Paul M. Skare for
Will Hutton
PNNL

MultiSpeak® Secure Protocol Enterprise Access Kit (MS-SPEAK)

Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

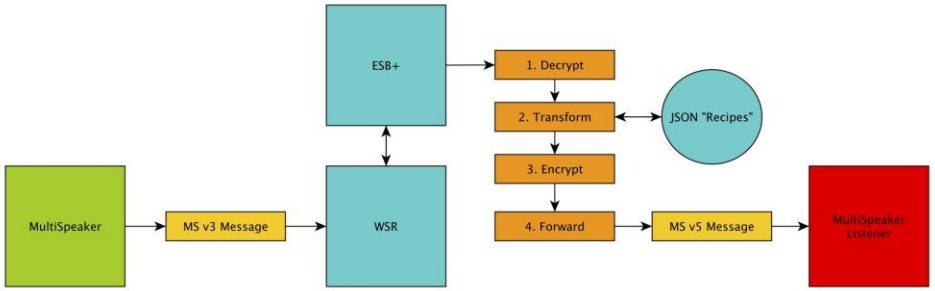
Summary: Project Title

Objective

Create an innovative ESB+ (enterprise service bus) for MultiSpeak that will support increased interoperability and security of the MultiSpeak standard and reduce costs in utilities that depend on MultiSpeak.

Schedule

- 4/1/2016 – 3/31/2019
- Prototype protocol handler tested 9/12/2016.
- Automated translation of MultiSpeak messages for interoperability between multiple standards.



Performer:	**Pacific Northwest National Laboratory**
Partners:	**National Rural Telecommunications Cooperative, Black Byte Cyber, LLC., National Rural Electric Cooperative**
Federal Cost:	**$1,500K**
Cost Share:	**$150K**
Total Value of Award:	**$1,650K**
Funds Expended to Date:	**21%**

Advancing the State of the Art (SOA)

- MultiSpeak v3 is over 10 years old and incompatible with newer, more secure versions of the standard. Inconsistent implementation of the standard has limited interoperability.
- We have demonstrated a closed loop method of translating v3 MultiSpeak messages to v5 as a cloud service.
- MS-SPEAK will validate and translate MultiSpeak messages from v3 to v3 for standards compliance, or v3 to v5 or the reverse for interoperability between currently incompatible components (meters, EMS, OMS, other utilities and vendors, etc.).
- Allow for phased implementation of upgrades, improved security, and improved access to information encapsulated in the MultiSpeak standard.

Challenges to Success

Mapping Potentially Incompatible Standards

- Technical approach to mapping MultiSpeak end points, functions, data elements, and data types 1:1 between specifications
- Subject matter expertise to define unknown mappings data across specifications (industry partners, utilities, and IAB)

Subject matter expertise

- Leverage previous lab experience with MultiSpeak and cybersecurity expertise
- Work with utilities for representative network traffic and subject matter expertise

Encryption

- Evaluating multiple methods to provide decryption and packet inspection where needed while maintaining confidentiality and security between end points.

Progress to Date

Major Accomplishments

- Technical requirements document completed on 6/16/2016 (Milestone 1.0)
- Technical requirements document accepted by IAB on 7/15/2016 (Milestone 1.1)
- Prototype protocol handler tested on 9/12/2016 (Milestone 2.1)

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Asset owners, vendors, any organization that uses MultiSpeak will benefit from MS-SPEAK

Phase 1

- Field-testing of prototype protocol handler at select utilities (March 2017)

Phase 2 (FY17)

- Create an Application Program Interface to facilitate secure interoperability by integrators, utilities and vendors

Phase 3 (FY18)

- Implement a use-case using MS-SPEAK that has industry-wide impact based on IAB input:
  - Intrinsic value and broad applicability “as-is”
  - Genuine value as a template for the creation of additional use cases by integrators, utilities, and vendors.

Next Steps for this Project

Approach for the next year or to the end of project

- Phase 2: API
  (April 1, 2017 to March 31, 2018)
  - MS-SPEAK API framework submitted to DOE by 3/1/2018 (Milestone 5.1)
  - Demonstration of API with select MultiSpeak use cases and reference architecture by 3/1/2018 (Deliverable 3.0)
- Phase 3: Applied R&D Solution using ESB+
  (April 1, 2018 to March 31, 2019)
  - Select an appropriate problem with the IAB by 5/1/2018 (Milestone 7.1)
  - Solve IAB approved challenge worthy of a national laboratory by 4/1/2019 (Milestone 7.2)