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

Mark Hadley

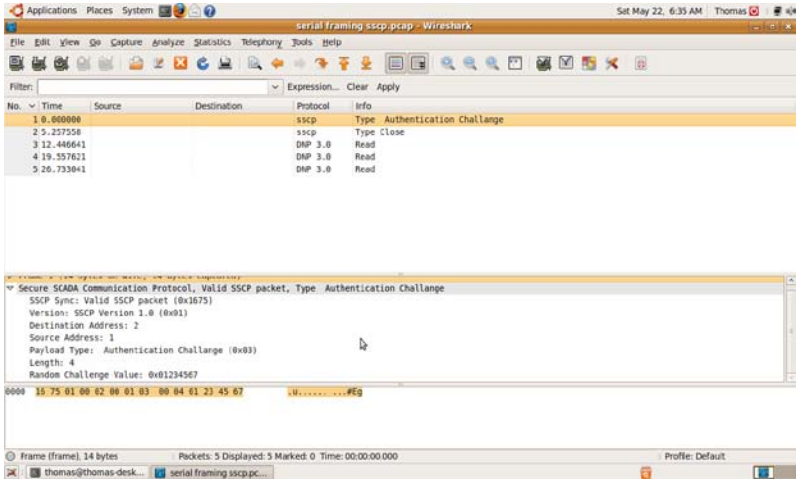
Pacific Northwest National Laboratory

Protocol Analyzer

PNNL-SA-73892

Summary Slide: Protocol Analyzer

- **Outcomes:** Provide operators of SSCP-deployed technologies the tools to view and troubleshoot SSCP-protected communication.
- **Roadmap Challenge:** Standardized test plans and upgrades for new technology are not widely available.
- **Major Successes:** Demonstration of Open Source solution shown at DistribuTECH.



- **Schedule:** Open source candidate (Q3), Demonstration (Q2)
- **Level of Effort:** $159K
- **Funds Remaining:** None
- **Performers:** Pacific Northwest National Laboratory
- **Partners:** Wireshark Project, ASE, FTE (future partner)

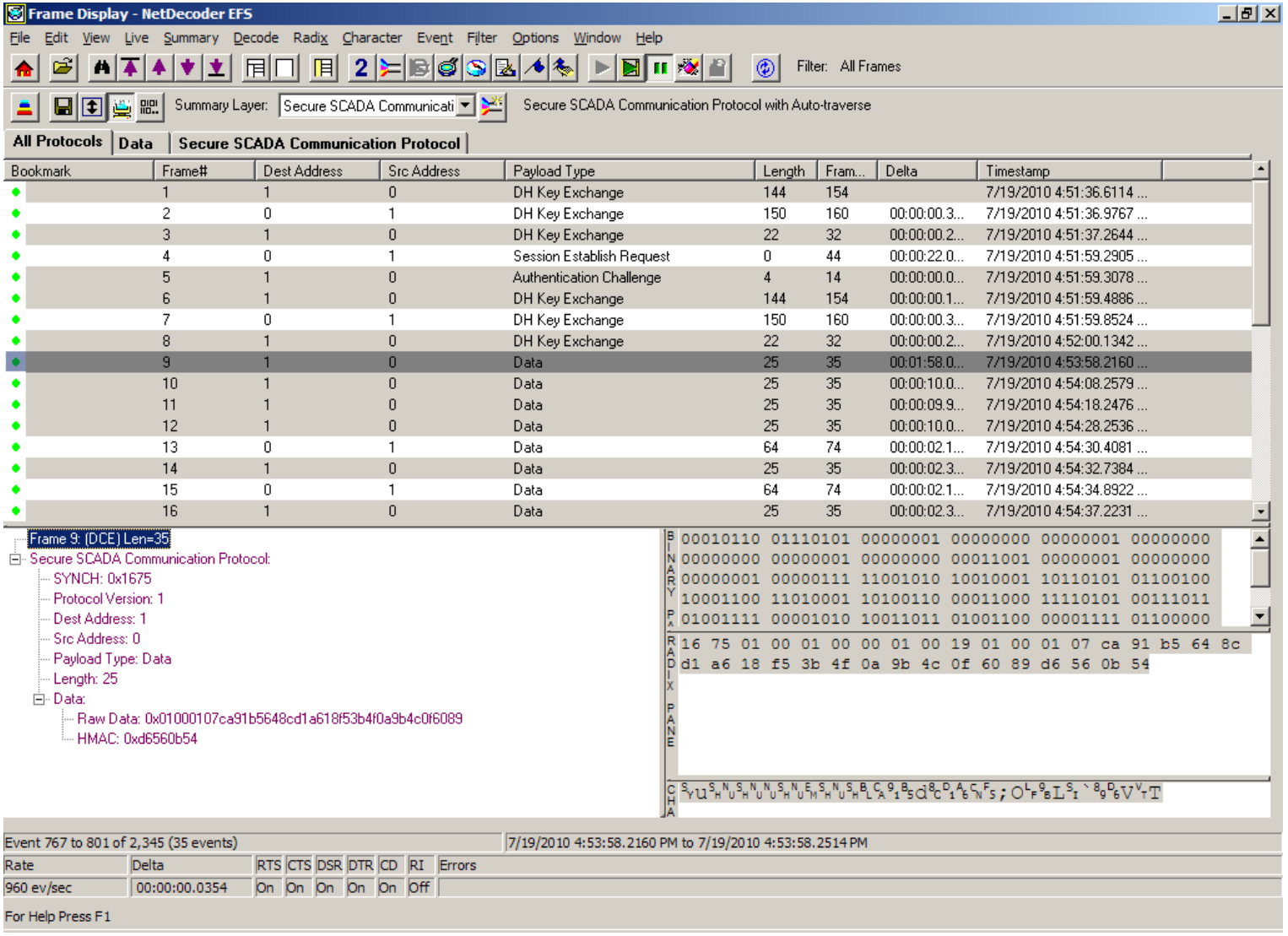
Technical Approach and Feasibility

- **Approach**
  - Utilize PNNL-developed technology to import SSCP protected data into Wireshark's normal interface
  - Add SSCP digester to Wireshark
  - Modify Wireshark (via libpcap) to natively process serial data
  - Hand off encapsulated control system protocol to its digester

Technical Approach and Feasibility

- **Metrics for Success**
  - Public demonstration of technology
  - Open source candidate released to community for review
  - Future commercial product support for SSCP

Technical Approach and Feasibility



Technical Approach and Feasibility

- **Challenges to Success**
  - Laboratory acceptance of open source technology transfer
    - Identified an advocate in PNNL Commercialization office
  - Catch-22 with commercialization vendor
    - Defined SSCP filter using FTE's NetDecoder script interface
    - Transfer to industry planned for FY11

Technical Approach and Feasibility

- **Technical Achievements to Date**
  - Wireshark library (Libpcap) updated to support serial traffic
  - SSCP digester defined within Wireshark
  - Defined SSCP using script language for NetDecoder protocol analyzer

Collaboration/Technology Transfer

- **Plans to gain industry input**
  - Leverage success of Hallmark project and other technology transfer efforts
  - Make the SSCP an industry standard, targeting IEEE and IEC
  - Encourage adopters of SSCP to request support from their protocol analyzer vendors

Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - Target protocol analyzer vendors currently supporting electric industry
  - Initial approach targets protocol analyzer products
  - Future integration into test set products desired
  - Operational support of cryptographically protected communication meets industry security objective of availability

Next Steps

- **Approach for FY11**
  - Incorporate SSCP into FTE's NetDecoder Product
  - Risks include acceptance by FTE and/or other protocol analyzer and test set vendors
- **This approach supports deployment of SSCP-enabled products. PNNL will collaborate with other CEDS projects to integrate serial and security technology into Wireshark.**