SC MAGAZINE

December 2004

Network & Security Technologies

NIST-led group offers industrial cybersecurity requirements

by Marcia Savage

An industry group led by the National Institute of Standards and Technology (NIST) has released a set of cybersecurity requirements for computer systems used to control industrial processes for water, electrical power, and other infrastructures.

Formed by NIST in 2001, the Process Control Security Requirements Forum has some 600 members, including users and vendors. The forum's draft document, "System Protection Profile (SPP) for Industrial Control Systems," is intended as baseline security requirements for new products and could be used by companies in procurement requests, said Keith Stouffer, forum chairman and mechanical engineer at NIST.

The requirements are designed to cover a variety of devices, including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Programmable Logic Controllers (PLCs).

"Until recently, security wasn't really an issue because these systems were stand-alone and not connected to other networks," Stouffer said. "Today everything is so interconnected. Now they're vulnerable to everything on the internet."

> The SPP is a good first step for providing security guidelines to utilities, said Adam Lipson, president and CEO of consultancy Network & Security Technologies.
>
> "In an effort to reduce operational costs, utilities are attempting to convert proprietary SCADA devices to lower cost IP-enabled systems.... Unfortunately, converting these to open systems has also created some new vulnerabilities," he said.

A lot of industrial control systems now are using Microsoft software, so they are vulnerable to viruses targeting Windows, he added. Plus, many legacy systems were designed with relability in mind, not security.

Security requirements in the SPP include addressing security throughout the system's lifecycle, taking a defense-in-depth approach, authenticating users and data, encrypting certain information, and ensuring that products are secure out of the box rather than requiring the end user to implement security capabilities.

The SPP is a good first step for providing security guidelines to utilities, said Adam Lipson, president and CEO of consultancy Network & Security Technologies.

"In an effort to reduce operational costs, utilities are attempting to convert proprietary SCADA devices to lower cost IP-enabled systems.... Unfortunately, converting these to open systems has also created some new vulnerabilities," he said.

Adam Lipson is president and CEO at Network & Security Technologies (www.netsectech.com), a provider of digital security consulting solutions.
