Protecting CII using the Fox DataDiode

Jeremy Butcher, Fox-IT

Fighting Cybercrime
Protecting Secrets
Intelligence
Digital Forensics
Fox-IT

A specialized security company that helps governments & companies to securely operate their most critical environments in a fast changing digital world

our mission: making technical and innovative contributions for a more secure society
Fox-IT provides security in a digital world for:

- Governments
- Financial Sector
- Critical Infrastructure
- High Security enterprise

- espionage
- hacking
- fraud
- terrorism
A little background on CII security
CII

Critical Industrial Infrastructures (CII) are the process and control systems (PCS) that manage vital parts of national/regional facilities such as water, sewerage, electricity and gas/oil supply. CII disruption may have a serious economic and human impact. CII Protection is therefore essential.
Typical CII

Internet
- Partners
- Vendors
- Customers
Out of our control

Business Systems
- Email
- Files
- Databases
Outside SCADA realm

Admin Network
- Monitoring
- Backups
- Logging

SCADA
- HMI
- Acquisition and Control
- Real-time control

Sensors
- PLCs
- RTUs
- Valves
Highly reliable
• Vendor Access
  – Remote monitoring
  – Remote access
Common Threats

• Electronic and IT systems in Critical Industrial Infrastructures are constantly threatened:
  - Operator/vendor mistakes
  - Sabotage by disgruntled employees
  - Terrorists/fundamentalists
  - Hackers (and wannabe hackers)
  - Cybercriminals (e.g. financial extortion)
  - Competition (espionage)
  - Foreign governments (want ability to cripple CI)
  - ...
Cyber Attacks on CII are no myth

Hackers Break Into Power Station, In Less Than A Day
By Humphrey Cheung
6:04 AM - April 10, 2008

San Francisco (CA) - It took hackers less than a day to take over several desktops at a major power company. Ira Winkler, a penetration testing consultant, and his team were able to trick company employees into clicking false links which contained self-installing Trojan horse software. Winkler says his team had complete control of the computers and could have caused even more damage to the company's power production and distribution systems.

Schoolboy hacks into city's tram system
By Graeme Baker
Last Updated: 2:46am GMT 11/01/2008

A teenage boy who hacked into a Polish tram system used it like "a giant train set", causing chaos and derailing four vehicles.

The 14-year-old, described by his teachers as a model pupil and an electronics "genius", adapted a television remote control so it could change track points in the city of Lodz.

Twelve people were injured in one derailment, and the boy is suspected of having been involved in several similar incidents.

The teenager, who was not named by police, told them...

Hackers Break Into Water Processing Plant Network
Darknet spilled these bits on December 14th 2006 @ 7:52 am

When things like this happen it's kinda scary, like a while back when someone managed to get into a highly secure power station network through a stupid contractors laptop that was connected to the net via dialup and to the uber 'secure' power station LAN.

Electricity Grid in U.S. Penetrated By Spies

WASHINGTON -- Cyber spies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.

The spies came from China, Russia and other countries, these officials said, and were believed to be on a mission to negate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war.
Common Threats

"The truth is also that a well-placed squirrel can wreak almost as much havoc as a cyber attack on a power grid."

Charles Palmer, Director
Institute for Advanced Security, IBM, June 2010

“We must find this well-placed squirrel, and ensure that it never falls into the hands of our enemies.”

Shawn Moyer, esq, The Internet, June 2010
Business vs. security
Business: Data Sharing

• Share more information **from CII systems**
  – Real-time billing
  – Reporting
  – Logging
  – JIT: Just-in-time delivery

• Remote vendor support
  – Decrease costs for support
CII: Continuity is paramount

• **Availability** of systems and data
  – Systems in the network must be able to process data all the time

• **Integrity** of the systems and data
  – Unauthorized persons or processes may not be able to interfere with the systems

• **Confidentiality** of the data
  – In most cases data in the network is not sensitive
Contradictory Requirements

• Maintain high continuity
  – Enhanced Protection
    • Disconnect process & control networks?

• Share more information
  – Business requirements
  – Remote vendor support
Business vs. security
What if you can have both?
What if you can disconnect the networks...

• From the threat perspective

• Be as safe as possible

• Disconnect your CII systems from cyberthreats
...and still share information

- From the CII perspective
- Meet your business requirements
- Allow for remote vendor support
CII security
The Fox DataDiode
Network Data Diode

• One-way communications
• Hardware only
  – no software, firmware or other complex logic
• Impossible to penetrate or attack
• Certified devices (up to CC EAL7+)
How does it work?

Hardware Data Diode

SERVER NIC

INPUT

ONE-WAY

OUTPUT

SERVER NIC

LIGHT EMITTER

LIGHT RECEIVER
How does it work?

Hardware Data Diode

SERVER NIC

INPUT

ONE-WAY

OUTPUT

SERVER NIC

LIGHT EMITTER

LIGHT RECEIVER

Possible
How does it work?

Hardware Data Diode

LIGHT EMITTER → LIGHT RECEIVER

Impossible
How does it work?

**Challenges:**

- How to handle three-way handshake (e.g. TCP)?
- How to ensure data integrity?
- How to manage flow control?

→ Proxy software is required, but this will not affect the security of the Data Diode solution.
Proxy Servers

Data is received or retrieved by the Proxy

Fox DataDiode Protocol

Data is forwarded or made available by the Proxy

Business Network
Typical Applications

- File transfers (FTP/CIFS/SMB)
- Email forwarding (SMTP)
- Streaming video/audio (UDP)

- Remote printing
- Database replication: Oracle, mysql, MSSQL, etc
- LDAP/Active Directory mirroring
- Repository mirroring
- Windows Server Update Service (WSUS)
- Anti-Virus: McAfee, Symantec, etc
- Web site/page mirroring
- Remote network monitoring (SNMP)

- **SCADA/Process Control Security**
Typical Deployment

- Read-only, redundant and fail-safe
- Reliable and proven third party software
- Real-time and historical data transfers
Enhance perimeter security

• Use data diodes to protect critical systems
• Use firewalls on less critical perimeters
Two-way Data Diodes

• Specific requests and responses
• Limited feedback

• Communications format is known and fixed, e.g. XML files

• Not suitable if two-way communications is extensive and/or unspecific
Two-way Data Diode Example

• Replication of Critical SCADA system in business network (other)

• Business network sends acknowledgement of received data in file

• Conditions:
  – Different paths; no routing, no feedback loop
  – No connections, only file drop and pick-up
  – File content filtering

Still more secure than firewalls and DMZ
Data Diode and VPN

- Applicable for remote vendor support

- Vendor remotely monitors status through diode

- Remote access is normally off, but can be activated on request for a limited time (with auto-off timer)

Still more secure than firewalls and DMZ
Efficient CII Protection

- Protection must be effective and efficient.

- Efficient protection is good security, and enables the business and has a low total cost of ownership.

- Let’s compare air gaps, firewalls and data diodes...
Air Gaps, Firewalls, Data Diodes

- **Air gaps**
  - Not real-time
  - Manual transportation
  - Security risks

- **Firewalls**
  - Prone to bugs, mistakes and hackers or disgruntled staff

- **Data Diodes**
  - One-way
### Efficient CII Protection

<table>
<thead>
<tr>
<th>Feature</th>
<th>Solution</th>
<th>Air Gap</th>
<th>Firewall</th>
<th>Data Diode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time Communications</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Automated, no manual intervention</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Not prone to bugs, mistakes or hacking</td>
<td>Yes</td>
<td>No</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Support multiple protocols</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Flexible (configuration, possibilities)</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>
Conclusion

• The CII security threats are real.

• Efficient CII protection is required, while enabling business to share information.

• Data Diodes provide CII protection effectively through their high-security property while enabling business information sharing.
Questions?