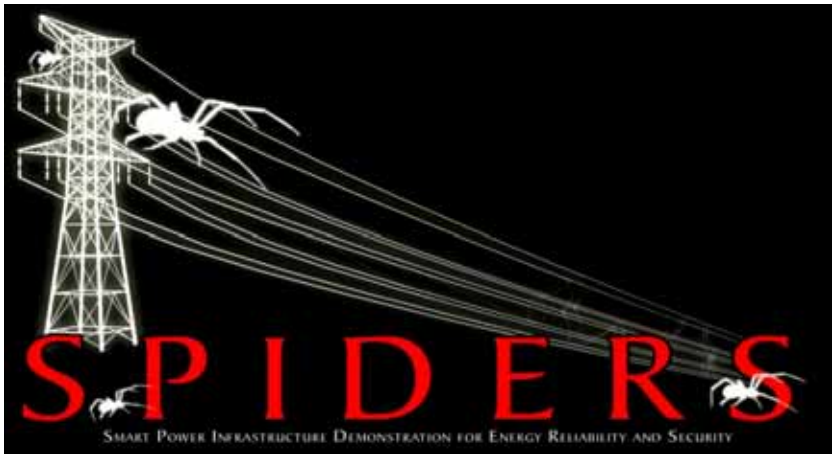


Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS)

Cyber Defense Overview Brief

Mr. Ross Roley
PACOM Energy Office Lead
SPIDERS Operational Manager
Sep 2013

UNCLASSIFIED

SPIDERS Program Summary

STAIRWAY TO ENERGY SECURE INSTALLATIONS

Phase 1

PEARL-HICKAM CIRCUIT LVL DEMO

- Renewables
- Energy Management
- SCADA Cyber Test at DOE National Laboratories

Phase 2

FT CARSON MICROGRID

- Large Scale Renewables
- Vehicle-to-Grid
- Smart Microgrid
- Critical Assets
- CONUS Homeland Defense Demo
- COOP Exercise

Phase 3

CAMP SMITH ENERGY ISLAND

- Entire Installation Smart Microgrid
- Islanded Installation
- High Penetration of Renewables
- Demand-Side Management
- Redundant Backup Power
- Makani Pahili Exercise

TRANSITION

- Template for DoD-wide implementation
- CONOPS
- TTPs
- Training Plans
- DoD Adds Specs to GSA Schedule
- Transition to Commercial Sector
- Transition Cyber-Security to Federal Sector and Utilities

CYBER SECURITY BEST PRACTICES

RIGOROUS ASSESSMENT WITH RED TEAMING IN EACH PHASE

SPIDERS Cyber Development Framework

Implementation

SNL/ORNL:

- "Reference Architecture" in preliminary design for Phase 2 (early draft) and 3 (more mature)

CERL:

- Develops solicitation language for each phase

Integration contractors:

- Completes and builds design, supports system owner in accreditation

Experimentation/ Assessment

PACOM:

- Cyber experiments in lab and on live microgrid for each phase

DHS/INL:

- CSET assessments X 3
- NAVV for phases 2 & 3
- Architecture review for 3

PNNL:

- Operational Demonstration including cyber assessment in each phase

Transition

NAVFAC EXWC:

- Coordinating with ongoing Navy (and other) ICS cyber efforts
- Future integration into enterprise ICS network
- Providing data to OSD I&E's EEIM TWG to support DoD ICS cyber standards

Reference Architecture Experiment Construct

Experimental Question: How do changes in compliance and access level affect the effectiveness and security of the different microgrid control network architectures (flat and enclaved)?

Independent Variables (Factors to be Varied)

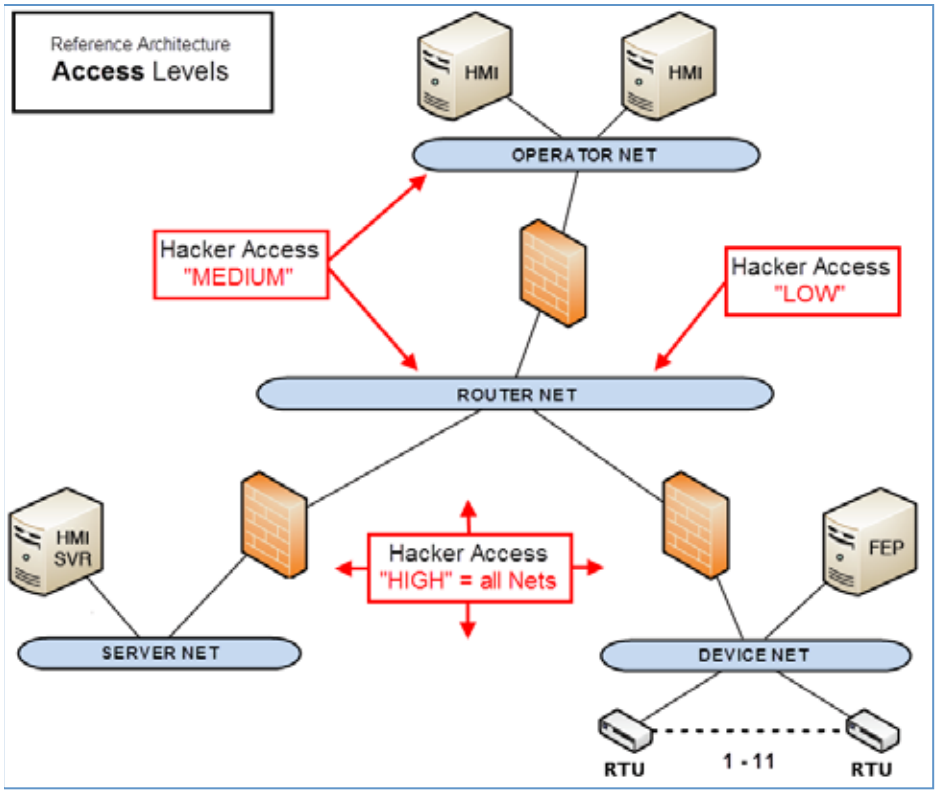
1. Architecture:
   - Flat network
   - Enclaved network (based on Reference Architecture)
2. Adversary Access:
   - Low, medium and high
3. Network Compliance:
   - Compliant, non-compliant

Dependent Variable (Response to be Measured)

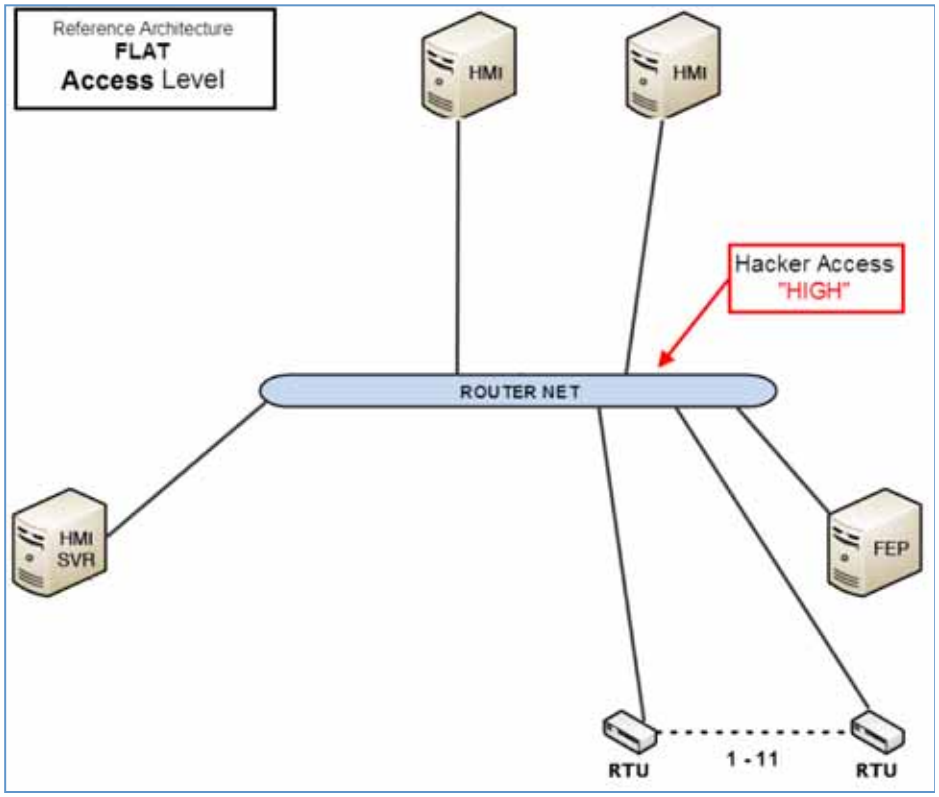
1. Effectiveness of network security
   - Score of 0 – 3 for confidentiality, integrity and availability for each data exchange

Reference Architecture Experiment Networks

Enclaved Network



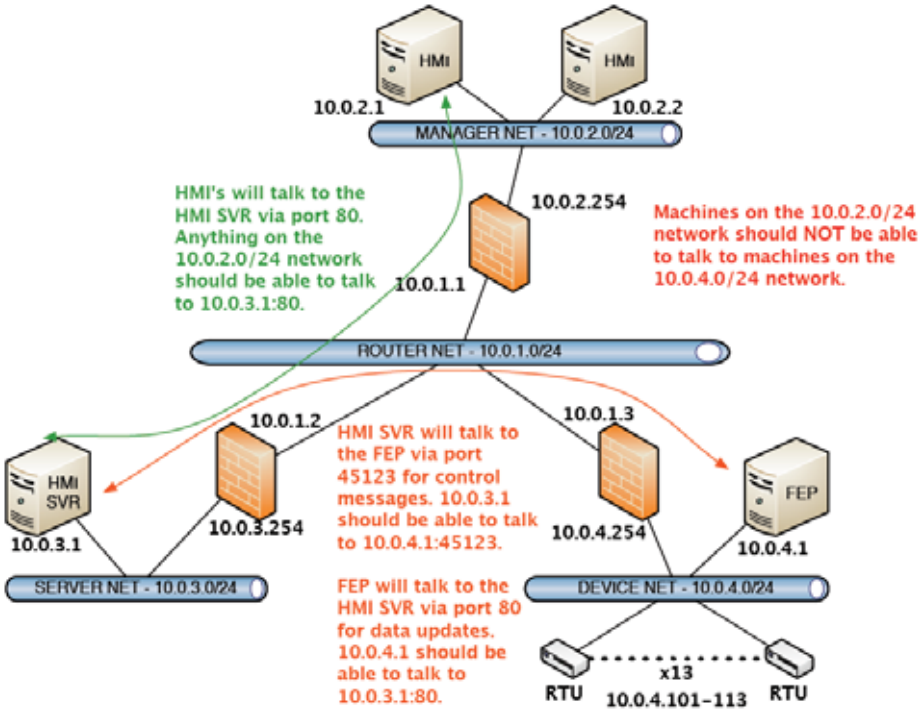
Flat Network



A "compliant" and "non-compliant" version of each network was built. The "non-compliant" network included common ICS vulnerabilities.

Reference Architecture Experiment Scoring

Networks scored points for successful defense of data exchanges against the red teams.



Reference Architecture Data Exchange Scores

Cyber Experiment Scoring Opportunities		
Human-Machine Interface Client/Human-Machine Interface Server		
Information Assurance Required	Read	Write
Confidentiality	medium (2)	medium (2)
Integrity	high (3)	medium (2)
Availability	medium (2)	medium (2)
Maximum Score - 13	7	6
Human-Machine Interface Server/Front-End Processor		
Information Assurance Required	Read	Write
Confidentiality	medium (2)	medium (2)
Integrity	high (3)	medium (2)
Availability	medium (2)	medium (2)
Maximum Score - 13	7	6
Front-End Processor/Remote Terminal Units		
Information Assurance Required	Read	Write
Confidentiality	low (1)	medium (2)
Integrity	high (3)	high (3)
Availability	high (3)	high (3)
Maximum Score - 15	7	8

Reference Architecture Experiment Results

Key Takeaways:

If attacker has limited network access points:

- Enclaving improves network security
- Enclaving mitigates vulnerabilities of non-compliant networks

Lesson Learned:

- Validated scoring system and test methodology

Architecture/Score	Availa-bility (Max: 14)	Confident-iality (Max: 11)	Integ-rity (Max: 16)	Total Score (Max:41)	Percent-age (Max: 100)
Flat/Non-Compliant (All Access)*	0	0	8	8	**19.5%**
Flat/Compliant (All Access)*	0	9	14	23	**56.1%**
Enclaved/ Non-Compliant/ High Access	0	0	8	8	**19.5%**
Enclaved/ Compliant/ High Access	0	9	14	23	**56.1%**
Enclaved/ Non-Compliant/ Medium Access	6	7	11	24	**58.5%**
Enclaved/ Compliant/ Medium Access	6	9	14	29	**70.7%**
Enclaved/ Non-Compliant/ Low Access	6	11	16	33	**80.5%**
Enclaved/ Compliant/ Low Access	6	11	16	33	**80.5%**

Joint Base Pearl Harbor-Hickam Experiment Preliminary Results

Key Takeaways:

SPIDERS JBPHH microgrid cyber security rated as "excellent"

- Unable to vary architecture, compliance and access
- N/A for integrity due to ROE
- Max for Confidentiality due to encryption

Lesson Learned:

- Further validated scoring system and test methodology
- Demonstrated the ability to experiment on a live microgrid with ROE

Architecture/Score	Availa-bility (Max: 15)	Confident-iality (Max: 9)	Integ-rity (Max:N/A)	Total Score (Max:24)	Percent-age (Max: 100)
Flat/Non-Compliant (All Access)*	N/A	N/A	N/A	N/A	**N/A**
Flat/Compliant (All Access)*	0	9	N/A	9	**37.5%**
Enclaved/ Non-Compliant/ High Access	N/A	N/A	N/A	N/A	**N/A**
Enclaved/ Compliant/ High Access	N/A	N/A	N/A	N/A	**N/A**
Enclaved/ Non-Compliant/ Medium Access	N/A	N/A	N/A	N/A	**N/A**
Enclaved/ Compliant/ Medium Access	N/A	N/A	N/A	N/A	**N/A**
Enclaved/ Non-Compliant/ Low Access	N/A	N/A	N/A	N/A	**N/A**
Enclaved/ Compliant/ Low Access	N/A	N/A	N/A	N/A	**N/A**

SPIDERS Phase 2 Cyber Assessment/Experimentation Evolving Plan

Lab Assessment/Experiment:

- PNNL vulnerability assessment to include static code analysis
- Actual IPERC hardware-in-the-loop
- 2 week PACOM red team experiment to explore enclaving/architecture strategies
  - Experimental question TBD

Live Grid Assessment/Experiment at Fort Carson:

- Strict Rules of Engagement (ROE)
- 2 week PACOM red team experiment to verify lab results

CSET Assessment:

- Cyber Security Evaluation Tool (CSET, offered free by DHS) assessment conducted by PNNL would be combination of lab, live and remote data collection

Schedule:

- 72-hr ops demo 21-24 Oct 13 to include Network Architecture Verification and Validation (NAVV) analysis by DHS
- 2-week lab cyber test in Mar 14 timeframe
- 2-week live cyber test in Apr or Jus 14