Applications of machine learning are everywhere, from fields that have existed for a while such as spam detection to emergent areas including self-driving cars or virtual assistants. Due to the increasing reliance on artificial intelligence, we need to understand which adversarial attacks have the greatest impact on a classifier's performance. In addition, while the majority of attacks are designed for images, many applications such as finance and cyber security require tabular data, a field with limited existing research. Thus, in this work, we explore the transferability of attacks on tabular data by observing the impact under the lens of performance parameters like Kullback–Leibler (KL) divergence, Area Under the Receiver Operating Characteristics (AUC)score, and accuracy of a classifier.

Kelly Morgan

BAS Information Technology at Navajo Technical University

Mentored by Dr. Tamal Bose, and Mr. Alex Berian (Electrical and Computer Engineering)

Partner: Emily Cawley

Blind Equalization for Nullifying Adversarial Filters

ABSTRACT: The Partnership for Proactive Cybersecurity Research and Training (PACT) provides students with research opportunities in the field of cybersecurity. The Wireless Cybersecurity research team investigated the use of neural networks to classify radio modulation signals. Regarding neural networks, the team also investigated the creation of adversarial attacks on radio signal data and their ability to both fool neural networks and increase neural network accuracy. Finally, the team explored the use of blind equalization in rendering the Gradient Ascent Filter (GAF) obsolete, achieved through construction of multiple blind equalization filters adjusted to a wide range of different radio modulation schemes.