Industrial Security: Going Beyond Defense in Depth

12 October 2010

Bradford H. Hegrat, CISSP
Principal Security Consultant

(Confidential – For Internal Use Only)
A Vendor’s Perspective

- Control System lifecycles are long (20+ years)
- Security is a team sport
  - Vendors & Customers
  - IT & Engineering
  - Pick your teams
- Human beings are imperfect
- Control System safety and security are closely linked
- Control System security is about managing variables
- Managing the security variables enhances uptime

UPTIME = PROFITABILITY
Security Design - the infrastructure

- Security is **not** a bolt-on
- Lead with a comprehensive ICS Security Program
- Implement an Automation DMZ for:
  - Remote Engineering Access
  - Remote 3rd Party Access
  - Secure MZ ↔ EZ programmatic data transfer
  - Secure EZ ↔ MZ management data transfer
  - A means to buffer inter-zone data in the event DMZ connectivity is disrupted
  - Wireless Integration

**Network Security Services Must Not Compromise Operations of the Cell/Area Zone**
Security Design - the DMZ

- Functional Security Sub-zones in the DMZs
- All traffic traverses the Firewall for DMZ communications
- Control-specific protocols should NEVER route to/through the DMZ
Security Design - the attributes

- **Principle of Least Route (PoLR)**
  - Principle of Least Privilege applies to Applications/User level system access
  - PoLR applies to network “reachability.”

- Zone Segmentation is required (i.e. DMZs)

- The ‘VLAN for Security’ model is BROKEN, ANTIQUATED, and RISKY.

- Monitoring is REQUIRED
  - Revisits the IDS/IPS argument
  - Is IDS dead?
  - Is IPS appropriate for the ICS environment? Interior? Fringe?

Don’t forget Microsoft:
IPsec Filters via GPO, netsh, WF/ICS, WMIC, PowerShell, etc...
Security Design - the Products

- **Anti-tamper capabilities**
  - Physical security (controller keyswitch)
  - CPU Lock (unauthorized access)
  - Read/Write Tags
  - Defined Constants (Persistent Tags)
  - Main Controller Function Blocks are not user accessible

- **Firmware signing**
  - Authenticity

- **Authorization & Authentication**
  - FactoryTalk Security (User Access Control)
  - Integration with Microsoft Active Directory (AD)

- **IP & Know-how Protection**
  - Source code
  - Custom routines
Industrial Security 2010 and Beyond

• It’s about continuing Partnering & Collaboration efforts
  – Users, Vendors, Researchers and Agencies
  – Cooperation and coordination

• It’s about enhancing Communication
  – Needs, desires and vigilance
  – Responsible disclosure
  – Consistency and Objectivity

• It’s about furthering Standards
  – Process, Policy & Procedures (with compensating controls)
  – Internal and emerging global standards
  – Continuous Improvement (Suppliers & Users)

• It’s about ongoing Acknowledgement and Addressing Risk
  – Everybody has something to lose
  – Everybody has something to protect

IGNORING RISK IS NOT AN OPTION
THANK YOU!!

Questions? Comments?

(Confidential – For Internal Use Only)