Control System Cyber Security

How to Upgrade the Security of Existing Control Systems?

Joe Bucciero
SANS
Process Control & SCADA Security Summit 2008
January 17, 2008

Agenda

- Problem Definition
- Issues We Face
- Security Difficulties
- Strategy and Direction
- What is Being Done? (Panel Discussion)
Problem Definition

• What can be done to secure real-time control systems from cyber attack?
• Due to inherent timing of control functions and system performance requirements, control systems are very sensitive to signal delays and are difficult to secure.
• Maintenance of the field devices typically requires them to be capable of remote electronic access
• Ease of maintenance and resource optimization issues are causing a trend to Internet access of these devices
• How to support this capability in a secure manner?

Issues We Face

• Control Systems Traditionally Designed for a ‘Safe’ (Trusted) Environment
• Control System Technology is Unique
• Common Security Solutions not Directly Applicable
• Many Different Types of Components Involved
  – Master Station
  – Remote Data Collection Devices (RTUs, IEDs, Relays, ...)
  – Self-contained Closed-Loop Control Systems
  – Others
• Equipment was Built to Last!
• Some Devices Difficult, if not Impossible, to Upgrade
• Significant Labor Component for Replacement
• Difficult Business Case to Justify
Security Difficulties

- Security Breach can Impact Safety and Reliability of Service
- Many Cross Sector Interdependencies Exist that can Impact Control System Cyber Security
- Control System Manufacturers are Global Companies for Products and Services
- Detection of Malicious Code Embedded in Control Systems can be Problematic
- Testing of Systems can Impact Operations

Strategy and Direction

- What Steps Can or Have been Taken to Ensure a More Safe, Reliable, and Secure Control System Operation?
- What Actions have been Performed to Help Protect the Control System Infrastructure?
- What Approaches should be Followed to Upgrade the Existing Control Systems?
- What Measures are Being Implemented to Protect and Overcome Cyber Security Vulnerabilities?
KEMA’s Approach

• Provide NERC CIP Standards Compliance and Pre-Audit Assessment Services
• Perform Vulnerability Assessments on Existing Systems and Replacement Systems
• Provide Penetration Assessment and Testing Services, where possible, on Real-Time Control Systems
• Provide Control System Procurement Specifications that Include Cyber Security Requirements
• Work with Industry Groups to Define New Standards
• Work with Suppliers to Evaluate and Improve Products Implemented to Protect Against Cyber Security Vulnerabilities

Panel Discussion

• Government
  – Gary Finco, Idaho National Labs
• Control System Suppliers
  – Paul Skare, Siemens
  – Sharon Xia, AREVA T&D
  – Robert McComber, Telvent
Thank You!

Joe Bucciero  
Sr. Vice President, KEMA  
GridWise Architecture Council Member  
joe.bucciero@kema.com  
215.997.4500 x206

Experience you can trust.