Network Function Insertion for Reliable and Secure Control Messaging Over Commodity Transport

Website: http://cred-c.org/researchactivity/nfimessaging

Researchers (UH): Deniz Gurkan, Nicholas Bastin, Stuart Baxley, R. Christopher Bronk, Wm. Arthur Conklin

Industry Collaboration:

- Currently seeking collaborators from industry, power utilities, or national labs to host the network function node in a realistic setup for prototype usage scenarios. Contact Deniz Gurkan to discuss how you can engage or collaborate with our research team.

Description of research activity: This activity encompasses the design and implementation of a network function which can be deployed without disruption into existing control networks, providing both reliable and secure transport for ICS communications over untrusted networks irrespective of the capabilities of the existing endpoint equipment. Similarly, new security protocols and policies may be injected into this network function deployment without impacting production sensor or control equipment. Such deployments allow for the secure and reliable use of commodity transport providers, including naturally lossy connections such as satellite and terrestrial wireless, without compromising the integrity of data or control messages across the overall system.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?

- **Assess and Monitor Risk:** Our Network Function (NF) provides for recording of exceptional network events, allowing for continual monitoring and serving as component data for higher level ongoing risk assessments across a given infrastructure.
- **Manage Incidents:** Our function provides multiple levers for incident management, from temporary in-band communications shutdown to easy replacement of compromised encryption keys. Forensic data maintained by the NF is available to be used in incident post-mortem analysis.
- **Sustain Security Improvements:** Our research focuses on sustainable improvements on the security of systems through minimal and least invasive solutions of network function insertion. The existing energy delivery systems control infrastructure will need no software or hardware updates in order to utilize the technologies developed in this project.

Summary of EDS gap analysis: Sensor data and control directives from oil/gas production facilities are commonly transmitted unencrypted using unreliable transport protocols over lossy network infrastructures. Even in cases where encryption or reliable transmission is used, network threats evolve on a time scale significantly faster than the upgrade schedules of industrial equipment. This activity decouples the implementation of secure, reliable transport from the actual industrial hardware, providing agility in responding to new threats without downtime of production equipment or waiting for vendor upgrades. We design and implement a network function which can be deployed without infrastructure disruption into existing control networks, providing both reliable and secure transport irrespective of the capabilities of the existing endpoint equipment.

Full EDS gap analysis: Our primary sources of gap analysis are the industry experience of our collaborator PI, Dr. Art Conklin and industry and consortium reports, including the Roadmap [1]. Organizations such as the Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC) [2], DHS Science and Technology Directorate, and NESCOR [3] have catalogued a lack of consistent communication security policy across the industry. These reports outline how sensor and automation systems have vulnerabilities in their network design and implementation [4]. To this end we are addressing the gap that is created by a lack of vendor solutions with programmable network functions. Specifically, industrial control systems in oil and gas technologies require measurement and control data exchanges. These exchanges often occur over lossy and insecure commodity transport networks [5]. Although such communication vulnerabilities are not

specific to oil and gas industry, the challenges become more pronounced with the disconnect between long industrial hardware lifecycles and the fast-changing environment of network communications and security [2]. Our proposed solution is vendor agnostic, independent of ICS hardware lifecycles, and has the programmability necessary to handle changing system demands over time as run-time needs and safety considerations evolve.

Bibliography:

[1] Roadmap to Achieve Energy Delivery Systems Cybersecurity, DOE, September 2011.

[2] Cyber Security Implications Of SIS Integration With Control Networks, LOGIIC re-distribution from ISA Automation Week 2011.

[3] Electric Sector Failure Scenarios and Impact Analyses National Electric Sector Cybersecurity Organization Resource (NESCOR), EPRI Technical Workgroup 1 Report, September 2013.

[4] The State of Cybersecurity in the Oil & Gas Industry: United States, Ponemon Institute, February 2017

[5] LOGIIC Real-time Data Transfer Project, Final Public Report, May 2016.