GSAW 2020 Tutorial L:

Practical Data Exploitation with Machine Learning for Cyber Defense

Length: Half day

Overview:
In today's changing space environment and the rapidly approaching future, space ground systems will be prime targets for adversaries and chaotic actors to attack in the cyber domain. As of today, there are limited characterizations of the threats, vulnerabilities and mitigations for the space segment and the space to ground interfaces. Aerospace has developed state of the art prototypes to address these issues.

This tutorial will encompass the entire stack of implementing such a solution from decoding data, streaming data, dashboards and visualization, rule-based intrusion detection systems, and the application of machine learning to this domain. Specific attack vectors will be covered. There will be a briefing portion where attendees will learn techniques they can take back and use on a daily basis to defend systems against cyber attacks. The briefing portion will be followed by an optional hands-on lab session where participants can try out some of the techniques they learn with instructors . Come for the machine learning; leave with the ability to protect your ground systems.

Those choosing to participate in the lab session should come prepared to write Python on their network-capable laptop. All data and tools necessary will be available via web browser on the local network. Those who do not wish to write code may observe others.

In this tutorial attendees will work attend a briefing with a Q&A based discussion section, followed by an optional hands-on lab section. Those choosing to participate in the lab session should come prepared to write Python on their network-capable laptop. All data and tools necessary will be available via web browser on the local network. Those who do not wish to write code may observe others.During the lab, attendees will work to protect a simulated spacecraft system, using both machine learning and more traditional rule-based methods.

The tutorial will center on three distinct applications of cyber security for space systems. Cyber security and machine learning practitioners will outline each of the attack vectors to secure and teach attendees one possible approach to implementing machine learning based cyber defenses. The first topic discussed will be using unsupervised deep learning techniques to detect a malicious actor within the system attempting to command the spacecraft. The second topic covered will cover utilizing machine learning for telemetry anomaly detection and will build upon what is learned during the first section of the tutorial. Preprocessing techniques specific to telemetry will be covered and attendees will discuss possible assumptions to be made dependent upon the ground system. The final section of the tutorial will cover anomalous network traffic detection using machine learning in two different ways, one supervised, and one unsupervised.

Following the briefing of the three applications of machine learning for ground system cyber security, a collaborative discussion will be held amongst the attendees and tutorial leads.

The optional hands-on lab will take place after the briefing. During the lab, attendees will work with simulated data in a provided lab environment on preprocessing techniques, streaming data, and implementing a deep learning approach for cyber command anomaly detection.

Instructors: Douglas Woodward and Nicholas Cohen, The Aerospace Corporation

Biographies:
Doug Woodward is a machine learning researcher and practitioner with a keen interest in the space domain. After working as a Software Engineer in the avionics industry, he graduated with his M.S. in Computational and Data Science from Chapman University where he authored his thesis on generating

light curves with variational autoencoders at the Machine Learning and Assistive Technologies lab. Since joining Aerospace, he has worked towards applying machine learning to a portfolio of space applications. Among his research interests are unsupervised learning, computer vision, anomaly detection, and generative models.

Nick Cohen is a cyber security expert with over a decade of experience in the field. Nick works in a range of areas including defensive cyber operations, spacecraft cybersecurity, software assurance, and penetration testing. Prior to joining Aerospace, Nick operated his own Internet Service Provider and learned how to defend servers against attackers on the Internet. Nick has a bachelor's degree from Carnegie Mellon University a master's degree in Electrical and Computer Engineering from Georgia Tech.

Description of Intended Students and Prerequisites:
Part 1 Presentation: An interest in cybersecurity, machine learning, and ground systems is all that is required.

Part 2 Lab: Python programmers with a laptop having network access (WiFi or ethernet), and a modern web browser (Firefox or Chrome recommended). Some experience with data science libraries such as numpy, keras, and tensorflow is encouraged.

What can Attendees Expect to Learn:
Come for the machine learning; leave with the ability to protect your ground systems.