

Login | Sign up

Whitepapers | Reg Hardware | Channel Reg

Biting the hand that feeds IT



Hardware Software Music & Media Networks Security Cloud Public Sector Business Science Odds & Sods
Crime Malware Enterprise Security Spam ID Compliance

Search site

Hackers can spring Death Row crims from cells

Cryptoboffins prove SCADA jailbreak risk

By **John Leyden** • [Get more from this author](#)

Posted in [Security](#), 8th November 2011 17:03 GMT

[Free whitepaper – Schlumberger uses IBM System Networking RackSwitch for HPC](#)

Computer systems used to control federal prison facilities are riddled with vulnerabilities that might allow criminals to meddle with cell door opening mechanisms or shut down internal communications systems, according to security researchers.

The vulnerabilities – which stem from flaws in industrial control systems and programmable logic controllers – were demonstrated by a team led by John Strauchs, who demonstrated the flaws at the recent Hacker Halted information security conference in Miami. Despite having no previous experience with SCADA (industrial control) kit, Strauchs and his colleagues were able to develop workable exploits, validated using a test rig that cost just \$2,500 to construct in the basement of his research partner, Teague Newman. Strauchs' daughter – attorney, professor and computer security researcher Tiffany Strauchs Rad – also contributed in the research.

The resulting [talk](#), *SCADA And PLC Vulnerabilities In Correctional Facilities* (abstract below), sounds absolutely gripping.

On Christmas Eve, a call was made from a prison warden: all of the cells on death row popped open. Many prisons and jails use SCADA systems with PLCs to open and close doors. Not sure why or if it would happen, the warden called physical security design engineer, John Strauchs, to investigate. As a result of their Stuxnet research, Rad and Newman have discovered significant vulnerabilities in PLCs used in correctional facilities by being able to remotely flip the switches to “open” or “locked closed” on cell doors and gates. Using original and publically available exploits along with evaluating vulnerabilities in electronic and physical security designs, this talk will evaluate and demo SCADA systems and PLC vulnerabilities in correctional and government secured facilities while recommending solutions.

The researchers have turned over a dossier on their findings to state and federal prison authorities, who have good reason to take its findings seriously. "We validated the researchers' initial assertion ... that they could remotely reprogram and manipulate [the ICS software and controllers]," Sean P McGurk, a former Department of Homeland Security cybersecurity director, told the *Washington Times*.

Possible exploits include overloading the electrical system that controls prison doors, locking them permanently open, or crashing either CCTV or prison intercom systems.

Strauchs began his project to investigate the security of industrial control systems in prisons after he was asked to investigate an incident during which all the cell doors on one (unnamed) prison's death row spontaneously opened. The cause was eventually traced back to a random power surge, but the incident got Strauchs thinking and prompted him to have a

MOST READ MOST COMMENTED

- **Apple expels serial hacker for publishing iPhone exploit**
- **UK Home Sec: 'I authorised biometric bypass pilot'**
- **DNS cache poisonings foist malware attacks on Brazilians**
- **Anonymous blasts El Salvador offline**
- **UK firm slammed for flogging spy software to Iran**

[Sign up, sign up for The Register's weekly IT security newsletter - click here](#)

UBUNTU REPUBLIC RIVEN BY CIVIL WARS



Can the Linux Jedi hold things together?

POPULAR WHITEPAPERS

Search for more Whitepapers

- | | |
|---|--|
| IBM System Networking RackSwitch and IBM System Networking solutions Intelligence and speed at the edge of your network | IBM System Networking RackSwitch G8264 Competitive performance evaluation |
| IBM System Networking RackSwitch G8124 Competitive evaluation versus Cisco Nexus 5010 | Schlumberger uses IBM System Networking RackSwitch for HPC To support high performance computing environment |
| VMready Virtual machine-aware networking | Bringing speed and intelligence to the network with Smarter Computing solutions for the data center |

COMPACT DISC DEATH FORETOLD FOR 2012

closer look at the security of industrial control systems in prisons.

Industrial control systems in prisons have no business being connected to the internet. Despite this, the team of researchers led by Strauchs discovered every prison system they looked at was connected to the internet one way or another.

In some cases, for example, the internet connection was set up so that remote maintenance of the kit could be carried out without the need for contractors to visit the jail. In other cases networks used to enable prison staff to access the net were poorly segmented from SCADA control systems. Infected USB drives contaminated with a Stuxnet-style worm posed another, wholly unguarded infection vector. SCADA systems might be deprogrammed by malware of this type either accidentally or (more plausibly) by either bribing or blackmailing a prison guard. A targeted malware-infected email might also be used to introduce a SCADA worm into a prison environment.

"You could open every cell door, and the system would be telling the control room they are all closed," Strauchs, a former CIA operations officer, [told](#) the *Washington Times*.

Anyone who got out of their cell this way would still have prison guards, dogs, guns and barbed wire to contend with if they hoped to escape. Strauchs said a more plausible scenario might be that the security weakness was exploited to slip assassins out of their cells in order to gain access to a targeted prisoner. ®

[Free whitepaper – Schlumberger uses IBM System Networking RackSwitch for HPC](#)


[READ MORE](#) [Stuxnet](#) [Scada Security](#) [Industrial Controls](#)

 [Share this article](#)  [Be the first to post a comment!](#)


Related stories

- [Critical Windows zero-day bug exploited by Duqu](#) (1 November 2011)
- [Stuxnet-derived malware found infecting SCADA makers](#) (18 October 2011)
- [Hacktivists pose growing threat to industrial computing](#) (18 October 2011)
- [PLCs a prison vulnerability: researchers](#) (1 August 2011)


WHITEPAPERS




ASCII uses 10 GbE grid computing and hi-def media streaming
Soution brief paper on how ASCII uses 10 GbE grid computing and hi-definition media streaming to support a countrywide computing access network.



Low-latency switches powerhigh-frequency trading
Latency measurements that were unachievable just a short time ago are now commonplace, this paper looks at how this network technology has evolved.



Smarter Networking for a smarter data centre
The problems of network consolidation, distributed apps and achieving solutions for a smarter data centre.



Centre Hospitalier d'Avignon Secures Patient Records
Case study on how The Centre Hospitalier d'Avignon deployed IBM System Networking technology to achieve a trouble-free approach to virtualization.

Ads by Google

- [IBM 2011 Security Report](#)
Get the Full Text of IBM X-Force's End of 2011 Security Report Now.
www.ibm.com/internet_security
- [BP's Work in the Gulf](#)
BP continues their work in the Gulf. Visit BP.com to learn how.
www.BP.com/GulfOfMexicoResponse
- [Security Awareness](#)
Security Awareness Course. Get a free demo and

- [Info Security Major](#)
Major in Information Security. Take Classes 100% Online or On-Campus!
Franklin.edu/Info-Security-Major
- [Computer Security](#)
Unlike Any Other Flash Drive You've Seen - Better, Stronger, Faster!
IronKey.com
- [Water/Wastewater SCADA](#)
Low Cost cellular to web telemetry Simple to install,



Major record labels to kill format?

SPONSORED LINKS

- [SQL Virtual Restore: relieves 8 causes of DBA pain](#)
- [End cluster clutter with vSMP Foundation; from \\$8000. Contact us today](#)
- [Slow Networks Blow, Change To Chelsio Unified Wire](#)
- [Switch your SSL Certificate to GeoTrust for FREE](#)