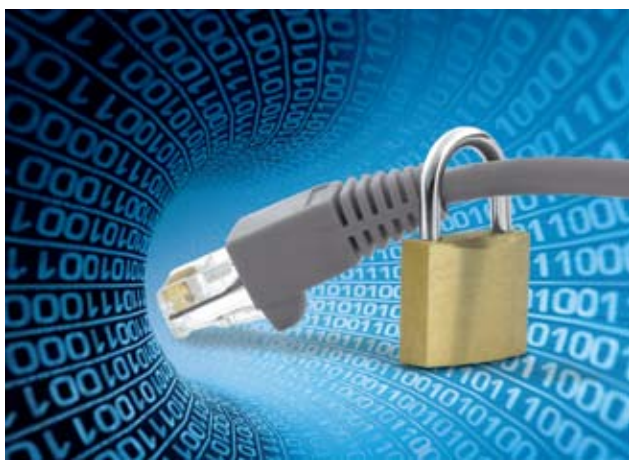
SCADA security for municipal water

How a major water and wastewater utility secures its automated networks

By Frank Dickman

The fact that water is the elixir of all life forms was known and understood long before Ponce de León searched for his legendary fountain. Human beings can live for months without food, but only for a matter of days without water. Life can exist for centuries—hundreds of them—without electricity and fossil fuels: Not so without freshwater.



Urban water usage worldwide measures 31 gal a day per person, with usage in undeveloped areas averaging 18 gal a day. In the western world, 100 to 150 gal per person per day is more typical, although people only consume 10% of the total production supply. Agriculture consumes about 70%, and industry about 20%.

Providing and protecting the security of that supply is a reasonable mandate. The water supply is an essential part of the critical infrastructure. The water industry recognized that these systems needed increased security after the 2006 conviction of a hacker who seized control of a water treatment facility's SCADA system in Australia. This security breach resulted in the dumping of millions of gallons of raw sewage onto a resort hotel's grounds for a period of three months.

As a result, water providers realized that many industrial controls would benefit from virtual private network (VPN) connectivity and diversified firewalls behind the typical front-office firewalls. Here is how one leading and progressive utility is securing the industrial control networks of its extensive infrastructure.

Meet the Utility

United Water operates and manages water and wastewater systems that serve about 7 million people across the U.S. in 23 states. For more than 30 years, it has used a variety of methods to connect to remote sites, including modems, leased lines, dry pairs and licensed radio. United Water supports more than 300 remote field sites companywide.

In 2009, the organization planned to increase the security of its SCADA control networks. The systems engineering group, corporate IT department and an outside consulting firm were involved in the project and the security product evaluations. A leading IT network solution initially was considered, as this path reflected the corporate office network standard, but there were other considerations.

"We needed an industrial solution, particularly for our remote sites," said Keith Kolkebeck, systems engineering project manager for United Water. "We needed a solution that was easy to configure, powered by 24VDC, met our IT security standards and could hold up to years of operation in a harsh environment. In the past, we had mixed results using office network-grade products that were expensive, required special skills to configure and failed frequently."

Solution in Action

In early 2010, United Water was introduced to the family of mGuard industrial network security devices from Phoenix Contact, created and developed by its subsidiary Innominate Security Technologies. The system includes small, industrial-rated modules that incorporate router, firewall, encrypted VPN tunnels, filtering of incoming and outgoing connectivity, authentication, and other functions to provide layers of distributed "defense-in-depth" economically and without disturbing production.

Various industrial-rated designs are available for DIN-rail mounting, for 19-in. rack mounting in cabinets, as PCI cards or as dongle-style patch cords for roaming technicians. The hardened, industrial version of mGuard has been in production since 2005 and has proven to be effective in tens of thousands of demanding installations. Rated IP 20 for mounting in factory enclosures, it is installed easily and enabled by technicians rather than network administrators. Customers in the automotive and other industries

have used these versions with excellent results in providing security for older production systems.

Installation can be as simple as mounting the device, providing 24VDC power, plugging in the network cable and using a patch cord to connect to the server, human machine interface PC or production equipment cell to be protected. Using the Internet capability of the production control console with a password-protected login, the security device can be set up and enabled in moments from a template on the device manufacturer's website.

After review of the technology, United Water's IT department was receptive to the concept because it would allow process personnel to deploy and maintain their own networks, freeing up IT for other tasks. United Water installed a dozen devices as a test bed.

"The ability [of] the mGuard to do AES-256 encryption along with its industrial design was key," Kolkebeck said. "It was easy to deploy, cost-effective and met our standards. By default, the device is configured in its most secure configuration. Previously, it would require a day's time of an experienced IT technician, whereas now we can roll out a new VPN device in 10 minutes. The mGuard is very easy for someone with minimal network knowledge to roll out."

In "Stealth Mode," these products are completely transparent, automatically assuming the MAC and IP address of the equipment to which they are connected so that no additional addresses are required for the management of the network devices. This was a feature that appealed to initially skeptical IT personnel. No changes need to be made to the network configuration of the existing systems involved. Yet the devices operate invisibly and transparently, monitoring and filtering traffic to the protected systems by providing a stateful packet firewall according to rules that can be configured via templates from a centrally located server. With bidirectional wire speed capability, the devices will not add any perceptible bottlenecks or latency to a 100-Mb/s Ethernet network.

If required, the security of networked equipment may be enhanced further. Configuration of specific user firewall rules can restrict the type and duration of access to authorized individuals who must login from specific locations, PCs and IP addresses before authenticating themselves. VPN functions provide for secure authentication of remote stations and the encryption of data traffic. Optional CIFS Integrity Monitoring functionality can protect file systems against unexpected modifications of executable code (i.e., by Stuxnet-derived malware) by sending alerts to administrators.

"We were implementing multiple measures into our SCADA network in order to monitor activity on our system," Kolkebeck said. "We utilize network segmentation, VLANS and centralized firewalls and were looking to introduce intrusion detection and intrusion prevention systems into our network."

United Water needed to protect remote terminal units, programmable logic controllers (PLCs), remote card access and video systems. As industrial systems migrate toward an IP network, more timely information and control is available. All new PLCs have IP capability. Power monitoring is a common example. All new variable-frequency drives for motors, switchgear, pumps and generators have power-efficiency monitoring capabilities that need to be tied into the SCADA systems. Following field trials, the mGuard appliances were utilized to provide protection from vulnerabilities through firewall, VPN, routing and trap functions.

Results

"We currently have mGuard security modules deployed in multiple locations throughout the Northeast," Kolkebeck said. "We have used the products both for our SCADA networks and our security networks at remote, unmanned locations. We have interfaced the mGuard devices with our existing CISCO infrastructure. We are saving money on remote support from our staff and outside contractors. Site visits are no longer required for minor code changes and troubleshooting." WWD

Frank Dickman, BSMAE, RCDD, is a Chicago-based engineering consultant. Dickman can be reached at frankdickman@yahoo.com.

For more information, write in 1104 on this issue's Reader Service Card.