Technology | DOI:10.1145/3014392 Alex Wright

Mapping the Internet of Things

Researchers are discovering surprising new risks across the fast-growing IoT.

As more and more physical objects get connected to the Internet—from consumer products like webcams and pacemakers to industrial equipment like wind turbines and power plants—the contours of the Internet are shifting beyond the realm of screen-based devices to encompass a much broader swath of the world around us.

Wherever the Internet goes, security risks seem to follow. As the Internet of Things (IoT) continues to expand, those risks are taking on new dimensions well beyond the familiar threats of stolen passwords and credit cards.

"When you say 'Internet of Things,' the first thing most people think of are Apple Watches or Fitbits," says David O'Brien, a senior researcher at Harvard University's Berkman-Klein Center for the Internet and Society. "They're not thinking about programmable logic controllers or other infrastructure devices."

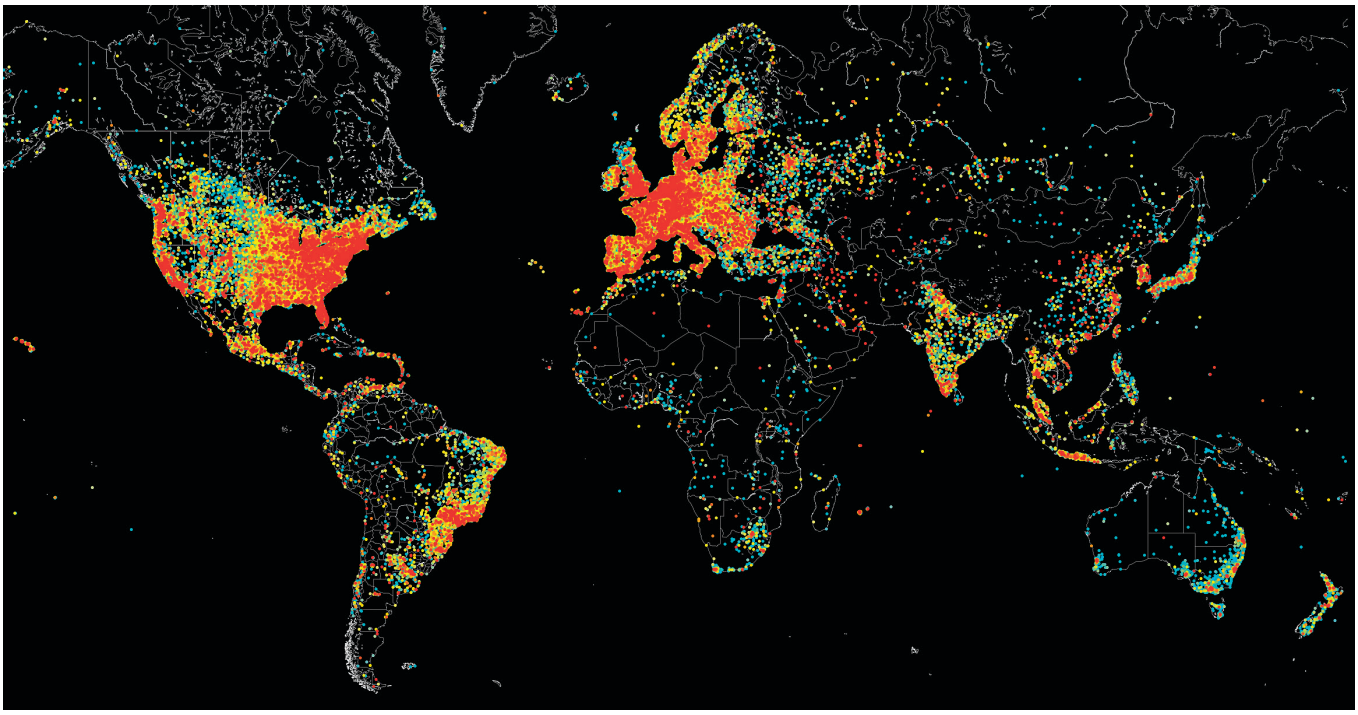
Industrial computing devices are a vast, largely invisible realm of the IoT, one that remains out of sight to most of us, yet plays a critical role in sustaining our everyday quality of life: power plants, water pumps, and oil rigs all rely on industrial computers connected to the Internet, and these devices appear to be far less secure than we might assume.

The lack of security across the industrial IoT has come to light largely thanks to an experimental search engine called Shodan. First launched in 2009, the service now crawls nearly four billion devices over the IPv4 network, as well as a number of IPv6-connected devices. At any given time, it monitors about 700 million devices (depending on network connectivity, and whether the devices are turned off or on).

Shodan's creator, John Matherly, first started work on the service as a teenager in the mid-2000s. "The idea for Shodan came to me during the age of peer-to-peer software such as Napster and E-mule. The original concept was to provide a tool that would let security researchers scan networks and share the data (via P2P) with others."

Unlike Web browsers that traverse the Internet via the Hypertext Transport Protocol (HTTP), Shodan surveys other TCP/IP-connected ports including FTP, SSH, SNMP, SIP and RTSP ports in search of responsive servers. When it receives a welcome message (or any response), it retrieves what metadata it can find, and catalogs the information.

At first, Matherly envisioned collecting data on the kinds of Internet-connected products in use, and create a repository of information about patches, site licenses, and other useful meta-



Shodan founder John Matherly used the search engine to map all Internet-connected device in the world.

IMAGE COURTESY OF JOHN MATHERLY/SHODAN (WWW.SHODAN.IO)

data. Like many a project that started out as an interesting hack, however, Shodan has since taken on some interesting, unexpected applications.

Over the past few years, Shodan users have uncovered a series of alarming network vulnerabilities in Internet-connected devices, including a nuclear reactor; the cyclotron at the Lawrence Livermore National Laboratory outside Berkeley, CA; a water treatment plant outside Houston; electric power generators; oil rigs; and even a crematorium.

Eireann Leverett, a researcher in the Centre for Risk Studies at the University of Cambridge, U.K., used Shodan to identify more than 100,000 vulnerable IoT devices in 2011, concluding these flaws left them vulnerable to attack by "malicious actors." In a similar vein, Billy Rios at Google and Michael McCorkle of Boeing also have identified a series of serious security exposures across a wide range of connected industrial devices.

To Matherly's surprise, many of these devices turned out to be special-purpose industrial computers: control systems that perform highly specific tasks, like regulating the flow of water and other utilities, transportation systems, and even entire power grids—all controlled over the network by remote supervisory staff.

Unlike the consumer-facing Websites that most of us can find readily using commercial search engines like Google, industrial control systems (ICS) have largely remained hidden in plain view, invisible to web crawlers. Since Shodan's launch, however, it has shone an unforgiving light on some of these devices' glaring security flaws.

"Industrial control systems have relied on security by obscurity," says Mather, who now spends much of his time consulting with organizations on strengthening the network security of these devices.

Most of these devices rely on proprietary hardware and software protocols that tend to mask their vulnerabilities—but also make it difficult for security researchers to develop generalized and replicable approaches to security. "The more accessible the technology, the easier it is for people to find and fix vulnerabilities," says Mather.

More troublingly, many vendors failed to treat these risks seriously, assuming these systems could only be addressed directly, rather than over an external network. As a result, many hardware makers have tended to treat potential vulnerabilities lightly.

"It's a technical problem, but it's also closely tied to business interests ... these days, the way companies tend to look at security is as a loss leader."

O'Brien feels these exposures stem not just from technical failures, but from a fundamental lack of industry focus on security. "It's a technical problem, but it's also closely tied to business interests," he says. "These days, the way companies tend to look at security is as a loss leader."

Moreover, customers for these systems—like, say, power plant operators—tend to resist adding layers of security, to ensure their ability to respond quickly in case of emergency. End-users within these organizations often see additional security controls—like layers of password prompts—as more of a burden than a benefit.

Given the lack of customer demand, product managers at hardware companies often find it difficult to justify investing resources in preventive security measures that do not add new functionality. Complicating matters further is the difficulty of sending updates and patches to these devices without user-initiated firmware updates—a common practice for Web-based software applications. As a result, these industrial devices can often remain vulnerable for extended periods of time.

"To be fair, many of these systems were designed before the age of ubiquitous connectivity," says Mather, "so the engineers didn't worry about hardening their device against software attacks."

Mather also points to economic factors at play: "There wasn't a push by the ICS operators to demand better computer security from the manufacturers." Instead, they tended to focus more on issues of availability and reliability, and treated security as a secondary consideration.

That is now starting to change, thanks in part to the visibility that Shodan has brought to these vulnerabilities. In a similar vein, an open source project called Onionscan has made considerable headway in exposing the possible vulnerabilities of physical devices over the Internet.

Looking ahead, Shodan is focused on developing more sophisticated tools and visualizations to make the data more accessible to non-technical users.

Elsewhere, Nathan Freitas of the Guardian Project is spearheading an effort to use Tor—a free software package often used by hackers and journalists to protect their privacy via a worldwide network of volunteer-run servers—to safeguard IoT devices by means of Home Assistant, a Python-based system that allows for Tor to be used for physical devices. The system relies on a Raspberry Pi computer running Tor's software to mask the location of smart home devices by means of an authenticated hidden service that prevents anyone from locating and connecting to the devices without access to a passcode that the developers describe as a "cookie."

While this technology remains in the experimental stage, Freitas hopes it will pave the way for more fully developed commercial IoT security applications in the figure.

Amid the rise of connected devices and growing public concern about Stuxnet-style attacks on major infrastructure projects, the conditions seem ripe for IoT security applications to find more traction in the marketplace. Yet Mather feels the industry at large remains too blithe about these dangers.

"We keep deploying new devices that are insecure-by-default," he explains. "The vulnerable IoT devices of today that get installed are going to stick around a long time and they have access to the internal networks of many homes and businesses."

That might seem like a borderline-paranoid fantasy, but the rapidly accelerating development of "smart hardware" devices may bring these risks closer to home—and soon. For example, some firms are developing light bulbs that serve as Internet

hubs, relaying Wi-Fi signals, connecting thermostats, or even interfacing with a home security system. As these everyday devices become increasingly interconnected, the security risks multiply exponentially.

O'Brien believes the long-term solution to IoT security will require a balanced approach to technological innovation and public policy-making to create a more reliable physical computing infrastructure.

"We're at a point where we're rethinking what the role of government ought to be," he says. Despite a number of high-profile cyberattacks in recent years, securing critical infrastructure remains an area of unclear jurisdictional ownership within the federal government, partially involving the Federal Bureau of Investigation (FBI), Department of Homeland Security, and other agencies. The White House recently released a statement clarifying the role of first responders in cybersecurity attacks, but there is plenty of work left to do on this front.

Meanwhile, Mather worries people fail to recognize the growing sophistication of seemingly everyday devices like light bulbs or coffee machines that are fast becoming part of a deeply interconnected—and potentially insecure—worldwide network of smart objects. "Those devices are full-fledged computers nowadays," he explains, "and with the increasing number of IoT devices that are being deployed, those vulnerabilities become a real concern."

Securing critical infrastructure remains an area of unclear jurisdictional ownership within the U.S. federal government.

Further Reading

Leverett, E.
Quantitatively Assessing and Visualising Industrial System Attack Surfaces. University of Cambridge Computer Laboratory, Darwin College, June 2011. http://www.cl.cam.ac.uk/~fms27/papers/2011-Leverett-industrial.pdf

National Science and Technology Council, *Federal Cybersecurity Research and Development Strategic Plan: Ensuring Prosperity and National Security*, 2016. https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf

Olsen, M., Schneier, B., Zittrain, J.
Don't Panic: Making Progress on the 'Going Dark' Debate. Berkman Center for Internet and Society, Harvard University, February 1, 2016. https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

Seitz, J.
Dark Web OSINT With Python and OnionScan. Automating OSINT, July 28, 2016. http://www.automatingosint.com/blog/2016/07/dark-web-osint-with-python-and-onionscan-part-one/

Alex Wright is a writer and researcher based in Brooklyn, NY.

Milestones

New CS Education Framework for U.S. Schools

ACM is part of a committee of computer science organizations that has released a framework to inform implementation of computer science education in K–12 schools throughout the U.S.

ACM, Code.org, the Computer Science Teachers Association, the Cyber Innovation Center, and the National Math and Science Initiative recently announced the launch of the K–12 Computer Science Framework, intended to inform the development of standards, curriculum, and computer science pathways, and also to help school systems build capacity for teaching computer science.

Developed through partnerships with states, districts, and the computer science education community, the K–12 Computer Science Framework is a significant milestone for computer science in the U.S. It promotes a vision in which all students critically engage in computer science issues; approach problems in innovative ways; and create computational artifacts with a personal, practical, or community purpose.

The framework is not a set of standards; it is a set of guidelines put forth by the community that can inform standards, curricula, and many other supports for computer science education. The framework's learning progressions describe how students' conceptual understanding and practice of computer science grow more sophisticated over time. The concepts and practices are designed to be integrated to provide authentic, meaningful experiences for students engaging in computer science.

"The K–12 Computer Science Framework not only includes technical concepts about computing, but also stresses the importance of creating an inclusive culture in the field, promoting collaboration among students, and communicating effectively about technology," said Mehran Sahami, Associate Chair for Education in the computer science department at Stanford University. "In this regard, the framework provides skills that generalize beyond computer science while also giving students an understanding of fundamental computing concepts that will serve them well in whatever career they choose to pursue." Sahami also co-chairs ACM's Education Board and Education Council.

ACM, CSTA, INFOSYS ANNOUNCE AWARDS FOR CS TEACHING EXCELLENCE

Infosys Foundation USA, ACM, and CSTA, the Computer Science Teachers Association, recently announced the launch of the Awards for Teaching Excellence in Computer Science. Up to 10 awards of $10,000 each will be awarded annually.

Funding for the awards is being provided by Infosys Foundation USA. Mark R. Nelson, CSTA's Executive Director, said Infosys "is sending a powerful message to these computing educators worldwide that what they are doing is indeed important."

"Great computer science education starts with great teachers," explains ACM President Vicki L. Hanson. "This new award reinforces our long-held goals of recognizing the contributions of computer science teachers and building a framework that supports their professional development."

Winners of the 2016 awards were announced in December (after press time). The prizes will be awarded at the 2017 CSTA Annual Conference in Baltimore in July.