SWEDISH EMERGENCY MANAGEMENT AGENCY

SCADA: A New Direction

Personal Reflections and Comments by SEMA

Dr. Åke J. Holmgren, Senior Analyst
Information Assurance Department, SEMA

SWEDISH EMERGENCY MANAGEMENT AGENCY

Background and Disclaimer

- SEMA has overall governmental responsibility for society's information assurance issues in Sweden
- SEMA has been working to increase the security of SCADA systems in critical societal functions for more than ten years
- SEMA supports this talk, but all comments and remarks does NOT necessarily represent the official position of SEMA

SWEDISH EMERGENCY
MANAGEMENT AGENCY

Security through obscurity is dead!

… “the enemy knows the system“ (Claude Shannon)

We need to fix this in less that 10-15 years!

SWEDISH EMERGENCY MANAGEMENT AGENCY

This was true in 2001 …

Example of SCADA systems information (network map) published openly

SWEDISH EMERGENCY MANAGEMENT AGENCY

… as well as in 2008.

Example of SCADA systems information (network map) published openly

SWEDISH EMERGENCY MANAGEMENT AGENCY

Securing People, Processes, and Products

- Need for common approaches of SCADA system security testing
- Secure ’out of the box’ products

  ’Basic security’ should be included (a matter of normal product quality)

  Additional security will cost more (vendors should offer it, users should ask for it)

SWEDISH EMERGENCY MANAGEMENT AGENCY

Cooperation and Information Sharing

SEMA's position: Public-Private Partnerships is key
(technical regulations will not solve this)

- How far can we expand 'the circle of trust'?
- The 'culture clash on the plant floor' continues all the way up through the government sphere
- Interdependent infrastructures and small nations calls for European and international collaboration
- We need better processes for sanitizing information and formal ways of sharing information
- Law enforcement must be more involved (SCADA forensics?)
- Cyber exercises are important, but feedback must be better

SWEDISH EMERGENCY MANAGEMENT AGENCY

Awareness

- Raising awareness of the need for better SCADA security is the most important short term task in Europe

- Less FUD – more about solutions
  (We must not only be threat-driven)

SWEDISH EMERGENCY MANAGEMENT AGENCY

Vulnerability Disclosure and Incident Reporting

SEMA's position: Structured vulnerability management is important

- We need information to build business cases!
- There are too many urban legends out there!

Vulnerability disclosure:

- How do we facilitate the distribution of vulnerabilities?
- The role of CERTs?
- Not all vulnerabilities are created equal, but ranking is difficult

Incident reporting:

- Difficult - National (homeland) security as well as commercial matters makes it sensitive
- Create an open format (template) for reporting incidents
- Maintain closed industry data bases, but report general incident statistics openly

SWEDISH EMERGENCY MANAGEMENT AGENCY

Assurance and Standards

SEMA's position: International standards high priority

- Coordination of standardization activities needed
- Let's not invent the wheel again!
- Standardization does not replace own judgment, tacit knowledge or skills!
- The 'culture of compliance' is dangerous
- Self-assessment tools are valuable, but keep it simple

SWEDISH EMERGENCY MANAGEMENT AGENCY

The Challenge

- The increasing level of complexity in large technical systems (critical infrastructures) demands holistic and systematic risk management
  - The distinction between corporate IT security and SCADA security disappears more and more
  - Implement an 'all threats, all hazards' approach
  - Create a culture of security and safety

Learn from other disciplines – e.g. corporate IT security, safety, finance - and fast track this knowledge!