NEW AMERICA

CYBERSECURITY INITIATIVE

JASON HONG

TOWARD A SAFE AND SECURE INTERNET OF THINGS

JUNE 2016

About the Author

Jason Hong is an associate professor in the Human Computer Interaction Institute, part of the School of Computer Science at Carnegie Mellon University. He works in the areas of ubiquitous computing and usable privacy and security, and his research has been featured in the *New York Times*, *MIT Tech Review*, CBS *Morning Show*, CNN, *Slate*, the World Economic Forum, and more. Hong is an associate editor for IEEE Pervasive Computing and ACM Transactions on Human Computer Interaction, and is on the editorial board for Communications of the ACM. He is also an author of the book The Design of Sites, a popular book on web design using web design patterns. Hong is a cofounder of Wombat Security Technologies, which focuses on effective and measurable cybersecurity training. He received his PhD from Berkeley and his undergraduate degrees from Georgia Institute of Technology. Hong has participated on DARPA's Computer Science Study Panel, is an Alfred P. Sloan research fellow, a Kavli fellow, a PopTech Science fellow, a New America national cybersecurity fellow, and currently holds the HCII Career Development fellowship.

Acknowledgments

Special thanks to the Giotto Internet of Things Expedition team and to many researchers for many discussions about privacy and security over the years. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of New America or the persons and organizations above.

About New America

New America is committed to renewing American politics, prosperity, and purpose in the Digital Age. We generate big ideas, bridge the gap between technology and policy, and curate broad public conversation. We combine the best of a policy research institute, technology laboratory, public forum, media platform, and a venture capital fund for ideas. We are a distinctive community of thinkers, writers, researchers, technologists, and community activists who believe deeply in the possibility of American renewal.

Find out more at **newamerica.org/our-story**.

About the Cybersecurity Initiative

The Internet has connected us. Yet the policies and debates that surround the security of our networks are too often disconnected, disjointed, and stuck in an unsuccessful status quo. This is what New America's Cybersecurity Initiative is designed to address. Working across our International Security program and the Open Technology Institute, we believe that it takes a wider network to face the multitude of diverse security issues. We engage across organizations, issue areas, professional fields, and business sectors. And through events, writing and research, our aim is to help improve cybersecurity in ways that work—for the countries, for companies, and for individuals.

Find out more at **newamerica.org/cybersecurity-initiative**.

Contents

CYBERSECURITY AND THE INTERNET OF THINGS

About 540 million years ago, our planet saw a sudden and major diversification of organisms, with a vast number of species suddenly appearing in the fossil record. Paleontologists call this event the "Cambrian explosion." The computing world is currently experiencing its own version of the Cambrian explosion. Two decades ago, computers were primarily large beige boxes that came with a monitor, keyboard, and mouse. Today, computers come as smartphones, tablets, glasses, cars, watches, clothes, fitness trackers, health monitoring devices, parking meters, electronic locks, smart mirrors, drones, and more.

This Internet of Things (IoT) represents the third wave of computing. The first wave focused on computation, making the basics of computing work. The second wave centered on networking, connecting all of these computers together in a global network. The third wave, of which we are in the early stages, looks at making computers part of the physical world in which we live. Computation and communication are being embedded into everyday objects. These computers can also use different kinds of sensors— such as accelerometers, cameras, microphones, GPS, heart rate sensors, and more— to perceive the physical world. In some cases, they can even interact with the physical world, by automatically changing the heating and lighting in an office building to balance comfort and energy usage, adjusting orders based on real-time inventory to keep supply chains smooth, or modifying the shape of smart hospital beds to apply proper support to patients who may be resting or trying to get up.

Gartner estimates that there will be over 20 billion connected IoT devices by 2020.[1] Cisco predicts the global Internet of Things market will be $14.4 trillion by 2022.[2] The vision of IoT is rapidly becoming a reality due to advances in processors, sensing, displays, storage, wireless networking, and battery life. IoT also offers tremendous opportunities for education, energy, healthcare, transportation, and more.

However, these same technologies pose many new and daunting challenges for cybersecurity. What happens if an attacker compromises a self-driving car? How can we prevent people from snooping on implanted medical devices? We can barely manage the security of the laptops, corporate networks, and cloud infrastructure we have today. How can we protect the billions of smart toys, smart appliances, and smart buildings of tomorrow?

THE HIERARCHY OF IoT DEVICES

While IoT is often talked about as a single monolithic concept, it is more useful to think of it as a three-tier pyramid. Each tier represents a different class of device, based on the computational power of the device, as well as the amount of interaction and attention a person needs to devote to each device. Each tier also poses different kinds of security challenges due to the nature of the devices in that tier. See **Figure 1** for an overview.

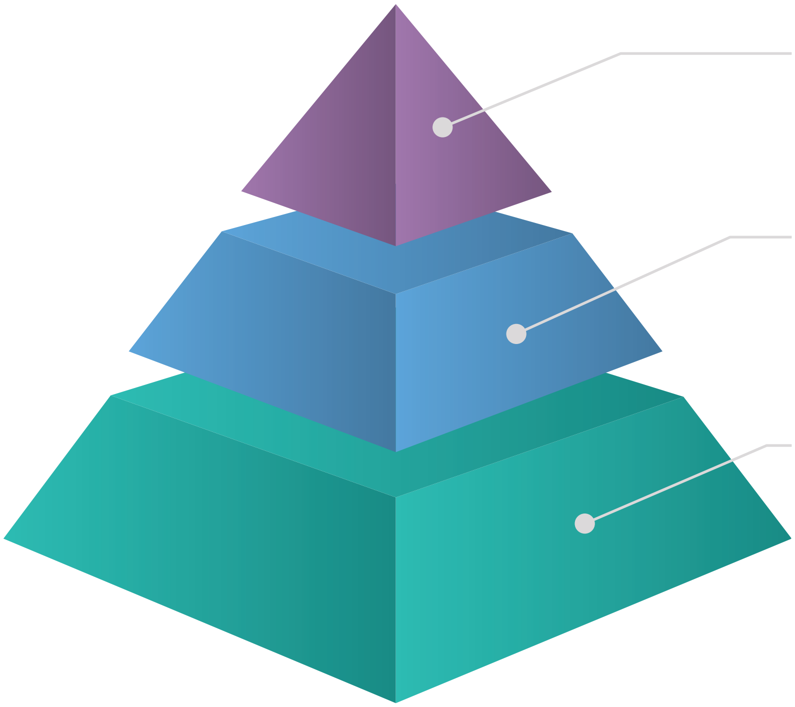
At the top of the pyramid, each person will have a few devices that have a great deal of computational heft and require the majority of one's attention. These include laptops, smart glasses, tablets, smartphones, gaming consoles, and other kinds of highly interactive devices. Most of these devices will have common operating systems, and will be manufactured by large corporations that can devote a lot of effort towards building in and supporting reasonable levels of safety and security.

In the middle are dozens of devices that a person will only use a few times a day, each of which will only require a little bit of our attention to use. Examples include TVs, smart watches, self-driving cars, refrigerators, thermostats, electronic whiteboards, cable boxes, and interactive toys. While a few of these devices will have advanced computing capabilities and security built-in, most will be fairly basic and be spotty in terms of security protections.

At the bottom of the pyramid are hundreds of devices that lie far in the background of our attention. These might include RFID-enabled ID cards and badges, clothes, HVAC, digital light bulbs, smart toilets, smart meters, security systems, implanted medical devices, digital picture frames, cheap environmental sensors, electronic locks, and more. Devices in this tier will have very little computational resources, might have few (if any) software updates, and use a wide range of software and operating systems. Cybersecurity will be especially weak here, in part due to cost, but also because of lack of software development experience by hardware manufacturers.

Figure 1 | Tiers of the Internet of Things

The Internet of Things can be organized into different tiers, based on the amount of computational power of devices, as well as the amount of interaction and attention a person needs to devote to each device.



Tier 1:

- Tablets
- Glasses
- Laptops
- Smartphones

Tier 2:

- TVs
- Refrigerators
- Thermostats
- Smart watches
- Smart toys

Tier 3:

- HVAC
- RFIDs
- Implanted medical devices
- Digital picture frames
- Smart toilets

Characteristics of Each Tier

Tier 1	Tier 2	Tier 3
• Few devices per person • Requires high user attention • High computational power	• Tens of devices per person • Requires sporadic user attention • Moderate computational power	• Hundres of devices per person • Little explicit interaction • Requires little user attention • Low computational power

Cybersecurity Issues

Tier 1	Tier 2	Tier 3
• Cybersecurity efforts good today • Lots of effort today to protect • Can run endpoint protection software • Large corporations supporting these	• Cybersecurity efforts weak today • Weak effort today to protect • Basic capabilities for protection • Spotty security protection	• Cybersecurity efforts weak today • Little effort today to protect • Few capabilities for protection • Developers with low security experience

WHAT MAKES SECURITY FOR IoT DIFFERENT?

Cybersecurity for IoT has much in common with the challenges that we are already facing with desktop computers, cloud computing, and enterprise systems. These same problems will still exist for IoT. The same kinds of attackers will also be present. These include script kiddies with low levels of skill; skilled individuals looking to exploit vulnerabilities for personal gain; criminal gangs looking to make money by targeting corporations or everyday consumers; and nation-states and non-state actors seeking state secrets or intellectual property, or potential new ways of disrupting an adversary. However, IoT also poses some unique differences that require new kinds of tools and new kinds of thinking to address.

Cybersecurity will need to expand to protect people's physical safety and physical security.

Most cybersecurity today focuses on protecting the digital world. However, given that IoT devices are embedded in the physical world, physical security and physical safety have become paramount. For example, an attacker that has breached a device can easily use its sensors to continuously monitor people. Some sensors pose obvious risks, such as GPS, cameras, and microphones, but even seemingly innocuous sensors can be used to make sophisticated inferences about people's behaviors. Past research has shown how disruptions in airflow can be used to estimate motion in a house,[3] or how water pressure sensors can be used to detect people's activities at home.[4] Inferences like these can also be used over time to build an aggregate and surprisingly detailed picture of a person or an organization's behaviors.

Similarly, it does not take much to imagine new kinds of attacks with IoT. An obvious one is deliberate attacks using IoT devices, such as crashing drones or autonomous vehicles into buildings. However, outside of non-state actors, these cases are likely to be isolated in the near future, as they would bring the full force of law enforcement on perpetrators. While some hacker groups are interested in mayhem (e.g. Anonymous and LulzSec), many others are professional criminals looking for repeatable (albeit illicit) ways to make money. As such, the kinds of attacks on IoT will likely be new versions of old attacks. Familiar forms of spam, denial of service, and botnets will be updated as entrepreneurial hackers develop new kinds of business models for a connected world.

In particular, it is likely that ransomware will become the dominant class of cybersecurity problems for IoT. We have already seen ransomware attacks on hospital IT systems,[5] during which attackers encrypted hospital data and would only decrypt the data if they were paid. A future attack might involve an attacker locking you out of your smart house or threatening to make public an embarrassing video recorded by your own webcams, unless you send some Bitcoins their way. IoT also allows for new kinds of subtle attacks that would be infuriatingly hard to pinpoint, such as repeatedly tripping the circuit breakers in a business by turning on multiple devices at once, or remotely adjusting a person's thermostat to make it hard to get a good night's sleep.

Billions of connected devices will need to be secured.

There will be orders of magnitude more IoT devices per person than the traditional computing devices we have now, and all of them will need to be secured. Today, a person interacts with perhaps a dozen computers every day, most of which are hidden in everyday objects and few of which are connected to the network. Tomorrow, there will be hundreds of networked devices per person. These will include not only the smartphones and laptops we typically think of as computers, but also everyday objects in the middle and bottom tiers of the IoT hierarchy. The sheer number of these devices will make what would ordinarily be trivial tasks into significant challenges. For example, configuring a security policy for a single device is tractable. Configuring a security policy for hundreds of devices, each of which has a different user interface, is not. Similarly, it is easy to have unique passwords for a few devices, but less so for a house or building full of devices, many of which do not even have keyboard input or displays. It is also easy to physically lock down a few computers to prevent them from being stolen, but it is very difficult to do the same for large numbers of IoT devices. Even worse, many of these IoT devices can be easily lost or stolen due to their small size, or even tampered with to send back fake data.

It is also important to emphasize that the sheer number of connected IoT devices makes new kinds of large-scale attacks possible. A good example is spying on strangers on the Internet by making use of well-known default passwords. For example, Shodan.io claims to be the first search engine for the Internet of Things and allows people to search for unsecured webcams all over the world.[6] It's not hard to imagine similar kinds of attacks taking place on popular Internet-enabled toys or on smart TV sets. However, while sensing this data may be intrusive, the real danger here is in gaining control over devices that can interact with the physical world. A nightmare scenario would be an enemy nation-state or non-state actor finding a security vulnerability in a common implanted medical device and using that to hold thousands of people hostage virtually.

The diversity of devices and protocols will make it hard for security solutions to gain traction.

The diversity of these devices will make it hard for any single cybersecurity approach to dominate. First, the vast majority of IoT devices will be those at the bottom of the pyramid, having very little CPU processing power and limited battery life. Devices like digital light bulbs will not be able to run conventional encryption algorithms or security software. Second, there will be hundreds of IoT manufacturers all using different kinds of operating systems, different kinds of wireless networking (Zigbee, Z-Wave, Bluetooth, Wi-Fi), different kinds of configuration software, and different kinds of formats for access logs.

The upshot is that compatibility and interoperability will be extremely difficult in the near future. There are several competing standards for different parts of the IoT ecosystem, each with different tech companies backing them. For example, the Open Interconnect Consortium includes Intel, Samsung, GE, Dell, and others. The AllSeen Alliance is led by Qualcomm and includes Microsoft, Cisco, Sony, LG, and Philips. Google and Apple are working on their own IoT standards, and Amazon has its own cloud services for IoT devices. Numerous other standards-setting bodies exist, though no one has emerged as dominant In some cases, incompatibility will be deliberate as IoT manufacturers try to get people to buy into their ecosystem exclusively. As such, the IoT ecosystem will be chaotic until open or de facto standards start to win out.

One result of this fragmentation is a difficult market for cybersecurity companies. Vendors of software and hardware solutions want a certain kind of predictability, compatibility, and potential market size before committing a great deal of resources to developing products. However, uncertainty over which platforms will become dominant will slow down development and deployment of these solutions, leading to weaker cybersecurity in the foreseeable future.

Manufacturers' lack of cybersecurity experience will lead to serious vulnerabilities.

Most manufacturers have little experience with cybersecurity. Traditional software companies that are also looking to develop IoT hardware already understand the need for good security practices. However, many hardware manufacturers—which include makers of automobiles, household appliances, toys, lighting, medical equipment, and more—often do not yet realize that they also need to be software companies. This means having people who understand good software engineering processes, using tools for developing and testing secure software, knowing how to create and distribute software patches, and having experience in best practices and in avoiding common mistakes.

As a simple example, past research has demonstrated serious security vulnerabilities in several of today's medical devices[7] and automobiles.[8] From a computer science perspective, these vulnerabilities were due to what are known as "buffer overflow" attacks, which have been fairly common and well-studied since the Morris Internet worm in 1988. However, despite the fact that we know how to structure software to avoid them, and despite the number of tools for detecting these vulnerabilities, they still plague a lot of software. It is also important to emphasize that buffer overflows are just one of many common pitfalls in developing secure software, and these kinds of errors will be exacerbated as more and more companies with little experience deploy IoT systems.

> **Many hardware manufacturers often do not yet realize that they also need to be software companies.**

A related issue is that some manufacturers might not be able or willing to devote resources to support their products. For example, if you look at KickStarter campaigns, there are currently 77 items if you search for "iot," 281 for "sensor," and 517 for "wireless." Small-scale manufacturers are focused primarily on core product functionality and often have little time to consider cybersecurity. At the other end of the spectrum, even large companies have product lifecycles and may end product support at some point—or worse, discontinue the product or even go bankrupt. In all cases, the problem is that these IoT devices will still exist for a long time and may become an entry point for cybersecurity attacks.

Emergent behaviors between IoT devices will make it difficult to protect entire systems.

A major challenge for IoT is that devices will interact with each other in unexpected and unintended ways, and these emergent behaviors will make it extremely difficult to reason about and manage the security of the entire systems. As a trivial example, a friend told me that a person once annoyed a bunch of people wearing Google Glass by shouting out "Ok Glass, take a picture," causing everyone's wearable to take a picture. As a more serious example, let's say that an attacker has found a software vulnerability in a smart toaster and causes it to burn some toast and start a small fire. The networked smoke detector sets off an alert and automatically opens up the window, allowing a thief to easily enter. While this is a contrived scenario, it demonstrates the challenges of understanding the overall safety and security properties of a system when it is comprised of parts that were not explicitly designed to work with one another.

A PATH FORWARD TO A SECURE INTERNET OF THINGS

Given this landscape for the Internet of Things, what can we as a community do to move forward? It is important to keep in mind that the IoT landscape is still very chaotic and will continue to be so for the foreseeable future. There will be a lot of battles between major corporations as they compete to become the dominant platform for certain tiers of the IoT pyramid. However, even in this context, there is still much that researchers and policymakers can do.

Push more strongly for requiring cybersecurity education in computer science curricula.

Today, it is possible for an undergraduate to get a degree in computer science without having taken any courses in cybersecurity. Many groups have pointed out this same issue and have offered recommendations for ameliorating the situation. For example, in the 2012 *National Initiative for Cybersecurity Education Strategic Plan*,[9] the authors advocate for increasing the number and diversity of cybersecurity classes, and offering cybersecurity competitions to increase student participation and for use as a recruiting event for companies. A 2013 Association for Computing Machinery report on cybersecurity curricula[10] has a similar position, arguing that students should be required to take at least one class in a security-related area, and that institutions should offer credentials or certificates to help with employers. However, these recommendations are just that, and they currently have little weight or resources behind them. Even President Obama's recently announced $4 billion initiative, Computer Science for All, does not seem to have a specific push on cybersecurity.

As such, our recommendation here is for industry and the federal government to help operationalize the findings from the above reports by funding the creation of sample curricula, teaching materials, and teaching guides, making it much easier for instructors to adopt parts of or the entire set for their own classes. For example, in past work, I helped create a teaching guide for usable privacy and security,[11] which has been used by several other faculties around the United States.

Furthermore, while teaching materials for many courses can and should be developed, most students will only take one course on cybersecurity. Thus, there should be a core set that offers a balance of pragmatic issues of software engineering—such as secure programming practices, basics of human factors, authentication, and avoiding common pitfalls—as well as theoretical ones, such as encryption and anonymity.

Another recommendation here is to expand the scope of cybersecurity education for people outside of computer science, going beyond just awareness and looking at issues that affect product design. Offering cybersecurity education just to computer science majors would be too narrow and overlooks the intense effort required to design IoT products and bring them to market. Individual parts of the teaching materials and teaching guides could be used and tied to a wide range of courses. For example, students in psychology could learn about behavior change in the context of cybersecurity, looking at topics of social proof or motivation. Students in industrial or graphic design could learn about the design of visual warnings and underlying cognitive models. The key here is not to be bound by existing academic departments, as the world is very complicated and rarely fits cleanly into the silos of academia.

Establish virtual centers of excellence for creating and disseminating best practices in developing and deploying IoT systems.

As noted earlier, it is very easy to make software development and operational mistakes with respect to cybersecurity. For example, the 2009 RockYou data breach, the 2011 Sony data breach, and the 2012 Yahoo Voice data breach were all made worse because the passwords were stored in what is known as plaintext instead of being hashed, which made it trivial for anyone who has access to the password file to break into all of the accounts. These kinds of errors are well-known and easily avoidable.

One reason these kinds of mistakes continue to occur is the widespread lack of experience with cybersecurity best practices. Our recommendation is to have industry and the federal government fund the establishment of virtual centers of excellence that can gather, analyze, publish, and disseminate best practices. These virtual centers could be hosted through industry consortia or at universities, and they could host a website of best practices, as well as periodically hold workshops to help elicit new knowledge and disseminate findings. One other option could be to build on existing centers of excellence, like NIST's National Cybersecurity Center of Excellence.

One format for these best practices might be a checklist of items that developers should verify before deploying their IoT systems. Example items might include checking for buffer overflows, not having a common and well-known default password for all devices, only storing hashed passwords rather than plaintext, avoiding accounts without passwords, having access logs where possible, having secure mechanisms for patch updates, and so on.

Another format might be a collection of design patterns focusing on IoT cybersecurity. Design patterns describe well-accepted solutions to common problems, presenting several exemplars and linking individual patterns together to form a pattern language. Design patterns have been very successful for software engineering [12] and user interface design,[13] but aside from a few reports,[14,15] there has been little work in this context for cybersecurity. These patterns should also focus on the whole range of activities involved with cybersecurity, including system architectures, design, implementation, user interfaces, testing, maintenance, and management of multiple devices.

A third format would be code samples that developers can directly use by copying-and-pasting into their software. Past work has found that developers rarely start from scratch, but rather search for examples of code and adapt them to their needs.[16] However, many examples online have bugs in them, which can inadvertently propagate security errors. Having a canonical source of good and vetted examples could help mitigate this problem.

Holding workshops on best practices could also be used as a way to foster coordination between manufacturers of IoT systems. Participants could agree on standards for logging to facilitate anomaly detection, or on how to authenticate IoT devices in the lowest tier of the pyramid.

Push for more data sharing about failures in IoT safety and security.

In the past few years, we have seen multiple spectacular data breaches on major companies and governments, including Sony, RSA, Yahoo, LinkedIn, Target, the U.S. Office of Personnel Management, and more. A major problem, however, is that there has been little published information about how those breaches happened, making it hard for the community as a whole to understand what failed, why, and how to mitigate these kinds of risks in the future.

These failures are the cybersecurity equivalent of the Tacoma Narrows bridge collapse. Interestingly, after that bridge failure, a federal commission was set up to investigate the root causes. It also led to a great deal of fundamental research into aerodynamics and resonance. Perhaps most importantly, the collapse has been seared into the minds of every engineering student as an example of a massive failure, and also as an example of their responsibility to society to make sure they get things right.

In contrast, the software developer community's response to these massive data breaches has been rather anemic, and we do not seem to be learning many lessons from these repeated catastrophic failures. The same will likely be the case for IoT, unless a concerted effort is made to document these failures and understand how to avoid them in the future. The recently passed Cyber Intelligence Sharing and Protection Act offers some hope of better data sharing of cybersecurity breaches in general, but it does not do much in terms of disseminating knowledge. What is needed in the long-term is the cybersecurity equivalent of the U.S. National Transportation Safety Board, [17] which investigates major accidents with our railroads, highways, and aviation systems (see past reports at **https://www.ntsb.gov/investigations/reports.html**). The goal would not be to assign blame, but rather to determine probable causes for a failure, evaluate the effectiveness of procedures and cybersecurity systems, and offer actionable recommendations. These reports should also be part of the virtual centers of excellence as described above, and should be distilled into simple formats that developers can immediately implement and instructors can use in their classes.

Push for more research to help generate a greater understanding of cyber-risk.

Cybersecurity insurance for IoT devices could hold promise as an incentive for stronger cybersecurity. However, the cybersecurity insurance market remains relatively immature. One of the major impediments preventing the cybersecurity market from expanding is uncertainty on the part of actuarials and insurers as to how to price cyber-bourn risk. More research and critical thinking is needed in academic and public policy circles to generate a greater understanding of cyber-risk.

Manufacturers respond to incentives, but there are currently few forces pushing them for stronger cybersecurity. Legislation is a blunt instrument that would be hard to apply to get IoT manufacturers to improve. One intriguing alternative that offers more flexibility is to push for more cybersecurity insurance. The Department of Homeland Security notes that typical commercial insurance policies cover general liability and property, but often exclude cybersecurity issues, treating it as a separate kind of coverage.[18] Having cybersecurity insurance would offer market-based approaches for compensating people who experience data breaches or material loss due to IoT system failures, and would also improve software engineering, as insurers would likely set premiums based on level of experience and adoption of best practices. Insurance companies could thus be used as a way to help gather and disseminate better approaches to cybersecurity.

Offer better and clearer legal protections for researchers for analyzing the security of IoT systems.

Previously, security researchers who probed computer systems with the goal of advancing science or helping society had little protection under the anti-circumvention provisions in the Digital Millennium Copyright Act. In its 2015 triennial review, the U.S. Library of Congress recently provided some exemptions for independent verification of security for consumer devices, motorized land vehicles, and medical devices, making it so that researchers who do their work in good faith no longer have to get permissions from rights holders before investigating a system or publishing results.

While this is clear progress, there are still some improvements that are needed. Our recommendation is for policymakers to set broader and longer-lasting legal protections for researchers who are analyzing the security of IoT systems. More specifically, the exemption for security research is fairly narrow and needs to be expanded beyond consumer devices, automobiles, and medical devices, as there will be a great number of IoT devices that will not fit in these categories. The exemption also needs to be made longer or permanent. Exemptions are currently up for review every three years, and there is a heavy burden on advocates in requesting changes. Furthermore, many of the cybersecurity issues being examined are outside of the areas of expertise of the Library of Congress.

Fund large research centers on IoT safety and security.

From a science and engineering perspective, there are still a great number of fundamental research challenges that need to be addressed before IoT systems can be successfully deployed at scale. For example, how can we specify, check, and enforce system-wide properties for physical safety and security when systems are comprised of hundreds or thousands of devices? How can we help developers improve the safety and security of their software, especially when developers have little experience? How can we help users of IoT systems easily configure and manage hundreds or thousands of devices? What kinds of protections can we put into the network itself to help protect low-end devices, or devices that are no longer supported? Are there new kinds of programming models and interaction models that can greatly improve cybersecurity for IoT?

The challenge here is that the funding climate for academic research is quite difficult. Federal spending on research has been fairly flat for the past few years, as has industry support. Furthermore, much of the funding is diffuse, as agencies tend to spread money around to multiple institutions. However, this approach also leads to smaller ideas with shorter time horizons, making it hard to reach critical mass and achieve major breakthroughs.

Our recommendation here is to have the federal government fund several large research centers focusing on IoT reliability, safety, and security. These research centers should have a strong focus on long-term research, pushing scientists to bridge the gaps between hardware, networking, theory, operating systems, programming languages, machine learning, user interfaces, and behavioral sciences. These centers should also emphasize the importance of having researchers use and live with their IoT systems, so as to better understand the issues at hand, and of disseminating results to industry, so that the research has a better chance of being adopted in practice.

CONCLUSION

We are currently at a crossroads—not just in computing, but in human history. There is only one point in time when a global computing network will be created, and that time is now. There is only one point in time when the foundation is laid for how computation, communication, and sensing will be woven into our physical world, and that time is now. The Internet of Things offers tremendous potential in terms of improving healthcare, safety, sustainability, education, transportation, and more. But this vision is possible only if we can find new ways of making billions of these devices and systems understandable, reliable, and secure.

In this white paper, I have sketched out some of the major challenges to a secure Internet of Things, as well as several recommendations for a better tomorrow. These recommendations look at the entire ecosystem, and include:

1. improving computer science education with respect to cybersecurity,
2. better sharing of best practices,
3. more data sharing of IoT data breaches and security failures,
4. cybersecurity insurance as a way of nudging IoT manufacturers to do better,
5. better and clearer protections for security researchers, and
6. funding the creation of large research centers for IoT reliability, safety, and security.

It is not an understatement to say that modern society depends on our information and communication technologies being safe, understandable, and dependable. So let's make sure we create a connected world in which we would all want to live.

Notes

[1] Gartner. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. November 10, 2015. http://www.gartner.com/newsroom/id/3165317.

[2] Bradley, J., J. Barbier, and D. Handler. Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion. 2013. https://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf.

[3] Patel, S.N., MS Reynolds, GD Abowd. Detecting human movement by differential air pressure sensing in HVAC system ductwork: An exploration in infrastructure mediated sensing. Pervasive Computing. 2008.

[4] Froehlich, J.E., E. Larson, T. Campbell, C. Haggerty, J. Fogarty, S.N. Patel. HydroSense: infrastructure-mediated single-point sensing of whole-home water activity. Proceedings of the 11th International Conference on Ubiquitous Computing. 2009.

[5] BBC News. Three US hospitals hit by ransomware. March 23, 2016. http://www.bbc.com/news/technology-35880610.

[6] Brown, J. and A. Cohen. Terrifying IoT Search Engine Lets You Spy On Strangers' Webcams. Vocativ. January 25, 2016. http://www.vocativ.com/news/275331/the-search-engine-for-webcams/.

[7] Halperin, D., T. Kohno, T.S. Heydt-Benjamin, K. Fu, W.H. Maisel. Security and privacy for implantable medical devices. IEEE Pervasive Computing. 2008.

[8] Koscher, K., et al. Experimental security analysis of a modern automobile. IEEE Symposium on Security and Privacy. 2010.

[9] National Initiative for Cybersecurity Education. Strategic Plan. 2012. http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf.

[10] McGettrick, A. Toward Curricular Guidelines for Cybersecurity: Report of a Workshop on Cybersecurity Education and Training. 2013. https://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf.

[11] Cranor, L., J.I. Hong, M. Reiter. Teaching Usable Privacy and Security: A guide for instructors http://cups.cs.cmu.edu/course-guide/.

[12] Gamma, E., R. Helm, R. Johnson, J.M. Vlissides. Design Patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley, 1995.

[13] van Duyne, D., J.A. Landay, J.I. Hong. The Design of Sites: Patterns for Creating Winning Web Sites (2nd Edition). Prentice Hall. 2006.

[14] Yoder, J. , and J. Barcalow. Architectural Patterns for Enabling Application Security. Proceedings of the 4th Pattern Languages of Programming Conference, 1997. http://hillside.net/plop/plop97/Workshops.html.

[15] Dougherty, C., K. Sayre, R.C. Seacord, D. Svoboda, K. Togashi. Secure Design Patterns. CMU/SEI-2009-TR-010. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9115.

[16] Brandt, J., M. Dontcheva, M. Weskamp, M., and S.R. Klemmer. Example-centric programming: integrating web search into the development environment. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2010.

[17] Others have previously floated the idea of an NTSB for cybersecurity; it is time to give this idea serious consideration. To New America's knowledge, the first appearance of the proposal came from Richard Bejtlich in 2006 (http://taosecurity.blogspot.com/2006/08/national-digital-security-board.html) and was expanded upon in a 2012 RAND study (http://www.rand.org/blog/2012/06/the-case-for-a-cyber-security-safety-board-a-global.html).

[18] Department of Homeland Security. Cybersecurity Insurance. http://www.dhs.gov/cybersecurity-insurance.

All photos in this report are supplied by, and licensed to, **shutterstock.com** unless otherwise stated. Photos from federal government sources are used under section 105 of the Copyright Act.