Society | DOI:10.1145/3317675 Samuel Greengard

Deep Insecurities: The Internet of Things Shifts Technology Risk

A more connected world sounds alluring, but without better protections, the Internet of Things could lead to disaster.

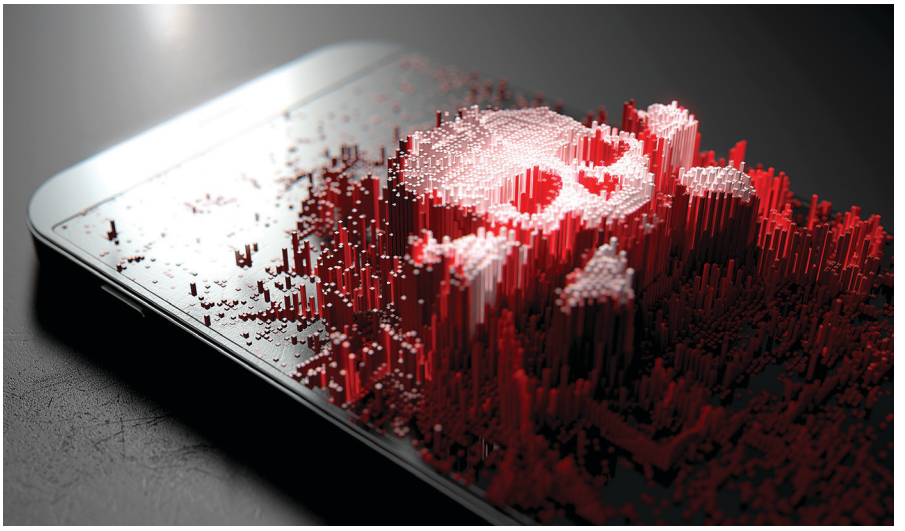

IMAGE BY INKED PIXELS

IT IS HUMAN nature to view technology as a path to a better world. When engineers and designers create devices, machines, and systems, the underlying premise is to deliver benefits. The Internet of Things (IoT) is certainly no exception. Smartphones, connected cars, automated thermostats, smart lighting, connected health trackers, and remote medical devices have made it possible to accomplish things that once seemed impossible. Everything from toothbrushes to tape measures are getting "smart."

However, at the center of the tens of billions of connected devices streaming and sharing data lies a vexing problem: cybersecurity. It is no secret that hackers and attackers have broken into baby monitors, Web cameras, automobiles, lighting systems, and medical devices. In the future, it is not unreasonable to assume that cybercriminals could take control of a private citizen's refrigerator or lighting system and demand a $1,000 ransom in bitcoin in order to restore functionality. It is also not difficult to fathom the threat of a vehicle that won't brake, or a pacemaker that stops working due to a hack. Hackers might also weaponize devices and take down financial systems and power grids.

The thought is chilling, and the repercussions potentially far-reaching. "All these devices, which now have computing functionality, affect the world in a direct physical manner—and that just changes everything," observes Bruce Schneier, an independent computer security analyst and author of *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (W. W. Norton & Company, 2018). "Today, computers can actually kill you."

Adds Stuart Madnick, John Norris Maguire Professor of Information Technologies at the Massachusetts Institute of Technology (MIT) Sloan School of Management, "We are entering a dangerous period. We have to wake up to the risks."

Dangerous Liaisons

What makes the IoT so powerful—and so dangerous—is the fact that devices and data now interconnect across vast ecosystems of sensors, chips, devices, machines, and software. This makes it possible to control and manipulate systems in ways that were never intended.

For example, in December 2015, a massive cyberattack shut down the power grid in the Ukraine. An estimated 230,000 people were left without electricity for a period lasting from one to six hours after hackers compromised systems at three energy distribution companies. In 2018, researchers at Upstream Security Ltd. found that attacks on connected cars had increased sixfold over a four-year period. Hackers entered through servers, keyless entry systems, onboard diagnostics ports, infotainment systems, mobile apps, wireless connections, sensors, and more.

The stakes continue to grow. In February 2018, security researchers Billy Rios and Jonathan Butts of security consulting firm WhiteScope LLC discovered a vulnerability in the Medtronic CareLink 2090 portable computer system, which uses wireless telemetry and over-the-air programming to control pacemakers and oversee home monitors for cardiac patients. "Someone could sit at a Starbucks and commandeer the pacemaker programmer," Rios says. "They could alter the way the device works and potentially impact a patient's safety." Medtronic, which is subject to U.S. Food and Drug Administration (FDA) regulatory oversight, wound up issuing a recall for the device so it could patch the vulnerability.

Rios, one of the world's top ethical hackers, says the level of security embedded in most devices is woefully inadequate and the situation shows no

sign of improving. "A huge problem is that computing devices were originally designed to operate in a closed system. The underlying hardware and software weren't designed for a connected world. Devices and communications systems are built on intrinsically insecure protocols. Now we have all these devices that are using these protocols to connect cars, trains, airplanes, and more. You cannot flip a switch or make a small code change and protect these systems."

A cyber-9/11 event, on par with the physical attacks on the U.S. that occurred in 2001, is not outside the realm of possibility, even if some of the concepts seem like science fiction today, experts say. Privacy is yet another concern because today's devices incorporate data recorders and logs, GPS connectivity, health and fitness data, and detailed information about how people live and move about. Already, an interactive toy doll named *My Friend Cayla* has been banned in Germany because it surreptitiously recorded conversations and stored them unprotected on the Internet.

Says Benson Chan, senior partner at consulting firm Strategy of Things, "In a hyperconnected world, the biggest security risk is that there's a lack of transparency. You just have millions of machines talking to each other, making decisions and taking action autonomously based on machine learning algorithms. There is very limited visibility about what data is passed through and how decisions are made."

Finding a Fix

At the center of this frightening scenario is a simple but profound fact: the technical resources largely exist to address the risk of a hyperconnected world, but the political, economic, and social impetus is lagging. "The fundamental problem is that companies are interested in getting products to market quickly. The market does not reward security," Schneier says. Adds Madnick: "It has become apparent that we cannot rely on manufacturers and vendors to consistently include the essential security protections."

Addressing the lack of security and privacy in IoT devices won't be easy. What's more, the repercussions could have enormous impact on product liability, particularly if injuries and deaths occur. Ultimately, IoT security experts say a two-pronged approach is required. It's critical to change the way manufacturers build products, but also to introduce regulations and laws that support security and privacy. Business leaders must recognize there are advantages to building a more secure IoT, Madnick says. "At some point—and it's already something that some companies understand—it is much easier and less expensive to build security into every aspect of a product than it is to reverse-engineer it later on."

Security experts say a two-pronged approach is needed: manufacturers must change how they build their products, and new laws must support security and privacy.

Enhancing industry security and privacy standards for the IoT is gaining momentum. An industry body, the Online Trust Alliance (OTA), is spearheading efforts to establish security and privacy by design. A "Security by Design" framework has also been promoted by the Open Web Application Security Project (OWASP), which focuses on a multipronged approach: minimizing attack surfaces, establishing secure default settings, adopting the principle of least privilege (granting users only the minimum access they require to accomplish a task), adopting a defense in depth framework (which features a layered series of defensive mechanisms), embracing a zero-trust model, fixing security flaws promptly and correctly, and several other tactics.

Schneier says such a framework must encompass several elements. These include vendor transparency about how products work, software that is patchable, extensive preproduction testing, security out of the box, the

ACM Member News

INTEREST IN ROBOTS LEADS TO R&D FOR SELF-DRIVING CARS

"When I was a kid, I was very interested in reading science fiction about robots," says Li Erran Li, adding that this early interest would influence the future trajectory of his education and career. Today, Li is chief scientist at Pony.ai, a start-up developing autonomous driving technology.

Li earned his undergraduate degree in automatic control from the Beijing University of Technology, and his master's degree in computer vision from Beijing's Chinese Academy of Sciences. He then came to the U.S. and obtained his Ph.D. in computer science from Cornell University.

Before joining Pony.ai in May 2018, Li was part of the perception team at Uber's Advanced Technology Group, as well as working with that company's machine learning platform team. Prior to Uber, Li spent 14 years working for Bell Laboratories.

Li's current research is primarily focused on machine learning, computer vision, and learning-based robotics, and their applications to autonomous driving.

As chief scientist at Pony.ai, Li leads the company's research efforts. He also serves as vice dean of the Pony.ai Research Institute in Guangzhou, China, where computer scientist and computational theorist Andrew Yao, who received the 2000 ACM A.M. Turing Award, is the honorary dean.

Li says he is passionate about pushing the frontiers of artificial intelligence for autonomous driving, and is active in the machine learning and computer vision communities. He often provides tutorials and organizes workshops on machine learning for autonomous driving at academic conferences, such as the International Conference on Machine Learning (ICML) and the Conference on Neural Information Processing Systems (NIPS).

—John Delaney

ability for systems to fail predictably and safely, the use of standard protocols, the ability to preserve offline functionality, and widespread encryption and authentication of data.

He also believes vendors should support responsible security research. Such security research is severely lacking. The IoT Security Foundation (IoTSF) reported in August 2018 that only 9.7% of companies making IoT products have a public disclosure policy that allows researchers to probe known vulnerabilities.

This voluntary and lackadaisical approach has prompted many, including Schneier, to call for increased industry and government regulation. He would like to see broader and expanded regulations on products and product categories, a licensing system for professionals and products, more stringent testing and certification requirements, and more widespread adoption of industry best practices. This framework would include tax breaks for businesses that do things right, and rules that punish negligence and bad behavior.

Rules and Regulations

Although several past attempts to institute regulations and laws in the U.S. have failed, the landscape is changing. Massachusetts, New York, and California have all stepped up efforts to punish companies for data breaches and similar abuses. In August 2018, California took the boldest step forward when it adopted an IoT law, SB327, which establishes baseline security standards for IoT devices. The law, though intentionally vague, mandates that IoT device manufacturers must equip their products with "reasonable" security features to address wide-ranging issues such as authentication, device use, modification, and destruction. It will go into effect January 1, 2020.

The idea of regulating IoT devices is also gaining momentum elsewhere. For example, in Indonesia, the federal government is finalizing regulations that standardize the use of IoT devices, though the goal is primarily to create a framework for business. Japan, Canada, Mexico, Australia, and other countries also have addressed data governance through regulations, though most countries have not yet established a formal IoT regulatory framework. According to a 2015 study conducted by consulting firm Deloitte, the trend is toward greater regulation for electronic systems, including the IoT. The number of privacy laws has grown from 20 in the 1990s to more than 100 today.

Says Chan, "In the end, the biggest danger isn't a device failing or a grid shutting down; it's a loss of trust in technology."

Meanwhile, organizations such as EPIC (the Electronic Privacy Information Center) are stepping up lobbying efforts for the U.S. and Europe to adopt more stringent IoT cybersecurity and privacy standards. Europe, which has emerged as perhaps the most powerful regulatory entity in the world, adopted the General Data Protection Regulation (GDPR) in May 2018. It imposes standards for data use and sharing, along with sizeable fines for non-compliance. Although GDPR doesn't specifically pertain to the IoT, connected devices play a critical role in the regulatory framework. In addition, the EU is finalizing the ePrivacy regulation, which addresses the use of personal data through entities such as Facebook, SnapChat, and the Web, along with smartphones and other IoT devices.

Ultimately, any single approach is likely to fail, Schneier says; "None of them will work in isolation." Minimum security standards alone won't solve the underlying problem, he says; what is needed is a series of mutually reinforcing policies that can slide the dial to greater safety and security.

A Matter of Trust

The clock is ticking, Rios says. "As we move toward a far more connected world, the risk grows. You can't simply reboot a system and put a train back on the right track, or help a patient that has died because a medical device has failed." Moreover, as the IoT ripples across devices and systems, entire cities and groups will likely be affected. "Right now, manufacturers are not rewarded for building cybersecurity into products, but they can definitely be punished. We need to move toward a societal model where they are both rewarded and punished. We need to rethink and revamp the entire framework by which we create, manage, and use IoT devices," Rios says.

Chan believes it is crucial to think about IoT devices as more than individual components that can be hacked and manipulated. As these devices become more pervasive and entrenched in business and life, everything connecting to them—including data and algorithms—become potential targets for manipulation and abuse. Says Chan, "It's only a matter of time until we see ransomware, attacks on devices and connected networks, and perhaps even a cyber-9/11 event.

"But, in the end, the biggest danger isn't a device failing or a grid shutting down; it's a loss of trust in technology. If you can't trust devices to operate correctly and safely, then you won't use them ... when that happens, our world will be a very different place."

Further Reading

Schneier, B.
Click Here to Kill Everybody: Security and Survival in a Hyper-connected World.
W. W. Norton & Company (September 4, 2018).

Conti, M., Dehghantanha, A., Franke, K., and Watson, S.
Internet of Things Security and Forensics: Challenges and Opportunities. *Future Generation Computer Systems*, Volume 78, Part 2, January 2018, pp. 544-546. https://www.sciencedirect.com/science/article/pii/S0167739X17316667

Alaba, F.A., Othman, M., Hashem, A.T., and Alotabi, F.
Internet of Things Security: A Survey. *Journal of Network and Computer Applications*, Volume 88, 15 June 2017, pp. 10-28. https://www.sciencedirect.com/science/article/pii/S1084804517301455

Mosenia, A. and Jha, N.K.
A Comprehensive Study of Security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing*, Volume: 5, Issue: 4, Oct.-Dec. 1 2017, pp. 586–602. https://ieeexplore.ieee.org/abstract/document/7562568

Samuel Greengard is an author and journalist based in West Linn, OR, USA.