

You are currently viewing the printable version of this article, to return to the normal page, please [click here](#).

The Washington Times

Prisons bureau alerted to hacking into lockups

Expert: 'Could open every cell door'

[1 Comment and 2 Reactions](#) | [Share](#) | [Tweet](#) | [Email](#) | [Print](#) |

By [Shaun Waterman](#)

The Washington Times

Sunday, November 6, 2011

MIAMI — Federal authorities are concerned about new research showing U.S. prisons are vulnerable to computer hackers, who could remotely open cell doors to aid jailbreaks.

The Federal Bureau of Prisons is "aware of this research and taking it very seriously," spokesman Chris Burke told The Washington Times.

Mr. Burke was reacting to research by private experts who found that the security systems in most American prisons are run by computer software vulnerable to hackers.

"You could open every cell door, and the system would be telling the control room they are all closed," said John J. Strauchs, a former CIA operations officer who helped develop a cyber-attack on a simulated prison computer system and described it at a hackers' convention in Miami recently.

The security systems in most American prisons are run by special computer equipment called industrial control systems, or ICS. They are also used to control power plants, water treatment facilities and other critical national infrastructure. ICS has increasingly been targeted by hackers because an attack on one such system successfully sabotaged Iran's nuclear program in 2009.

A malicious cyber-intruder could "destroy the doors," by overloading the electrical system that controls them, locking them permanently open, said Mr. Strauchs, now a consultant who has designed security systems for dozens of state and federal prisons..

Hackers could "shut down secure communications" through the prison intercom system and crash the facility's closed-circuit television system, blanking out all the monitors, he added.

Mr. Strauchs, 67, and his daughter — attorney, professor and computer security researcher Tiffany Strauchs Rad, 37 — told an audience at the recent Hacker Halted conference about the attack they developed in the basement of a Washington area home for less than \$2,500.

"Personally, I think the greatest danger is assassination," Mr. Strauchs told The Washington Times afterward. "You create chaos as a way to [implement a plan to] kill someone."

Mr. Strauchs said he and his daughter had been careful to work with U.S. authorities to alert them to the risk before publicly disclosing their attack. They organized a briefing for federal agencies over the summer at CIA headquarters in Northern Virginia.

Sean P. McGurk, who led the Department of Homeland Security's efforts to secure ICS until leaving in September, said the department had looked into the researchers' claims using the special ICS computer test bed at the Idaho National Laboratory.

"We validated the researchers' initial assertion ... that they could remotely reprogram and manipulate" the special software controllers that run the systems, Mr. McGurk said.

Teague Newman, another member of their team, said ICS systems are not supposed to be connected to the Internet.

"But in our experience, there were often connections" to other networks or devices, which were in turn connected to the Internet, making them potentially accessible to hackers, he said.

In some of the facilities the team visited for their research, guards had used the same computer that controls the prison's security systems to check their personal email, exposing it directly to potential hackers, Mr. Teague said.

In many prisons, technical support staff would add connections to enable them to update the system's software remotely after the ICS systems were installed by security specialists.

"We saw that a lot, a lot," said Mr. Teague.

Mr. McGurk said he found Internet connections in every one of the 400-plus onsite inspections of control systems in the government and private sector he had overseen in three years at the Homeland Security Department.

"In no case did we ever not find connections," he said. "They were always there."

Even systems that were successfully cut off from the Internet could be attacked by malicious insiders or anyone with enough access to insert a thumb drive into a computer work station, Mr. Strauchs said.

"The mostly likely vector would be to bribe a prison guard to insert a USB drive with malicious programming. Hard to stop and hard to find out who did it," he said.

Mr. Teague said the team's attack was "pretty easy" to develop.

"I had no prior experience with programming ICS" Mr. Newman said, "We did not spend a lot of time, it was cheap, and we did it in my basement."