Institute for Information Infrastructure Protection

http://www.thei3p.org

National Cyber Infrastructure Bulletin
No. 1; October, 2005

PROCESS CONTROL SYSTEMS SECURITY

A June 2005 I3P workshop examined the security of process control systems in the oil and gas industry. Participants included representatives from leading oil and gas companies, Supervisory Control and Data Acquisition (SCADA) and IT vendors, and government experts and researchers. The following are the main findings from the workshop:

Process Control Systems Remain Vulnerable to Physical and Cyber Attacks:

- Process control systems were not built with security in mind – companies use a complex mix of hardware and software systems, often without any basic security (authentication, intrusion detection, encryption, logging).
- The prevalence of old technology and the real-time environment limit security options – shutting down process control systems upon suspicion of an attack is often not possible.
- The oil and gas infrastructure is vulnerable to physical attacks due to the wide distribution of assets and volatility of the material.
- Safe and reliable operation of the oil and gas industry depends heavily on other critical infrastructures, such as telecommunications, electric power, water and transportation.

Threats Against Process Control Systems Are Real:

- Process control system operators should consider serious threats like professional hackers and organized cyber-terrorism.
- A coordinated attack along several threat vectors is a serious long-term threat. A thorough analysis of the real risks (vulnerabilities, threats and probability of occurrence) and consequences (damage restoration time and costs) is critical.
- Access to information about control systems and software tools to compromise them is readily available, often on the web. These industrial automation technologies are used worldwide in the oil and gas industry.

Security Issues from the Industry Perspective:

- How Does it Help Us Make Better Oil? Process control system security is all overhead – asset owners need a business case for implementing security to convince senior management.
- In the oil and gas industry, safety (not security) is always the primary concern. Security strategies must fit into this framework.
- Dependability, reliability and redundancy are critical for SCADA – the availability of systems trumps everything else.
- Control systems are often remotely accessible and increasingly connected via the Internet or through wireless networks.
- In many cases attackers can access critical control systems through non-critical corporate networks.
- Insider attacks from disgruntled employees with detailed system knowledge are one of the most serious security challenges.
- The high cost of patching and constant software security fixes puts a strain on the oil and gas industry and reduces security.
- The increasing use of commercial software and networking technologies introduces known vulnerabilities.
- Inadequate information sharing within the industry and with government may contribute to an apparent dearth of incident and threat information.

How These Problems Can Be Addressed at the National Level:

- Solutions require close collaboration between oil and gas operators, vendors, the research community and the government.
- Widely-accepted security standards, best practices and metrics for the oil and gas industry are urgently required.
- Inherently secure SCADA systems and technologies need to be developed.

I3P Program on Process Control System Security:

- I3P is addressing the threat characterization, the development and demonstration of cyber security tools and technologies, and the generation of sustainable security practices for process control systems.
- These efforts fit within a broader government strategy for process control system security research and development, with particular focus on the transition of technologies to industry for use in real-world digital control environments.

The Institute for Information Infrastructure Protection is a national research Consortium composed of more than two dozen research entities, including academic institutions, federally funded labs and non-profit organizations. In collaboration with government and industry, the I3P is able to bring Consortium member experts together to identify and help mitigate threats aimed at the U.S. information infrastructure that we depend on to sustain our way of life. In effect, the I3P functions as a virtual national lab with the ability to organize and reconfigure research teams with the skill sets required to study the vulnerabilities within the information infrastructure.

This work is supported under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this [document] are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College. Copyright© 2005 Trustees of Dartmouth College.