Paul Skare for Thomas Edgar

PNNL

Automated, Disruption Tolerant Key Management System

Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

Summary: ADTKM

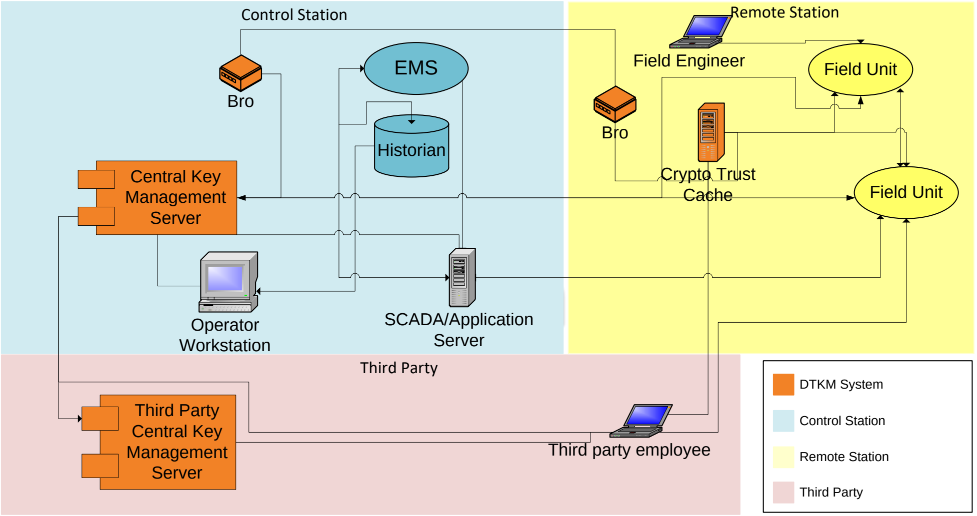
Objective

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
- Increase assurance of 3rd-party connections

Schedule

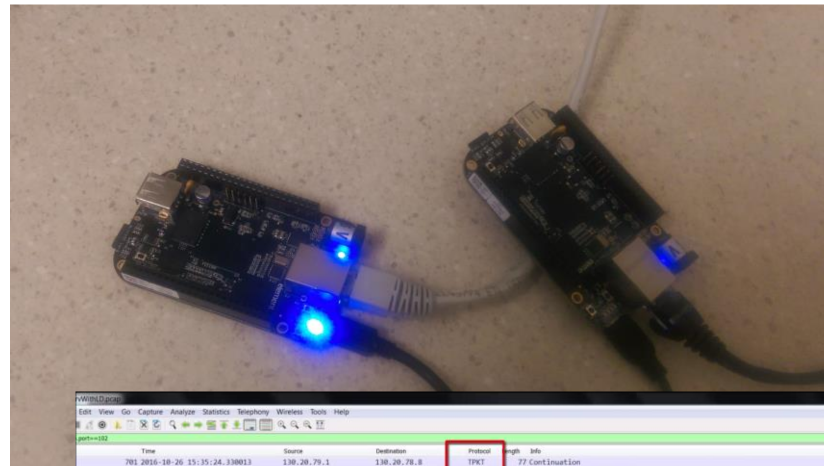
- 10/1/2015-9/31/2018
- Key deliverables and dates expected/met
- What capability will result from this effort that will be transitioned to the energy sector?

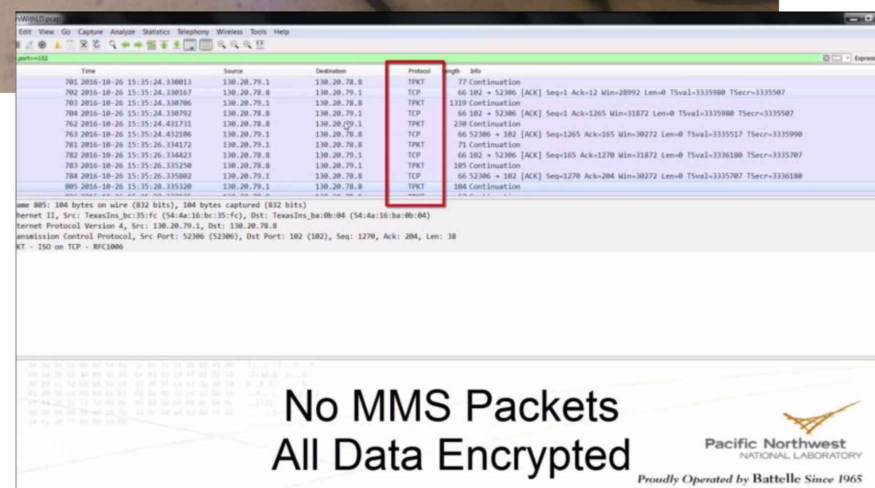


Performer:	**Pacific Northwest National Lab**
Partners:	**Lawrence Berkeley National Lab, ABB, Intel/Alterra**
Federal Cost:	**$1.9 Million**
Cost Share:	**$0**
Total Value of Award:	**$ 1.9 Million**
Funds Expended to Date:	**%**

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:
- Combine ideas from enterprise key management, identification, and authorization protocols
  - Kerberos – cached authorization
  - 802.1x – device identity and authentication
  - Key Management Interoperability Protocol (KMIP) – Legacy system support
  - Self monitoring for attack detection





Challenges to Success

Support of Interoperability

- Necessary to redesign system such that no new protocols were used to ensure ease of interoperability of solution

Integration in Field Devices

- Working with Intel to develop an R&D platform with realistic applications for testing of field device cyber security capabilities

How to Evaluate?

- Going to define and execute test cases against ADTKM prototype and IEC 62351 systems to quantitatively evaluate approaches

•Development board delays

- Mitigated by using BeagleBone Black as interim development platform as it uses a similar ARM chip.

Progress to Date & Next Steps

Major Accomplishments

- Added Intel/Alterra as project partner and working with them to define a cyber security research and development platform for field devices
- Redesigned system architecture to only use standardized protocols
- Defined a distributed sensoring framework for monitoring key management processes
- Created prototype field devices that are able to use our key management libraries to enable secure IEC 61850 communication

Approach for the next year or to the end of project

- Develop prototypes of distributed authentication and authorization services
- Test prototype sensoring framework
- Comparative study between ADTKM approach and IEC 62351

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Key management crosses all business boundaries (Asset owners, vendors, integrators, etc.)
- Open source the PNNL developed R&D development platform software
  - Work with Intel to provide a means to distribute with their development kit or reference a publicly accessible site
- Executive comparative study to quantitatively showcase benefits and negatives
  - Contribute test cases and process to community for comparison of other existing or future solutions
- Work with vendor partners to investigate integration into products

Fernando Alverez, ABB: "There are great benefits to the project approach of defining special (edge) cases, and especially to come out with test scenarios."