NPS Defense Energy Program Presents:

DEFENSE ENERGY SEMINAR

WWW.NPS.EDU/ENERGY

Non-Traditional Attack Surfaces to CIP and IIOT networks

20 July 2018 – ME Auditorium – 1300

With Guest Lecturer Mr. Aaron Fansler

Founder, AMPEX Information Systems

Mr. Aaron Fansler

Abstract:

Mr. Fansler will discuss the use of machine learning in cyber security. Some significant steps have been made in the I.T. world but not in the O.T. world. The only advances come from the attacker's side where they are now getting smarter and faster. Their success is accomplished by implementing machine learning algorithms.

Machine learning is a branch of computer science aimed at enabling computers to learn new behaviors based on empirical data. The goal is to design algorithms that allow a computer to display behavior learned from past experience, rather than human interaction. Machine learning is a rapidly developing field at the intersection of statistics, computer science, and applied mathematics, and it is having transformative impact across the engineering and natural sciences.

In the past, Machine Learning has not had as much success in cyber security as in other fields. Many early attempts struggled with problems such as generating too many false positives, which resulted in mixed attitudes towards it. Some have argued that that while machine learning is very good at finding similarities, it is less successful at finding anomalies, and therefore, not suited to Cyber Security. On the other hand, cybersecurity is "basically broken," and machine learning is one of the few "beacons of hope." Mr. Fansler will present his opinion of the latter.

Machine learning will enable 24/7/365 monitoring of larger data loads. It will still require human interaction and intervention. Machine learning will require tuning and lots of learning in order to accurately filter real attacks from what appear suspicious but are actually benign activity. It will complement traditional defenses to create a more multi-layered defense. It is inevitable that this is where the future of cyber security is.

Ampex's objective is to design, develop, and demonstrate the use of distributed machine learning techniques in a mesh network to optimize sharing of Graphics Processing Units (GPUs) across platforms which will will provide a cyber-capability created specifically for control systems in the form of a high speed, high capacity, rugged computer devices, which can detect, define, analyze, and mitigate cyber threats and vulnerabilities.

Abridged Biography:

Mr. Aaron A.D. Fansler specializes in studying and evaluating critical infrastructures such as the electric power grid, and water and POL pipelines for potential vulnerabilities and critical interdependencies. Since 2002, Aaron has worked in the arena of assessing and exploiting potential vulnerabilities with Industrial Control Systems (ICS), Smart Grids, and Microgrids.

Recently, Aaron has developed and received a provision patent for his SCADA Network Independent Endpoint Protection (SNIEPR) tool which is a first of its kind ICS defensive capability.

Aaron has extensive working experience and business relationships with DARPA, DOE, AFRL, NGB ARPA, NSA, and other US intelligence organizations. These organizations include DHS, U.S. Army, U.S. Air Force, and commercial organizations such as Areva, Lubbock Power & Light, Florida Power & Light, Siemens, Kinder Morgan, Electric Reliability Council of Texas (ERCOT), and Saudi Aramco and the country of Kuwait. Aaron has been called upon to provide subject matter expert testimony and guidance to senior-level policymakers in U.S. Congress, and also at the State, and local levels.

Prior to becoming the Chief Technologist for AIS, Aaron worked for Northrop Grumman Aerospace Systems as a Program Manager where he led Research and Development (R&D) efforts on cyber network operations (CNO) capabilities for ICS devices. Before that, Aaron was a member of the Technical Staff in the National Security Division at the Pacific Northwest National Laboratory (PNNL), where he was a member of the Department of Energy's Field Intelligence Element (FIE). Aaron also worked for AT&T Government Solutions where he supported the USAF with their offensive cyber efforts for Computer Network Operations. Prior to that Aaron served 9 ½ years in both the Air Force and Army.

Aaron earned his Bachelor's degree in Applied Mathematics from the University of Colorado. He has earned two Master's degrees, one from Capitol College in Information Assurance and Computer Security, and the other from the University of Texas. He is currently working on his Ph.D., in Information Assurance. Aaron also holds the Certified Ethical Hacker (CEH), Certified SCADA Security Architect (CSSA), Certified Hacking Forensics Investigator (CHFI), and Certified Penetration Tester certifications.

NAVAL
POSTGRADUATE
SCHOOL