



Hot or Not: SCADA security is hot

Amol Sarwate, manager, Vulnerabilities Research Lab, Qualys
April 23 2009

The notion of supervisory-control and data-acquisition system security, SCADA, seemed not long ago to be a topic of interest only to those who ran complex industrial control systems, water treatment plants, and power generation – and in some ways it still is. But for anyone who attended the SANS 2009 SCADA and Process Control Summit recently, it became clear that the convergence of IT security and physical security is accelerating.

This is happening as more IT systems are managing physical systems – and it's no longer only utilities and the critical infrastructure that rely on SCADA systems for management. These days we see more traditional industries, such as manufacturing, turning to SCADA systems, while health care and many other industries are, or soon will be, using telematics to manage all types of far-flung devices. In coming years, the security of physical control systems will be part of many IT security managers' bag of responsibilities.

Today, many experts disagree on just how vulnerable the nation's critical infrastructure really is to digital attack. They'll often cite how specialized SCADA systems are, or how few successful SCADA attacks we hear about. Yet, wasn't application security a specialty in 1999? And how many web application attacks were making the news back then? Not many, but such attacks today have become almost daily news.

One thing certainly is clear to me after researching the subject: Many SCADA systems are inherently vulnerable. First, these systems never were designed with network security in mind, and these systems increasingly are being connected to the internet. That's not an especially encouraging situation.

In fact, increasingly, SCADA devices are falling vulnerable to the same kind of software vulnerabilities that have been plaguing IT systems and applications for years. Just last month, Paris-based Areva warned its customers that an important part of its energy management software was vulnerable after software flaws were found in several versions (5.5, 5.6, 5.7) of its e-terrahabitat package. As the U.S. Computer Emergency Readiness Team (US-CERT) [warned](#), a number of buffer overflow and denial-of-service vulnerabilities made versions 5.5, 5.6, and 5.7 of e-terrahabitat susceptible to tampering. Customers using earlier versions needed to upgrade as well.

"An unauthenticated attacker may be able to gain access with the privileges of the e-terrahabitat account or an administrator account and execute arbitrary commands, or cause a vulnerable system to crash," US-CERT's Vulnerability Not VU#337569 stated. The note advised users to apply the patch immediately.

This advisory resembles just about any vulnerability that affects today's applications and operating systems. However, SCADA systems affect not just data but water, sewage, chemicals, and, as in the case of AREVA – energy.

The Idaho National Laboratory, as part of the Department of Energy's SCADA Test Bed program, evaluated numerous SCADA systems, and found several classes of vulnerabilities that significantly affect the security of these systems: change management deficiencies, unencrypted services common in IT systems, weak user credential security, information leaks through unencrypted proprietary communication protocols, and others.

Finding these types of vulnerabilities certainly isn't reassuring.

Theoretically, SCADA systems should not be exposed to the internet, but I fear they increasingly are being connected to IP networks. In most industries, SCADA systems should be completely air-gapped from data networks, thus significantly mitigating the risk of attack. However, more installations are using SCADA to manage their systems remotely, or even connect the systems to an internet-enabled corporate network to collect and analyze data. As this trend continues, SCADA systems increasingly must be treated as any other networked device: They must be identified, inventoried, and analyzed for vulnerabilities.

For more information about SCADA security, the U.S. Department of Energy has published [information](#) that includes more details on the National SCADA Test Bed, Center for SCADA Security, as well as other resources. I think that in the not-so-distant future, more of us will need greater understanding of how to harden these systems.