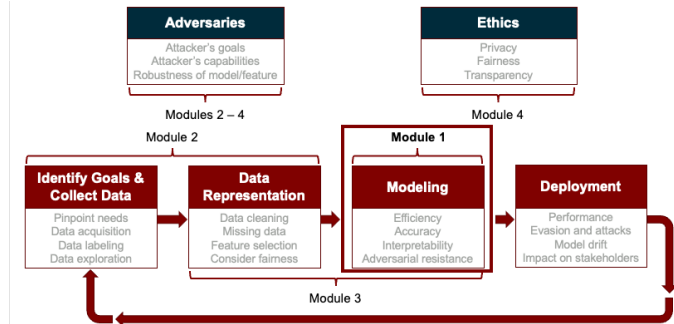
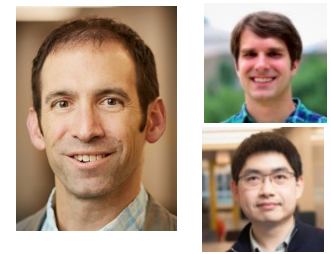


EAGER: SaTC-EDU: Training Mid-Career Security Professionals in Machine Learning and Data-Driven Cybersecurity

Nick Feamster, Yuxin Chen, Blase Ur, University of Chicago

<https://professional.uchicago.edu/lp/professional-education/machine-learning-cybersecurity/rfi>
<https://nprint.github.io/>



Challenge

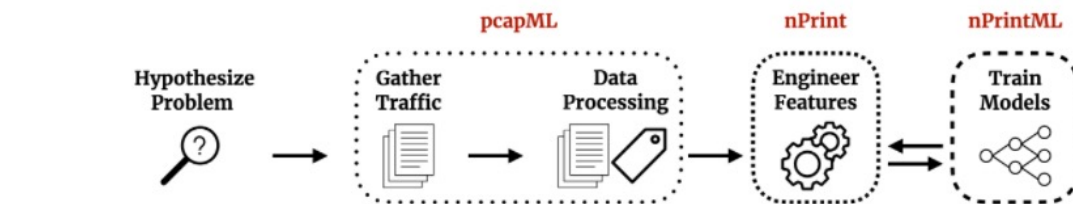
Advancement and re-skilling the United States cybersecurity workforce through large-scale, online training in data-driven and ML methods is critical for keeping the country secure and the workforce competitive.

Solution

The project team will address this critical need by developing curricula for large-scale, online training of mid-career security professionals who aim to develop the skills to apply both conventional and cutting-edge ML tools to cybersecurity.

Impact

- (1) online curricular development in data-driven security, to provide mid-career professionals foundations and practical tools for applying these methods to practical problems in network security;
- (2) formative research to elicit desired skills and use cases from the workforce;
- (3) modular public toolkits and datasets for use in both courses and as resources for professionals to apply in practical settings; and
- (4) augmented teaching materials, tailored to individual students, based on intelligent tutoring systems.



Applied Machine Learning for Networking

Noah Apherpe and Nick Feamster

Table of Contents

- Chapter 1: Introduction
- Chapter 2: Identifying Problems and Examples
 - Attack Detection
 - Anomaly Detection
 - Performance Inference and Diagnosis
 - Performance Prediction
 - Programming
 - Homeworks
- Chapter 3: Network Measurement
 - Metrics: What to Measure
 - Active Measurement
 - Passive Measurement
 - From Data to Analysis
- Chapter 4: Machine Learning Pipelines
 - Data Preparation
 - Model Training
 - Model Evaluation
 - Supervised Example: IPNetML
 - Unsupervised Example: anomaly
- Chapter 5: Supervised Learning Models
 - Non-Parametric Models
 - Linear Models
 - Regularization
 - Ensemble Methods
 - Tree-Based Models
 - Ensemble Methods
 - Deep Learning
- Chapter 6: Unsupervised Learning
- Chapter 7: Automating Machine Learning
- Chapter 8: Privacy, Legal, & Ethical Concerns
- Chapter 9: Looking Ahead
- About This Book
- About The Authors



The pcapML Benchmarks

The goal of this repository is to centralize, standardize, and track the progress of techniques in network traffic analysis for a variety of tasks. This repository was modeled after the incredibly successful `nllprogress` repository.

Contributing

Results

- Results reported in published papers are preferred; an exception may be made for influential preprints.

Adding a New Result

If you would like to add a new result, you can just click on the small edit button in the top-right corner of the file for the respective task.

This allows you to edit the file in Markdown. Simply add a row to the corresponding table in the same format. Make sure that the table stays sorted (with the best result on top). After you've made your change, make sure that the table still looks ok by clicking on the "Preview changes" tab at the top of the page. If everything looks good, go to the bottom of the page to commit the change.

Add a name for your proposed change, a description, and indicate that you would like to "Create a new branch for this commit and start a pull request", and click on "Propose file change".