Adrian R Chavez

Sandia National Laboratories

Artificial Diversity and Defense Security (ADDSec)

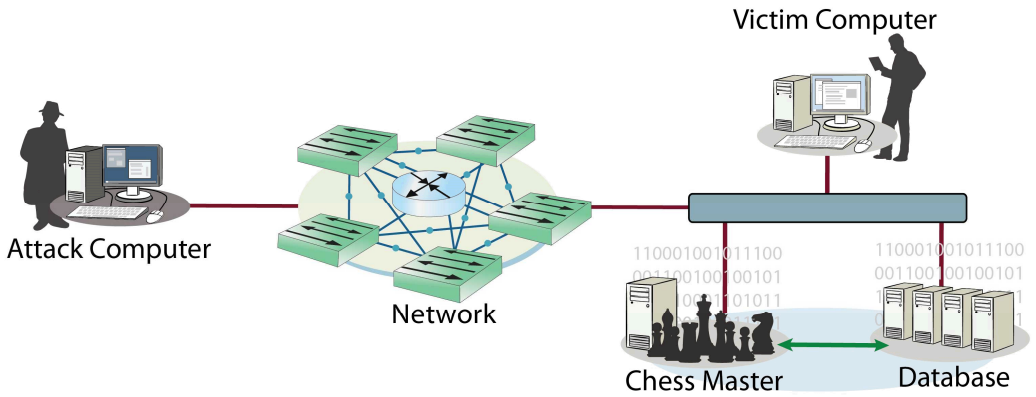
Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

Summary: ADDSec

Objective

- Introduce Moving Target Defense (MTD) and Dynamic Defense (DD) technologies to proactively defend energy delivery systems from the reconnaissance phase of an attack while minimizing operational impacts.



Schedule

- February 2015-February 2018
- Initial Ft. Belvoir microgrid scenario developed (July 2016)
- Completed proof-of-concept demonstration (Oct 2016)
- Interoperable MTD reference implementation – SEL-2740

Performer:	**Sandia National Laboratories**
Partners:	**Schweitzer Engineering Laboratory (SEL), Chevron, Lawrence Livermore National Laboratory (LLNL), Grimm**
Federal Cost:	**$3M**
Cost Share:	**$0**
Total Value of Award:	**$3M**
Funds Expended to Date:	**33%**

Advancing the State of the Art (SOA)

- Current MTD and DD approaches do not take into account energy sector needs
  - Real-time constraints
  - High availability
  - Minimal operational impact
- Automate detection and mitigation strategies
  - Ensemble of machine learning algorithms
  - Software Defined Networking (SDN) to whitelist traffic
  - Randomize network configurations (IP addresses, application port numbers)
  - Randomize application libraries
- Working with partners to drive requirements and solution
  - Representative testbed and microgrid environment
  - Independent 3rd party red team assessment
  - SME cross-cutting government, vendors, and end users

Advancing the State of the Art (SOA) (Cont.)

- ADDSec technology developed with transition path to end user
  - Reference implementation completed
  - Operational performance metrics collected
  - Interoperable solution using multiple vendor SDN technologies including SEL-2740
  - Open source SDN controller supported by major SDN switch manufacturers
  - Published results near conclusion of project
- Additional layer of defense to actively defend control systems
  - Framework to automatically detect and respond to threats
  - Introduce uncertainty to an adversary in the early phases of an attack
  - Scalable solution that is transparent to end devices
  - Modular implementation that supports new mitigation strategies to be integrated
  - Improve situational awareness and increase adversarial workload

Challenges to Success

MTD transparency to maintain high availability

- Implementation leverages SDN technology
- Assume mix of SDN and non-SDN capable devices
- Working with OpenFlow 1.3 standard and actively developed controller

DD data collection

- Leveraging publicly available data sets
- Working with partners to standup microgrid environment

Deployment within representative environment

- SEL provides vendor perspective
- LLNL integrates previous CEDS funded NeMS tool
- Ft. Belvoir implementing microgrid to evaluate ADDSec

Progress to Date

Major Accomplishments

- Operational requirements collected during kickoff meeting
- Ported POX controller to OpenDaylight controller
- Scaled MTD deployment to 300 node environment
- MTD performance metrics collected
- Combine DD and MTD into proof-of-concept demonstration
- Developed network schematics to be implemented at Ft. Belvoir
- SEL-2740 released end of September 2016
- LLNL integrated SDN flows into NeMS tool

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Selected into DHS Transition To Practice program for additional pilot partners
- Designed to interoperate with SEL-2740 SDN-capable switch
- Independent 3rd party red team assessment of reference implementation
- Publish implementation and results
- TRL 8 – System/Subsystem Development at project completion
- Communicate results to Industry Advisory Board established through CEDS outreach tasks
  - 20+ Utilities, asset owners and end users
- Demonstration at Ft. Belvoir microgrid planned for 2nd Quarter FY18

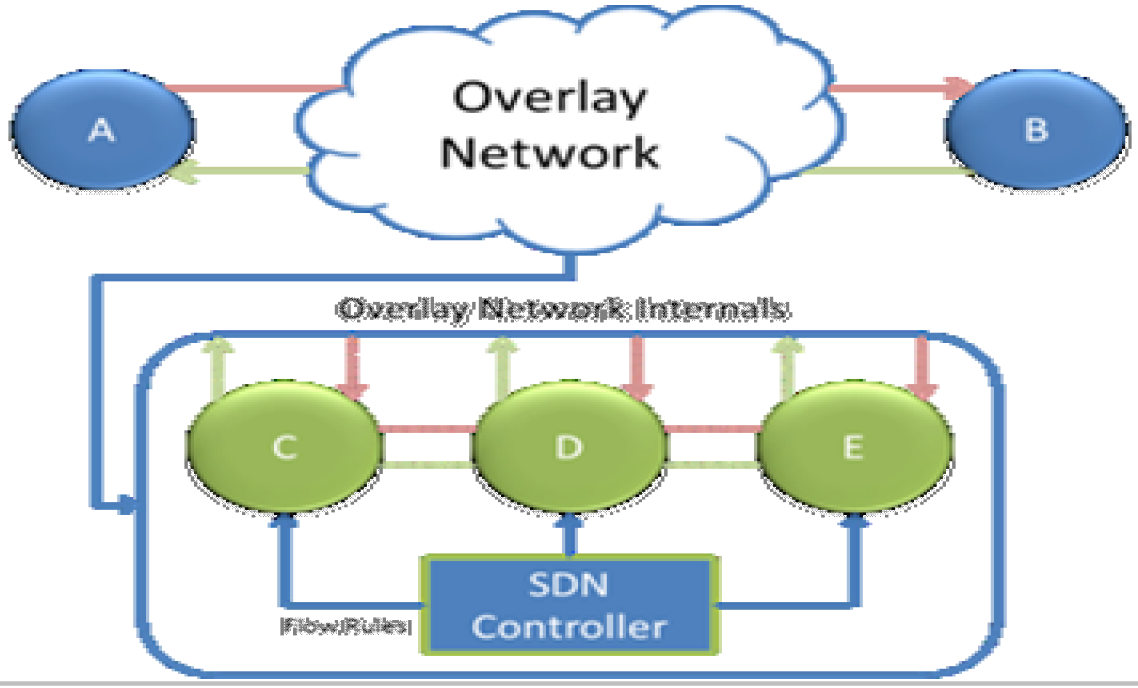
Next Steps for this Project

Approach for the next year or to the end of project

- Phase 1 has focused on developing the DD and MTD technologies in preparation for transition to practice
- Phase 2 shifts focus to applying technology to representative energy delivery system
- Initial laboratory tests performed with SEL, LLNL and SNL
- Representative system tests performed at Ft. Belvoir
- Capture metrics and effectiveness of MTD and DD strategies
- Publish results and continue outreach efforts to extend collaboration beyond existing partners

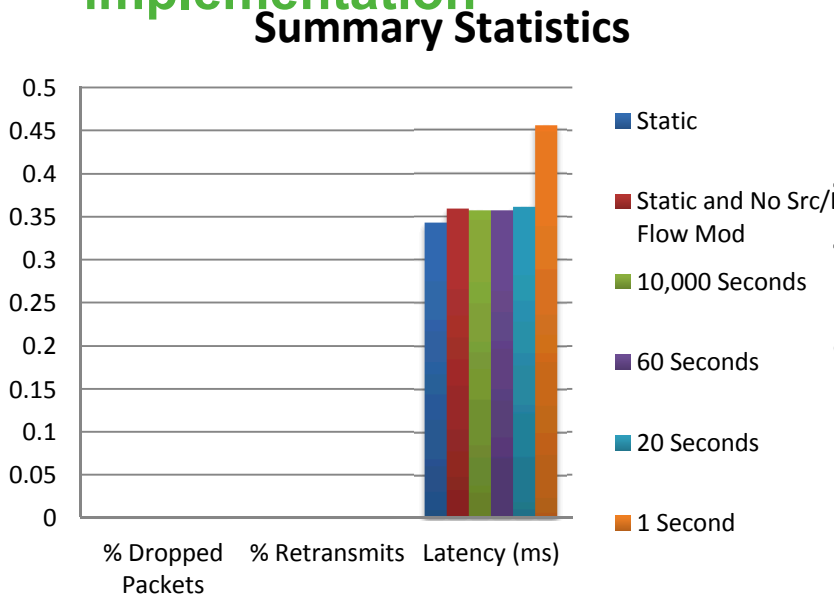
MTD Overview

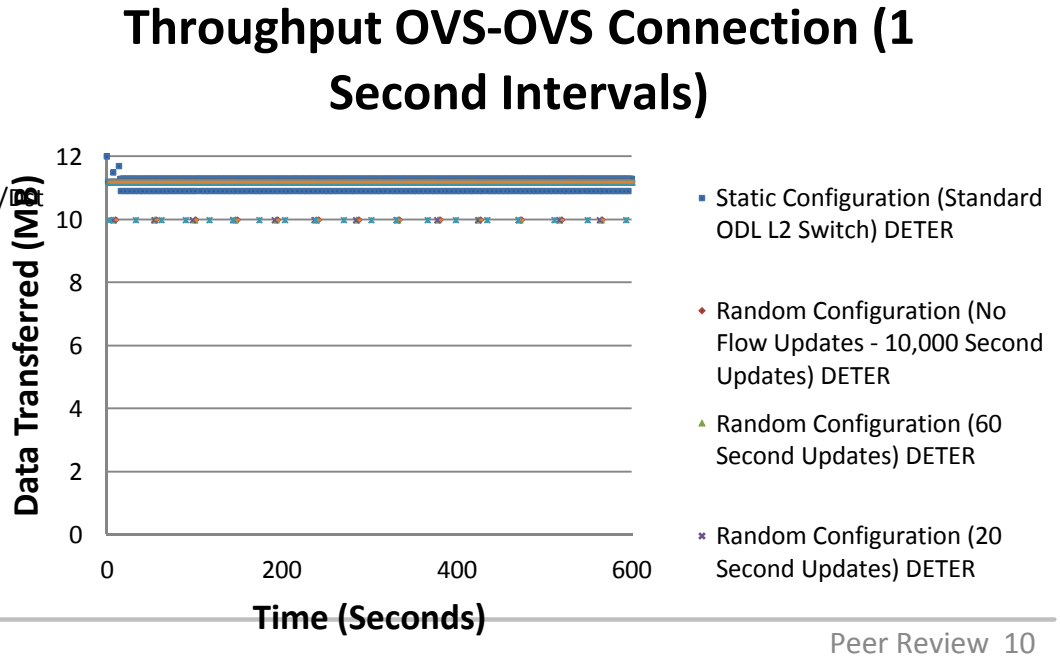
- Current MTD demonstration uses OpenDaylight controller, Open vSwitch, HP 2920 Switch
- Overlay network introduced to disrupt reconnaissance phase of an attack
- Frequency of movement is user configurable



MTD Metrics

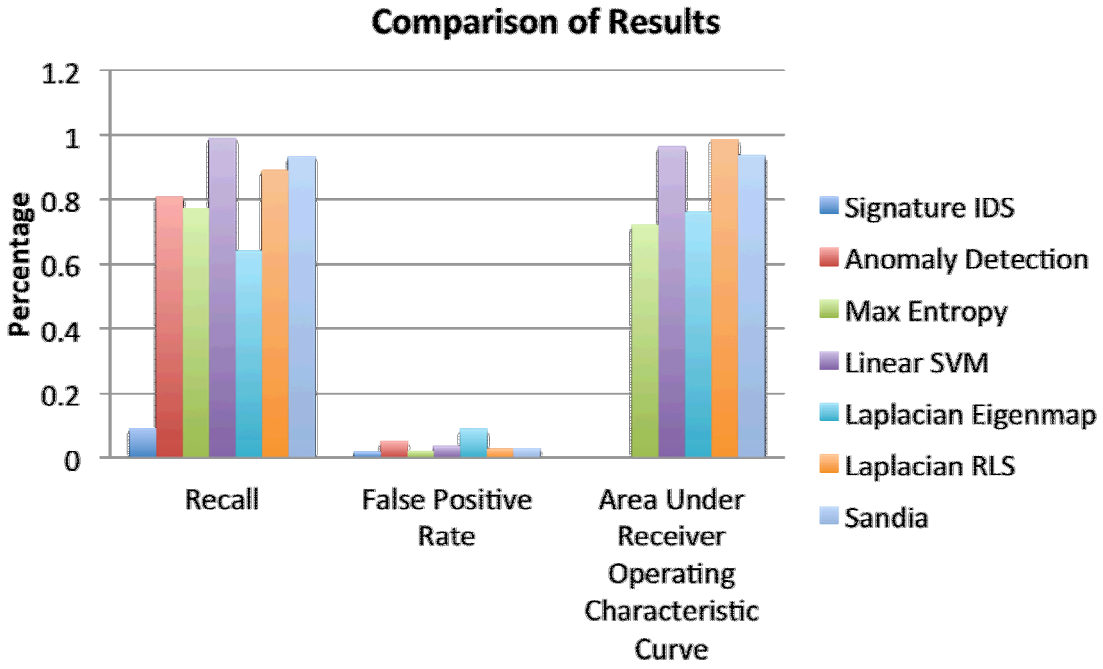
- Metrics captured for varying frequencies of movement of IP Addresses to measure operational impact of SDN integration
- Test environment includes 30 end devices and 3 network switches (Open vSwitch and HP 2920 switch with 600 flow updates/sec)
- Open vSwitch outperformed HP 2920 due to software flow table implementation





DD Overview/Metrics

- DD algorithms compared against openly published algorithms
- Recall measures percent of correctly identified positive events
- AUC measures probability a randomly selected positive event is ranked higher than a randomly selected negative event
- Demonstration detects hitlist worm that triggers MTD as a defense strategy



Ft. Belvoir Demonstration

- Ft. Belvoir planned demonstration consists of 10 buildings
- Evaluation of DD and MTD in progress and demo planned FY18