RAPID7

Comments to "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things"

Docket No. 160331306–6306–01

June 1, 2016

Rapid7 submits these comments in response to the National Telecommunications and Information Administration's (NTIA) request for public comment on "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things."[1]

Rapid7 is a cybersecurity analytics software and services company that helps organizations reduce the risk of a security breach, detect and investigate attacks, and build effective IT security programs. Identifying and addressing the vulnerabilities inherent in technical systems is a critical measure in mitigating cyber threats, reducing opportunities for attackers, and diminishing risks of harm to the victims of a security breach. Rapid7 conducts extensive research into the security of IoT devices.[2] We also offer security assessment and consultancy services for manufacturers and operators of IoT technologies.

I. Defining the Internet of Things[3]

IoT devices generally refer to computers that generate and communicate data about the characteristics or status of physical objects, often embedded in or otherwise attached to the physical object. We can think of a “Thing” with “Internet” as simply a physical device (regardless of size, use, or form factor) that contains a CPU and memory, runs software, communicates with other devices over a network, and typically uses sensors to collect and communicate data about its status or environment. The concept encompasses large and expensive objects such as vehicles, as well as small and inexpensive objects such as light bulbs.

These Things tend not to resemble traditional computers – they lack a typical keyboard and mouse interface, and they often have a user interface not centered around a monitor or other text-filled screen. Importantly, because IoT devices do not normally look or behave like traditional computers,

---

[1] National Telecommunications and Information Administration, Notice, Request for public comments, *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things*, 81 FR 19956, Apr. 6, 2016, https://www.ntia.doc.gov/files/ntia/publications/fr_rfc_iot_04062016.pdf.

[2] For a sample, please see Rapid7 Community, Information Security, Internet of Things, https://community.rapid7.com/community/infosec/content?filterID=contentstatus%5Bpublished%5D~category%5Binternet-of-things-iot%5D (accessed Jun. 1, 2016).

[3] In response to question 2.

they are often marketed and treated as if they are single purpose devices, rather than the general purpose computers they actually are. As a result, basic precautions to thwart even casual attackers, which manufacturers might take with traditional computers, can fail to make it into production of IoT devices.

As a broad term encompassing many product categories, the "Internet of Things" is more of a collection of markets, rather than a single market. For the purpose of advancing policy discussion, it may be most practical to classify IoT in terms of existing legal authorities – such as the regulatory systems for medical devices, connected vehicles, or critical infrastructure – though these regulations should be harmonized where feasible. From a cybersecurity perspective, we believe an essential classification of IoT devices should be based on a spectrum of risks related to safety, damage, and other harm – such as IoT devices that, if compromised, could result in mass injury or loss of life, individual injury or loss of life, damage to critical infrastructure, damage to property, or breach of sensitive information.[4] Many IoT devices will not present a high risk in these areas, but others will – and it should not be overlooked that a cybersecurity flaw in a low-risk connected device can be part of an attack vector that ultimately compromises another system which poses a more serious safety risk.

II. Technical Challenges[5]

IoT devices are actually general purpose, networked computers running relatively complex network-capable software. It is widely accepted that such software ships with exploitable bugs and implementation-based exposures. Add in external components and dependencies, such as cloud-based controllers and programming interfaces, the surrounding network, and other externalities, and vulnerabilities and exposures are all but guaranteed. IoT is typically composed of multiple interactive components hardware, software, firmware and cloud technologies, requiring consideration of how the security of each individual component can affect the security of the other components. Since IoT devices are highly diversified and include very inexpensive items manufactured by companies with limited security experience, the result can be a considerably more exploitable environment than the status quo.[6] Because IoT devices tend to interact directly with physical objects and infrastructure, the risks of physical danger posed by cybersecurity flaws in some devices can be greater than that for purely digital applications.

These challenges can be mitigated in time, as IoT evolves and technology advances. However, sustained effort and coordination among IoT stakeholders to strengthen cybersecurity will be needed.

A. Insufficient update practices

[4] In response to question 4.
[5] In response to questions 1.a, 6,
[6] Ashkan Soltani, *What's the security shelf-life of IoT?*, Federal Trade Commission, Feb. 10, 2015, https://www.ftc.gov/news-events/blogs/techftc/2015/02/whats-security-shelf-life-iot?utm_source=govdelivery.

Today, a commonly accepted way to effect a rapid rollout of patches for IoT devices simply does not exist. IoT devices, unlike traditional computers, often lack an effective update and upgrade path once the devices leave the manufacturer's warehouse. Without a patching capability, it is difficult to correct devices' known security flaws at a large scale. As a result of the growth of IoT, unpatchable IoT devices are coming online at an unprecedented rate,[7] creating a wave of unsecurable-after-the-fact devices. Although we are optimistic that patchable IoT devices will become more common, unpatchable legacy devices will likely linger on the market for some time.

One factor that should be considered is that many manufacturers entering the IoT space traditionally work with development processes and timeframes that are vastly different to those typically associated with software or cloud services development cycles. For example, many cloud services work in essentially continuous develop-and-deploy cycles that see updates made to the service on a weekly, or even daily, basis. In comparison, manufacturing new versions of cars or medical devices may take years. It is challenging for drawn out processes to incorporate quick response practices for vulnerability handling and patching, yet doing so critical given the potential risks of inaction.

Rapid7 encourages the Dept. of Commerce to encourage industry to implement and adopt an update management program for IoT. Rapid7 generally views security update and advisory mechanisms as a mandatory component of device or software cybersecurity plans. We also do not believe the technical challenges to updating IoT devices are insurmountable at present. Effective patching is challenging even for mature market sectors such as smartphones and routers, but those sectors nonetheless have update mechanisms.[8] Because connectivity may be new to many product categories (e.g., a toaster versus a connected toaster), many IoT companies may be relatively unfamiliar with the complex mechanics of update management, but we believe it is essential that updating becomes a more regularized and extensive practice for IoT.

B. Supply chain

Many IoT devices incorporate an element of a cloud service or mobile application, and many offer integrations or connectivity with third party systems to enhance functionality and convenience. In some cases, devices/services leverage third party services to provide login or social sharing functions. This level of interconnectivity and interdependence of systems, applications, and services makes managing the supply chain for IoT even more complex, and adds to the confusion around responsibilities and practices for security.

This complexity and confusion over ownership is increased by the use of commodity, third party hardware, software, and cloud-based resources, which is prevalent in the IoT industry. Manufacturers of IoT devices often implement much of the technology used by their products as embedded systems subcomponents, sourced from third party suppliers. While reusing off-the-shelf technologies helps to

[7] Gartner estimates at least 20 billion connected devices in 2020. *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent from 2015*, Gartner, Nov. 10, 2015, http://www.gartner.com/newsroom/id/3165317.
[8] Liam Tung, *Google: Android Marshmallow on steady rise, unpatchable phones falling*, ZDNet, May 4, 2016, http://www.zdnet.com/article/google-android-marshmallow-on-steady-rise-unpatchable-phones-falling.

keep costs of production low, it introduces an ambiguity of ownership for developing and deploying patches and other upgrades. This patchwork of common components can lead to confusing interdependencies, and can leave end-users exposed while the details of remediating vulnerabilities are worked out between vendors.

The upstream vendors of IoT subcomponents tend to run very large operations, producing millions of units in a given year, and any change in this supply chain can be both time consuming and expensive. Due to the nature of this time-lagged supply chain, individual software components may be months to years old before being assembled into the final product, bringing old and commonly known software vulnerabilities along with them. The widespread use of common components also means that a vulnerability in one subcomponent can be present in many disparate devices.

C. Infrastructure and workforce[9]

The presence of devices that are non-secure by default, difficult to patch, and impossible to directly monitor by today's standard corporate IT security practices constitutes not only a threat to the IoT device and its data, but also to the networks to which it's connected. These risks to infrastructure, companies, and network owners are exacerbated by the fact that IoT brings connectivity to more business sectors that previously did not provide networked products – and which may be relatively unprepared to deal effectively with cybersecurity threats.

As with other general purpose computers, attackers may be able to leverage an exposure or vulnerability to gain and maintain persistent access to an IoT device. A compromised device can be used to pivot to other computers or networks by taking advantage of the unsegmented, fully trusted nature of some networks. This can put multiple networks to which the device connects, and the resources provided through those networks, at risk.

For example, office environments and home environments are, increasingly, literally the same environment. The percentage of employees and contractors who are working from home on at least a part time basis continues to rise across every modern economy.[10] These employees are connecting to their workplace virtually, either through VPN connections or through the use of cloud services shared by colleagues. Today, however, employees' home networks are rarely, if ever, "in scope" for organizational penetration testing exercises, nor are they subject to centralized vulnerability scanners. Given the current lack of monitoring of these and other networks, such as café Wi-Fi, remediating attacks may prove quite difficult once underway. Even within the corporate office environment, personal IoT devices – such as smart watches – can raise new risks that existing security policies may not cover.

[9] In response to questions 8-10, 14.
[10] Alina Tugend, *It's Unclearly Defined, but Telecommuting Is Fast on the Rise*, New York Times, Mar. 7, 2014, http://www.nytimes.com/2014/03/08/your-money/when-working-in-your-pajamas-is-more-productive.html?_r=0.

D. Specific cybersecurity issues[11]

The items below describe some common vulnerabilities and exposures for IoT devices. Not all IoT devices suffer from all of these software, firmware, and hardware issues, but, in our experience, it is rare to find an IoT device that doesn't exhibit at least one serious failing.

1. Lack of transport security: Many passive and active network attacks can be defeated simply by using encrypted protocols, such as HTTPS and SSH. However, IoT devices often fail to use modern cryptographic standards, risking exposure of user data in transport over both the public internet and local area networks. The problem is exacerbated by devices built with commodity components and software, which often fail to use modern cryptographic standards.

2. Unencrypted storage: IoT devices and related services should store data in industry standard, encrypted formats – both if data is captured on the device or held in the cloud. However, services connected with IoT devices often fail to adhere to this increasingly common standard.

3. Remote shell access: IoT devices often ship with default or otherwise unconfigured portable operating systems, and are often host to a Linux or other POSIX kernel with a set of stock utilities. While these are useful for developing hardware, they should not be made available on production systems where shell access is never desired or required.

4. Backdoor accounts: As IoT devices are developed, manufacturers occasionally include either default accounts or service accounts, which are either difficult or impossible to disable under normal usage. Furthermore, these accounts often use default or easily guessable passwords, and tend to share the same unchangeable password, SSH key, or other secret-but-universally-shared token. Finally, these accounts may be protected by a password unique to the device, but the password generating algorithm is easily deduced and the passwords for all devices can be guessed with low attacker effort.

5. UART access: Universal Asynchronous Receiver/Transmitter (UART) interfaces often enable a physically close attacker to access and alter IoT devices in ways that bypass the normal authentication mechanisms via a serial cable connection. In addition, UART interfaces tend to grant root access, far exceeding the permissions of regular users. UART access is both a useful diagnostic tool and a means of "jailbreaking" consumer devices. However, such activities can also enable persistent attacks on devices. If an IoT device must offer UART access, the device should ideally be tamper-evident, providing the owner or investigator with some obvious indication that it has been altered.

6. Mobile application access: Mobile applications, which are often used to control and manage IoT technologies, are regularly granted more access rights to a device then what is needed for the application to function properly. These elevated rights can then be leveraged to exploit a

[11] In response to question 16.a.

system or compromise other applications running on the mobile devices.

7. Lack of segmentation: When different components of a device share the same memory or circuitry, a flaw in one component can lead to exploitation of another component. For example, an attack on the infotainment system of a vehicle can lead to access of the critical driving functions, such as acceleration or braking.[12] Non-critical systems should be physically and logically separated from physical systems.

Another possible concern is the raw computing power potentially available to attackers in the form of millions to billions of IoT devices. In total, the teraflops of processing power may be effectively harnessed by bad actors to launch powerful distributed denial of service (DDoS) attacks, and other kinds of malicious activity, against connected targets.[13]

III. Policy Issues[14]

A. Independent security research

Independent security researchers will be critical to match the greater need for security as IoT devices are more widely deployed. Independent security researchers access software and computers to assess and report security vulnerabilities. This may refer to users or administrators who uncover issues incidentally or accidentally, or security professionals who intentionally test systems to identify problems, and raise awareness to vendors and users so the issue is resolved. To reduce cybersecurity risk exposure, it is desirable for vulnerabilities and other security issues to be discovered and reported by security researchers. This research strengthens cybersecurity because the researchers call attention to vulnerabilities that manufacturers may have missed or ignored, which encourages manufacturers or other parties to make the appropriate fixes or mitigations to keep people safe.

The growth of IoT devices will create a much larger attack surface for malicious actors. It is increasingly crucial to foster an environment where disclosure of security issues in devices or systems is taken seriously and openly, rather than with threats or avoidance. This is particularly important in systems that have safety implications.

Several existing laws chill security research, which can hinder independent efforts to assess the security of IoT devices. The Computer Fraud and Abuse Act (CFAA), Section 1201 of the Digital Millennium Copyright Act (DMCA), and other laws contain broad prohibitions on access to computers

[12] I Am The Cavalry, Five Star Automotive Safety Program, https://www.iamthecavalry.org/domains/automotive/5star (accessed Jun. 1, 2016).
[13] Mark Stanislav and Tod Beardsley, *Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities*, Rapid7, Sep. 2015, pg. 6, https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf.
[14] In response to questions 1.b, 3.a, 3.b, 16.c, 17a,

and software without distinguishing between malicious attackers and individuals that seek to enhance cybersecurity.[15] Although we recognize the beneficial role of these laws in deterring cybercrime, balancing greater flexibility for researchers and innovators with law enforcement needs is increasingly important as IoT proliferates.

As compared to several years ago, policymakers more frequently recognize the value of independent security research. For example, in Oct. 2015, the U.S. Copyright Office approved a temporary exemption to Sec. 1201 of the DMCA for security research.[16] Another example: in April 2016, the state of Washington enacted the Washington Cybercrime Act to revise the state's computer crime laws, including helpful exceptions for white hat security researchers.[17]

However, some federal and state legislative proposals related to IoT would impose broad and redundant restrictions on access to connected devices. These proposals would hinder researchers and independent repair services that can assess and fix the devices' cybersecurity vulnerabilities. For example, in Oct. 2015, a House Energy and Commerce Subcommittee released draft legislation that would have levied heavy fines on anyone accessing a car's software without authorization for any reason – regardless of whether the accessor purchased the car, or if the car was accessed for cybersecurity research purposes.[18] Similarly, a bill restricting access to vehicle software was introduced in the Michigan Senate.[19] Proposals such as these are not just overbroad, but largely redundant of existing laws prohibiting unauthorized access and use of computers.[20] While safety is certainly an important consideration for IoT, new regulations related to IoT should not undermine cybersecurity by imposing blanket access and use restrictions that further chill independent research and repair.

B. Ownership of devices

As software is integrated with more physical objects, issues regarding ownership will become more prevalent. If purchasers of an IoT device, such as a smart vehicle, own the physical parts of the device but only license the integrated software, questions arise regarding the purchaser/licensor's legal authority to access, modify, or repair the device software. Depending on the licensing terms, the

---

[15] Deirdre Mulligan, Nick Doty, and Jim Dempsey, *Cybersecurity Research: Addressing the Legal Barriers and Disincentives*, Berkeley Center for Law and Technology, Sep. 28, 2015, http://ondoc.logand.com/d/5689/pdf.
[16] Jen Ellis, *New DMCA Exemption is a Positive Step for Security Researchers*, Rapid7, Oct. 28, 2015, https://community.rapid7.com/community/infosec/blog/2015/10/28/new-dmca-exemption-is-a-positive-step-for-security-researchers.
[17] Washington (state) legislature, H.B. 2375 - 2015-16, Sec. 3(10)-(11). Signed into law Apr. 1, 2016. Available at http://app.leg.wa.gov/billinfo/summary.aspx?year=2015&bill=2375.
[18] Discussion Draft on Vehicle and Roadway Safety, United States House of Representatives, Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade (Oct. 13, 2015), Sec. 302, http://docs.house.gov/meetings/IF/IF17/20151021/104070/BILLS-114pih-DiscussionDraftonVehicleandRoadwaySafety.pdf.
[19] Michigan (state) senate, S.B. 0927, Sec. 4(2), (Apr. 28, 2016), https://www.legislature.mi.gov/documents/2015-2016/billintroduced/Senate/pdf/2016-SIB-0927.pdf.
[20] Harley Geiger, *Draft Car Safety Bill Goes In The Wrong Direction*, Center for Democracy & Technology, Oct. 20, 2015, https://cdt.org/blog/draft-car-safety-bill-goes-in-the-wrong-direction.

authority to control who may access, modify, or repair device software may reside only with the software creator or device manufacturer.[21] In the context of cybersecurity, licensing terms may prevent the purchaser of an IoT device from independently accessing the device software to assess security vulnerabilities, modify the software to correct vulnerabilities, or authorize a third party (such as a repairman or security professional) to do so on the device purchaser's behalf. More vulnerabilities may simply go unaddressed if independent security and repair services for IoT devices are chilled due to unclear or restrictive ownership rules.

C. Privacy

Proper security of information collected and transmitted by IoT devices, including remediation and management when flaws are discovered, will be a critical privacy control to prevent breach and protect end users. A key feature of many IoT devices is the collection and transmission of data, including data about the device's environment or the individual wearing a device. Since some IoT devices – like medical devices – will compile sensitive or personally identifying data about individuals, and the combined collected data of many IoT devices can paint a detailed profile of an individual, the consequences of data breach can be severe to both individuals and businesses. Cybersecurity vulnerabilities create risks of both accidental and intentional breach of data stored in or transmitted through IoT devices. Although this is not unique to IoT, IoT can involve a large quantity of devices, wide variety of applications and environments, and a significant volume of data collection.

IV. Recommendations[22]

A. Focus on cybersecurity, but maintain flexibility[23]

The Internet of Things has great potential for technological innovation, economic growth, and enhanced quality of life. To reap these benefits while safeguarding consumers, businesses, and infrastructure, comprehensive cybersecurity protections will be needed. Many of the technical and policy issues related to IoT are not unique to this field. However, the diversity and quantity of IoT devices apply familiar issues to new business sectors at a larger scale – security vulnerabilities that once affected laptops and smart phones can now affect refrigerators, implantable medical devices, automobiles, and more. We urge both the public and private sectors to focus on strengthening the security of IoT as it grows.

The technology and marketplace for IoT are rapidly evolving, so IoT-specific regulation is likely premature at this time – and any regulation would need to be flexible enough to accommodate quickly

[21] Some vehicle manufacturers openly oppose greater access to vehicle software by independent cybersecurity researcher and repair services. See, e.g., Darin Bartholomew, *Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201*, John Deere, Mar. 27, 2015, pg. 5-6, http://copyright.gov/1201/2015/comments-032715/class%2021/John_Deere_Class21_1201_2014.pdf.
[22] In response to questions 6.b, 10, 13.c, 21, 23, 26
[23] In response to question 7.

changing security threats, tools, and standards, as well as broad enough to apply to the many segments converging under the IoT umbrella. While the Government can and should play a valuable role in driving awareness and resolution of the issues facing IoT development – particularly as pertains to cybersecurity and ownership – taking an aggressive approach to regulating this space may stifle important innovation. Rather, the Government should continue to play a role in raising awareness of these issues, urge coordination and standardization among IoT stakeholders to improve security, and recognize the growing need for decentralized security services to independently discover, assess, and correct cybersecurity vulnerabilities.

Any efforts towards regulation that are made should be focused in segments where cybersecurity challenges have safety implications, and should be undertaken by bodies that already regulate those industries and have deep knowledge of their practices. Ideally those bodies would work in a coordinated fashion to provide consistency across segments, assisted by cybersecurity experts who can help them evaluate approaches and outcomes.

B. Encourage adoption of coordinated vulnerability disclosure policies

We believe IoT device manufacturers should design products with security in mind from the start, rather than attempting to retrofit security features into products and services never designed for those features. However, since cybersecurity vulnerabilities cannot be completely eliminated from IoT devices pre-market, organizations must be prepared to discover, assess, and remediate cybersecurity flaws in their IoT devices throughout the device lifecycle. To do this effectively, it is critical for organizations to have a plan and policy in place to receive and process vulnerability information from external sources, such as independent security researchers.

Rapid7 has witnessed a wide range of responses in our experience researching cybersecurity flaws in IoT devices – some vendors were impossible to contact, others did not respond, while still others had an established process for handling incoming product vulnerabilities and worked closely both with us and upstream vendors to remediate the flaw. Unfortunately, the latter group has traditionally been by far the smallest to date, though, this is slowly starting to improve. Businesses and government agencies are increasingly implementing coordinated vulnerability disclosure policies.[24] Still, a flexible, mature process for handling unsolicited vulnerability reports is not yet the norm in the IoT industry.

We urge the Dept. of Commerce and other Executive Branch agencies to encourage IoT vendors and operators to develop and implement plans to receive and process cybersecurity vulnerability disclosures from external sources, and to ensure those disclosures and vulnerabilities do not go unaddressed. The Dept. of Commerce's multistakeholder process on vulnerability disclosure is laying

[24] *See* Sean Gallagher, *GM embraces white-hat hackers with public vulnerability disclosure program*, Ars Technica, Jan. 8, 2016, http://arstechnica.com/security/2016/01/gm-embraces-white-hats-with-public-vulnerability-disclosure-program. *See also* Dept. of Defense, *Statement by Pentagon Press Secretary Peter Cook on DoD's Partnership with HackerOne on the "Hack the Pentagon" Security Initiative*, Mar. 31, 2016, http://www.defense.gov/News/News-Releases/News-Release-View/Article/709818/statement-by-pentagon-press-secretary-peter-cook-on-dods-partnership-with-hacke.

the groundwork for this engagement, which Rapid7 supports, but promoting broad industry adoption and effective implementation will require a sustained effort.

C. Support independent security research

Rapid7 supports balanced and responsible approaches to protecting security research in regulation and government policy. As noted above, we believe independent security research will grow in importance to cybersecurity as IoT adoption spreads to more consumer, business, and infrastructure environments – the quantity and variety of connected devices will prevent manufacturers alone from catching all vulnerabilities without independent expertise and manpower, and consumers are less likely to take steps themselves to effectively secure flawed devices.

We recognize and appreciate the Copyright Office's adoption of a temporary exemption for security research in Sec. 1201 of the DMCA, as well as NTIA's role in urging the Copyright Office to do so.[25] However, very few similar protections are in place at the federal level at this time – instead, as noted above, several existing statutes continue to chill independent access to computers and software for cybersecurity research purposes. Rapid7 urges the Dept. of Commerce, and NTIA in its role as principal advisor on telecommunication and information issues, to work with federal and state agencies and legislatures to ensure new regulations on access and use to computers and software do not unduly restrict independent research and repair of cybersecurity vulnerabilities.

D. Supply chain coordination for security patches

The devices being built and shipped today are establishing the status quo of how they will be designed, assembled, commoditized, and supported in the future. We must take the opportunity, now, to bring clarity to the IoT supply chain, evaluate the vulnerabilities and exposures most common to these devices, and implement update management programs to work both post-market and across the manufacturing process.

Due to the interconnectivity and interdependence of systems, Rapid7 believes the IoT supply chain is likely too complex to rely on one-to-one communication between vendors and manufacturers. We support a collaborative, open source model based on transparent guidelines and public vulnerability disclosure, with as much automation as reasonably possible. In the financial payments industry, which – like IoT – involves a complex ecosystem of many organizations, the major credit card organizations formed the Payment Card Industry Security Standards Council and developed the Payment Card Industry Data Security Standard.[26] A modified version of this model may be helpful to coordinate security issues across the IoT supply chain. In addition, the Dept. of Commerce should

[25] Recommendations of the National Telecommunications and Information Administration to the Register of Copyrights, Sep. 18, 2015, pg. 71, http://copyright.gov/1201/2015/2015_NTIA_Letter.pdf.
[26] PCI Security Standards Council, PCI Security, https://www.pcisecuritystandards.org/pci_security (accessed May 31, 2016).

draw upon the National Institute of Standards and Technology's guidance on security for an organization's supply chain.[27]

This is an area where the government could play a valuable role and support a more open, transparent, and secure ecosystem. It would be valuable to establish system or authority that can help researchers identify affected manufacturers and service providers, and assist with the disclosure, tracking and remediation of vulnerabilities, and coordinate with relevant third parties both domestically and internationally. Today, CERT does much of this, but CERT is in need of greater support and funding, and could build these functions out far more – including vulnerability reporting, classification, and tracking – to deliver even more value and long-term impact. This would also support the cybersecurity information sharing goals that were broadly expounded by various parts of the Government during the CISA debate, and subsequent passing of the Cybersecurity Act of 2015.

With regards to the Dept. of Commerce specifically, Rapid7 believes it could play a valuable role in working with companies to develop security patching guidelines and organize an industry body to foster cybersecurity standards development and collaboration across vendors and their supply chains. This may be an area in which the Dept. of Commerce could explore public-private partnerships or a multistakeholder process. To the extent that the Dept. of Commerce advises other government agencies on IoT-related cybersecurity issues, such as vehicles or medical devices, Rapid7 urges Commerce to prioritize updating as an essential component of security.

E. Coordinated IoT guidelines[28]

Many government agencies, trade organizations, and standards bodies have issued or collaborated on some form of guidance related to IoT security. A small sample:

- Cyber Physical Systems Public Working Group, Framework for Cyber-Physical Systems[29]
- IEEE 2413[30]
- The Federal Trade Commission's report on building security in the Internet of Things[31]

---

[27] National Institute of Standards and Technology, SP 800-161 *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Apr. 2015, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

[28] In response to questions 6, 27.

[29] Cyber Physical Systems Public Working Group, *Framework for Cyber-Physical Systems, Preliminary Discussion Draft*, Release 0.7, Mar. 3, 2015, http://www.cpspwg.org/Portals/3/docs/CPS%20PWG%20Draft%20Framework%20for%20Cyber-Physical%20Systems%20Release%200.8%20September%202015.pdf

[30] IEEE Standards Association, P2413 - *Standard for an Architectural Framework for the Internet of Things (IoT)*, https://standards.ieee.org/develop/project/2413.html (accessed May 31, 2016).

[31] Federal Trade Commission, *Careful Connections, Building Security in the Internet of Things*, Jan. 2015, https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.

- The Food and Drug Administration's Postmarket Guidance for Cybersecurity of Medical Devices[32]
- National Highway Traffic Safety Administration, National Institute of Standards and Technology (NIST) Cybersecurity Risk Management Framework Applied to Modern Vehicles[33]

It is positive that different entities are taking proactive measures on IoT security. International coordination is also key, since IoT supply chains, device usage, and data transmission will be global in many cases. However, it would be additionally helpful if there were a national strategy with a set of overarching, high-level, voluntary principles generally accepted by government agencies and industry, which IoT security guidelines should follow. This can enhance coordination and give agencies, regulated entities, and consumers a roadmap to incentivize development, awareness, and adoption of IoT security standards. This may be an area in which to explore a multistakeholder process through NTIA, or as part of a workshop.[34] As an initial matter, Rapid7 believes this guidance should include

- Robust update and upgrade paths across supply chains and postmarket,
- Encrypting network and transport security,
- Encrypting data at rest on devices and in the cloud where feasible,
- Authentication requirements to access wireless signals, APIs, and data at rest,
- Coordination and information sharing with suppliers and vendors,
- Adopting a vulnerability disclosure policy, and
- Segmenting critical and non-critical components in devices with safety implications.

F. Support strong encryption

Encryption is a fundamental means of protecting data from unauthorized access or use. Commerce, government, and individual internet users already depend on strong security for communications, and this reliance on encryption will grow as IoT applications take off. As noted above, weak transport security, unencrypted storage, and faulty authentication are vulnerabilities Rapid7 has encountered in researching the security of IoT devices. To protect against these and other cybersecurity flaws, Rapid7 believes IoT companies and innovators should be able to use the encryption protocols that best protect their customers and fit their service model – whether that protocol is end-to-end encryption or some other system.

However, because strong encryption can pose challenges to law enforcement access to data, some policymakers have called for regulations that would forbid the use of encryption without providing a

[32] Food and Drug Administration, *Postmarket Management of Cybersecurity in Medical Devices*, Draft Guidance for Industry and Food and Drug Administration Staff, Jan. 22, 2016, http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf.
[33] National Highway Traffic Safety Administration, *National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles*, Oct. 2014, http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812073_NatlInstitStandardsTechCyber.pdf.
[34] In response to question 25.

means of access to data, such as an encryption "backdoor" or custom software that removes product security features.[35] While we do not find fault with law enforcement agencies attempting to execute valid search or surveillance orders, proposals to undermine encryption would incur broad negative implications for IoT cybersecurity by creating new breach risks and attack surfaces for cybercriminals.[36] Rapid7 urges the Dept. of Commerce and other Executive Branch agencies to support the ability of businesses and innovators to use strong encryption to secure IoT.

V. Significant initiatives and research[37]

There is already a growing body of significant initiatives and research on the Internet of things. Here is a short sample of IoT research, initiatives, and resources involving Rapid7:

- Rapid7 primer on IoT security research.[38]
- Rapid7 case study on hacking baby monitors.[39]
- Rapid7 research on gas station tank gauges.[40]
- Rapid7 research on home security system.[41]
- Rapid7 research on multifunction printer.[42]
- Rapid7 research on smart toys.[43]
- Build It Secure.ly[44]
- Online Trust Alliance Internet of Things Working Group.[45]

---

[35] See, e.g., Sen. Dianne Feinstein, *Intelligence Committee Leaders Release Discussion Draft of Encryption Bill*, Apr. 13, 2016, http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649.
[36] Harley Geiger, *Security vs. Security, Rapid7 supports strong encryption*, Mar. 31, 2016, https://community.rapid7.com/community/infosec/blog/2016/04/01/security-vs-security-rapid7-supports-strong-encryption.
[37] In response to question 5.
[38] Mark Stanislav, *A Primer on IoT Security Research*, Rapid7, Mar. 10, 2015, https://community.rapid7.com/community/infosec/blog/2015/03/10/iot-security-research-whats-it-take.
[39] Mark Stanislav and Tod Beardsley, *Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities*, Rapid7, Sep. 2015, https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf.
[40] Jon Hart, *The Internet of Gas Station Tank Gauges – Take #2*, Rapid7, Nov. 11, 2015, https://community.rapid7.com/community/infosec/blog/2015/11/18/the-internet-of-gas-station-tank-gauges-take-2.
[41] Tod Beardsley, *R7-2015-23: Comcast XFINITY Home Security System Insecure Fail Open*, Rapid7, Jan. 4, 2016, https://community.rapid7.com/community/infosec/blog/2016/01/05/r7-2015-23-comcast-xfinity-home-security-system-insecure-fail-open.
[42] Deral Heiland, *12 Days of HaXmas: Advanced Persistent Printer*, Rapid7, Dec. 9, 2015, https://community.rapid7.com/community/infosec/blog/2015/12/26/advanced-persistant-mfp.
[43] Mark Stanislav, *R7-2015-27 and R7-2015-24: Fisher-Price Smart Toy & hereO GPS Platform Vulnerabilities*, Rapid7, Jan. 25, 2016, https://community.rapid7.com/community/infosec/blog/2016/02/02/security-vulnerabilities-within-fisher-price-smart-toy-hereo-gps-platform.
[44] BuildItSecure.ly, Building an IoT Device and Don't Know Where to Start?, https://builditsecure.ly/#resources (accessed May 31, 2016).
[45] Online Trust Alliance, Initiatives, Internet of Things, https://otalliance.org/initiatives/internet-things (accessed May 31, 2016).

* * *

We appreciate the opportunity to share our views. If there are additional questions or if Rapid7 can provide any further assistance, please contact Harley Geiger, Director of Public Policy, at Harley_Geiger[at]Rapid7.com. Thank you.

END