U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Cybersecurity for Energy Delivery Systems

2010 Peer Review

Alexandria, VA ♦ July 20-22, 2010

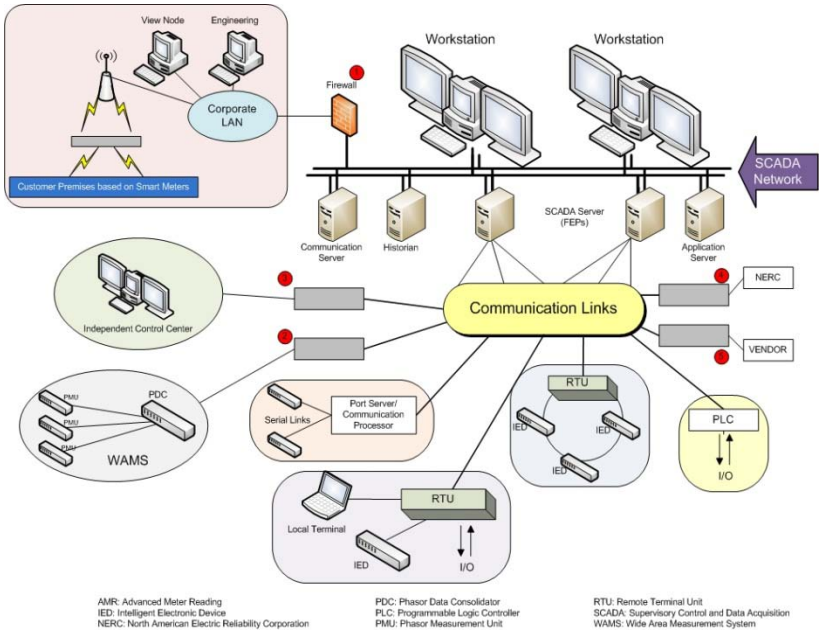
RE Mahan & JD Fluckiger

Pacific Northwest National Laboratory

Secure Data Transfer

Summary Slide: Secure Data Transfer

- **Outcomes:** Best practices guidance for technical staff on the implementation of secure data transmission technology in the SCADA environment.
- **Roadmap Challenge:** Primary focus is on development and integration of protective measures.
- **Major Successes:** Produced a unified view of significant security issues and developed in-depth guideline for addressing security issues in client/server applications.



- **Schedule:** Guidance for developers by 9/30/2010
- **Level of Effort:** 1.25 fte
- **Funds Remaining:** $174K
- **Performers:** PNNL
- **Partners:** N/A

Technical Approach and Feasibility

- **Approach**
  - Identify & document deficiencies/issues
  - Identify & document existing “best practices” for protecting SCADA environment
  - Establish level of protection (what is/is not included)

Technical Approach and Feasibility

- Provide guidance for developing or maintaining SCADA systems including legacy (checklist preferred)
  - Architecture/design recommendations
  - Recommend development tools
  - Implementation recommendations
  - Develop tests to identify residual weaknesses
  - Develop & document solutions
  - References

Technical Approach and Feasibility

- **Metrics for Success**
  - Best practices usable for procurement, development, or on existing implementations.
  - Specifically actionable (best practices, checklists, test and mitigation tools, references to dig deeper).
  - Documentation usable for implementation

Technical Approach and Feasibility

- **Challenges to Success**
  - Complexity overwhelming to Process Control System (PCS) user organizations.
    - Use checklist and/or table format for documentation.
  - Generality of existing “best practices”.
    - Need to be detailed, explicit, actionable guidance.
- **Achievements to Date**
  - Milestone - Literature search for comprehensive and explicit best practices.
  - Milestone – Completed draft guidance for client/server services.
  - Milestone – Current bibliography (will be maintained throughout project).

Detailed Technical Approach

- **Literature Survey**
  - Focused on weaknesses,“best practices”, and standards related to PCS/IT cyber security.
  - Identified 25 most often referenced PCS weaknesses (NERC, DOE Labs, Homeland Security).
  - Identified standards and “best practices” associated with avoiding or mitigating these weaknesses.
- **Conclusion**
  - Standards and practices exist, but tend to be generalized, lack specific detail, and require expertise not widely found in existing end organizations.
  - Guidance that is explicit, but easy to follow is needed.
  - Guidance should be useful for external procurement, internal development, or for assessing existing systems.

Detailed Technical Approach

- **Guidance Model**
  - Followed the CWE/SANS Top 20 and Open Web Application Security Project (OWASP) model to describe cyber security issues, guidance, and references.
  - Modified to use a checklist format and/or refer to checklists where appropriate (e.g., OWASP, CWE/SAN, NIST).
- **Status**
  - Documented in draft for client/server applications.
  - In process of expanding to all identified weaknesses.
- **Issues/Remaining Questions**
  - Appropriateness of model for all identified weaknesses.
  - Final complexity of the result (will it still be overwhelming?).
  - Will vendors respond in positive way.

Collaboration/Technology Transfer

- **Plans to gain industry input**
  - Test bed trial implementation of guidance.
  - Attend workshops or conferences that emphasize SCADA
  - Present at conferences or to specific vendors to get their support
  - Challenges to gaining this input?
    - Vendors resist sharing work in process.
    - Most existing tools out of date
- **Plans to transfer technology/knowledge to end user**
  - User will be PCS/IT technical staff to include in procurement, development, and/or applied to existing systems.
  - Meet with larger vendors considered leaders in field
  - Participate in conferences emphasizing SCADA
  - Leverage existing cyber security standards (e.g., NIST 800-53/CIP)
    - Work with standards bodies and recommend updates to standards.

Next Steps

- **Approach For the Next Year**
  - Complete the guidance package and release draft version.
- **Project results that may form the basis of future control systems security work or link to other programs/organizations**
  - The best result would be that the guidance would be commonly used in the PCS industry by vendors for design, by utilities for internal or external requirements, and mitigation of existing systems.
  - Work with any vendors presently under contract