SPIDERS Industry Day
Information Assurance and Cybersecurity Considerations

Fred Terry

Topics

- Information Assurance (IA) and Cybersecurity
- Reference Architecture
- Phase 1 Network
- Phase 2 Network
- Lessons Learned
- Challenges
- Questions

Definitions

- 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

Reference Architecture

- Isolation
- Segregation through enclaves
- IDS/IPS
- IPv6
- IPSec/SSL

Phase 1 Network

- Hardened network
- IPv6 used for devices
- Single enclave
- Isolated (air-gapped) network
- Encryption

Phase 2 Network

- Hardened network
- IPv6 used for devices
- Multiple enclaves
- Peak shaving server in a DMZ
- Firewall and Intrusion Prevention System
- Whitelisting
- Air-gapped but connectable
- Encryption

Lessons Learned

- Red Team Attack at Hickam
  - Added “Port Security” to the network configuration
  - Adjusted DHCP spoofing configurations
- Red Team Experiment at IPERC
  - Add “RA Guard” to network configuration
  - Throttle traffic at the switch interface

Challenges

- Lack of adoption in the commercial sector
- Lack of recognition of need in the commercial sector
- Lack of adequate and consistent policies across organizations
- Lack of experience applying security in the ICS space
- Multiple stakeholders/owners can slow adoption
- “Cost”, or difficulty in assessing value of security improvements
- User inconvenience

Questions?

Fred Terry, CISSP
Burns & McDonnell
fterry@burnsmcd.com
@pfterry
816-822-4293