Control System Cyber Incident Handling: A Law Enforcement Perspective

Panelists:

Mr. Jeff Morgan, FBI

Cpl. Darren Sabourin, RCMP

SSA Susan Ferensic, FBI

Moderator:

Mark Fabro, Lofty Perch

Introductions

Jeff Morgan, FBI

Process Control Systems Analyst, Cyber Division

Darren Sabourin, RCMP

Corporal, RCMP Technological Crime Unit

Susan Ferensic, FBI

Supervisory Special Agent, Cyber Division,
SCADA Program Manager

FBI

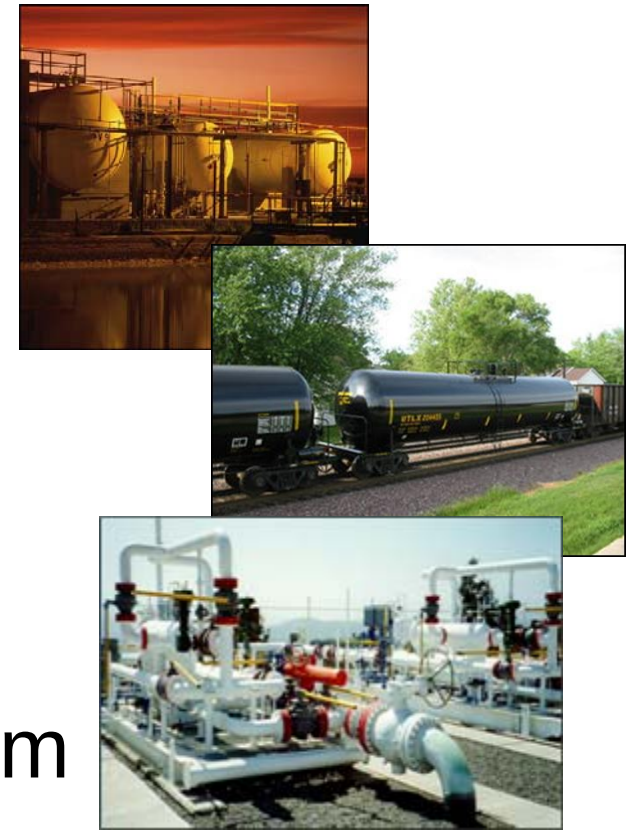
- FBI's cyber mission focuses foremost on serious computer intrusions.
- Trained cyber squads at all 56 field offices and FBI Headquarters.
- Dedicated analysts focused on Process Control / SCADA (PCS) issues and USG collaboration.
- Cyber Action Teams trained in PCS issues and ready to respond.
- Outreach efforts to PCS owners / operators.

RCMP

- Eight (8) Integrated Technological Crime Units (TCU) across Canada
  - Technological Crime Branch in Ottawa.
- Mandate is extensive
  - Computer/Network Intrusions, Computer Forensics, Internet-based Investigations, Mobile/Embedded Device Examination.
- Dedicated positions in each TCU to Critical Information Infrastructure Protection
  - Training/investigational support to areas such as Botnets and SCADA/Control Systems.
- Align strategies with Public Safety Canada's "National Strategy and Action Plan for Critical Infrastructure".
  - Document scheduled for release in Mar/2009.
- October, 2008 SCADA Security Workshop
  - Bringing together Private-Sector owner/operators and Government
  - Learn about Control System Cyber Security and the importance of partnerships and information-sharing.
- Work closely with other National departments and International Law Enforcement.

Emerging Issues

- The changing landscape
  - Trending
  - Chatter
  - National efforts
- Working with the public
- Working with the legal system
- Finding the resources/talent



Observations From the Field

- Lessons from outreach efforts
- What investigators can/should expect
- What asset owners can expect
- Public perceptions of LE actions
- Applying current methods to SCADA/ICS

Research Initiatives – What can be done to help?

- What is needed by L.E. to bring response capability closer to the crime
  - Incident handling
  - Forensics
    - OS vendor cooperation
    - ICS vendor cooperation
  - Bag and tag – how does it differ with ICS?

Open Discussion