U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Secure SCADA Protocol (SSP-21) Characterization and Standardization

Lawrence Livermore National Laboratory (LLNL)

Domingo Colon

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Summary: Secure SCADA Protocol (SSP-21) Characterization and Standardization

Objective

- Advance SSP21 (Secure SCADA Protocol for the 21st Century) toward industry acceptance through characterization of network behavior and development of an industrial key infrastructure (IKI).

Schedule

- Project start: March 2018
- Key deliverables:
  - SSP-21 Network Characterization Study (Jan 1, 2019)
  - Build network and SSP-21 model in NS-3 (March 2019)
  - Run characterization tests of communications between SSP-21 enabled devices and those without SSP-21 (March 2019)
  - Standardization efforts and industry outreach

Total Value of Award:	**$ Year 1: 800K, Year 2: 800K, Year 3: 790K**
Funds Expended to Date:	**258K (Through Sept 30, 2018)**
Performer:	**LLNL**
Partners:	**Automatak (Pending)**

- Transition Plan:
  - Public report describing network characterization of SSP21 and IKI
  - Open source IKI specifications and reference implementation

Strategy for a resilient electric grid

	Adversary Tier 1&2	Adversary Tier 3&4	Adversary Tier 5&6
Identify	Risk Assessment, Asset Inventory and Management, Critical Failure/Component Analysis		
Protect	Basic cyber hygiene	**Encryption, Network Segmentation, Cyber grid planning tools (SSP-21 Encryption)**	**Firmware verification, Control verification (SSP-21 Authentication)**
Detect	Anti virus	Data aggregation, threat detection (MMATR)	Cross-domain operational intelligence, novel data analytics for threat detection
Respond	Manual mitigation of known threats	Orchestration and remediation	Cyber-physical fault isolation, dynamic network segmentation
Recover		OT forensics analysis tools, cyber event reconstruction	Optimized black start strategies leveraging DER
Endure	Microgrids, Component diversification, Cyber safe mode		

Advancing the State of the Art (SOA)

State-of-the-Art Comparison:

- Secure SCADA Communications Protocol (SSCP) (IEEE 1711)
  - Based on shared secrets, not public key cryptography
  - Serial communications focused
- SSP21 - Integrity, Authentication & Authorization for *all* ICS Communications
  - Leverages public key cryptography and modern authenticated encryption (AE)
  - A protocol/PKI that is better suited for ICS than TLS
- Public Key Infrastructure (PKI)
  - High-profile breaches of root certificate authorities
  - Designed for global internet. Too complex for isolated ICS.
- SSP21 - Industrial Key Infrastructure (IKI)
  - Seamless integration of key management with ICS Operations
  - Simplicity and automation of implementation and operations

Characterize the network behavior and develop IKI for SSP21 to enable standardization and industry adoption. Leverage expertise in modelling and simulation (NS-3).

Advancing the State of the Art (SOA)

End-User Benefits:

- Facilitate acceptance of the protocol by manufacturers and asset owners by developing an IKI
  - Reduces the risk of protocol adoption
  - Increased likelihood of robust SSP-21 compatible device ecosystem
  - Transparency through open-source

Advancing the Cybersecurity of Energy Delivery Systems:

- This emerging protocol “provides for cybersecure communications needed to operate resilient grid systems and/or components, at the generation, transmission or distribution levels without reliance on the public internet” by adding authentication and encryption capabilities to OT communications.
- Provide integrity, authentication, and authorization for ICS communications
  - Resilient defense against man-in-the-middle, spoofing, authenticity, replay and data modification, message injection, and fuzzing attacks

Challenges to Success

How to increase exposure, engage potential early adopters and gain acceptance of experimental results

- Focus on an open source and community driven approach

Ensure the selection of appropriate evaluation measures

- Webinars, peer reviewed publications and conference participation

NS-3 model fidelity

- Novel approach to automation (Network mapping to NS-3 model generation)

Scaling SSP-21 based NS-3 simulations

- Leverage experience gained from CES-21

Selecting the appropriate test and evaluation architecture

- Utilize diverse LLNL resources – HPC mod/sim and Skyfall hardware

Progress to Date

ICS/SCADA Community Involvement

- SSP-21 has completed open-source review and will soon be public (Automatak)
- IKI network characterization (SDG&E)
- Impact of SSP-21 on operational ICCP usage (August MRO Webinar - WAPA)

Virtual Machine Based SSP-21 Bump–in–the-Wire Evaluation

- The experimental platform provides LLNL researchers with an initial modelling/simulation based capability to evaluate the impact of the SSP-21 protocol.

Performance statistics and network feature survey

- This study will inform researchers conducting upcoming NS-3 simulations on the most important metrics that should be measured.

Automating simulated activity model

- The LLNL team continues to develop a data processing pipeline that will automate the construction of user activity models from raw network data provided by 3rd party partners – Speeding up the time necessary to conduct HPC-based trials

Experimenting with NS-3 Direct Code Execution (DCE)

- LLNL researchers are working to implement a Direct Code Execution (DCE) path for SSP-21 to improve the performance of the SSP-21 code libraries

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Open sourcing SSP-21 and the Industrial Key Infrastructure (IKI) specification and reference implementation
- Strong focus on SSP-21 library documentation
- User guides and Best practice guides
- Publish white-papers, peer-reviewed publications and present in open-forums
  - Describe the results of community sourced use-cases
  - Focus on “Verification and validation”
- What are your plans to gain industry acceptance?
  - Partner with equipment vendors (Year 2 - 3)
  - Source 3rd party test facilities (Year 2 - 3)
  - Work with a demonstration partner to highlight SSP-21 capabilities

Next Steps for this Project

Year 1

- Collect initial SSP-21 communications network and performance data
- Conduct SSP-21 parameter study Skyfall Laboratory
- Build network model in NS-3
- Build SSP-21 model for NS-3
- SSP-21 Network Characterization Whitepaper

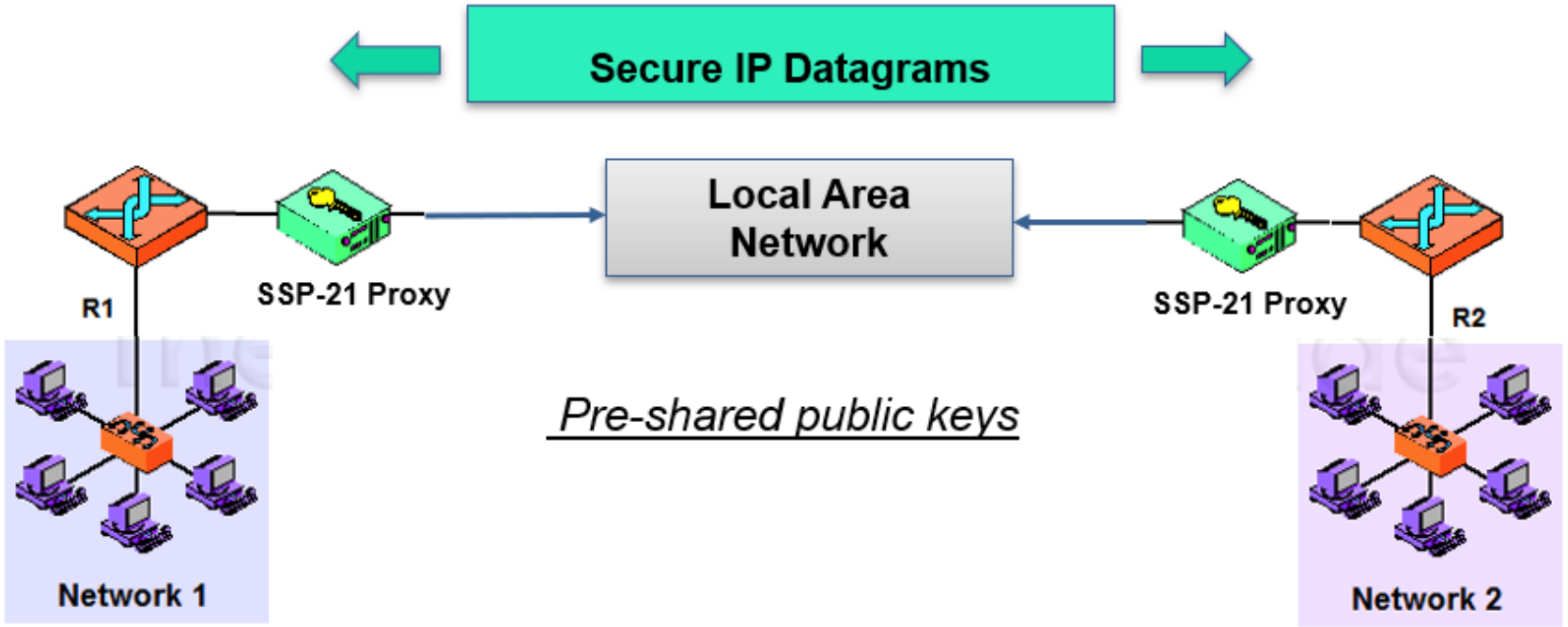
Year 2

- Run characterization tests of communications between SSP-21 enabled devices and those without SSP-21
- Iteratively design IKI specification and reference implementation
- Conduct analysis of potential grid impacts caused by network impacts (if any)
- Refine SSP-21 specification if necessary
- Implement IKI and SSP-21 enhancements in NS-3
- Conduct analysis of potential grid impacts caused by network impacts (if any)
- Refine IKI and SSP-21 specifications if necessary

Year 3

- Implement IKI and SSP-21 enhancements in NS-3
- Run characterization tests of communications between IKI system, SSP-21 enabled devices and those without SSP-21
- Conduct analysis of potential grid impacts caused by network impacts (if any)
- Final report

Virtual Machine Based SSP-21 Bump–in–the-Wire Evaluation



Test Environment 1
Qemu Emulator
RedHat Linux 7.0
DNP3 Activity Model

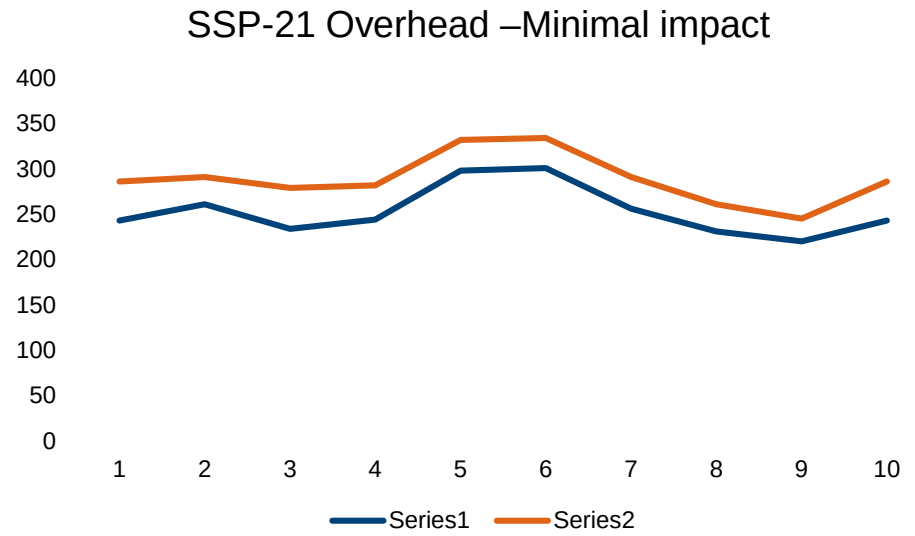
Test Environment 2
Virtualbox Hypervisor
Ubuntu Linux 16.04
HTTP Activity Model

Image/icon source: http://www.tcpipguide.com/free/diagrams/ipsecbitw.png

Validating SSP-21 Requirements

SSP-21 Requirements (SSP-21 Documentation)

- **Low overhead and processing compared to TLS /RSA / x509**
  - Lower CPU and bandwidth for embedded systems.



Evaluation Metrics:

- # of packets
- Time connected
- Bytes Sent
- Average packet size
- Average Inter-packet arrival time
- Data byte rate
- Data bit rate