U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Artificial Diversity and Defense Security (ADDSec)

Sandia National Laboratories (SNL)

Adrian R Chavez

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

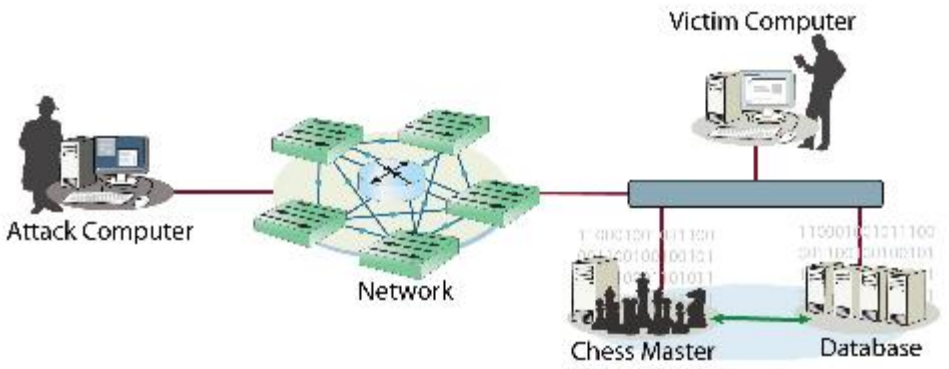
Summary: Artificial Diversity and Defense Security (ADDSec)

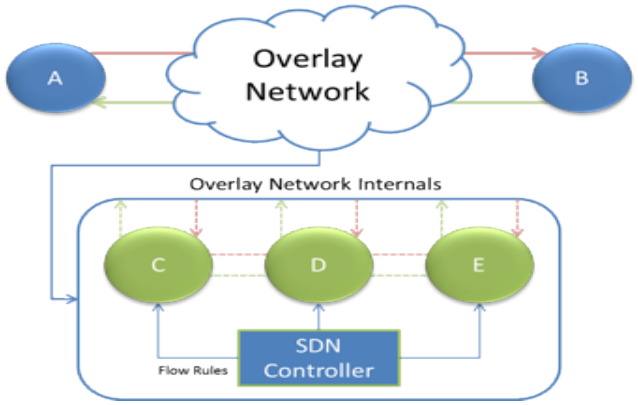
Objective

- Build a framework to proactively detect and appropriately respond to threats while meeting the constraints of an ICS environment. Detection is based on machine learning algorithms and responses are focused on moving target defenses.

Schedule

- 9/22/2015- Present
- Laboratory testing 1/20/17; Ft. Belvoir NVESD demonstration 7/27/18; Report documenting technology and demonstration 4/30/18
- Machine learning algorithms and moving target defense solution leveraging Software Defined Networking compatible with devices using OpenFlow 1.3





Total Value of Award:	**$3M**
Funds Expended to Date:	**90%**
Performer:	**Sandia National Laboratories**
Partners:	**Chevron, Grimm, LLNL, SEL, and Ft. Belvoir NVESD**

Advancing the State of the Art (SOA)

- **Current defenses are reactive**
- **Moving target defense is an active area of research**
  - ASLR
  - IT Focused
  - Need to account for OT requirements and constraints
- **Responses are manual and requires operator intervention**
- **Software Defined Networking primarily used within IT sector**

Advancing the State of the Art (SOA)

- **We have developed a framework to automate detection and response to threats within OT environments**
  - Meet operational requirements (< 20 μs of delay)
- **Machine learning algorithms**
  - Ensemble set of ML algorithms that continuously evolve
- **Moving target defense strategies**
  - IP randomization
  - Port randomization
  - Communication path randomization
  - Application library randomization
- **Building off of Software Defined Networking**
  - Compatible with OpenFlow 1.3

Progress to Date

Major Accomplishments

- Developed detection modules (3/25/16)
- Developed response modules (9/2/16)
- Independent red team assessment (3/10/17)
- Laboratory testing (5/3/17)
- Partner site testing (2/1/18)
- Final report (4/30/18)

Challenges to Success

Evaluation of machine learning algorithms with representative datasets

- Initially work with publicly available datasets
- Capture host-based and network-based events for partner systems

Meet constraints and requirements of partner site OT environment

- Maintain connectivity between active communication sessions by building off of SDN
- Measure operational impacts of several randomization frequencies

Apply and combine ADDSec technologies within partner site

- Work with partners throughout entire project lifecycle

Collaboration/Technology Transfer

Continue working with partners and expanding detection response framework

- 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 complete
- Demonstration and testing complete at partner site
- Compatible with OpenFlow 1.3
  - Existing open source and commercial SDN switches compatible with ADDSec
- Patent issued on ADDSec technology

Demonstration