RCMP Technological Crime Branch

SCADA/Control Systems – Moving Forward

2011 North American SCADA and Process Control Summit
Orlando, Florida
Technological Crimes - CIP

• Technological Crime Units in Provinces throughout Canada – headquartered in Ottawa.

• Mandate to investigate computer crimes; including network/computer intrusions, cyber or internet-related complaints, and completing forensic examinations of computers, mobile and embedded devices.

• Process Control Systems are specifically addressed in Canada’s Cyber Security Strategy.

• Workshops providing training to owners/operators/Gov’t in Control Systems Cyber Security started in 2008.

Royal Canadian Mounted Police  Gendarmerie royale du Canada
Critical Infrastructure Protection

• Absolute need, and commitment to work with all levels of Government, Public and Private Sector (two-way).
• **Absolute need to work Internationally**
• When assessing criticality, it is key to understand the degree to which your assets are interdependent on other key assets/resources.
• Need to collaborate internationally with FBI, ICS-Cert, and other law enforcement.
• The time is now...not after an incident!
Working alongside the RCMP

• During an investigation, focus is to work alongside key network professionals to identify critical and key data, important to our investigation, and target the acquisition of that data – becoming more prevalent to do this in a live state.

• Operators/Owners: Know who to call!

• Commitment to working with companies has seen benefits.
SCADA/Control System Forensics

• RCMP have committed resources into the development of a tested incident response model for law enforcement.

• Part of the model will include:
  – Porting of traditional forensic tools and techniques to determine what logging, network and system OS information may be available for forensic examination.
  – Leveraging significant experience in traditional computer and network forensics.
  – Determining ingress/egress of data, best methods to connect and obtain data with least impact to system.

• Could this information help you with mitigation/remediation?
SCADA Network Security - Testbed

- Recognition that there is a need to test response strategies within a testbed environment.
- Allow researchers, system engineers and IT Professionals to test architecture, technologies and best practices.
- Government, vendors, owners and operators involved.
- Focal point for collaboration between private operators and public sector stakeholders.
- Opportunities for testing of forensic capabilities within Control System domain.
Thank you

Cpl. Darren Sabourin
Technological Crime Unit
Royal Canadian Mounted Police
email: darren.sabourin@rcmp-grc.gc.ca