Current PNNL Studies: Cybersecurity for Synchrophasors and NASPInet 2.0

A. DAVID MCKINNON, PH.D.

National Security Directorate, PNNL

NASPI Work Group Meeting, October 14-15, 2015, Chicago, IL

Study Motivations

- Future mission-critical synchrophasor applications will require strong cybersecurity and state-of-the-art data networks

- Cybersecurity
  - Cybersecurity is a rapidly growing area of concern
  - Utility cybersecurity constraints vary significantly from the web's constraints
  - Staff may be overwhelmed with thousands of pages of cybersecurity regulation and guidance

- NASPInet 2.0
  - The NASPInet (2008) specification is outdated
  - Existing synchrophasor data networks are not leveraging "state of the art" practices

- PNNL and NASPI have begun two studies focused on future synchrophasor cybersecurity and network requirements

Cybersecurity—Goals

- Specify readily available cybersecurity best practices
  - Basic architectures
  - Existing and emerging security measures
  - Practices for mission-critical systems
- Identify existing sources, guidance and requirements for additional cybersecurity measures and practices
- Focus is on the security of future, mission-critical synchrophasor applications

Cybersecurity—Best Practices

- Risk assessments
- Lifecycle security
  - Cradle-to-grave: executive accountability, procurement, installation/configuration, operations, decommissioning
- Using standards
- Network architecture
- Strong identity
- Time security
- Personnel training
- Data protection
- Cloud security

NASPInet 2.0—Goals

- Revitalize NASPInet efforts
  - ARRA Smart Grid Investment Grants synchrophasor deployments outpaced the original NASPInet specification of 2008
- Specify readily available networking best practices
  - Basic architectures
  - Existing and emerging (data) networking measures
  - Practices for real-time, low-latency, mission-critical systems
  - Practices for federating data across multiple organizations
- Focus is on the resiliency of future, mission-critical synchrophasor data networks and applications

NASPInet 2.0—Lessons from the 2014 D&NMTT Networking Survey

- Stakeholder roles vary significantly
  - RCs do not directly control physical network resources
  - Some PMU owners simply transmit their data to RCs (w/o using it internally)
  - Both in-house and third-party networks are used
- Network oversight is often lacking
  - 67% of respondents had no Quality of Service (QoS) mechanisms to ensure or monitor real-time delivery of PMU data
  - Most have no Service Level Agreements (SLA) with their WAN provider (Survey did not ask if this was because in-house WANs were being used)
  - Over 50% cannot tell if their time source has been compromised
- All plan to interconnect with other user networks for wide-area data transport

NAPSInet 2.0—Core Features

- Cybersecurity—data and applications must remain secure
- Core services must run across heterogeneous networks
- Support for data and resource discovery
- “Application aware” routing and data forwarding
- Real-time network performance and data quality monitoring
- Support for multiple types/classes of applications:
  - Real-time visualization
  - Real-time diagnostics for operator decision support
  - Real-time grid protection and closed-loop control
  - Off-line engineering and forensic analysis tools

Summary

- Studies were kicked off in the summer
- Technical review committees have been formed
- Cybersecurity and NASPInet landscape have been reviewed
- Best practices are being distilled
- Draft results will be provided to the NASPI community for review & comment
- Results will be published in 2016