Data Diode Cybersecurity Implementation Protects SCADA Network and Facilitates Transfer of Operations Information to Business Users

Speaker:
Dr. Ronald Mraz, President & CEO
Owl Computing Technologies

2016 ISA Water / Wastewater and Automatic Controls Symposium
August 4-6, 2015 – Orlando, Florida, USA
Presenter

- Dr. Ronald Mraz, President & CEO
- Founder of Owl Computing Technologies
- 20 years of private sector experience including IBM & Westinghouse
- Doctorate from Carnegie Mellon University, Masters of Science from Syracuse University, BS from Drexel University
- Senior Member of IEEE, holds 12 patents
Presentation Outline

• Introduction to Owl
• DHS Recommendations for Defending Industrial Control Systems/SCADA
• What is a Data Diode
• Applying Data Diodes to Protect SCADA, PLCs, Historians
• Use Cases
• Summary
About Owl Computing Technologies

US owned and operated
- US supply chain
- US R&D & manufacturing
- US based Technical Support & Service
- US Secret and Top Secret Clearances
- Self-funded Development

Experience
- Exclusive focus on cybersecurity for 17 years
- Over 2000 deployments globally
- Global Sales and Service
- Accreditation Services
- Configuration Management Services

Multi-Market Solutions
- Government Cross Domain Solutions
- DoD & Intelligence Agencies
- Critical Infrastructure Network Defense
- Utilities: Electric, Gas, Water
- Energy: Oil & Gas, Petrochemical
- Telecommunications
- Financial Services

Technology Innovator
- Single 1U, all-in-one solution
- Server based Communication Card Systems
- 24 technology patents
- Deterministic one-way transfers
  - Non-routable protocol
  - EAL Certified
  - UCDSMO Base Line
  - Penetration Tested
Cybersecurity Challenges for Critical Infrastructure (per DHS)

Cyber threats to critical infrastructure systems are increasing with increased frequency. For many industrial control systems (ICS), it’s not a matter of if intrusion will take place, but when. In Fiscal Year (FY) 2015, 297 incidents were reported to the Critical Infrastructure Cybersecurity (CIC) program, and many more that were not reported or not identified. The capabilities of the adversaries have grown, and cyber attacks are occurring more frequently. Tightening a network with a defensive perimeter alone is no longer adequate. Simply blocking access to the network leaves too many vulnerabilities. Well-planned and well-implemented strategies that rely on a good network architecture, however, can help in identifying and responding to intrusive attacks.

This paper presents several strategies that can be implemented to protect critical systems from cyber threats and incorporates additional risks. The primary objective of this paper is to provide a framework to guide the design and implementation of robust cybersecurity strategies.

Cyber Threats

- Execution of Malware: 38%
- Unpatched Systems: 29%
- Open Connections: 17%
- Perimeter Breaches: 4%
- Compromised Credentials: 1%
- Exploit Back doors: 2%
- Miscellaneous exploits: 1%
DHS Seven Strategies for Defeating Threats

1. Application Whitelisting
2. Configuration/Patch Management
3. Reduce Attack Surface
4. Defendable Environment
5. Manage Authentication
6. Implement Secure Remote Access
7. Monitor & Respond

Highlights the use of Data Diodes

These strategies could have prevented 98% of attacks in 2014 and 2015
According to third party analysts, data diodes provide the highest level of network security next to physical separation (air gap).
Three Ways Data Diodes Support Various DHS Strategies

1. **One-Way Communications Out of the Plant**
   - **Build a Defendable Environment**: Segment networks and restrict host-to-host paths
   - **Reduce Attack Surface Area**: use a *data diode* to provide network segmentation
   - **Implement Secure Remote Access**: Implement monitoring only with access enforced by *data diodes*

2. **One-Way Communications Into the Plant**
   - **Configuration/Patch Management**: Provide secure configuration/patch management program centered on safe importation of trusted patch updates

3. **Two-Way Communications with the Plant**
   - **Reduce Attack Surface Area**: If bidirectional communication is needed use a single port over a restricted path
Implementing the Three Uses
What is a Data Diode?

- Hardware based cybersecurity designed to be only One-way
- Impervious to software changes or attacks (hardware cannot change)
- Defends the perimeter of the source network
- Transfers data out of the protected network
How does it work?

- Data Diode products are separated into two halves with one diode on each side working together to create a DualDiode®

  Blue - **send** only side  \hspace{1cm}  Red - **receive** only side

- Specific circuitry allows each side to only perform a single task
- Physically prevents data from ever moving in the opposite direction
• Hardware DualDiode, two communication cards in series
• Creates optical “air gap” and enforces network separation
• IP Proxies – terminate and originate IP traffic
• One-way hardware constrained by single fiber optic cable
What do Data Diodes look like?

- 1U – single box solution
- DIN rail – single box solution
- Server based PCIe card kit solution
But the Dual Diode is just the foundation …

Menu management only – no command line

Separate “blind” routing tables

Role Based Access Controls

Physically separate admin access to each side

Physical separation fans, power supplies, network connections

White Listing

Routable information (MAC, IP addresses) never transferred

Only the Payload is transferred

Protocol Break - ATM protocol used for data transport

Air Gap created between Source and Destination networks

Owl data diodes form a Defense In Depth solution
Critical Infrastructure Use Cases

- **Water, Wastewater**
  - HMI Screen replication
  - Historian data

- **Power Generation**
  - Turbine, Nuclear, Fossil, Hydro plant performance data
  - Historian replication
  - Secure remote monitoring – syslog, alarms, events

- **Substations, T&D**
  - Secure monitoring of alarms, events, syslog messages
  - Transfer of Files, email, security video

- **Oil and Gas**
  - Transfer of historian data, alarms, events
  - Interfaces: MODBUS, OPC,

- **Financial Services**
  - ATM machines, data repositories
  - Remote branch transfers to HQ, DB replication

- **Compliance Reporting**
  - Transfer of consolidated information
Supports simple and easy security and established data replication flows
Multi-Facility Architecture

OT Networks

IT/Corp Network

Historian, Syslog & other data

Replicate Historian, Syslog & other data
Range of Supported Vendors

- ABB
- Cisco
- Dell
- General Electric
- Honeywell
- IBM
- Industrial Defender
- InStep eDNA
- Invensys Wonderware
- McAfee
- Mitsubishi
- PAS Alarm Company
- Rockwell Automation
- Rockwell Collins
- Rolls Royce
- Schneider Electric
- Scientech
- Siemens
- Stratus
- Symantec
- Tripwire
Support for Critical Infrastructure Vendor Applications

Supported Transfer Applications

- Fox Guard Patch Management
- GE Proficy Historian
- GE OSM Support
- PAS Alarm Management
- Schneider RemoteWatch
- Schneider Wonderware eDNA Historian
- Schneider Wonderware Historian
- Scientech R*Time
- OSIsoft PI historian
- Rockwell Automation
  - RSLinx Classic
  - FactoryTalk Gateway
  - FactoryTalk – Historian
- Rolls Royce PMS
Supported Protocols

- Email Alerts and Events (SMTP)
- FTP/SFTP
- Modbus
- OPC Foundation Certified, Supporting DA, A&
- Remote File Transfer for Reporting, Alarms, Events
- Remote HMI Screen Replication
- SQL Database Replication
- SNMP Traps
- Syslog Transfer
- TCP Transfers
- UDP, Multicast, Broadcast, Unicast (Data Transfer and Video)

Ability to interface and transfer a wide range of data types, protocols and formats for a variety of situations
Summary

- Firewalls are being hacked every day
- Defense In Depth is imperative
- Department of Homeland Security is recommending:
  - Multiple Strategies
  - Data Diodes
- Data Diodes are:
  - Hardware-based cybersecurity
  - Impervious to software attacks
  - Deployed in numerous scenarios globally