Science fiction-style sabotage a fear in new hacks

23 October 2011, By JORDAN ROBERTSON , AP Technology Writer

Researcher Dillon Beresford poses for a photo at his office, Wednesday, Aug. 31, 2011, in Austin, Texas. Beresford said it took him just two months and $20,000 in equipment to find more than a dozen vulnerabilities in electronic controllers of the same type used in Iran. The vulnerabilities, which included weak password protections, allowed him to take remote control of the devices and reprogram them. (AP Photo/Eric Gay)

When a computer attack hobbled Iran's unfinished nuclear power plant last year, it was assumed to be a military-grade strike, the handiwork of elite hacking professionals with nation-state backing.

Yet for all its science fiction sophistication, key elements have now been replicated in laboratory settings by security experts with little time, money or specialized skill. It is an alarming development that shows how technical advances are eroding the barrier that has long prevented computer assaults from leaping from the digital to the physical world.

The techniques demonstrated in recent months highlight the danger to operators of power plants, water systems and other critical infrastructure around the world.

"Things that sounded extremely unlikely a few years ago are now coming along," said Scott Borg, director of the U.S. Cyber Consequences Unit, a nonprofit group that helps the U.S. government prepare for future attacks.

While the experiments have been performed in laboratory settings, and the findings presented at security conferences or in technical papers, the danger of another real-world attack such as the one on Iran is profound.

The team behind the so-called Stuxnet worm that was used to attack the Iranian nuclear facility may still be active. New malicious software with some of Stuxnet's original code and behavior has surfaced, suggesting ongoing reconnaissance against industrial control systems.

And attacks on critical infrastructure are increasing. The Idaho National Laboratory, home to secretive defense labs intended to protect the nation's power grids, water systems and other critical infrastructure, has responded to triple the number of computer attacks from clients this year over last, the U.S. Department of Homeland Security has revealed.

For years, ill-intentioned hackers have dreamed of plaguing the world's infrastructure with a brand of sabotage reserved for Hollywood. They've mused about wreaking havoc in industrial settings by burning out power plants, bursting oil and gas pipelines, or stalling manufacturing plants.

But a key roadblock has prevented them from causing widespread destruction: they've lacked a way to take remote control of the electronic "controller" boxes that serve as the nerve centers for heavy machinery.

The attack on Iran changed all that. Now, security experts - and presumably, malicious hackers - are racing to find weaknesses. They've found a slew of vulnerabilities.

Think of the new findings as the hacking equivalent of Moore's Law, the famous rule about computing power that it roughly doubles every couple of years. Just as better computer chips have accelerated the spread of PCs and consumer electronics over the past 40 years, new hacking techniques are making all kinds of critical infrastructure - even prisons - more vulnerable to attacks.

One thing all of the findings have in common is that mitigating the threat requires organizations to bridge a cultural divide that exists in many facilities. Among other things, separate teams responsible for computer and physical security need to start talking to each other and coordinate efforts.

Many of the threats at these facilities involve electronic equipment known as controllers. These devices take computer commands and send instructions to physical machinery, such as regulating how fast a conveyor belt moves.

They function as bridges between the computer and physical worlds. Computer hackers can exploit them to take over physical infrastructure. Stuxnet, for example, was designed to damage centrifuges in the nuclear plant being built in Iran by affecting how fast the controllers instructed the centrifuges to spin. Iran has blamed the U.S. and Israel for trying to sabotage what it says is a peaceful program.

Security researcher Dillon Beresford said it took him just two months and $20,000 in equipment to find more than a dozen vulnerabilities in the same type of electronic controllers used in Iran. The vulnerabilities, which included weak password protections, allowed him to take remote control of the devices and reprogram them.

"What all this is saying is you don't have to be a nation-state to do this stuff. That's very scary," said Joe Weiss, an industrial control system expert. "There's a perception barrier, and I think Dillon crashed that barrier."

One of the biggest makers of industrial controllers is Siemens AG, which made the controllers in question. The company said it has alerted customers, fixed some of the problems and is working closely with CERT, the cybersecurity arm of the U.S. Department of Homeland Security.

Siemens said the issue largely affects older models of controllers. Even with those, the company said, a hacker would have to bypass passwords and other security measures that operators should have in place. Siemens said it knows of no actual break-ins using the techniques identified by Beresford, who works in Austin, Texas, for NSS Labs Inc.,

Yet because the devices are designed to last for decades, replacing or updating them isn't always easy. And the more research that comes out, the more likely attacks become.

One of the foremost Stuxnet experts, Ralph Langner, a security consultant in Hamburg, Germany, has come up with what he calls a "time bomb" of just four lines of programming code. He called it the most basic copycat attack that a Stuxnet-inspired prankster, criminal or terrorist could come up with.

"As low-level as these results may be, they will spread through the hacker community and will attract others who continue digging," Langer said in an email.

The threat isn't limited to power plants. Even prisons and jails are vulnerable.

Another research team, based in Virginia, was allowed to inspect a correctional facility - it won't say which one - and found vulnerabilities that would allow it to open and close the facility's doors, suppress alarms and tamper with video surveillance feeds.

During a tour of the facility, the researchers noticed controllers like the ones in Iran. They used knowledge of the facility's network and that controller to demonstrate weaknesses.

They said it was crucial to isolate critical control systems from the Internet to prevent such attacks.

"People need to deem what's critical infrastructure in their facilities and who might come in contact with those," Teague Newman, one of the three behind the research.

Another example involves a Southern California power company that wanted to test the controllers used throughout its substations. It hired Mocana Corp., a San Francisco-based security firm, to do the evaluation.

Kurt Stammberger, a vice president at Mocana, told The Associated Press that his firm found multiple vulnerabilities that would allow a hacker to control any piece of equipment connected to the controllers.

"We've never looked at a device like this before, and we were able to find this in the first day," Stammberger said. "These were big, major problems, and problems frankly that have been known about for at least a year and a half, but the utility had no clue."

He wouldn't name the utility or the device maker. But he said it wasn't a Siemens device, which points to an industrywide problem, not one limited to a single manufacturer.

Mocana is working with the device maker on a fix, Stammberger said. His firm presented its findings at the ICS Cyber Security Conference in September.

Even if a manufacturer fixes the problem in new devices, there's no easy way to fix it in older units, short of installing new equipment. Industrial facilities are loath to do that because of the costs of even temporarily shutting its operations.

"The situation is not at all as bad as it was five to six years ago, but there's much that remains to be done," said Ulf Lindqvist, an expert on industrial control systems with SRI International. "We need to be as innovative and organized on the good-guy side as the bad guys can be."