Cyber Security Research Needs- An Energy Sector Perspective

Kyle Hussey, Grant County PUD

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security | cred-c.org

IT and OT interoperability

- Observations
  - OT and IT environments still believe they are Unique
    - The majority of the attack vectors are not from the form and function of the application or operations the technology performs, rather it is from the inclusion of interconnections and distributed architectures
      - In order to advance automation and efficiency the once isolated information (data) and operations are now incorporated in the vast world of firmware, OS's, Databases, Applications, and of course the great vulnerabilities of interconnectivity.
    - ICS, IOT, and SCADA Vendor Technologies not really developed well enough to play correctly in the TCP/IP world.
      - Memory control
      - CPU cycles
      - Process Isolation
      - Vulnerability
      - DDOS protection
      - Access Controls
      - Logging/Event analysis

IT and OT interoperability

- Technology companies still believe they are isolated from the accountability and criticality of the business world.
  - Technology vendors are still focused on first to market and feature enhancement, thus leaving open all the vulnerabilities due to unsecure code, bug handling, and dependency on opensource. No good Quality Assurance in products related to Cyber Security.
  - No accountability or liability for the technology vendor. All major attacks have been found to be the fault of the implementation and or company personnel using the product, even if the vulnerability was due to miss-behaved applications and/or bugs in the software.
    - Why do we not hold the vendor accountable for flawed or unsecure products.
      - Ex: Automobile industry crash safety test, recalls, and safety requirements?
      - Chemical industry label and education warnings. (lawsuits)
      - Product quality controls, EPA, FDA, FCC, etc….

IT and OT interoperability

- Problems:
  - OT and IT vendors still fighting for market value by keeping protocols unique and proprietary and not required to conform to standards.
  - No incentive to develop hardened or secure product by nature.
    - Regulations and customer demand are slow at best.
  - IT environments have evolved, by having dedicated specialists in functional areas, where as ICS, OT, IOT, follows the old approach where the system engineer, system admin does everything.
    - Generates an isolation from interoperability through functional areas of control
  - IT vendors are not required to build product to the resiliency and standards of OT devices.

IT and OT interoperability

- Problems Continued…..
  - Compliance requirements focus on operational function and not on interconnectivity, thus fueling the isolationist mentality.
    - CIP-for electric grid, PCI-DSS for banking industry, SOX, HIPPA etc… this creates even further isolated environments.
      - The irony here is that there are way more commonalities between all the technologies that fall into these operational environments than there are dissimilarities.
  - Too many standards allow environmental uniqueness
    - NERC CIP, FERC, FCC, ISO-27001, NIST-800, EC 61858, IEEE, etc….

IT and OT interoperability

- Summary
  - Focus has been on the uniqueness of every operational environment.
    - Causes isolated silohs in all industries and a lack of focus on the fundamental attack vectors
  - The vendors are not being held accountable for vulnerabilities in their product or adherence to a set of basic security measures
    - Too many requirements that are unique to specified functional areas for the vendors to invest any interest in developing their product to meet everyone's need.
    - If the market does not demand a set of standards then the vendor will not invest in them.
  - IT and OT interoperability awareness
    - Cyber security is everyone's responsibility, not just the IT or OT departments and domains of control continue to be the backdoor for the perpetrator.
  - KISS
    - Find the root attack surface, the common framework, and develop governed standards of operation base on those not on the unique functional areas.

IT and OT interoperability

- Thoughts /Research needs
  - Vendor Certification Standards (Across the board for IT, OT, ICS, IOT)
    - Set a common set of technology minimum standards (ie access control, firmware, OS, application, protocol, hardware).
    - Focus the certification on the common framework, not the unique function.
  - Build/Adopt/coordinate a common protocols for baselines of Cyber Security
    - What this is **Not**:
      - Another guideline
      - Another best business practice
      - Another compliance regulation based on Industry or function.
    - What this **is**
      - Common set of protocols with specific risk mitigation controls (FCC, IEEE, etc…)
      - A governing body
      - with authority to enforce and regulate

IT and OT interoperability

Questions ?

Contact Information:
Kyle M Hussey
Grant County PUD
khussey@gcpud.org
(509)793-1575

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

http://cred-c.org

@credcresearch

facebook.com/credcresearch/

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security