Take the bull by the horns

BSI recommendations for ICS testing

Jens Wiesner

Recommendations for Harmonized ICS Testing
Capability in the EU / Tallinn 01.10.2013

Agenda

- Needs and necessities
- Efforts of the BSI
- Requirements to a testbed
- Summary

needs and necessities

- “End the uncertainty”
- High demand for certification of devices
  - By asset owners / end users
  - And vendors
- Make ICS more secure

Efforts of the BSI

- Awareness
  - Industrial associations
  - End users / Asset owners
  - Vendors
- Publications
- Spot tests of devices
  - Determine flaws and errors
  - get in contact with vendors
  - Establish a trusted relationship
  - Help vendors to set up their own testing capabilities
- Public-Private-Partnership
  “Alliance for Cybersecurity”

Requirements to a testbed

- Awareness
- Education
- Research
- ICS testing
- Device testing

Awareness

- Campaigns
- Media
- Fairs
- Live-Demos
- Different approaches in each country

→ European testbed not suitable

Education

- National (non-governmental) Efforts
  - Commercial Providers
  - ICS-Skilltraining
    - Hacking
    - Red/Blue-team Training
- Necessary (European) approved Skill-Certificate

→ centralized facility not needed

Research / Knowledge coordination

- Many local uncoordinated efforts
- Necessary to coordinate throughout Europe
- Distribution of Classified Knowledge

→ Establish a platform for coordination purposes

ICS testing

- Complex Scenarios
- Unique Scenarios
- Unsecure if executed “compliance-only”

→ not feasible for large scale systems in a testbed

Device testing

- Penetration testing, e.g. robustness, common protocols (http, ftp, ssh, etc.), proprietary protocols (e.g. debugging service), industrial protocols (modbus, profibus, etc.), local interfaces (USB, CF cards, …)
- Firmware Analysis
- More sophisticated attacks such as hardware based (JTAG/SPI)

→ Recommend a public guide for test beds and vendors to test and certify single devices to a given standard at a single time

Arguments against an EU-wide testbed

- Security is not only achieved by secure components
  - Secure integration engine builders
  - Secure operation by asset owners
    [this is why IEC 62443 is a good approach]
- “Compliance is not Security”!
- Acceptance of a EU certification on the international market?
- Unique features in comparison to NERC CIP and others?

Summary

Need

- Make ICS more secure
- Help Users, Asset owners and Vendors

Necessity

- Build common basis for distribution of
  - Knowledge
  - Guidelines
  - Procedures

Do we need a european testbed?

- Depends on the organization and design
- At the moment the necessity is not given

Contact

Federal Office for Information Security
(BSI)

Jens Wiesner

53175 Bonn

Tel: +49 (0)22899-9582-6022
Fax: +49 (0)22899-10-9582-6022

ics-sec@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de