HACSAW: A Trusted Framework for Cyber Situational Awareness

Submitted by Katie Dey on Sat, 03/10/2018 - 5:25pm. Contributors:
William GlodeckLeslie Leonard

BIOS

William Glodek is currently President of BreakPoint Labs - a cybersecurity service provider supporting Federal and Commercial customers. He previously served as a computer scientist and Network Security Branch Chief at the US Army Research Laboratory. Mr. Glodek is the creator and developer of Dshell, an open source Python-based network forensics analysis framework that has been extensively used in the Law Enforcement and Counterintelligence agencies since 2009. Mr. Glodek's research includes network forensics, digital forensics and incident response, and the application of machine learning methods in the cybersecurity domain. Mr. Glodek received a commendation from the Director of the Federal Bureau of Investigation in 2011 for technical contributions and support during a joint investigation. He holds a MS in Computer Science obtained from Florida State University in 2008.

ABSTRACT

The HPC Architecture for Cyber Situational Awareness (HACSAW) was established by the Department of Defense (DoD) High Performance Computing Modernization Program (HPCMP) to combine a rich computational environment with operationally relevant data to perform cutting edge cybersecurity research that will increase HPCMP's current and predictive understanding of cyberspace on the Defense Research and Engineering Network (DREN). The data repository created by this unique environment includes the collection of unclassified data sources from the edge of the network (i.e., Internet Access Points) down to the host-level, across more than one hundred (100) different DoD enclaves. Through the application of high performance computing (HPC) resources, HACSAW explores novel and innovative analytical capabilities based on a comprehensive cybersecurity dataset. The integration of HPC within the cyber workflow provides an opportunity for fusion and assessments of disparate data streams and real-time analysis using data science algorithms and machine learning (both structured and unstructured data). Our approach is designed to ultimately leverage high performance computing resources to significantly reduce the time to respond to changes in the cyber environment from days to minutes.

Understanding the operational status of information systems, the missions (friendly and adversary) being pursued, and the threats and vulnerabilities that impact them is essential for effective mission accomplishment. This understanding is referred to as Cyberspace Situational Awareness (Cyber SA). Today's decision makers require meaningful Cyber SA to safeguard sensitive data, sustain fundamental operations, and protect national infrastructure. Cyber SA forms part of the broader context of the command and control (C2) of forces and operations, constituting Battlespace Awareness for the cyber domain. It informs deliberate and crisis planning and force application decision making at tactical, operational and strategic levels. The need and responsibility of Cyber SA spans multiple organizations within the DoD, across the entire government and in the private sector. Concepts and approaches for providing and using Cyber SA are still emerging, and numerous efforts throughout DoD focus on meeting Cyber SA challenges by integrating combinations of existing government off-the-self (GOTS) and commercial off-the-shelf (COTS) products. Products used within HACSAW have been inspected with an open source software compliance process to ensure products used for this effort meet predefined standards.

The lack of relevant and recent real-world network enterprise data has hampered many cybersecurity research efforts to develop and validate algorithms or methods under realistic conditions. HACSAW has reduced this technical barrier with a development environment that provides computational and data-rich information to researchers to test, develop, model, measure and refine data-driven analytics. This

environment is the proving ground for novel ideas, algorithms and approaches that are suitable for large scale execution in a dedicated HPC environment. Currently, HACSAW as an aggregation of over one (1) petabyte of DREN data to include network-based monitoring and intrusion detection results, web content filtering, vulnerability scanning, firewall, sensor health, etc. Context is applied to each cyber event through the use of custom enrichment that provide downstream analytical processes with information that may be useful in determining the nature of the event. Additionally, Internet Protocol (IP) addresses are enriched with country code, autonomous system number (ASN) and organizational mappings.

During this talk, we will discuss HPCMP's initial approach to addressing Cyber SA through a Call for Proposals (CFP) to the data science, cyber, and HPC communities. Selected collaborators will receive funding for a one-year effort that demonstrates potential for integration into DREN's Cyber SA operational environment and aligns with identified Mission Essential Tasks (METs). METs will ensure decision makers have the understanding necessary to make effective decisions. Such tasks include monitoring, detection, alerting, cyber threat analysis, cyber risk and event analysis, and sharing and collaboration. METs are used to assist with the development of cyber data science algorithms that apply to HPC. Initial and future contributions in the areas of modeling and simulation, clustering and deep learning are anticipated and results will be shared at a later date.

William Glodeck | Leslie Leonard

Other available formats:

HACSAW: A Trusted Framework for Cyber Situational Awareness

Switch to normal viewerSwitch to experimental viewer

Presentation Presentations