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

Automated, Disruption Tolerant Key Management System (ADTKM)

Pacific Northwest National Laboratory (PNNL)

Thomas Edgar, PM/PI

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

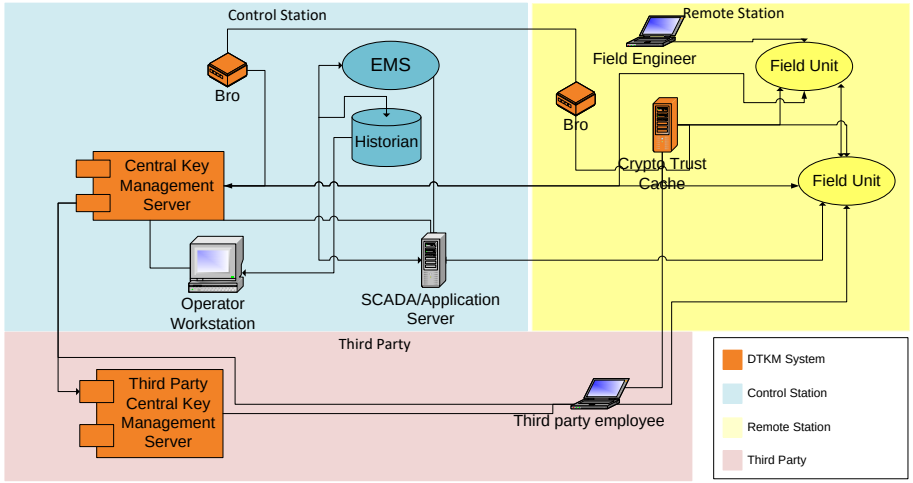
Summary: Project Title

Objective

- Design a Key Management system to meet the unique requirements of EDS
- Disruption-tolerant
- Centrally managed
- Automated key management services for devices
- Self-monitoring system
- Integrated enterprise security

Schedule

- October 2015 – January 2019
- Year 1: System design; research grade test kit Complete
- Year 2: Prototype system; component tests Complete
- Year 3: Experimentation/performance testing Complete
- Year NCTE: Open source documentation; Publishing

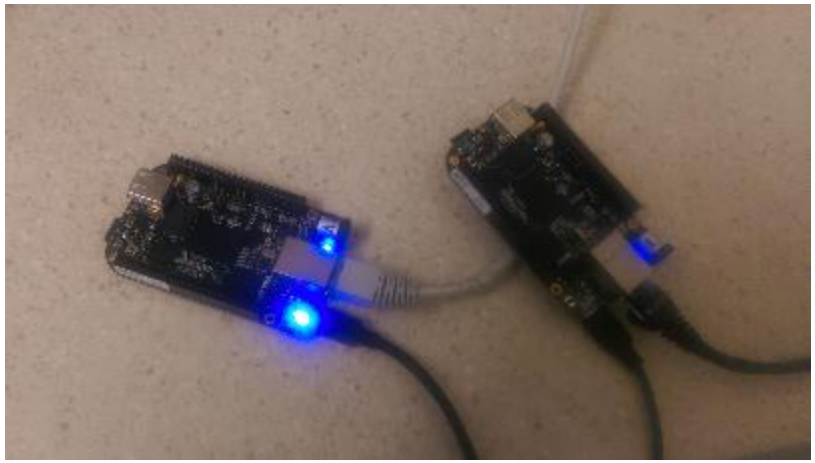


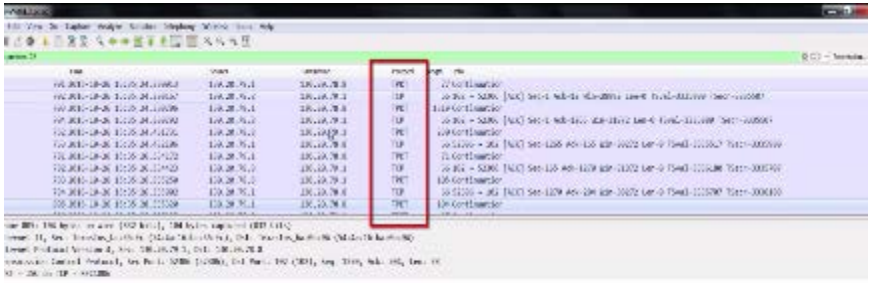
Total Value of Award:	**$1,900,000**
Funds Expended to Date:	**94%**
Performer:	**Pacific Northwest National Laboratory**
Partners:	**LBNL, ABB, Intel (Alterra), APS**

Advancing the State of the Art (SOA)

Current key management architectures:

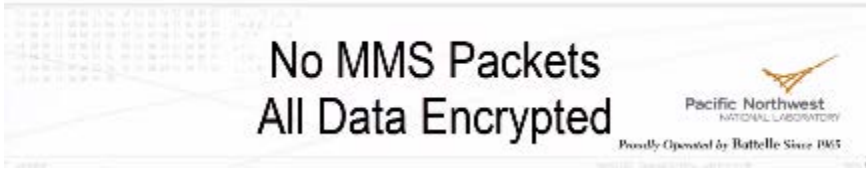
- Are not designed for machine-to-machine communication
- Are designed around “online” mentality
- Are often burdensome to manage (key distribution, revocation lists, governance, etc.)





ADTKM approach combines ideas from enterprise key management, identification, and authorization protocols:

- Kerberos – cached authorization
- 802.1x – device identity and authentication
- Self monitoring for attack detection



Challenges to Success

Comparison to 62351

- Worked with Triangle Microworks to update DTM to allow updating certificate expiration
- DTM is only fully implemented testable suite for 62351
- Only provides a CRL style key management and not the OCSP default mechanism
- Bias results for comparison

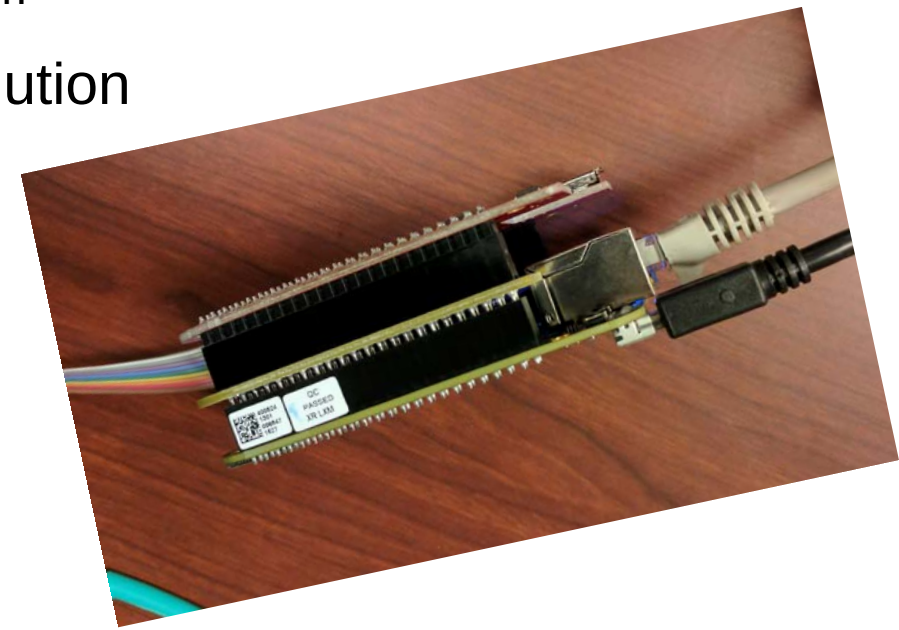
How to evaluate?

- Execute test cases against ADTKM prototype and IEC 62351 systems to quantitatively evaluate approaches
- Need implementation of IEC 62351 with key management
- Working with Triangle Microworks (DTM software)

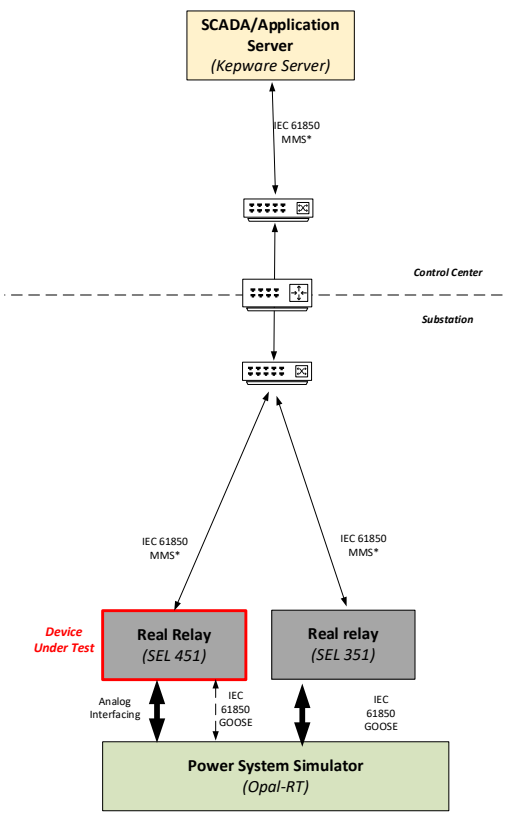
Progress to Date

Major Accomplishments

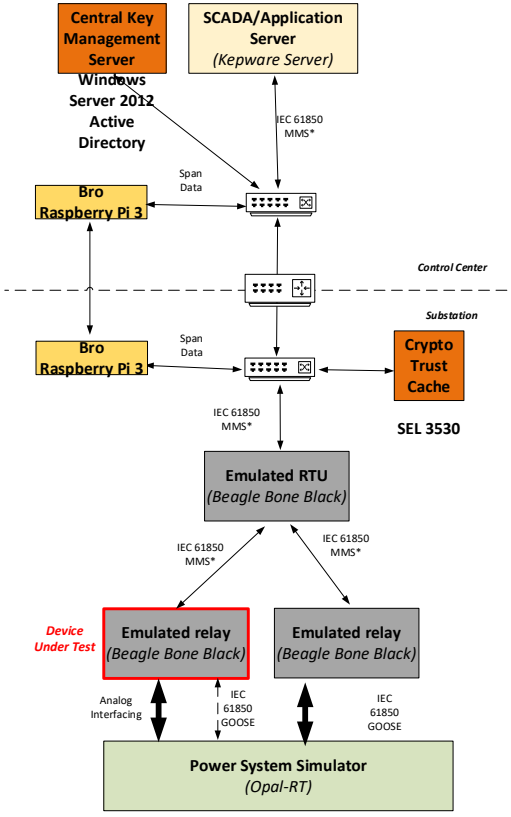
- Open sourced technology developed under this project
  - Code and designs uploaded to Github (links in later slide)
- Created an RTU 61850 application
  - Provides Master and Slave interface between OPC server and relays
  - Necessary to enable test case system
- Executed laboratory testing of solution



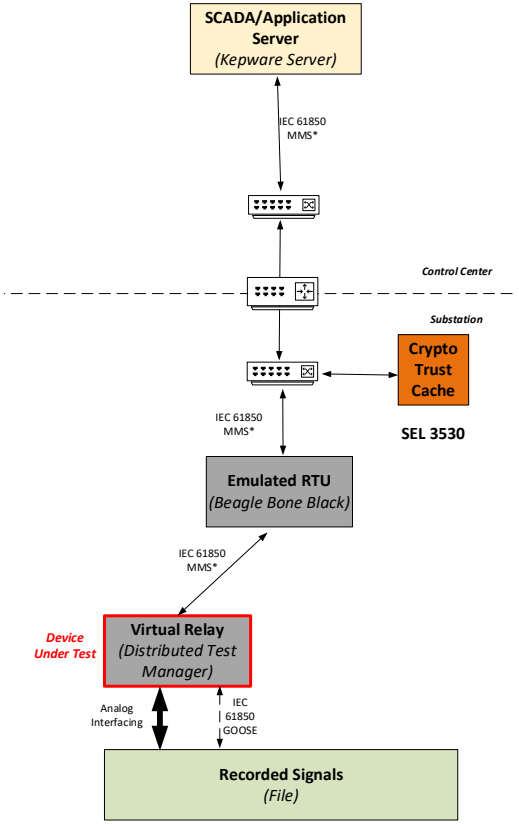
Test Design



Phase 1 Baseline Test Setup

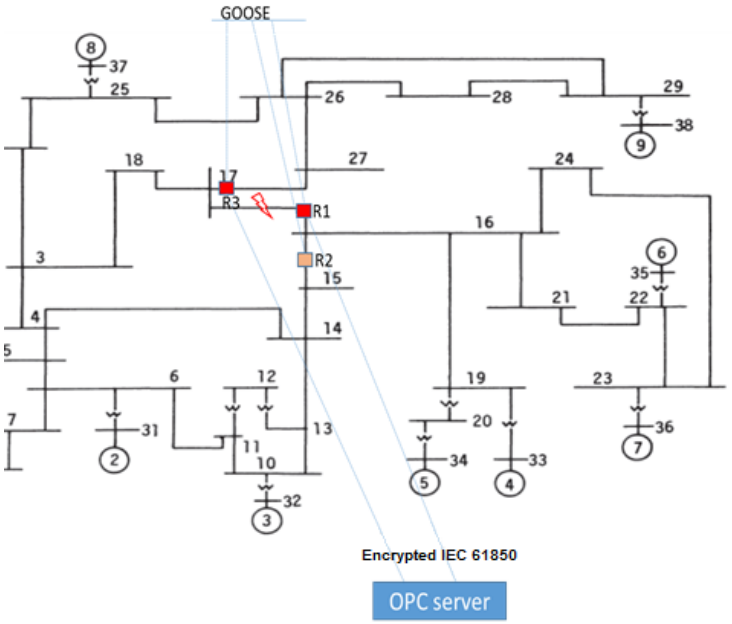


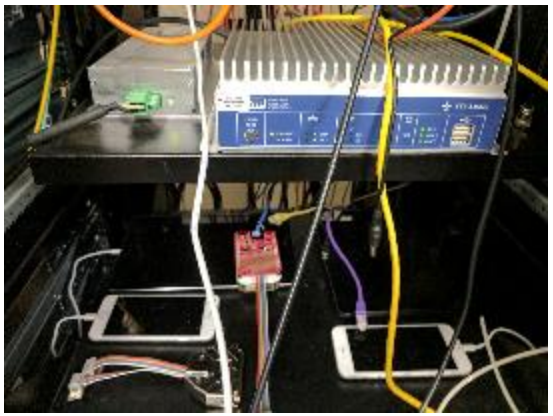
Phase 2 ADTKM Test Setup

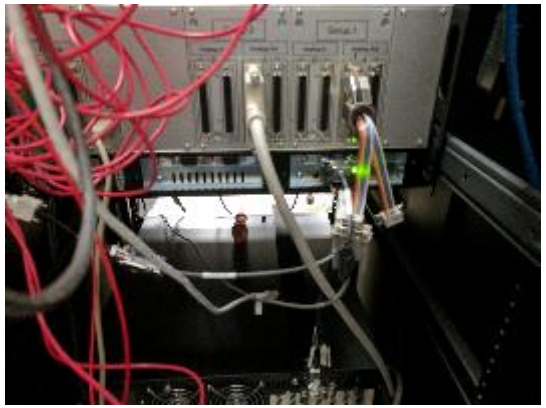


Phase 3 IEC 62351 Test Setup

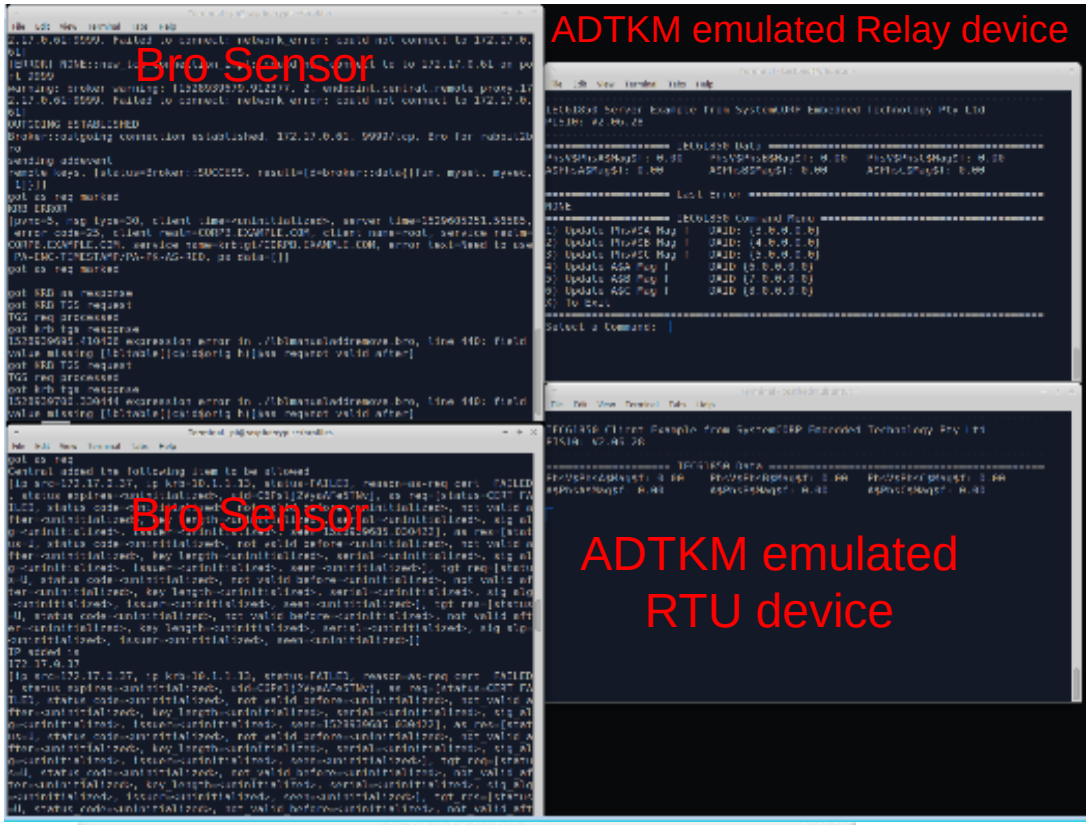
Test Setup


GOOSE
8
37
25
26
28
29
38
9
18
17
27
24
R3
R1
16
3
R2
6
35
15
21
22
4
14
5
6
12
19
23
7
31
13
20
36
2
11
34
33
10
5
4
32
3
Encrypted IEC 61850
OPC server

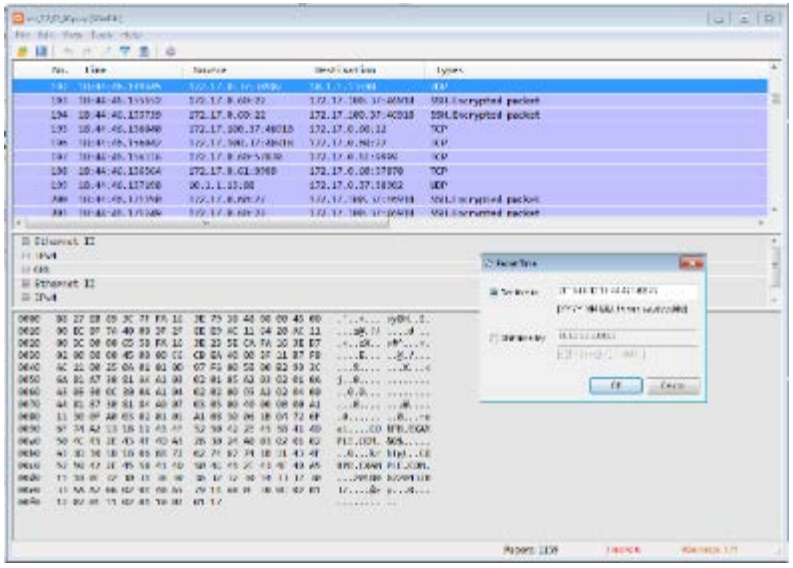


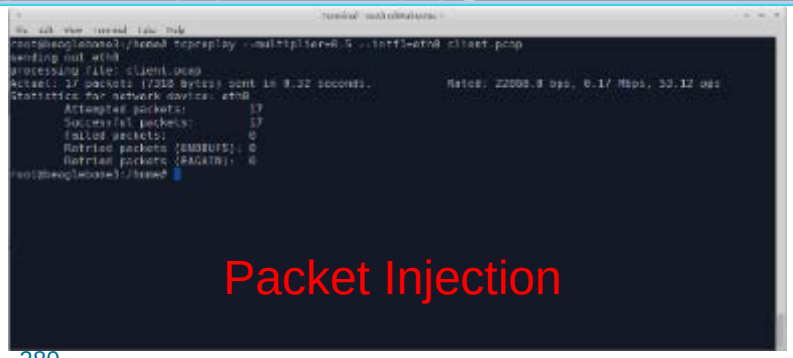


Testing



Packet Manipulation





Collaboration/Technology Transfer

- Open source the project technologies developed under this project
  - Including:
    - ADTKM services: https://github.com/pnnl/ADTKM
    - Bro sensoring additions: https://github.com/lbnl-cybersecurity/dtkm-sparcs
    - BeagleBone Black development platform: https://github.com/pnnl/ADTKM
  - Coming soon:
    - Improved user documentation
    - Tutorials/Walk-throughs
- Comparative study to quantitatively showcase benefits and negatives
  - Contribute test cases and process to community for comparison of other existing or future solutions
- Interaction with DNP3 Secure Authentication
  - Expressed interest in maybe leveraging some of our approach in their Key management process
  - They are trying to get renewed funding for the DNP3 Key Management working group

Next Steps for this Project

- Write Technical documentation
  - User guide for tools
  - 2 papers planned for conference/journal submission
    - Paper documenting ADTKM approach and empirical evaluation results
    - Bro sensing analytics for Key Management