The Washington Post, Everyday machines vulnerable to hacking 4 June 2012

Cyber search engine Shodan exposes industrial control systems to new risks

By Robert O'Harrow Jr., Published: June 3

It began as a hobby for a -teenage computer programmer named John Matherly, who wondered how much he could learn about devices linked to the Internet.

After tinkering with code for nearly a decade, Matherly eventually developed a way to map and capture the specifications of everything from desktop computers to network printers to Web servers.

He called his fledgling search engine Shodan, and in late 2009 he began asking friends to try it out. He had no inkling it was about to alter the balance of security in cyberspace.

"I just thought it was cool," said Matherly, now 28.

Matherly and other Shodan users quickly realized they were revealing an astonishing fact: Uncounted numbers of industrial control computers, the systems that automate such things as water plants and power grids, were linked in, and in some cases they were wide open to exploitation by even moderately talented hackers.

Control computers were built to run behind the safety of brick walls. But such security is rapidly eroded by links to the Internet. Recently, an unknown hacker broke into a water plant south of Houston using a default password he found in a user manual. A Shodan user found and accessed the cyclotron at the Lawrence Berkeley National Laboratory. Yet another user found thousands of unsecured Cisco routers, the computer systems that direct data on the networks.

"There's no reason these systems should be exposed that way," Matherly said. "It just seems ludicrous."

The rise of Shodan illuminates the rapid convergence of the real world and cyberspace, and the degree to which machines that millions of people depend on every day are becoming vulnerable to intrusion and digital sabotage. It also shows that the online world is more interconnected and complex than anyone fully understands, leaving us more exposed than we previously imagined.

Over the past two years, Shodan has gathered data on nearly 100 million devices, recording their exact locations and the software systems that run them.

“Expose online devices,” the Web site says. “Webcams. Routers. Power Plants. iPhones. Wind Turbines. Refrigerators. VoIP Phones.”

Homeland security officials have warned that the obscurity that had protected many industrial control systems was fast dis-appearing in a flood of digital light.

“This means that these delicate [control computers] are potentially reachable from the Internet by malicious and skilled adversaries,” a Department of Homeland Security paper concluded in 2010.

The number of intrusions and attacks in the United States is rising fast. From October to April, the DHS received 120 incident reports, about the same as for all of 2011. But no one knows how often breaches have occurred or how serious they have been. Companies are under no obligation to report such intrusions to authorities.

A weak link in the system

Industrial control systems are the workhorses of the information age. Like other computers, they run on code and are programmable. Unlike laptops, smartphones and other consumer technology, they’re stripped down and have little style or glitz.

Costing as little as a few thousand dollars and up to $50,000, they're often housed in plain metal boxes with few lights or switches. Control systems now open and shut water pipes, regulate the flow of natural gas, manage the production of chemicals, and run data centers, power-plant turbines and commuter trains.

The control computers collect data from electronic sensors, analyze it and send it on to desktop computers that serve as the "human-machine interface." They afford managers precise and remote control of the machinery.

The most far-flung and powerful of these networked systems are called supervisory control and data acquisition, or SCADA. They give companies central control of large numbers of pumps, generators, oil rigs and other operations.

The allure of long-distance network control is hard to resist. Manufacturers of control computers have promised that such networks can cut costs by reducing the number of workers in the field. Siemens Industry Inc., a leader in the field, said in a recent marketing brochure that it is "more important than ever" to adopt control devices "to respond to the increasing international competitive pressure."

The systems are often hardened against weather or tough conditions and can run nonstop for months or years. But many were designed for another era, before the mesh of networks reached into every corner of the globe, and some of the systems rely on outdated hardware and software.

A recent examination of major control systems by six hacker-researchers working with the security firm Digital Bond found that six of seven devices in the study were riddled with hardware and software flaws. Some included back doors that enabled the hackers to download passwords or sidestep security completely.

Researchers found that one machine made by General Electric, the D-20, uses the same microprocessor installed in Apple computers two decades ago. The company that made its operating software stopped updating it in 1999. It is often shipped to customers with no meaningful security. "Security is disabled by default," the manual says. "To log in, enter any name; you do not need a password."

In a statement to The Washington Post, General Electric said: “The D-20 was designed for deployment in a layered security environment, in which asset owners and operators employ a range of measures to prevent, detect and respond to intrusions. GE actively works with our customers to design and support those security measures.”

The company added that the software for the machine “is designed to be secure and includes a layer of password-protection, which can be activated if the customer chooses to do so.”

Other machines had flaws that enabled the researchers to take control through electronic back doors.

In January, Digital Bond said the results were “a bloodbath, mostly.”

“Most of the guys were able to hack their controllers in a single day,” said K. Reid Wightman, a Digital Bond security researcher and former Pentagon cyberwarrior. “It’s just too easy. If we can do it, imagine what a well-funded foreign power could do.”

The owners of control computers long assumed that few outsiders understood or cared how power plants and other facilities worked. They also figured the systems were safe within their facilities, disconnected from outside networks.

But like much of the rest of the world, the systems were rapidly being linked to global networks, often through indirect connections. Many of those connections came as executives sought more refined detail about their operations. With few exceptions, corporate networks used by executives are linked in some way to the Internet.

Because of the strange nature of cyberspace, even an employee passing through a plant with a wireless connection on a laptop can create a temporary data link that exposes control systems to intruders.

“They have sort of connected through osmosis,” said Marty Edwards, a senior cybersecurity official at the Department of Homeland Security. “What we have done is connect to everything.”

An accidental discovery

The idea for Shodan came to John Matherly in 2003, when he was a teenager attending community college in California. Obsessed with the digital world, he named his project after a malevolent character in a video game called System Shock II. The character, Sentient Hyper-Optimized Data Access Network, or Shodan, is an artificial intelligence entity that thinks it is a goddess and sets out to eradicate humans.

Matherly, who grew up in Switzerland, toyed with his system for years as he earned a degree in bioinformatics from the University of California at San Diego and built his career as a programmer, data miner and Web developer. His early Shodan versions found only hundreds of devices a day on the Web, and the information was not searchable. After devoting months to the project in 2009, he made a breakthrough, solving the search problem and locating many more devices.

When he launched his first live version of the program, in November of that year, he thought it might catch on with software makers who wanted to know about the systems being used by potential customers. On his Web site, Matherly described his program as “the world’s first computer search engine that lets you search the Internet for computers. . . . Find devices based on city, country, latitude/longitude, hostname, operating system and IP.”

The Shodan software runs 24 hours a day. It automatically reaches out to the World Wide Web and identifies digital locators, known as Internet protocol (IP) addresses, for computers and other devices. The program then attempts to connect to the machines. If a connection is made, Shodan “fingerprints” the machine, recording its software, geographic location and other data contained in the identification “banner” displayed by devices on the Internet.

Such identifying information is called “metadata” — and it’s far more common, useful and problematic than anyone had realized. Shodan compiles the information in Matherly’s servers — about 10 million devices every month now — and makes it almost as easy to query online as a Google search.

At first, the Shodan discoveries seemed trivial: devices commonly linked to networks such as printers and Web servers. But as queries became more sophisticated, troubling findings started emerging. One researcher using the system found that a nuclear particle accelerator at the University of California at Berkeley was linked to the Internet with virtually no security. Another identified thousands of data routers — the devices that make networks possible — open to anyone. Because they required no passwords, they could be taken over with ease.

“It was only after nearly a year that individual researchers began digging deeper through the Shodan data to locate devices that weren’t part of the known, discovered Internet,” Matherly said. “Water-treatment facilities, power plants, particle accelerators and other industrial control systems had been hidden from traditional search engines.”

As the dimensions of the challenge posed by Shodan became clear, the DHS Industrial Control Systems Cyber Emergency Response Team issued a stark warning in October 2010, noting “the increased risk” of brute-force attacks on “systems available on the Internet.”

The alert recommended placing all control system assets behind firewalls, using secure remote-access methods and disabling default passwords.

A researcher at Cambridge University, Eireann Leverett, used Shodan to identify more than 10,000 control computers linked to the Internet, many of them with known vulnerabilities. Leverett concluded that many operators had no idea how exposed they were — or even realized that their machines were online.

”This could be used to carry out remote attacks on selected devices or identify networks for further reconnaissance and exploitation,” Leverett wrote in a thesis, “Quantitatively Assessing and Visualising Industrial System Attack Surfaces,” published in June 2011. “Malicious actors might already be doing this.”

In the United States, security experts Billy Rios and Terry McCorkle said this spring that their research suggests the situation is worse than even Leverett demonstrated. Rios, who works for Google, and McCorkle, who works for Boeing, are both Shodan users who study control systems on their own time.

“The number of control systems on the Internet is far greater than anybody realizes,” said McCorkle, who along with Rios recently discussed control computer vulnerabilities at the National Defense University at Fort McNair. “These systems are insecure by their nature.”

Matherly said he wants his search engine used to improve security. But he said it can be used to shred it as well.

“Shodan has lifted the barrier. There’s no going back,” Matherly said. “Once you shed light on it, you can’t go back into hiding.”

A history of digital attacks

One story from the Cold War shows that cyberattacks on control systems have been in the imagination for a long time. Though some details are hard to confirm, it describes an attack that experts believe could happen today.

In 1981, a Soviet KGB colonel who became a spy for France, code name Farewell, shared Soviet plans to use a Canadian front company to secretly acquire technology to automate the Trans-Siberian gas pipeline, according to “At the Abyss: An Insider’s History of the Cold War,” by Thomas Reed, a former Pentagon official. Tipped off by the French, U.S. officials set up a front company to sell the technology, but only after they made some undetectable alterations to the computer code.

The alterations eventually “reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds,” Reed wrote two decades later. “The result was the most monumental non-nuclear explosion and fire ever seen from space.”

A KGB veteran later disputed the account. A document on the CIA’s Web site confirmed only that “contrived computer chips” were provided to the Soviets and “flawed turbines were installed on a gas pipeline.”

Evidence of the threat to control computers mounted.

In 1997, a teenage hacker using a personal computer and a dial-up connection shut down part of a telephone network in Worcester, Mass., cutting off the local airport’s air-traffic-control communications.

In 2000, Vitek Boden, a supervisor at a technology firm in Australia, was bitter that he did not get a job with the Maroochy Shire Council, according to Joseph Weiss, author of “Protecting Industrial Control Systems From Electronic Threats.” Using a radio transmitter, Boden launched an attack against a wastewater-treatment system in Queensland, remotely accessing the control systems and releasing hundreds of thousands of gallons of raw sewage into local streams and parks. He was sentenced to two years in jail.

“Marine life died, the creek water turned black and the stench was unbearable for residents,” an Australian Environmental Protection Agency official said later.

In 2007, skeptics still claimed that the threat of cyberattacks on real-world machinery was theoretical. In a demonstration called Project Aurora, the Department of Homeland Security along with power industry officials decided to test the theory themselves.

In the end, many doubters were silenced.

The target was a 5,000-horsepower diesel engine, the kind of machine that often serves as a backup generator for manufacturers and large organizations. Engineers at the Idaho National Laboratory hacked into the generator's embedded control computer through a network. By repeatedly triggering circuit breakers, they created massive torque on the machinery, which eventually started to shake, smoke and tear itself to pieces.

Mark Zeller, who specializes in industrial power systems at Schweitzer Engineering Laboratories Inc., said the Aurora Project set off a scramble in the power industry to identify links to cyberspace and improve "electronic" perimeter security.

Those efforts include assessing the links between control systems and networks and creating layers of defenses against intruders. In some cases, that means creating "air gaps" — physical separations that cannot be breached by wireless connections — between networks and control systems along with stronger password protection.

"They have really taken this electronic security perimeter thing seriously," Zeller said. "It's a big issue now."

At the same time, the DHS has stepped up its efforts, including providing advice and assistance to industries to reduce cyber-risks.

The government now routinely issues alerts about new threats to control systems. Alerts are also issued by a private industry group, the North American Electric Reliability Corp., or NERC, the organization of electrical grid operators in the United States.

Three weeks ago, NERC said that control computers on the Internet "face increased exposure" because of Shodan and hacking tools. The NERC alert said that "it is possible that hackers or hacktivist groups may cause sporadic component failures as they identify and interact with these devices."

A sophisticated new virus called Flame, apparently aimed at intelligence collection against Iran, was revealed last week, underscoring anew the threats in cyberspace. But the most powerful and

ingenious cyber-attack ever publicly disclosed involved industrial control systems in Iran. Called Stuxnet when its code was discovered on the Internet in the summer of 2010, the attack alerted the world to the true potential for attacks on critical infrastructure.

Last week, the New York Times reported that Stuxnet was part of a U.S.-Israeli covert operation against Iran approved by President Obama. Stuxnet targeted a control computer called an S7 produced by Siemens and used by the Iranian government to operate centrifuges in the process of enriching uranium.

The malicious code designed to attack the machines was included as payload in a package of software called a computer "worm."

The worm was launched into the Internet and spread rapidly around much of the world, like a virus during flu season. But most of the computers and systems infected were in Iran.

The worm code was designed to self-replicate. Investigators said it apparently infected flash drives in Iran, helping it jump from networks to unconnected computers at the Iranian nuclear processing facility in Natanz.

Stuxnet took advantage of four unknown software flaws, or zero days, to crack through security in a variety of computer systems. The attack code eventually directed the S7s to operate uranium-refining centrifuges at speeds beyond their tolerances while sending misleading data to monitors showing that all was well.

It was brilliant and devastating. Analysts believe that hundreds of centrifuges were damaged, though no one outside the operation knows for sure.

"The real-world implications of Stuxnet are beyond any threat we have seen in the past," said the authors of an analysis of the worm issued by Symantec, a computer security firm. "Stuxnet is the type of threat we hope to never see again."

Among those shaken to the core was Siemens.

“Stuxnet marked a turning point for the entire automation industry, turning theoretical problems into headlines,” Raj Batra, president of the industry automation division at Siemens, told The Post.

Exploiting flaws

News of Stuxnet jolted hackers around the world like a double shot of espresso, waking them up to the once-

obscure world of industrial control systems.

One of them was Dillon Beresford, an energetic hacker and security consultant in Texas. He read an article about the attack in Wired magazine.

“It inspired me,” Beresford said. “I wanted to disprove that it would take a nation-state to pull this off.”

“I’m like, no, I’m going to do this in my living room.”

Beresford wasn’t just being brash. He had found zero-day vulnerabilities over the years. “At the end of the day, it’s all just code,” he said.

Starting in January 2011, Beresford worked almost nonstop for two months. He focused on the Siemens S7 line of controllers.

Like any good hack, it started with research. Beresford found an online “coding library” run by a German researcher. It contained source code for a wide variety of computers, including the S7s.

Night after night he studied, focusing in particular on what is known as the machine's communications protocol.

He discovered the protocol was designed to make it easier for machines to communicate with the Internet. Security was an afterthought.

Beresford persuaded his boss at the time — a manager at NSS Labs, a security firm — to buy him four of the industrial control systems for thousands of dollars each. "If you do find something, let people know you're from NSS," his boss told him.

The devices came mounted on heavy boards, ready for testing. The S7 is a plain rectangular metal container with heat vents and ports for cables, about the size of a large shoe box.

Beresford set them up on his workbench in the bedroom of his apartment in suburban Austin. He connected them to his laptop and began to hunt.

"I was up every night until 5 a.m.," he said. "I love to write code."

Several weeks into his experiments, Beresford made the first of several discoveries of flaws in the S7s. One of them took advantage of the fact that the protocol did not encrypt its communication with other networks, allowing a hacker to easily read and steal the "plain text" passwords.

Beresford said the protocol was created by designers who assumed the machines would operate behind the safety of an "air gap" between them and open networks. At the time, no one anticipated the use of thumb drives to close such gaps, as in the Stuxnet attack.

He also found a digital back door that enabled him to read the device's internal memory, including the password stored on the device.

In May 2011, Beresford sent his findings to the DHS. The feds studied his work and confirmed it. In an alert issued on July 5, the agency announced it was working with Siemens on the S7 vulnerabilities.

“I crushed it,” he said. “All average guys, your typical hacker, could very easily replicate this.”

Since then, using his Shodan account, Beresford has found more than 100 S7s online, all of them potential targets.

Batra of Siemens acknowledged the vulnerabilities and said the company is working hard to address them. The company last week announced it is offering new security enhancements for its industrial control systems.

“Siemens’s automation products are rigorously tested with regard to industrial security and yet must be designed to also balance the requirements of open industrial solutions, which drive productivity,” he said. “There will never be an endpoint when it comes to industrial security threats, but companies can better protect their systems by staying up to date with the research community, following the guidance of governmental agencies, and by working with responsible, technologically innovative vendors like Siemens.”

Something to prove

Other hackers also began turning their attention to industrial control computers after hearing about Stuxnet.

One of them, an anonymous hacker who calls himself pr0f, is a bright, unemployed 22-year-old who favors hoodie sweatshirts and lives in his parents’ home somewhere overseas. He is among the growing numbers of Shodan users.

After studying control systems in the wake of Stuxnet, he thought the insecurity of the devices seemed crazy and irresponsible.

“Eventually, somebody will get access to a major system and people will be hurt,” he later said. “It’s just a matter of time.”

He vowed to prove how easy it was to get in. On Nov. 17, he saw an article online about an apparent industrial control system attack in the United States. The article said a hacker in Russia had apparently destroyed a pump in a water utility in Springfield, Ill.

Pr0f had been expecting something like this, but he was incredulous when he read a statement in the story from a DHS official.

“At this time there is no credible corroborated data that indicates a risk to critical infrastructure entities or a threat to public safety,” the statement said.

The hacker fumed: How could Homeland Security play down something so important?

“It was the final straw,” pr0f said. “I was angry. I said, ‘Yep, let’s do something.’ ”

The Springfield episode turned out to be an accident not connected to Russia, but he did not learn that until later. Impulsively, he began programming his computer to search the Internet for a Siemens S7 controller. The first one he found just happened to be an S7 in South Houston, a small town thousands of miles and an ocean away from where he sat.

The hacker navigated to the machine’s Internet address. When prompted to identify himself as an approved operator, he knew just what to do, because he had read the manual. He typed in the default password: three simple digits. A moment later, he was at the controls of a water plant that serves 16,000 Texans.

“This required almost no skill,” the young man wrote online a short time later, using an e-mail address in Romania to cloak his identity.

The S7 was installed when the town upgraded its water plant more than a decade ago. That was long before most people thought of industrial control systems as targets. “Nobody gave it a second thought,” Mayor Joe Soto said. “When it was put in, we didn’t have terrorists.”

The intrusion took all of 10 minutes. The hacker did not cause any damage. Instead, he recorded images of the control system as proof of how easy it was for him to get in.

“I didn’t actually know what the machine was going to control when I started, but I logged in, and well, saw the stuff I took screen shots of,” he said in an e-mail exchange. “I was just amazed.”

So was Soto, after he saw images of the plant’s control panels on the Internet. He and other town officials ordered the gap closed immediately and then considered the implications.

“We’re probably not the only one who is wide open,” Soto said later. “He caught everyone with our pants down.”