



Security

America's Hackable Backbone

Andy Greenberg, 08.22.07, 6:00 PM ET

The first time Scott Lunsford offered to hack into a nuclear power station, he was told it would be impossible. There was no way, the plant's owners claimed, that their critical components could be accessed from the Internet. Lunsford, a researcher for IBM's Internet Security Systems, found otherwise.

"It turned out to be one of the easiest penetration tests I'd ever done," he says. "By the first day, we had penetrated the network. Within a week, we were controlling a nuclear power plant. I thought, 'Gosh. This is a big problem.'"

In retrospect, Lunsford says--and the Nuclear Regulatory Commission agrees--that government-mandated safeguards would have prevented him from triggering a nuclear meltdown. But he's fairly certain that by accessing controls through the company's network, he could have sabotaged the power supply to a large portion of the state. "It would have been as simple as closing a valve," he says.

In Pictures: America's Hackable Backbone

The disturbingly vulnerable system that Lunsford hijacked is powered by Supervisory Control and Data Acquisition software, or SCADA, a type of software made by companies including Siemens, ABB, Rockwell Automation and Emerson.

SCADA systems are used around the country to control infrastructure like water filtration and distribution, trains and subways, natural gas and oil pipelines, and practically every kind of industrial manufacturing. And as some security professionals are pointing out, those weaknesses are increasingly connected to the Internet, leaving large parts of America's critical infrastructure exposed to anyone with moderate information technology training and a laptop.

At the DefCon hacker conference earlier this month, security researcher Ganesh Devarajan gave a presentation detailing how researchers can find flaws in SCADA systems using "fuzzing," a technique that floods software with data and tracks which input causes a crash, allowing hackers to inject their own commands.

"These are simple bugs, but very dangerous ones," says Devarajan, associate security analyst at 3Com-owned security firm TippingPoint. He says he's alerted SCADA software vendors to all the flaws he's found, but he nonetheless imagines a scenario in which someone plants a contaminant in a water reservoir and hacks into water-quality sensor systems to prevent detection. "If someone can provide false data," he says, "They own the system."

To be sure, the threat of attacks on major SCADA systems isn't entirely new, and the wave of cyberterrorism predictions that followed Sept. 11, 2001, have largely been dismissed as hype and paranoia. But given SCADA systems' vulnerability, many experts wonder why those attacks haven't yet materialized.

One answer may be the sheer complexity of major infrastructure systems: Though SCADA computers have weak external security, controlling them takes engineering expertise. Most hackers could only gain enough control to create the fear that they're capable of something worse, says Alan Paller, director of the SANS Institute.

That means that even if outright attacks aren't increasing, there's a growing threat of extortion, says Paller. In fact, the SANS Institute hosts a crisis response center for cyberattacks, and Paller says he's learned of multiple threats within the last year and a half from hackers claiming to have infiltrated SCADA systems and demanding ransom. Other shakedowns have likely gone unreported.

Paller predicts that those incidents will increase. "There's been very active and sophisticated chatter in the hacker community, trading exploits on how to break through capabilities on these systems," he says. "That kind of chatter usually precedes bad things happening."

Extortion is more than an economic problem; racketeers could easily trigger an accident while trying to demonstrate control over a facility, says Marcus Ranum, chief security officer for Tenable Security. "To spin a pump or move a valve, you don't have to be a petroleum engineer," he says. "Then again, you could spin the wrong pump and blow something up."

Not every SCADA sabotage scenario is so hypothetical. In 2000, Vitek Boden, a 48-year-old man fired from his job at a sewage-treatment plant in Australia, remotely accessed his former workplace's computers and poured toxic sludge into parks and rivers; he hoped the plant would re-hire him to solve the leakage problem.

In January 2003, computers infected with the Slammer worm shut down safety display systems at the Davis-Besse power plant in Ohio, though the plant was already shut down at the time. Seven months later, another computer virus was widely suspected by security researchers of leading to a power loss at a plant providing electricity to parts of New York State, despite the Nuclear Regulatory Commission's argument that no evidence of virus-involvement was found.

SCADA systems' lack of security features is a symptom of their age; most were developed at a time when critical infrastructure systems weren't connected to the Internet and needed no intrusion prevention. Some have a 20-year life span, making them obsolete for years after they're installed. And many of the companies that develop SCADA software make installing security patches difficult or, fearing that patches will hamper the software's operation, don't offer customer support for patched systems.

All of which still leaves U.S. infrastructure open to crippling attacks by criminal hackers or cyberterrorists, says Jim Christy, director of future exploration at the Department of Defense's Cyber Crime Center. "This is an Achilles' heel for several of our critical systems," Christy says. "Nation-states and terrorist organizations are definitely looking at this as an option, a weapon of mass disruption."

That kind of risk means major security changes are necessary, says Christy. But because SCADA systems are largely owned by the private sector, critical infrastructure like power plants and water systems may remain vulnerable until the problem affects profits--or leads to disaster. Christy argues that we can't wait that long: His unofficial opinion is that SCADA needs government regulation.

"The government mandates fire sprinklers. Those cost builders money, but they save property and lives," he says. "If critical infrastructure is important to our national security, shouldn't there be minimum standards it has to meet?"

In Pictures: America's Hackable Backbone

Block