Containerized Application Security for Industrial Control Systems

Sandia National Laboratories (SNL)

Adrian R Chavez

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018
Summary: Containerized Application Security for Industrial Control Systems

Objective

• Increase the availability and resiliency of control systems by dynamically migrating, updating, and restoring applications during a cyber incident.

Schedule

• 5/10/18-5/9/21
• Kickoff meeting 5/10/18; Literature review 7/12/18; libmodbus containerized 10/4/18
• Updating software and creating a moving target defense at the application level in near real-time without interruptions in availability or operation.

<table>
<thead>
<tr>
<th>Total Value of Award: $2.5M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Funds Expended to Date: 4%</td>
</tr>
<tr>
<td>Performer: Sandia National Laboratories</td>
</tr>
<tr>
<td>Partners: Chevron, Grimm, PNNL, SEL, and Ft. Belvoir NVESD</td>
</tr>
</tbody>
</table>
Currently, interruptions in service are necessary to update/upgrade software.

BlackEnergy, Shamoon, and Stuxnet are examples of malware that targeted an application to propagate through a control system network.

Application containers used within IT environments but not within OT environments.

Virtual machines used within OT environments but heavyweight.
Advancing the State of the Art (SOA)

- We will leverage open source and open platform tools
  - Docker, SoftPLC, libmodbus, and opendnp3
- Containers isolate applications and help prevent lateral movements
- Docker containers checkpoint/restore in userspace
  - Update/patch/upgrade software in near real-time
  - Increase resilience of OT environments
- Moving target defense in live-migration creates uncertainty for adversary
Progress to Date

Major Accomplishments

- Kickoff meeting (May 10, 2018)
  - Completed contracts for all partners

- Completed literature review on available container solutions (July 12, 2018)
  - Docker, Buildah, CoreOS Rocket, Linux Containers, Virtual Machines, Orchestration engines, …

- Developed use cases and scenarios (July 12, 2018)
  - Libmodbus, openDNP3, and SoftJace
  - SoftPLC

- Developed threat scenario and con-ops (July 12, 2018)

- Libmodbus containerized (October 4, 2018)
Challenges to Success

Minimize downtime during upgrade/patching software in OT environments

- Leverage Docker CRIU capability
- Identify upgrade points with minimal state in software
- Checkpoint and transfer state of old software to upgraded software

Migrate application containers

- Leverage orchestration technologies (Kubernetes)
- Reroute traffic using SDN

Develop an interoperable solution

- Docker is portable across a number of operating systems
- Applications can be containerized with the aid of an executable or source code
Collaboration/Technology Transfer

Continue working with partners throughout R&D process

• Targeting both vendors and asset owners

• Working with Chevron, Ft. Belvoir, and SEL to guide/drive our R&D towards commercialization

• Independent red team assessment scheduled towards the end of year 2
  • Continuous input and communication throughout

• Demonstration and testing scheduled for project close out at partner site