

Information Security Needs for Electric Power Applications

Open Group Real Time and Embedded Systems Forum

July 18, 2001

Joe Weiss

Technical Manager, EPRI EIS Program

650-855-2751

joeweiss@epri.com

1



Operational Systems

- Highly reliable, real-time systems that require secure two-way communication of dynamic data
 - Supervisory Control and Data Acquisition (SCADA)/Energy Management Systems (EMS), etc
 - Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), etc
- Operational systems designed to maximize performance and flexibility
 - Electronic security was not a significant consideration
 - Electronic security technology can inhibit performance
- Legacy systems assumed not to be vulnerable
 - Web-based applications can make them vulnerable
- Open systems can be vulnerable
 - eg, Microsoft NT, Solaris, etc

Operational Systems (cont)

- E-commerce information security technology assumed directly applicable
 - Firewalls, intrusion detection, encryption, etc
 - Backfit of this technology could adversely impact system operation
- IT security policies and procedures assumed to apply to operational systems
 - Unique attributes of real time systems are often not addressed
 - Improved network security does not improve efficiency of the process
- Technical expertise assumed readily available
 - Very few experts in both information security and real time systems

Real Time Systems Unique Attributes for Security

- Deterministic
 - Precise timing for interrupts and other operations (Quality of Service)
- Secure real time operating systems
 - Develop security policies for the kernels
- Very high reliability
- Two way communication
- Ability to accept dynamically changing data
- Short response times (could be milliseconds)
- Minimal amount of computer resources available

Vulnerable Hardware

- T&D and Customer Facilities
 - Supervisory Control and Data Acquisition (SCADA)
 - Energy Management Systems (EMS)
 - Remote Terminal Units (RTU)
 - Protective Relays and Intelligent Electronic Devices (IED)
 - Customer meters/Power quality meters
 - Communications
- Process Plant and Electrical Generation Stations
 - Plant Distributed Control Systems (DCS)
 - Programmable Logic Controllers (PLC)
 - Field devices
 - CEMs
 - Maintenance systems

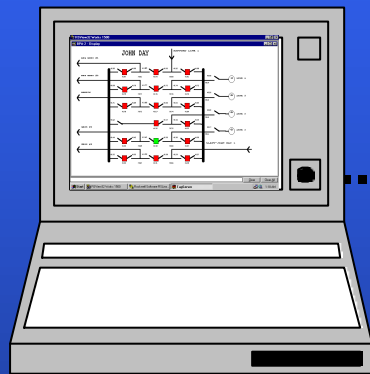
Vulnerable Software /Protocols

- Operating Systems
 - NT, 2000, Linux, Unix, Solaris
- Fieldbus, MODBUS, and other buses
- Vendor Software
- Protocols
 - Inter Control Center Protocol (ICCP-TASE.2)
 - Common Information Model (CIM)
 - DNP
 - CORBA

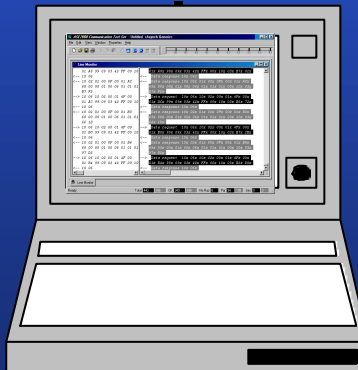
Other Concerns

- ActiveX
- X-Windows
- PCAnywhere
- SSL
- Telecom and other communication media
- Field implementation can negate security certification
- Uniform Computer Information Transaction Act
 - (UCITA)

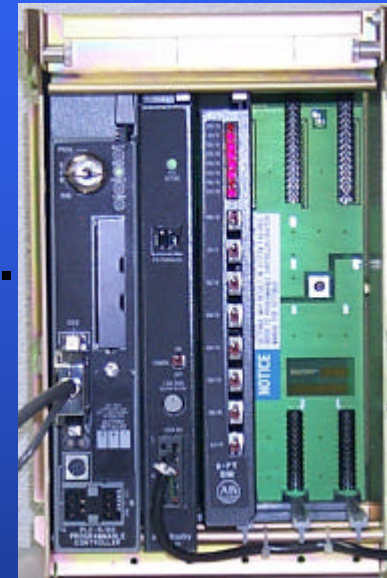
SCADA Vulnerability Demonstration



Operator Interface

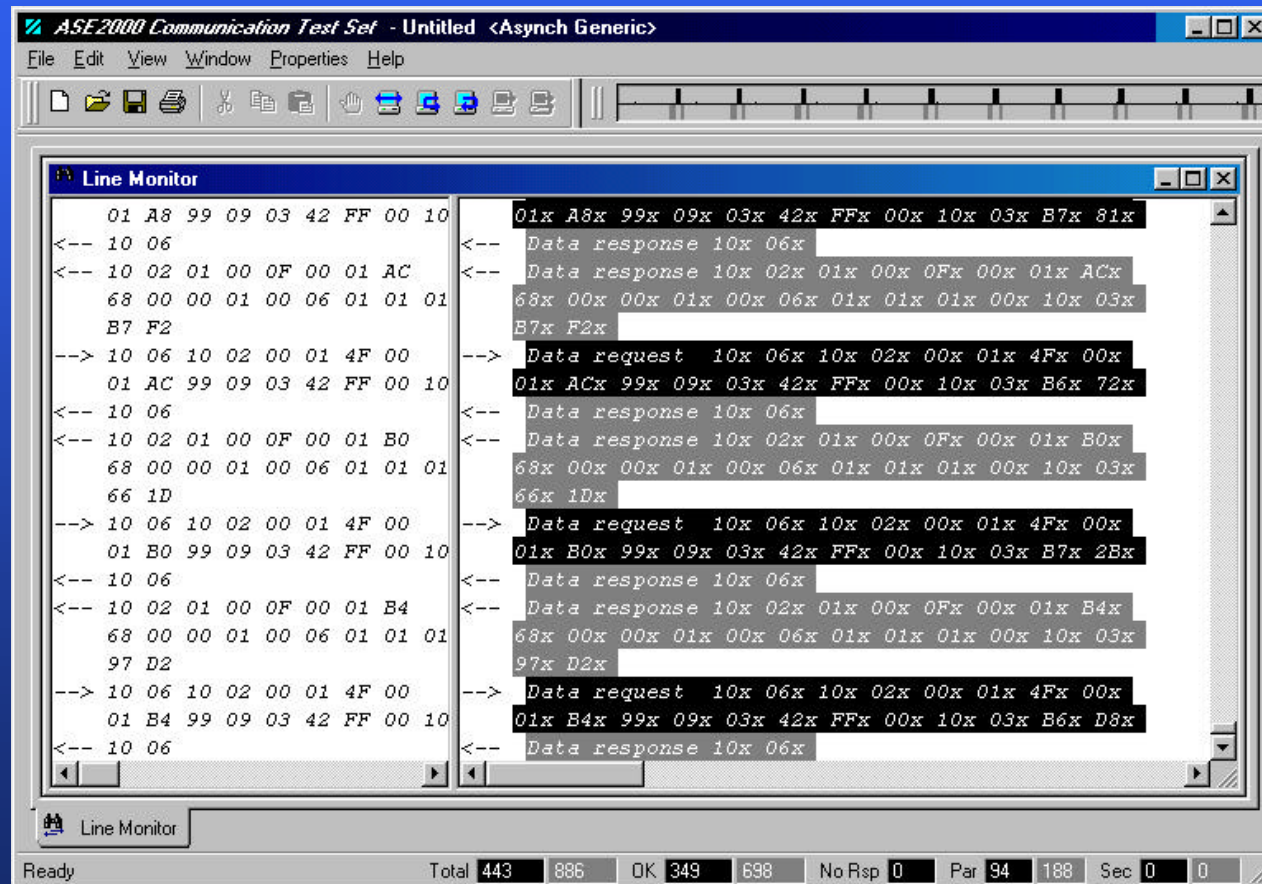


RTU Test Set
(Intruder)



Field Device
(RTU, IED or PLC)

SCADA Message Strings



Repeating easily decipherable format

Captured by RTU test set

Electric Company Vulnerability Assessment

- Conducted by 4 National Labs and consultant
 - Followed a previous assessment from an IT security consultant
- Able to assemble detailed map of perimeter
- Demonstrated internal and end-to-end vulnerability
- Intrusion detection systems did not consistently detect intrusions
- X-Windows used in unsecured manner
- Unknown to IT, critical systems connected to internet
- Modem access obtained using simple passwords
- Located many internal mission critical systems
 - DCS, SCADA, Call Management Systems

Paper Company Vulnerability Assessment

- Conducted by internal IT organization
- Self Assessments
- Vulnerability Scans
 - Modem hunt
 - Run scripts against Internet interfacing device
- Preliminary Results
 - Found connected modems to control systems unknown to IT
 - Used PCAnywhere on DCS console without password access
 - Once able to penetrate open console, ability to navigate network to systems at other plant locations

Industry Technical Efforts

■ IEC TC 57 WG 15

- SCADA/EMS suppliers, National Lab, EPRI, Consultants
- Develop protection profiles for SCADA/EMS
- Treating the computer as a black box
 - » Not addressing RTOS
- Focus is on security of protocol and telecommunication links
 - » Not looking at security of computer at either end

■ Process Controls Security Requirements Forum (PCSRF)

- NIST, NSA, DOE, EPRI, Petrochemicals, Paper
- Develop protection profiles for process controls equipment
 - » For sample case,
 - Define TOE, security environment, security objectives, write protection profile

Industry Technical Efforts (cont)

- IEEE Substations
- NIST
- Open Group
 - Combine security with real time
- Object Management Group - CORBA
 - Combine security with real time
- Vendors
 - Equipment and security
- PCIS

What Do We Want from The Open Group

- It is anticipated the Real Time Security Working Group will be establishing APIs or other hooks for an RTOS kernel security policy
- It is anticipated the Quality of Service Working Group may also address security requirements
- We want to make sure that industrial control needs are included
 - This includes performance requirements

EPRI EIS Program

- Participating in industry activities
 - IEC TC57 WG15, IEEE Substations, PCSRF, OASIS, Open Group, Object Management Group, CSI, SANS, ITAA, NERC CIP, PCIS, Vendors, PKI Forum, Others
- Developing technical understanding of issues
- Forming vendor teams
 - SCADA/EMS
 - DCS
- Developing guidelines and training programs
 - Security Primer, T&D Primer, Power Plant Primer, T&D Guidelines, Substation Guidelines, Integrated Security Procedures, Security Testing Procedures
- Workshops