

Welcome Guest. Log In Register Benefits



- RSS Feeds
- Subscribe
- Newsletters
- Events
- Whitepapers

Home News Blogs Video Slideshows Tech Centers

Software Security Cloud Mobility Social Business Personal Tech Hardware Windows Global CIO Government Healthcare Financial

SMB

- | | | | |
|----------------------|--------------------------|------------------------------------|------------------|
| Application Security | End User/Client Security | Security Administration/Management | Security Stories |
| Attacks/Breaches | Perimeter Security | Security Blog | Storage Security |
| Encryption | Privacy | Security Reviews | Vulnerabilities |



3 Like Share 0 Permalink

Get InformationWeek Daily

Don't miss each day's hottest technology news, sent directly to your inbox, including occasional breaking news alerts.

Prisons May Be Vulnerable To Stuxnet-Style Attack

Researchers found easy-to-write malware could subvert prison control systems, cause spontaneous opening of all cell doors.

By **Mathew J. Schwartz** InformationWeek
November 10, 2011 01:49 PM

It's Christmas Eve in a maximum security prison, when all of the cell doors on death row simultaneously open without warning. What happened? That was the question posed by the warden of a prison in which that exact scenario occurred.

At last month's Hacker Halted Conference in Miami, the group formed to answer that question presented the results of its [research](#) into "SCADA and PLC Vulnerabilities in Correctional Facilities." In short, they discovered that there are numerous vulnerabilities in the industrial control--often referred to as supervisory control and data acquisition, aka SCADA--systems and programmable logic controllers (PLCs) used in today's modern and highly automated prisons, which could be remotely exploited to compromise such systems.

"Using the PLC's own software library, we were able to not only unlock any door in the prison system, but we could also send false status signals back to central and/or housing control reporting that the door is closed and locked," said researcher John Strauchs on his [blog](#). "Our results were far better than we expected." Furthermore, the team said that acquiring the hardware and software required for its research cost only \$2,500, although by not bothering to pay for legitimate software licenses, that cost could have been reduced to about \$500.

[Concerned about shoring up your systems against Stuxnet-style attacks? Learn [5 Things To Do To Defend Against Duqu.](#)]

The group of researchers was composed of Strauchs, a former CIA operations officer who's conducted security engineering or consulting for more than 114 justice industry design projects, including 14 federal prisons, 23 state prisons, and 27 city or county jails; Tiffany Rad, the president of ELCnetworks; and Teague Newman, a Washington-based information security consultant with experience in penetration testing.

More Security Insights

White Papers

- [SCM: The Blocking and Tackling of IT Security](#)
- [Ovum Technology Audit: Arbor Pravail DDoS Protection Solution](#)

[More >>](#)

Reports

- [Will IPv6 Make Us Unsafe?](#)
- [Database Defenses](#)

[More >>](#)

Webcasts

- [Outsourcing Security: What Every Potential Cloud Security Customer Should Know](#)
- [Effective IT Inventory and Asset Management: From Quagmire to](#)



THIS WEEK'S ISSUE



- [Subscribe to Digital](#)
- [Read the Cover Story](#)
- [Read This Week's Issue](#)
- [Download Current Issue](#)

[Back Issues](#)

Free Print Subscription

TECHNOLOGY WHITEPAPERS

Quick Fix

[More >>](#)

A Federal Bureau of Prisons spokesman this week said that the agency is "aware of this research and taking it very seriously," according to [The Washington Times](#). Likewise, the research team

said it's been working with multiple manufacturers and government agencies to identify current vulnerabilities and craft workarounds.

Of course, security experts have been warning about these types of [control system vulnerabilities](#) for years. But it wasn't until [Stuxnet showed up](#) that many control system users seemed to grasp the potential risks the systems might pose, given that many control systems weren't designed to resist Internet-borne threats, or perhaps ever see patches, although many run on Windows.

Ralph Langner--the German computer security expert credited with discovering Stuxnet-- has [warned](#) that "one can use exploit code to attack PLCs without any insider knowledge at all." Unlike a highly targeted attack such as Stuxnet, which was designed to only [sabotage high-frequency convertor drives](#) used in a specified uranium enrichment facility in Iran, Langner said that script kiddies could easily create PLC attacks without understanding the target environment.

Likewise, the prison control system and PLC research team reported that all three of its members quickly learned to "put together a PLC exploit in only a few hours," according to their research paper, owing to the simplicity of the programming languages involved. But an attacker might not even have to bother with that. "There are many exploits that are publicly available and can be found online such as on [exploit-db.com](#)," they said.

Given the potential threat posed by a cyber attack against the control systems or PLCs employed in prisons, what should be done? In particular, the research team suggests eight improvements, including restricting the use of physical media (which could carry malware) in facilities, segmenting networks properly, improving [patch practices](#), as well as using heightened security procedures in all areas that rely on PLCs. Also reevaluate current prison designs. "Many modern prisons/jails were designed 10 years ago, before these attack vectors were known," they said.

On his blog, Strauchs said that whenever possible, prison systems also shouldn't be Internet-connected. "The correctional facility security system should not have external connections, or if that can't be avoided, connections need to be safeguarded by security protocols--not security-through-obscurity--and systemic technical countermeasures," he said. In addition, "no one should ever be permitted to use workstations for personal activities like checking private email or viewing images--both of which our team saw during onsite evaluations of correctional facilities."

Thankfully, said Strauchs, fixes appear to be underway. "We believe that the manufacturers are working on what they can fix and, as a result, we are not advocating removing PLCs from facilities but, instead, addressing the vulnerabilities through awareness and education of the people working in facilities with PLCs," he said.

Read our report on how to guard your systems from a SQL attack. [Download the report now](#). (Free registration required.)

T-Shirt Giveaway: Each week we're selecting one great comment from our readers. The author of the comment will receive an InformationWeek Community t-shirt. So get posting!


Did you know you can style comments using [HTML](#) tags and upload your avatar photo? To upload your avatar photo, first [complete your Disqus profile](#). Once your profile is complete, you may [add your avatar photo](#).

Like

[Login](#) or [Register](#) to Comment

Real-time updating is **paused**. ([Resume](#))

Showing 0 comments

Sort by oldest first 

 [Subscribe by email](#)  [RSS](#)

 [Subscribe to RSS](#)

- [Solution Brief: Customer Benefits of the New Blue Coat WebFilter Categories](#)
- [Optimize Application Delivery for the Cloud](#)
- [Optimize VDI Delivery with Microsoft RDP 7.1 and Cisco WAAS](#)
- [A Comprehensive Overview of Enhanced Optimization with Context-Aware DRE](#)
- [Validated Network Deployments for WAN Optimization](#)

FEATURED WHITEPAPER

Secure iPhone Access to Corporate Web Applications

This technical brief describes how the BIG-IP Edge Portal app for iOS devices provides simple, streamlined access to web applications that reside behind BIG-IP APM, without requiring full VPN access, to simplify login for users and provide a new layer of control for administrators.

[Learn More](#)

FEATURED REPORTS

- [Will IPv6 Make Us Unsafe?](#)
- [Database Defenses](#)
- [Research: State of the IT Service Desk](#)
- [2010/2011 Computer Crime and Security Survey](#)
- [For Stronger Security, Partner With Compliance Pros](#)

Network Security for ...

InformationWeek & INTEROP December 1st
VIRTUAL EVENT
Attend & be eligible to win great prizes [REGISTER TODAY](#)

BYTE IS BACK

VIDEO



WATCH: [A Big Data, Big Decisions, Big Impact" ...](#)



WATCH: Solar-Powered Mobile Device Charging Goe ...



WATCH: Q&A: Reid Hoffman, Partner at Greylock, ...

[View All Videos](#)

