Project Robus

-search for vulnerabilities in ICS/SCADA protocol

Cost
FREE for IEEE PES and CS members
***$10 for non-member**

**** Lunch will be served**

When
May 19, 2014 (Monday)
11:30PM– 12:30 pm

Where
Rm 704, Entergy Building
639 Loyola Ave
New Orleans

1 PDH awarded

RSVP
Chan Wong
cwong@entergy.com
Chris Crayton
ccrayto@entergy.com

Abstract

Project Robus is a search for vulnerabilities in ICS/SCADA protocol stack implementations. Most research and commercial tools to date have focused on the PLC/RTU/controller (server). Project Robus tests both the RTU server and the master (client) sides of DNP3 and Modbus protocol stack implementations. Attacking the DNP3 master in the control center can eliminate the ability to monitor and control an entire SCADA system, such as an entire electric transmission or distribution system … all from accessing a serial or IP connection in one unmanned substation. Multiple mitigation strategies will be discussed as well.

IEEE
IEEE COMPUTER SOCIETY
IEEE PES Power & Energy Society®
NEEA NOLA

Presenter Bio:

Chris Sistrunk is a Senior Consultant at Mandiant, focusing on cyber security for industrial control systems (ICS) and critical infrastructure. Prior to joining Mandiant, Chris was a Senior Engineer at Entergy (over 11 years) where he was the Subject Matter Expert (SME) for Transmission & Distribution SCADA systems. He has 10 years of experience in SCADA systems with tasks such as standards development, system design, database configuration, testing, commissioning, troubleshooting, and training. He was the co-overseer of the SCADA, relay, and cyber security labs at Entergy Transmission for 6 years.

He is a Senior Member of IEEE, member of the DNP Users Group, Mississippi Infragard, and also is a registered PE in Louisiana. He holds a BS in Electrical Engineering and MS in Engineering and Technology Management from Louisiana Tech University. Chris also founded and organizes BSidesJackson, Mississippi's only cyber security conference.