SCADA Hack Could Help Prisoners Escape

Another scary finding from the DefCon hackers' conference: prisoners could escape from their jails, if hackers decided to lend a hand and hack into the prison's security systems.

A couple of years ago a prison's cell doors accidentally opened after a power blackout, which led security engineer John Strauchs to make the startling discovery that it would be possible to maliciously release the cell doors in a similar way.

While he hasn't obviously tested it out on a living, breathing prison, it's worried Strauchs that prison guards use the internet on the very same computers that control their security systems. One click of a stray link, and the wall of security could fall away. [Huffington Post]

A Computer Error Released 450 Prisoners with "a High Risk of Violence"

Computer system errors accidentally released more than 450 inmates with "a high risk of violence" from California prisons. What might be even worse is that no attempt has been made to return any of them back to prison.

The prisoners were accidentally placed on 'non-revocable parole' which means they don't have to report to any parole officers. Non-revocable parole is a program originally created to combat the overcrowding of prisons by releasing inmates with a low risk of reoffending. Those with 'a high risk of violence' don't really qualify, you know.

Inmates are supposed to be excluded from non-revocable parole if they are "gang members, have committed sex crimes or violent velonies or have been determined to pose a high risk to reoffend based on an assessment of their records behind bars." But according to the inspection:

The computer program prison officials used to make that assessment does not access an inmate's disciplinary history. The program also relies on a state Department of Justice system that records arrests but is missing conviction information for nearly half of the state's 16.4 million arrest records.

Without that information about disciplinary history, they're completely disregarding their own criteria. And though prison officials say they've addressed some of the computer errors, they *still* can't access an inmate's disciplinary record. So the system is still fucked. And with the overpopulation of prisons a major issue in California, who knows if they'll even bother fixing it. [LA Times via BoingBoing]

Security Flaw Could Let Hackers Help Inmates Break Out Of Prison

Inmates have tried many ways to break out of prison: chip away at concrete, overpower guards, tie bedsheets together.

Now, they may have a new tactic: hack into the computer system that controls prison doors.

At the DefCon hacker conference in Las Vegas this weekend, researchers showed how they found a security flaw that could allow prisoners to escape if hackers breach the prison's computer system.

The issue came to light by accident a few years ago when a prison warden called security engineer John Strauchs with an alarming problem: all of the cells on death row had mysteriously opened.

The cause was a random power surge, but it got Strauchs thinking.

“If that can happen by accident, what would happen if you did it deliberately?” asked Strauchs, who has designed prison door control systems.

Then a few years later, a powerful computer worm called “Stuxnet” disabled Iran’s nuclear centrifuges. The worm, which is considered the most sophisticated cyberweapon ever made, attacked a “programmable logic controller,” which is a computer that is also used in the nation’s high-security prisons.

For about $2,500, the researchers bought one of these computers, which are manufactured by Siemens, and tested them in a laboratory.

The researchers said they have not simulated an attack on a correctional facility to test the possible flaw, but they believe it is possible to launch a cyber prison break, in large part because prison guards are not taking basic cybersecurity measures.

During a tour of one U.S. prison, the researchers found a guard in the control room checking his email on a computer that communicates with the system operating the doors. If that guard clicked on a malicious link or attachment, he could trigger a prison break, researchers said.

"If the computer had been attacked, we could open up and close the cell doors," said Tiffany Rad, president of ELCnetworks. "Any time you have a security product, the people operating it need to understand why certain operating procedures are in place."

The researchers said they briefed the federal government on the possible security flaw and received approval to give their presentation this weekend at the hacker conference.

Chris Burke, a spokesman for the Federal Bureau of Prisons, said he was unaware of the researchers' findings.

"We would take anything like that seriously and be wiling to take a look at that," Burke said.

Strauchs also noted that prison guards "don't get paid very much" and could be bribed to hack the prison computer system. But he said the security flaw could be subdued by prison officers performing basic cyber hygiene, like not using computers to check email.

"If the prisons change their security procedures, they could probably fix the problem 98 percent on their own," he said.

Description:

https://media.defcon.org/dc-19/presentations/Strauchs-Rad-Newman/DEFCON-19-Strauchs_Rad_Newman-SCADA-in-Prisons.pptx.pdf

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 publicly 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.

28th Chaos Communication Congress
Behind Enemy Lines

SCADA and PLC Vulnerabilities in Correctional Facilities

Tiffany Rad, Teague Newman, John Strauchs

Many prisons and jails use SCADA systems with PLCs to open and close doors. Using original and publically available exploits along with evaluating vulnerabilities in electronic and physical security designs, Newman, Rad and Strauchs 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. This talk will evaluate and demo SCADA systems and PLC vulnerabilities in correctional and government secured facilities while recommending solutions.
We figured out how to remotely hack into prisons cell and gate control systems by using publically available Siemens PLC exploits as well as creating our own. Teague and Tiffany did a walk-through a jail in the southwest, USA, saw PLCs in use, took pictures and saw prison guards accessing Gmail from the Control Room computers. We will be presenting the results of this research with John Strauchs discussing electronic and physical security vulnerabilities in modern prison design. Our research was presented at Defcon 19, Las Vegas, NV.

Links

- **White Paper**
- **Wired Magazine article about our work**
- **The Register article about our work**
- **Der Spiegel article about our work**

Researchers Say Vulnerabilities Could Let Hackers Spring Prisoners From Cells

Vulnerabilities in electronic systems that control prison doors could allow hackers or others to spring prisoners from their jail cells, according to researchers.

Some of the same vulnerabilities that the Stuxnet superworm used to sabotage centrifuges at a nuclear plant in Iran exist in the country's top high-security prisons, according to security consultant and engineer John Strauchs, who plans to discuss the issue and demonstrate an exploit against the systems at the DefCon hacker conference next week in Las Vegas.

Strauchs, who says he engineered or consulted on electronic security systems in more than 100 prisons, courthouses and police stations throughout the U.S. — including eight maximum-security prisons — says the prisons use programmable logic controllers to control locks on cells and other facility doors and gates. PLCs are the same devices that Stuxnet exploited to attack centrifuges in Iran.

"Most people don't know how a prison or jail is designed, that's why no one has ever paid attention to it," says Strauchs. "How many people know they're built with the same kind of PLC used in centrifuges?"

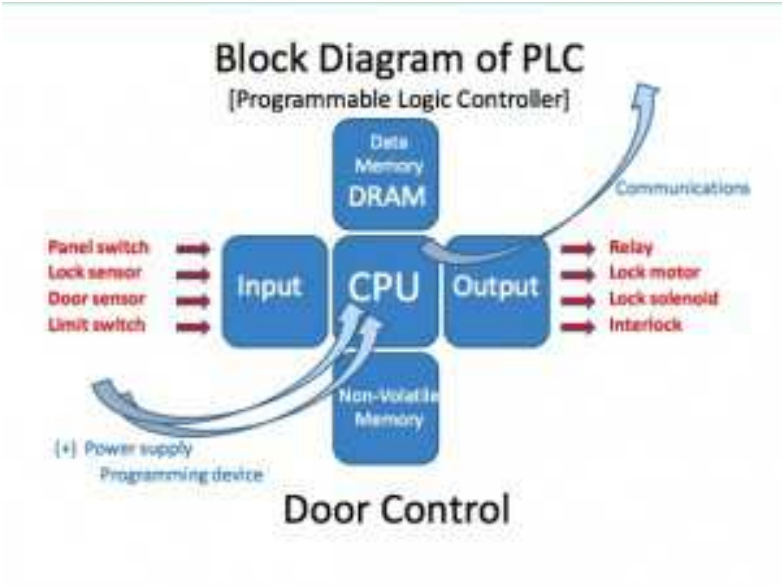

Diagram showing the typical parts of a PLC used for door-control systems. Image courtesy of Teague Newman

PLCs are small computers that can be programmed to control any number of things, such as the spinning of rotors, the dispensing of food into packaging on an assembly line or the opening of doors. Two models of PLCs made by the German-conglomerate Siemens were the target of Stuxnet, a sophisticated piece of malware discovered last year that was designed to intercept legitimate commands going to PLCs and replace them with malicious ones. Stuxnet's malicious commands are believed to have caused centrifuges in Iran to spin faster and slower than normal to sabotage the country's uranium enrichment capabilities.

Though Siemens PLCs are used in some prisons, they're a relatively small player in that market, Strauchs says. The more significant suppliers of PLCs to prisons are Allen-Bradley, Square D, GE and Mitsubishi. Across the U.S. there are about 117 federal correctional facilities, 1,700 prisons, and more than 3,000 jails. All but the smallest facilities, according to Strauchs, use PLCs to control doors and manage their security systems.

Strauchs, who lists a stint as a former CIA operations officer on his bio, became interested in testing PLCs after hearing about the systems Stuxnet targeted and realizing that he had installed similar systems in

prisons years ago. He, along with his daughter Tiffany Rad, president of ELCnetworks, and independent researcher Teague Newman, purchased a Siemens PLC to examine it for vulnerabilities, then worked with another researcher, who prefers to remain anonymous and goes by the handle "Dora the SCADA explorer," who wrote three exploits for vulnerabilities they found.

"Within three hours we had written a program to exploit the [Siemens] PLC we were testing," said Rad, noting that it cost them just $2,500 to acquire everything they needed to research the vulnerabilities and develop the exploits.

"We acquired the product legally; we have a license for it. But it's easy to get it off [eBay] for $500," she said. "Anyone can do it if they have the desire."

They recently met with the FBI and other federal agencies they won't name to discuss the vulnerabilities and their upcoming demonstration.

"They agreed we should address it," Strauchs said. "They weren't happy, but they said it's probably a good thing what you're doing."

Strauchs says the vulnerabilities exist in the basic architecture of the prison PLCs, many of which use Ladder Logic programming and a communications protocol that had no security protections built into it when it was designed years ago. There are also vulnerabilities in the control computers, many of which are Windows-based machines, that monitor and program PLCs.

"The vulnerabilities are inherently due to the actual use of the PLC, the one-point-controlling-many," Rad said. "Upon gaining access to the computer that monitors, controls or programs the PLC, you then take control of that PLC."

A hacker would need to get his malware onto the control computer either by getting a corrupt insider to install it via an infected USB stick or send it via a phishing attack aimed at a prison staffer, since some control systems are also connected to the internet, Strauchs claims. He and his team recently toured a prison control room at the invitation of a correctional facility in the Rocky Mountain region and found a staffer reading his Gmail account on a control system connected to the internet. There are also other computers in non-essential parts of prisons, such as commissaries and laundry rooms, that shouldn't be, but sometimes are, connected to networks that control critical functions.

"Bear in mind, a prison security electronic system has many parts beyond door control such as intercoms, lighting control, video surveillance, water and shower control, and so forth," the researchers write in a paper they've released (.pdf) on the topic. "Access to any part, such as a remote intercom station, might provide access to all parts."

Strauchs adds that "once we take control of the PLC we can do anything. Not just open and close doors. We can absolutely destroy the system. We could blow out all the electronics."

Prison systems have a cascading release function so that in an emergency, such as a fire, when hundreds of prisoners need to be released quickly, the system will cycle through groups of doors at a time to avoid overloading the system by releasing them all at once. Strauchs says a hacker could design an attack to over-ride the cascade release to open all of the doors simultaneously and overload the system.

An attacker could also pick and choose specific doors to lock and unlock and suppress alarms in the system that would alert staff when a cell is opened. This would require some knowledge of the alarm system and the instructions required to target specific doors, but Strauchs explains that the PLC provides feedback to the control system each time it receives a command, such as "kitchen door east opened." A patient hacker could sit on a control system for a while collecting intelligence like this to map each door and identify which ones to target.

While PLCs themselves need to be better secured to eliminate vulnerabilities inherent in them, Newman says prison facilities also need to update and enforce acceptable-use policies on their computers so that workers don't connect critical systems to the internet or allow removable media, such as USB sticks, to be installed on them.

"We're making the connection closer between what happened with Stuxnet and what could happen in facilities that put lives at risk," he said.

Photo: Folsom prison inmate Joseph Sweet uses his mirror to look at California Republican lawmakers visiting the inside of Folsom Prison, in Represa, Calif. By Brian Baer/AP.

- 1. Do not connect the door control system to the Internet.
  2. Require a 'double key' command sequence to affect any door lock (two separate commands from two physically separated consoles).
  3. 'Finger print' all door lock commands (use automatic fingerprint scanning or retinal recognition built into the command consoles).
  4. Institute extremely rigorous shift and control handover procedures for guard personnel (verify prisoner inventory, acknowledgement of incidents and anomalies, etc.).
  5. Require strong password access and enforce weekly password changes.

  Recognize that a PLC is nothing more than a software implementation of a hardware based control device. Before PLCs, we did everything with hardwired relays, timers and interlock switches, no software involved. It is possible to implement a PLC control scheme and subsequently burn it to OTP memory, preventing any manipulation of the control sequence. In many systems, 'blowing' a security 'fuse' will prevent all access to any underlying program code as well as preventing any future changes.

  - . Even if the control system isn't hooked up to the Internet, it might interface with systems which connect to the Internet. Read up on Stuxnet's delivery method. Anyway, good luck enforcing that policy.

    2. Requiring such a "double key" system would make disabling door lock/unlock mechanisms simpler. Break one system and you break both.
    3. Once biometric auth (fingerprints, retina scan) is compromised, it's permanently broken. If someone steals your password or key, you change the password or lock. If someone steals your fingerprint, what do you do? Get a new finger?
    4. Putting procedures in place is good, but again, how do you enforce that policy?
    5. If you make people change passwords weekly and choose strong passwords, they'll quickly develop a system to come up with new passwords because no one in their . Password1!, Password2!, Password3!, Password4!...

    Recognize that you don't know as much about information security as you think you do. There's a simple, easy solution for every problem and it's wrong. You don't need to change any code to exploit a flaw. In fact, if the code is harder to change it makes fixing problems harder. To give you an idea of how exploitation ACTUALLY WORKS, it's about figuring out how a system works to a very granular level, and determining what it allows you to do that you shouldn't be able to, or situations the code hasn't accounted for. You can't break the rules, but you might be able to find a loophole.

    http://www.youtube.com/watch?v=-YQ4CNZjD4w