

Information Security Status for the Electric Power Industry

Open Group Real-Time and Embedded Systems Forum

February 7, 2001

Joe Weiss

Technical Manager, EPRI EIS Program

650-855-2751

joeweiss@epri.com

Business Systems/Internet

■ Assumptions

- Technology developed and available
- No open issues
- Security policies and procedures available

■ Actual

- Significant open issues
 - » Interoperability
 - » Key management
 - » Encryption issues
 - » others
- Open issues impact completeness of IT security policies and procedures

Operational Systems

■ Assumptions

- Information has assumed to be secure
- Technology not available
- Specific security policies and procedures not available

■ Actual

- Information security technology not available
- Significant technical issues with real time systems
 - » Internet security technology may not be adequate
- Equipment security requirements not available
- IT security policies and procedures incomplete

Key Security Aspects of Process Control Systems

- Process Control Systems rely on the exchange of information amongst disparate systems inside and outside the enterprise
 - Networking of these systems is expanding rapidly
- Industry is moving to standard communication protocols, operating systems, networks, and integration techniques
- Confidential business information and plant safety make securing electronic information critical

Process Control Systems Security

- Legacy control systems use proprietary operating systems and protocols and are less vulnerable
 - Web-enabled applications make them vulnerable
- Newer systems use open systems and interfaces making them more vulnerable
 - eg, NT, Solaris, PCanywhere, ActiveX
- Integration with corporate, maintenance, and/or ERP systems open up new areas of vulnerabilities
- Fieldbus protocols designed to be open
 - Very vulnerable

Key Security Vulnerabilities of Process Control Systems

- Systems were not designed with security as a driver
- Security and functional performance are mutually exclusive
 - Trade-offs are necessary
- Electronic security vulnerabilities can exist at the network, system, and component level
- Internet-accessible hacking tools can be used
- Unique aspect of these systems may not be addressed by IT Security procedures or technology

Potential Electronic Security Vulnerabilities

■ Hardware Systems

- Generation
 - » DCS, PLC, field devices, maintenance systems
- T&D
 - » SCADA/EMS, RTU, Relays, IEDs
- Customer
 - » Automated meters, power quality meters

Potential Electronic Security Vulnerabilities

- Software/Protocols
 - Operating Systems
 - » NT, 2000, Linux, Unix, Solaris
 - UCITA
 - Fieldbus, MODBUS, etc
 - ICCP (TASE.2)
 - CIM
 - DNP
 - CORBA
 - ActiveX
 - X-Windows
 - PCAnywhere

Other Issues

- Security vendors and many of our systems vendors have not recognized need
- Information security concerns even with government agencies
- Any disgruntled employee is everyone's disgruntled employee
- Lack of information security at customer site could be major utility liability
- UCITA

EPRI EIS Program

■ Basic premise

- Address security requirements of operational systems

■ Current Status

- Developed three security primers and set of security guidelines
- Participating in IEC TC57 Working Group 15 on Transmission & Distribution (T&D) Security
- Participating in Process Controls working group
- Working with process controls vendors on security procedures
- Working with security vendors on process controls unique needs

Interactions

- IEC TC 57 WG15
 - Working group on T&D systems information security
- NIAP (NSA and NIST), DOE, and Paper Industry
 - Ad hoc working group on process controls information security
- PKI Forum
- Open Group
 - CORBA
- Open Management Group
- Utility equipment suppliers
- Security technology providers