Title: ANALYSIS OF REMOTE TRIPPING COMMAND INJECTION ATTACKS IN INDUSTRIAL CONTROL SYSTEMS THROUGH STATISTICAL AND MACHINE LEARNING METHODS

In the past decade, cyber operations have been increasingly utilized to further policy goals of state-sponsored actors to shift the balance of politics and power on a global scale. One of the ways this has been evidenced is through the exploitation of electric grids via cyber means. A remote tripping command injection attack is one of the types of attacks which could have devastating effects on the North American power grid. To better understand these attacks and create detection axioms to both quickly identify and mitigate the effects of a remote tripping command injection attack, a dataset comprised of 128 variables (primarily synchrophasor measurements) was analyzed via statistical methods and machine learning algorithms in RStudio and WEKA software respectively. While statistical methods were not successful due to the non-linearity and complexity of the dataset, machine learning algorithms surpassed accuracy metrics established in previous research given a simplified dataset of the specified attack and normal operational data. This research allows future cybersecurity researchers to better understand remote tripping command injection attacks in comparison to normal operational conditions. Further, an incorporation of the analysis has the potential to increase detection and thus mitigate risk to the North American power grid in future work.

Major: Modeling and Simulation

Educational Career:
Bachelor's of Foreign Languages, BS, 2008, United States Military Academy

Committee in Charge:
Bruce D. Caulkins, Chair, Modeling and Simulation
R. Paul Wiegand, Co-Chair, Modeling and Simulation
Scott Lathrop, Modeling and Simulation

Approved for distribution by Bruce D. Caulkins, Committee Chair, on June 1, 2018.

The public is welcome to attend.