Process Control and SCADA: Protecting Industrial Systems from Cyber Attack

Mark Fabro, CISSP, CISM
President and CEO
Lofty Perch Inc.
Agenda

• Review of Process Control System / SCADA terminology
• Threat and Risk as applied to industrial control systems
• Attack vectors / past incidents
• Mitigation Strategies
Disclaimer

References made herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by Lofty Perch Inc..

Please use any described security tools and techniques at “your own risk” – i.e. carefully evaluate any tool prior to using it in a production Control System Network.
Defining SCADA

- Supervisory Control and Data Acquisition Systems (SCADA) systems are:
  - Highly distributed systems used to control geographically dispersed assets (water supply systems, oil and gas pipelines, electrical power grids, railway systems).
  - Used where centralized data acquisition and control are critical (or practical) to overall system operation.
Defining Control Systems (CS)

- Control Systems (CS) are used to control manufacturing processes such as electric power generation, oil and gas refineries, and chemical, food, and automotive production.

- CS are integrated as a control architecture containing a supervisory level of control overseeing multiple, integrated sub-systems that are responsible for controlling the details of a localized manufacturing process.
Emerging Nomenclature

• Today, most people practicing business operations use the term Industrial Control Systems (ICS)
• This is slowly being accepted across all realms and usually understood by all fields
So what *is* a Control System?

*Usually found in a designated critical infrastructure sector, a control system is a collection of devices or components working together for a common process, controlled by a master entity that can direct, regulate, and refine the behavior of those devices or components through observations and commands.*
Critical Infrastructure Sectors

- Food
- Finance
- Energy and Utilities
- Government
- Healthcare

- Safety
- Communications and IT
- Transportation
- Water
- Manufacturing

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Information Technology

- National Monuments and Icons
- Nuclear Reactors, Materials, and Waste
- Postal and Shipping
- Public Health and Healthcare
- Telecommunications
- Transportation
- Water

SecTor – November 21/22, 2007 – Toronto
In the Last Several Years…

- Hackers have compromised:
  - major water utilities causing damage
  - dams and reservoir control systems
  - portions of the energy T&D capability
- Hostile mobile code and excessive packet storming have caused at least 4 nuclear facility shutdowns
- Network failures have cause more than 1000 in-flight planes to have no communications and force
- Major urban centers have had their traffic systems hijacked (lighting/signage)
- Hydro generation, refinery, and pipeline facilities have all experienced catastrophic damage and loss of life due to control system errors
Architecture Review: SCADA & PCS
Control Systems – Concerns

• Life Cycle for Many Control Systems Associated with Critical Infrastructure is on the Order of 15 Years

• Systems Designed for Functionality/Liability, Not Security – Resulting in Inherent Vulnerabilities

• Process Control Networks that Were Isolated Are Now Being Connected to Corporate Networks, Which Creates Cyber Attack Vulnerabilities
# Evolution of IT Security vs. Control System Security

<table>
<thead>
<tr>
<th>TOPIC</th>
<th>INFORMATION TECHNOLOGY</th>
<th>CONTROL SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-virus &amp; Mobile Code Countermeasures</td>
<td>Common &amp; widely used</td>
<td>Uncommon and often difficult to deploy</td>
</tr>
<tr>
<td>Support Technology Lifetime</td>
<td>3-5 years</td>
<td>15 to 20 years</td>
</tr>
<tr>
<td>Outsourcing</td>
<td>Common/widely used</td>
<td>Rarely used</td>
</tr>
<tr>
<td>Application of Patches</td>
<td>Regular/scheduled</td>
<td>Slow (vendor specific)</td>
</tr>
<tr>
<td>Change Management</td>
<td>Regular/scheduled</td>
<td>Legacy based – unsuitable for modern security</td>
</tr>
<tr>
<td>Time Critical Content</td>
<td>Delays are usually accepted</td>
<td>Critical due to safety</td>
</tr>
<tr>
<td>Availability</td>
<td>Delays are usually accepted</td>
<td>24 x 7 x 365 x forever</td>
</tr>
<tr>
<td>Security Awareness</td>
<td>Good in both private and public sector</td>
<td>Generally poor regarding cyber security</td>
</tr>
<tr>
<td>Security Testing/Audit</td>
<td>Scheduled and mandated</td>
<td>Occasional testing for outages</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Secure</td>
<td>Very good but often remote and unmanned</td>
</tr>
</tbody>
</table>
Threat Trends

Era of Legacy Control System Technology
- Password Guessing
- Back Doors
- Sweepers
- Network Management Diagnostics

Era of Modern Information Technology
- Distributed Attack Tools
- Attacks
- Probes/Scans
- “Stealth”/Advanced Scanning Techniques

Control System Zone of Defense
- Automated Probes/Scans
- WWW Attacks
- "Stealth"/Advanced Scanning Techniques

Intruder Knowledge
- High
- Low

Attack Sophistication
- High
- Low

Observations…

“.. on [Al Qaeda's] laptops, there had been all these [sic] probing of sites dealing with programming of supervisory control and data acquisition (SCADA) systems and control of SCADA systems within electrical and other power company scenarios.”

Cyber Security Vulnerabilities in Control Systems
OSI ARCHITECTURE

PROCESS ‘A’

Application Layer
Presentation Layer
Session Layer
Transport Layer (TCP)
Network Layer (IP)
Data/Link Layer
Ethernet (Physical)

APPLICATION PDU
PRESENTATION PDU
SESSION PDU
TRANSPORT PDU
PACKETS
FRAMES
BITS

PROCESS ‘B’

Application Layer
Presentation Layer
Session Layer
Transport Layer (TCP)
Network Layer (IP)
Ethernet (Data/Link Layer)
Ethernet (Physical)

COMMUNICATION CHANNEL
Examples: Protocol Vulnerabilities

- No authentication amongst ‘isolated’ components
- ICCP/DNP3 fully published and open for review
- OLE for Process Control (OPC)
Protocols (partial list)

- ANSI X3.28
- BBC 7200
- CDC Types 1 and 2
- Conitel 2020/2000/3000
- DCP 1
- DNP 3.0
- Gedac 7020
- ICCP
- Landis & Gyr 8979
- OPC
- ControlNet
- E/IP
- DH+
- ProfiBus
- Tejas 3 and 5
- OPC
- Modbus
- TRW 9550
- UCA

Many homegrown and proprietary protocols are available and used in control systems today.
Modbus

- Created in late 1970’s by Modicon
- Situated at Layer 7 (App) in OSI model
- Allows for a PLC to:
  - access another PLC
  - to respond to other devices
  - report errors
More Modbus

- **Modbus ASCII**
  - Serial RS-232 or RS-485

- **Modbus RTU** (Most common)
  - Serial RS-232 or RS-485

- **Modbus Plus (Modbus+, MB+)**
  - Proprietary to Modicon
  - Twisted pair up to 1Mb/s
  - Uses token rotation

- **Modbus TCP/Ethernet (developed for Internet)**
  - Transported within TCP/IP data packets
  - Uses Port 502

Some consider Modbus Plus to have some security through obscurity, but converters provide direct access to MB+ networks!!!
DNP3.0

- Developed by Harris Controls in 1990, made public in 1993
- Open protocol derived from EPA (other was IEC 60870-5-101)
- Widely used in water, O&G and electricity sectors
- Features include:
  - Peer-to-peer and master/slave
  - Addressing for 65535 devices
  - Confirmation, time-outs, error recovery, and time synchronization

- SCADA/EMS applications
  - RTU to IED communications
  - Master to remote communications
- Used in N.A., S.A, Aus (with IEC used in Europe)
- Also available as DNP over IP and uses port 20000
OLE for Process Control (OPC)

- Uses Microsoft© Object Linking and Embedding
  - DCOM/COM, RPC
- Original standard developed in 1996
- Designed to accommodate for huge diversity in vendor solutions
  - Industry required a way to allow for easy integration with diverse technologies
- Provides for various data scenarios and requirements
  - OPC for Data Access (OPC-DA)
  - OPC for Data Exchange (OPC-DX)
  - OPC Alarms and Events (OPC-A&E)
  - OPC Historical Data Access (OPC-HDA)
  - OPC XML Data Access (OPC-XMLDA)
OPC Foundation defines specific set of DLL’s to be used for ALL solutions.

Traditional model required 1:1 mapping of vendor technology and vendor drivers.
OPC Data Access (OPC-DA)

- Provides real-time access to control process and data
- Server allows for acquisition from any location
- Collects most current value available
  - may be last one resident in OPC server
  - may invoke secondary cal to field
- Data has three (3) attributes
  - Value
  - Quality
  - Time
- Usually only provides information for short time periods
- Compromised DA capability allows attacker to:
  - Read/write to system
  - Denial of service
  - Session hijacking
OPC Data Exchange (OPC-DX)

• Allows for server-to-server connections
  – Data sharing with remote locales/peers
• Does not require an intermediate OPC client
• Can create effective sharing for disparate OPC servers collecting different data (protocol) data sets
OPC Alarm & Events (OPC-A&E)

- Does not provide an on-demand stream of data
  - may only provide triggered (threshold) events
    - Rate increase; exceed fill points; operator changes
- A&E servers may report to multiple enrolled clients (use “callbacks”)
- Use usually for unsolicited massages indicating a notable state change
- Compromised A&E capability allows attacker to:
  - Change outputs to operator
  - Denial of service (alarm overload)
  - Modify common operating picture
OPC Security*

- Has three (3) levels
  - No security
  - Uses host OS DCOM security settings (of which there are 7)
  - OPCsec (OPC server defines access)
- OPC/DCOM Authentication uses local domain/AD credentials
  - Vulnerability to all RPC flaws
- Default 2000/XP does not perform DCOM connection, SMB, or object access
- Susceptible to remote server browsing
- Lack of authentication

*See DRAFT Whitepaper WP2 (BCIT/Digital Bond/Byres Security)
The Inter-Control Center Communications Protocol (ICCP) is being specified by utility organizations throughout the world to provide data exchange over wide area networks (WANs) between utility control centers, utilities, power pools, regional control centers, and Non-Utility Generators. ICCP is also an international standard: International Electrotechnical Commission (IEC) Telecontrol Application Service Element 2 (TASE.2).
• November 28 ’06
• DNP Scanning Dec ‘06
Experiences from Assessments
Findings - Policy

• Lack of security policy specific for control domain
• SCADA network separated only by VLANs and rudimentary ACLs
• No change management policy
• Physical security policy richly enforced (but OPSEC does not accommodate for access past defences)
• No Security Agreement (SA) with vendor, no SA with contractors
Findings – Vendor Defaults

• Vendor default accounts and passwords have not been changed
• Guest accounts still available
• No mechanism for schedule in place for updates/upgrades
Findings - Auto login

- Primary HMIs do not require username/password to get control
- HMIs may be secured physically but not electronically
- VNC enabled EWS
Findings – Internet Access from CS LAN
Findings – Direct Connection to CS LAN from Corporate
Findings – Dual Connectivity from Operations LAN
Direct Access to CS LAN from Internet (via VPN)
Findings – CS Applications

• Absence of testing of core OS
  – Standard SCADA builds are rare (unused SW remains on systems)
  – No testing in place for remaining applications

• Many insecure applications within key control servers
  – To aid in operator boredom
  – To aid in operator net access
  – To aid in data manipulation

• Assessments discovered rogue applications trying to call home
  – Hostile ICMP payloads
  – Covert channel over DNS
Assessment Findings – Networking

• Vendor access (direct via VPN) into control network
• Access to main switch is by unsecured telnet, and main switch gives all access to all comms
  – Switches use default access credentials
  – Traffic is not filtered by port (i.e. port filtering is not enabled)
• No encryption or authentication on the control network
• Dynamic ARP is used with no ARP monitoring
• Firewalls have some interesting rules, sometimes very simple:

  # $fw add-rule "allow udp from _any_ to _any_ 0-65535"
  # $fw add-rule "allow tcp from _any_ to _any_ 0-65535"
CS LAN Uses Corporate Services

- Outbound connections to use Corp services
  - DNS
  - HTTP
  - FTP
  - AD
Vendor-centric Commonalities

• Vendor provides turnkey solution in each customer location

• Commonality among deployments
  – Same remote access mechanism
  – Same username/password
  – Same technology (brand, device, etc.)
  – Same addressing schema
  – Same vulnerabilities
Assessment Findings – Field Devices

- PLCs unknowingly have embedded web servers
- PLCs have embedded webservice enabled
- Data used as a significant step in enumeration
- Compromised embedded servers allow attacker to gain highest trust level
Assessment Findings: Coding and Insecure Development Practices

- Basic flaws in programming can be discovered and leveraged
- Vendors (proprietary) are very vulnerable

**Least privilege**
- Buffer overflows (stack and heap)
- Suid errors
- Race conditions
- Poor cryptography
- Hard coded IP space
- RPC/DCOM

**Telnet**
- GUI
- Password use/storage
- File Access
- X-windows
- rsh (instead of ssh)
- sprintf / strcpy
- Accept all multicast
Anatomy of an Attack
Typical Attack Steps

1. Target Identification / Selection
2. Reconnaissance
3. System Access
4. Keeping Access
5. Covering the Tracks
Reconnaissance

• Mapping the target assets and resources
• Open Source Intelligence
  – External Web Site
  – Google (Internet) Searches
  – DNS Lookups
• Dumpster Diving
• Social Engineering
• War Dialing / War Driving
• Scanning
  – Asset/service discovery, network connectivity
• Insider Threat
Keeping Access

• Depending on goals, attacker may/may not care
• Escalation of privileges
• Account creation
  – Becoming a trusted user
• Password cracking
• Backdoors / Trojan Horses
• Rootkits
Covering the Tracks

• Physical damage
• Hiding files
• Log file modification / deletion
• Covert channels (loki, ncovert)
• Hiding activity
  – Altering operators view at HMI
Historical Security Events
Cyber Incidents and Infrastructure

- As early as 1982 (Gazprom)
- Worchester Airfield
- 1994 (Salt River Project)
More Interesting Cyber Events

- **2003** ‘Slammer’ disables Davis-Besse safety mechanism
- **May 2001** Cal-ISO attack
  - Undetected for 17 days from Californian and China (last source)
  - Compromise almost penetrated into energy provisioning systems
- **August 2003** Blackout
  - Malfunction in Alarm and Event Processing (AEPR) due to race condition
- **2004** ‘Sasser’ disables connect oil platforms for several days
- **Sept 2004** SOCAL air traffic control failure
  - Windows bug forced server to auto-reboot after 49.7 days
  - 800 planes in the air w/o contact for 3 hours
  - 400 delays, 600 cancellations
- **2005** ‘Zotob’ attacks Daimler-Chrysler
Case Study: Australia Maroochy Shire Waste Water Attack (April 2000)

**Event:** Hundreds of thousands of gallons of untreated sewage intentionally released into parks, rivers, and hotel grounds

**Impact:** Loss of marine life, public health jeopardized, $200,000 in cleanup and monitoring costs
Maroochy Waste Water Attack (2)

- **Incident Specifics:**
  - SCADA system had 300 nodes governing sewage and drinking water
  - Used OPC ActiveX controls, DNP3, and ModBus protocols
  - Used packet radio communications to RTUs
  - Executed almost 45 separate attacks over 2 months

- **Attacker Specifics:**
  - Was recently fired
  - Used commercially available radios and stolen SCADA software to make his laptop appear as a main pumping station
  - Had complete control
Case Study: Olympic Pipeline Explosion (1999)

**Event:** Bellingham, WA (not an attack) SCADA failure results in poor control and 250,000 gallons of gas to flow into river (where it ignited)

**Impact:** 3 fatalities, property damage >$45M, matching fines of $7.86M against two companies.
Olympic Pipeline Explosion (1999)

- Incident Specifics:
  - SCADA system used VAX controllers more than 100 miles from incident point
  - LAN connection to IT network with no in-depth security or mobile code countermeasures
  - Modifications to operational databases and historians caused state acquisition (scanning/polling) timing to change from 3 seconds to more than 360 seconds….

That’s more than a 6 minute delay!!
Varied Attack Schemas

- Protocol Attacks
  - Communications (OPC, ICCP, DNP3)
  - Hijacking
  - MITM
- Database Attacks
- SMTP Tunnelling
- DoS ICMP redirects/nmap etc.
- DNS corruption and redirects
- Remote Service Exploitation (X11)
- Fragmentation Attacks
- Core Dumping Attacks
- Covert Channel Attacks
- ARP spoofing and poisoning
- Reverse Engineering
- Vendor Specific Exploitation

http://www.us-cert.gov/control_systems/csddocuments.html
Mitigations
Defensive Strategies: Multiple Pieces

Proactive Security Model

- Map Architecture
- Risk Assessment
- Digital Asset ID
- Profile Model
- Identify/Remove Vulnerabilities
- Standardize Policies
- Incident Response
- Training

- USER AWARENESS
- ENCRYPTION
- ID
- IDS
- FIREWALLS
- SECURITY POLICIES
Key FW ‘components’ for CS

- Deployed with the golden rule
  - *That which is not explicitly allowed is denied*
- Mirror FW and ACL wherever possible to avoid mis-configuration
- Deployed with domain separation with session tracking
- Monitor activity on business domain for control ports
  - 102 ICCP, 502 ModBUS, 20000 DNP, etc
- Monitor system events and restrict outbound traffic
  - Counter piggyback on trusted connections
- Protected audit trails that have been created
- Use personal firewalls on control domain stations if possible
- Supports a ‘trusted path’ to users and a ‘trusted channel’ to other IT devices
Traditional FW-Centric Defensive Problems

• Denial of Service
  – Request overload
  – Reassembly attacks
  – Connection flooding
  – Key generation attacks

• Fragmentation
  – Perimeter bypass

• Covert Channels and Session Hijacking

• Bounce Attacks (where FW has inherent servers)

• Token-based ‘race’ attacks

• OOTB modifications lead to:
  – Transformation of FW into router
  – FW becomes a simple proxy gateway
  – Broken on-stack DNS (Divulge internal naming structure)
Emerging Solutions for CS and SCADA Firewalls

- Open source (Linux) firewall stacks
  - Using modified ‘netfilter’ for Modbus/TCP
  - Application-layer filtering
- PLC firewall using iptables
  - Auto discovery (passive) of IP and MAC for devices that are being protected
- Deep Packet Inspection Firewalls (DPI)
- PLC based micro firewalls (on the appliance)
- Kernel locking and operational ‘snapshots’
Defensive Strategies: IDS

- Intrusion Detection is ‘passive’
- Signature based
- Only minimal signatures available for CS domain
- After-market development required
  - Simple opens source signatures
Defensive Strategies: IPS

- Intrusion Prevention is usually ‘active’
- Activities may prove detrimental to real-time environments
  - Packet scrubbing
  - Packet sniping
- New work in DMZ to have passive IPS create sigs for IDS engines
Cryptography and SCADA

- Required to reduce the vulnerability regarding plaintext traffic
- Can be introduced in one of two ways
  - ‘bump in the stack
  - ‘bump’ in the wire
- Industry reticence may be due to possible latency
- Key management issues scale as size of control domain

*See AGA-12 ‘SCADA Crypto’*
Security Information Management (SIM) in Control Systems

“What do you have - and what is it doing?”

**Management**
- Administrative Controls
- System Monitoring
- System Audit Log

**Threat Mitigation**
- Attack Path Analysis
- Graphic Visualization
- Automated Incident Response

**Reporting**
- Real Time and Historical
- Defined and Customized
- High Speed Query

**Incident Analysis**
- Event Normalization and Categorization
- Rules-based Incident Creation

**Telemetry Aggregation**

**Network Awareness**
- Switches, Firewalls...
- Remote access
- Device Logs
- Network Topology
- Device Configs
- Network Traffic

**Archiving**
- Continuous
- Compressed
- System Audit Log, Incident, and Raw Event data
OPSEC Plan Elements

- Generate a cyber OPSEC program for control systems users
- Define management responsibilities and cultural considerations
- Define OPSEC management boundaries for control systems
- Write a cyber security OPSEC policy for control systems
- Ensure control system operator/user input on development of the security culture
- Implement and monitor a control system OPSEC program

See: OPSEC Security Recommended Practice, DHS, January 2007
Including Security in the Lifecycle

DESIGN
- Scalability
- Architecture
- Communications
- Reliability

BUILD
- Objects/Libraries
- Migration Path

MAINTAIN
- Reporting
- Diagnostics & Repair
- Reporting
- Operator Management

OPERATE
- Operator Visualization & Navigation
- Trending
- Reporting Capability

Technical Security Controls
System Controls
Trusted Recovery

Determine Risk

Change Management
Accountability

OPSEC Security Recommended Practice, DHS, January 2007

SecTor – November 21/22, 2007 – Toronto
All Together Now: Defense in Depth

• D-I-D creates and aggregate posture that is too difficult to break
• Uses basic security principles at each level of the overall architecture
• Use the concept of ‘zones’ to facilitate granular security
The Approach

- **Perimeter Security:** Policies, Firewalls, P2P, VPN, ACLs
- **Network/Host Security:** Firewalls, IDS/IPS, SIM
- **Perimeter Security:** Policies, Firewalls, P2P, VPN, ACLs
- **Core Services Security:** SCADA Policies, Firewalls, Custom IDS, SIMS, Correlation

**INCREASING OVERALL SECURITY**
SCADA Honeynets

• Like traditional honeynets, system is deployed to catch attackers
• Can use different schemas
  – Real systems
  – Fake ‘honeyd’ deployments
• Several operations in place now
  – Electric, academic, transportation
• Database of activity is growing
US-CERT Control Systems Security Program (CSSP)

• Dedicated function of US-CERT for supporting security of Control Systems
  – Supported by Idaho National Laboratory
  – Facilitate the US-CERT capability to coordinate control systems incident management and
  – Assess vulnerabilities and risks associated with control systems
  – Enhance control systems security awareness through training and outreach initiatives
  – Provide strategic recommendations for control systems security research and development needs

• CS2SAT Assessment Toolkit
• Recommended Practices program
• Procurement Language (v1.7)

http://www.us-cert.gov/control_systems/index.html
Thank You

fabro@loftyperch.com

15-505 Hood Road
Markham, Ontario, L3R 5V6
CANADA
(905) 489-2827
http://www.loftyperch.com