News Center | News Articles Collection

2013-06-17

Innovative Network Architecture Applied to Maritime Security Experimentation

Stewart, Kenneth A.

Monterey, California, Naval Postgraduate School

http://hdl.handle.net/10945/44776

Calendar | Directory SEARCH

About NPS

Innovative Network Architecture Applied to Maritime Security Experimentation

Article By: Kenneth A. Stewart

The Global Information Network Architecture (GINA), an innovative network architecture championed by network specialists at the Naval Postgraduate School (NPS), was recently utilized in a globe-spanning nuclear interdiction experiment conducted by the NPS Maritime Interdiction Operations (MIO) experimentation team in Europe and the San Francisco Bay.

"GINA is able to take programs and devices and represent them in a way that is understood by every other represented application in the GINA environment. Configuring – not programming – creates relationships between the individual components so that stove-piped technologies become accessible and part of the greater GINA universe," explained GINA subject matter expert Dr. Tom Anderson.

Experts from NPS' Information Technology and Communications Services (ITACS) utilize the unique GINA architecture to format data associated with previously stove-piped technologies in a manner that facilitates the sharing of data across a broad spectrum of digital formats.

"The problem with all of these different systems is that they speak different languages … GINA does not require the end systems to be modified to talk to them, GINA is built to understand all of the various data inputs or 'languages' and then creates links and relationships," said Ryan Hale, a network engineer and GINA expert with ITACS at NPS.

In the experiment, dubbed MIO 2013, NPS researchers worked in collaboration with the military special operations communities, local law enforcement and chemical, biological, radiological and nuclear (CBRN) experts in the both the U.S. and Europe to identify and secure nuclear material aboard a vessel in San Francisco Bay.

"The goal is to find the device in the fastest time possible and to establish a security perimeter," said NPS Department of Information Sciences Associate Professor Dr. Alexander Bordetsky. Bordetsky is the principal investigator for the NPS MIO experimentation campaign and the lead for the MIO 2013 experiment.

Once located, the CBRN material and associated intelligence are captured in a process known as Sensitive Site Exploitation (SSE). Hale and his counterparts were able to utilize the GINA architecture to make the SSE data gathered by special operations forces teams usable by a host of related CBRN experts and law enforcement officials via the NPS CENETIX (Center for Network Innovation and Experimentation) operated test-bed.

Ryan Hale, a network engineer and Global Information Network Architecture (GINA) expert with the Naval Postgraduate School's (NPS) Information Technology and Communications Service (ITACS), Hale recently utilized GINA in a globe-spanning nuclear interdiction experiment, conducted by the NPS Maritime Interdiction Operation (MIO) Experimentation team in Europe and the San Francisco Bay.

"We enabled the integration of the SSE data within the experiment's collaborative environment in a manner that allowed the free sharing of information to the experts and operators," said Hale.

"We instituted a secure file transfer service in order to upload SSE information from the devices to a secure file store. From the secure file store, analysts could pull down SSE to be used in social network analysis tools, GINA was used to essentially normalize the data," continued Hale.

According to Hale, a platform that allows for greater interoperability and information sharing like GINA is invaluable when sharing data across the multiple agencies and technology platforms that make experiments like Bordetsky's MIO 2013 work.

"Without GINA, human operators would have to convert the SSE data into another format that can be used by the various systems used by the experts involved in the experiment," said Hale. "If it wasn't for the secure file system that we built the SSE data would have stayed in its own stove pipe and would have been inaccessible to the other experts involved in the experiment."

The platform used to collect the SSE data so critical to identifying bad actors and thwarting terrorists attempts in the MIO 2013 experiment, relies upon a miniature Android-based database known as SQLITE. In the recent experiment, GINA operators were also able to format the SQLITE data in a manner usable by the powerful social network analysis tools developed at the NPS Department of Defense Analysis Common Operational Research Environment (CORE) Lab.

"Capturing relational data as part of SSE can provide a window into the social network's supporting these dark networks," said CORE Lab Co-Director, U.S. Army Special Forces Col. Greg Wilson. "Focusing solely on individual terrorists ignores the broader networks in which they are embedded."

Posted July 17, 2013