

**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

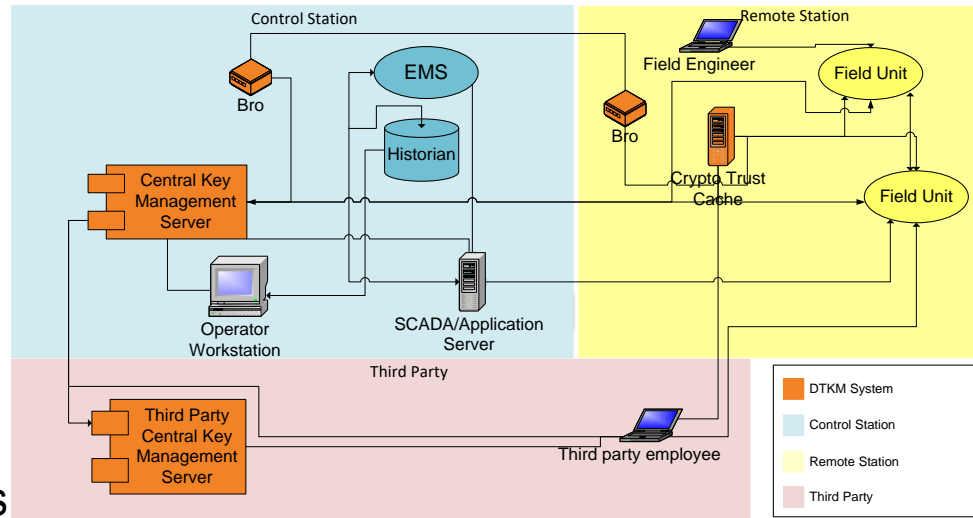
## Objective

## 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 3<sup>rd</sup>-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/Altera

**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)

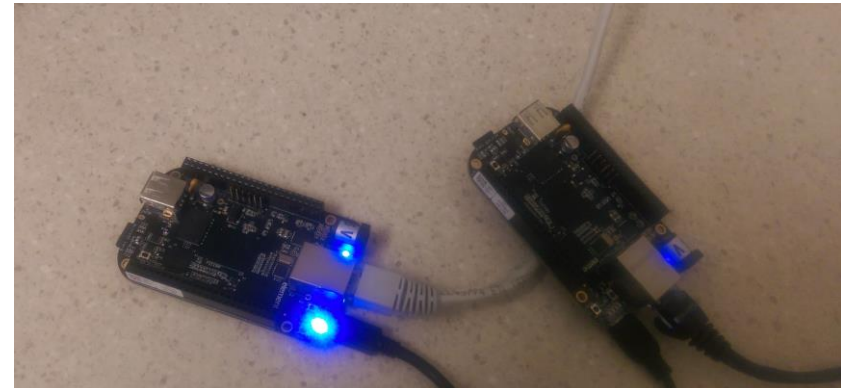
- Current key management architectures:

- 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



The image shows a Wireshark network traffic capture. The main pane displays a list of captured packets. A red box highlights the 'Protocol' column, which shows 'TPKT' (Transport Protocol) for several packets. The packet details pane shows the structure of a TPKT packet, including fields like 'Seq=1', 'Ack=12', 'Min=2892', 'Len=0', 'TSval=3335980', and 'TSecr=3335507'. The packet bytes pane shows the raw data, which is encrypted. The text 'No MMS Packets All Data Encrypted' is overlaid on the image. The bottom right corner features the Pacific Northwest National Laboratory logo and the text 'Proudly Operated by Battelle Since 1965'.

Time	Source	Destination	Protocol	Length	Info
701	2016-10-26 15:35:24.330813	130.20.79.1	130.20.78.8	TPKT	77 Continuation
702	2016-10-26 15:35:24.330817	130.20.78.8	130.20.79.1	TCP	66 382 → 52386 [ACK] Seq=1 Ack=12 Win=2892 Len=0 TSval=3335980 TSecr=3335507
703	2016-10-26 15:35:24.330786	130.20.79.1	130.20.78.8	TPKT	1319 Continuation
704	2016-10-26 15:35:24.330792	130.20.78.8	130.20.79.1	TCP	66 382 → 52386 [ACK] Seq=1 Ack=1265 Win=31872 Len=0 TSval=3335980 TSecr=3335507
705	2016-10-26 15:35:24.431731	130.20.78.8	130.20.79.1	TPKT	238 Continuation
706	2016-10-26 15:35:24.432186	130.20.79.1	130.20.78.8	TCP	66 52386 → 382 [ACK] Seq=1265 Ack=165 Win=30272 Len=0 TSval=3335517 TSecr=3335990
707	2016-10-26 15:35:26.334472	130.20.79.1	130.20.78.8	TPKT	71 Continuation
708	2016-10-26 15:35:26.334423	130.20.78.8	130.20.79.1	TCP	66 382 → 52386 [ACK] Seq=165 Ack=1270 Win=31872 Len=0 TSval=3336180 TSecr=3335707
709	2016-10-26 15:35:26.335250	130.20.79.1	130.20.78.8	TPKT	185 Continuation
704	2016-10-26 15:35:26.335082	130.20.79.1	130.20.78.8	TCP	66 52386 → 382 [ACK] Seq=1270 Ack=284 Win=30272 Len=0 TSval=3335707 TSecr=3336180
805	2016-10-26 15:35:28.335280	130.20.79.1	130.20.78.8	TPKT	184 Continuation

sum 805: 184 bytes on wire (832 bits), 184 bytes captured (832 bits) on interface 0  
Internet Protocol Version 4, Src: 130.20.79.1, Dst: 130.20.78.8  
Transmission Control Protocol, Src Port: 52386 (52386), Dst Port: 382 (382), Seq: 1270, Ack: 204, Len: 38  
TCP - ISO on TCP - RFC1006

No MMS Packets  
All Data Encrypted

Pacific Northwest  
NATIONAL LABORATORY  
Proudly Operated by Battelle Since 1965

# 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/Altera 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 sensing 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 sensing 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 Alvarez, ABB: "There are great benefits to the project approach of defining special (edge) cases, and especially to come out with test scenarios."*