

SPIDERS Industry Day Information Assurance and Cybersecurity Considerations

Robert Bradford



Topics

- Information Assurance (IA) and Cybersecurity
 - definitions
- SPIDERS Architectures
 - Phases I, II, III
- Guidance/Best Practices
- Challenges
- Conclusion
- Questions

Information Assurance and Cybersecurity

- IA - the confidence that information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users
- Cybersecurity – the state of being protected against the criminal or unauthorized use of electronic data, or the measures to achieve this

Information Assurance and Cybersecurity

- Provides for
 - Integrity – protection against unauthorized modification or destruction of systems
 - Confidentiality – protection against unauthorized access to or disclosure of information
 - Availability – assurance of access to systems and information
 - Authenticity, Utility, Possession/Control
 - Non-repudiation

SPIDERS Architectures

- Goal – cyber secure microgrid
- Basis – Sandia Reference Architecture
- Execution – best practices

SPIDERS Architectures

- Phase I – JBPHH, Hawaii
- Installed
- Isolated network
- IPv6
- Encryption
- Hardened switches and HMIs
- Single Enclave
- Platform IT Risk Assessment (PRA)
- Red Team attack

SPIDERS Architectures

- Phase II – Fort Carson, Colorado
- Construction in progress
- Isolated network – simulated connection to utility
- IPv6
- Encryption
- Hardened switches, HMIs, firewall, IPS
- Multiple enclaves
- DIACAP C&A
- Red Team attack (planned)

SPIDERS Architectures

- Phase III – Camp H.M. Smith, Hawaii
- Design in progress
- Isolated network – simulated connection to utility
- IPv6 and IPv4 (?)
- Encryption
- Hardened switches, HMIs, firewall, IPS(?)
- Multiple enclaves
- PRA or DIACAP C&A
- Red Team attack (planned)

Guidance/Best Practices

- NIST 800 series
- DoD 8500 series
- CNSSI 1253
- ISA ISA/IEC-62443 (Formerly ISA-99)
- Risk Management Framework (draft)
- PRA, DIACAP, STIGs
- Cyber Security Evaluation Tool (CSET) –
DHS ICS-CERT
- Sandia Reference Architecture
- NERC-CIP

Guidance

- Do No Harm!
- Engage installation CIO, NEC, BCO, etc. at the start
- Identify System Owner ASAP
- Coordinate appropriate IA pathway
- Use approved hardware and software
- See accreditation through to completion

Challenges

- Lack of adoption in the commercial space
- Lack of recognition of the need in the ICS space
- Lack of adequate and consistent policies across organizations
- User inconvenience
- “Cost”, or difficulty in assessing value of security improvements

Conclusions

- The focus of the SPIDERS program has been towards evolving Infrastructure Assurance and Cybersecurity measures towards the goal of having a cyber secure microgrid
- Infrastructure Assurance and Cybersecurity has simply become

The Cost of Doing Business

Questions & Discussion

Robert Bradford, GISP
Burns & McDonnell
rbradford@burnsmcd.com
816-822-3895

