Chess Master Project
Schweitzer Engineering Laboratories Inc. (SEL)

Dennis Gammel
Cybersecurity for Energy Delivery Systems Peer Review
November 6-8, 2018
Summary: Chess Master Project

Objective

• Establish strong deny-by-default programmable network access control, greater situational awareness and automated event response with SDN leveraging interoperable API

Schedule

• Oct 2016 – Sept 2019
• Key deliverables and dates expected/met
• Proactive policy based network access control with disruptionless scalability and automated event response

Total Value of Award: $ 5M
Funds Expended to Date: % \[\frac{(\text{spent}}{\text{total award value}})*100\]
Performer: Schweitzer Engineering Laboratories Inc.
Partners: Ameren, Sempra, and Veracity
Current “State of the Art”
Closed, Reactive and Restrictive

- Unicast, multicast, and broadcast forced behavior
- Dynamic MAC learning and flooding
- Slow and fixed reactive loop resolution and forced asset efficiency reductions
- Layers and layers of complexity attempting to changed the original specified behavior
- Vulnerable control plane – plane text, no authentication, no crypto, inherently trusted
- Decade old vulnerabilities in network recon, MAC table poisoning, and control plane spoofing
Advancing the State of the Art

- Secure control plane
- Physical and logical traffic engineering
- Mitigates legacy network vulnerabilities
- Multi-layer packet inspection at each hop
- Know who, what, and where is on your network
- Policy based flow management
- Pre-engineered event response
- Network automation
Advancing the State of the Art
Scalable and Interoperable Eco-System

Watchdog Project
SDN Project
Chess Master Project
Challenges to Success

Application Programming Interface supporting Energy sector product lifecycles

• Research lessons learned in other industries
• Talked to many suppliers beyond the Chess Master Project

Capture use cases for the new network security controls and the automation requirements

• System owner education and review
• Researched and collected feedback from many system owners

Test plan execution validating safe and reliability

• Leverage SEL’s established critical infrastructure test processes
• Set up and run proof of concept systems against the RTDS
Progress to Date

• Use cases and benefit whitepaper published and picked up in multiple trade magazines
  https://www.energy.gov/oe/articles/article-cybersecurity-energy-delivery-systems-ceds-program-s-chess-master-project-now

• Product development on schedule
  • Veracity to release security policy enforcement application by first of 2019
  • SEL to release DIN rail switch by mid 2019
    SEL to release flow crypto by Sept 2019

• Testing and validation on schedule summer of 2019
Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- SEL-2740S rack mount OT SDN switch available today
- SEL-5056 OT SDN flow controller available today
- SEL-2742S DIN rail mount OT SDN switch available mid 2019
- Veracity security policy enforcement application available first of the year
- If changes are suggested to OpenFlow they will be submitted late summer 2019
- SEL University has a three day hands-on training course
Next Steps for this Project

Approach for the next year or to the end of project

- Complete product development and commercially release
- Schedule and execute validation testing
- Complete technology supporting literature and update training material when product development is completed
Questions?