Response to the Department of Commerce National Telecommunications and Information Administration Request for Comment on Internet of Things

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

RFC No. 160331306-6306-01

May 22, 2016

Neal Krawetz, Eric Schultz, Valerie Kaminsky, Bill Tucker, et al.

The Department of Commerce (DoC) National Telecommunications and Information Administration (NTIA) issued a Request for Comments (RFC) in the Federal Register.[1] This issuance requested feedback on the current policy and technological landscape related to the Internet of Things (IoT). This document includes responses to the following items:

IoT Challenges

Issue #1 in the NTIA RFC requested information related to the challenges and opportunities arising from IoT. In particular, how they are similar to existing challenges and what aspects are novel. This topic is further discussed in other issues, including #6 (technological issues), #16 (cybersecurity), and #17 (privacy).

The challenges posed by the Internet of Things mirrors today's existing issues with mobile devices in regards to security, application, and networking. However, the IoT amplifies all of these issues and brings them to a critical level. The IoT is positioned to become invasive and integral to businesses and consumers across America. In particular, there are many areas of concern, including software patches, unsupported (legacy) devices, improper handling of personal information, disposable electronics,

[1] https://www.ntia.doc.gov/files/ntia/publications/fr_rfc_iot_04062016.pdf

insecure design, inherent vulnerabilities, backdoors, networking and infrastructure security, and economic impacts.

Software Patches

NTIA RFC issue #6 asks about technological issues that hinder the development of IoT. One of the biggest issues concerns software patches.

Active projects are constantly being updated and patched. Some updates offer new functionality, while others fix problems (bugs) or address security risks. Even if a particular piece of software has no direct vulnerability, it may be dependent on other software packages that require patches -- and those dependent updates may require additional updates to other software packages.

With large operating systems like Microsoft Windows, Mac OS X, and Ubuntu Linux, there are a limited number of official patch methods. For example, if you run Windows 8.1, then there is only one official patch distributor: Microsoft. If Microsoft releases a patch, then every Windows 8.1 system has the option to install the patch. Moreover, these software providers can limit the upgrade pathways; if you want to patch Internet Explorer 10 (part of Windows 8.1), then you must patch other parts of the system as well. Similarly, monumental software projects, such as Microsoft Office, Adobe's Creative Suite, and Google's Chrome browser, each only offer a single source for patches and updates.

Having a single source distributor for software permits creates a chokehold on the update path. Users can choose to update, but there are no choices for alternate patch solutions and few choices with regards to mixing and matching updates.

In contrast, there are tens of thousands of different cellphone makes and models. Samsung currently has over 1,060 different devices,[2] Motorola has over 400 different phones (a few samples are shown to the right),[3] and Nokia has nearly 500 different

[2] http://www.gsmarena.com/samsung-phones-9.php

[3] http://www.gsmarena.com/motorola-phones-4.php

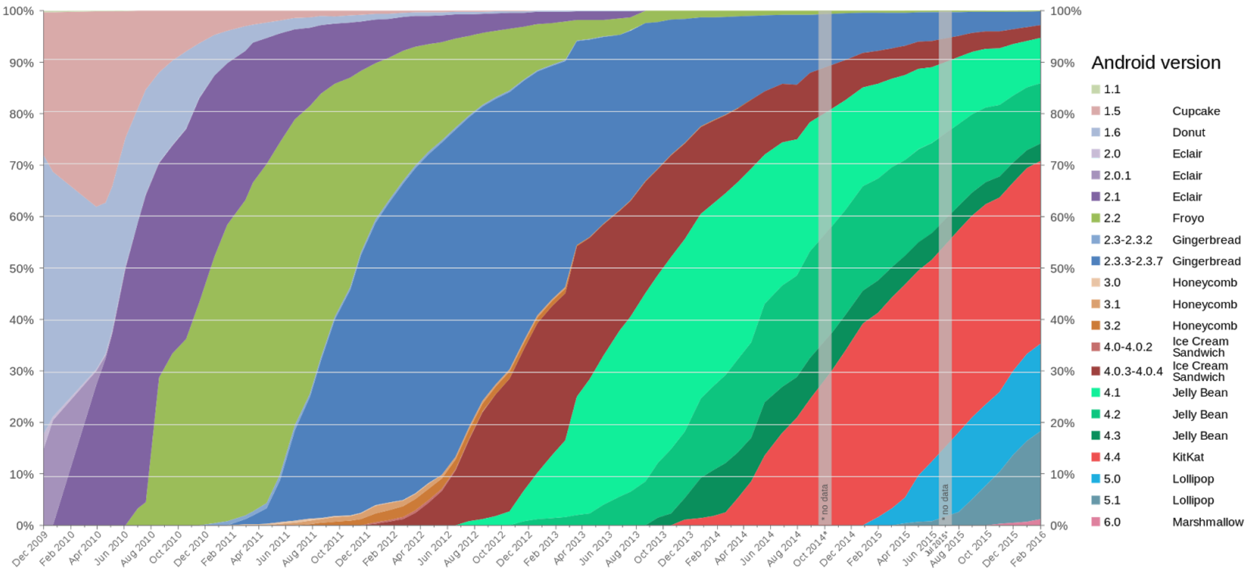
phones.[4] There are also phones from Sony, Huawei, Blackberry, Apple, and dozens of other manufacturers. There are flip phones, bar phones, feature phones, phones with big touch screens, small screens, slide-out keypads, front-face keypads, one camera, two cameras, and more. And each one of these devices uses a **unique set of software**.

When (not “if”) there is a problem that spans multiple cellphones, there is no single patch that will cover a majority of devices. There is also no single distribution method for getting the patches to the devices.

The wide variety of devices is not limited to the hardware or custom software; even the operating systems vary widely. Android (a mobile device operating system) has been repeatedly criticized for creating serious update and maintenance problems due to the wide range of available versions.[5] As Google noted,[6] less than 2% of Android devices are using the latest version of the operating system.[7] Unfortunately, many Android devices have no option for updating the operating system (e.g., the LG P509 smartphone). And in some cases, Google is explicitly leaving patch development for the operating system up to outside developers.[8] As a result, there are a significant number of smartphones running software that has known vulnerabilities and no patch options.

This update path problem is not limited to Android. WinPhones, Blackberry, Symbian, and even Apple’s iOS devices all have this problem to some degree. The graph (next page) displays the breakdown of the different Android versions that makes up the marketplace.[9] Note that Android is only one manufacture and that other manufactures have their own version breakdowns that follow similar adoption curves.

[4] http://www.gsmarena.com/nokia-phones-1.php
[5] http://www.tomshardware.com/news/google-android-update-problem-fix,29042.html
[6] http://www.cnet.com/news/hiroshi-lockheimer-android-google-alphabet/
[7] https://en.wikipedia.org/wiki/Android_version_history
[8] http://www.extremetech.com/mobile/197346-google-throws-nearly-a-billion-android-users-under-the-bus-refuses-to-patch-os-vulnerability
[9] https://en.wikipedia.org/wiki/Android_version_history



The IoT will only compound this problem with cellphones. Rather than viewing the IoT as internet-enabled TVs and refrigerators and smart houses, it should be viewed as millions of one-off devices: every different model of every different device from every different manufacturer will create a virtually infinite combination of components that define unique devices. Even if there is a known vulnerability in a widely-used common library (e.g., CVE-2014-0160 “Heartbleed”[10] impacting virtually every OpenSSL installation), there is unlikely to be a method for identifying all vulnerable IoT devices or for patching all IoT devices.

Unsupported Devices

Issue #8 in the RFC addresses the demands on existing infrastructure, business models, and stability, and issue #9 address IoT disruptions to infrastructures.

Single-source patch providers, such as Apple, Google, and Microsoft, determine if and when a patch is released. Unfortunately, most providers terminate support after a few years. For example, Apple first released iOS7 in September 2013, and stopped supporting iOS 7 in September 2014 (one year later).[11] Apple no longer provides security updates to devices running iOS 7.[12] Similarly, Microsoft dropped support for Windows XP in April 2014.[13] However, according to GoSquared and NetMarketShare, systems running iOS7 still represents nearly 4% of iPhones and Windows XP *still* accounts for over 10% of computers online.[14,15]

[10] https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160
[11] https://en.wikipedia.org/wiki/IOS_7
[12] http://gizmodo.com/cant-go-back-now-apple-stops-supporting-ios-7-1639930252
[13] https://www.microsoft.com/en-us/windows/enterprise/end-of-support.aspx
[14] https://www.gosquared.com/global/ios/9/#launch May 2016.

The same problem is seen with cellphones and mobile devices. Few consumers rush out to buy every latest-greatest version. Most consumers buy a phone and continue using it until it breaks, becomes incompatible with the carrier, or no longer works with essential online services.[16] This results in a plethora of unsupported and vulnerable devices.

The same is expected with IoT devices. An internet-enabled refrigerator typically costs over $4000; consumers are not expected to purchase a replacement refrigerator every few years. However, even though the LG Smart ThinQ™ Super-Capacity 3 Door French Door Refrigerator with 8" Wi-Fi LCD Screen (LFX31995ST) came out in 2014, LG already lists it as a discontinued product and offers no patches;[17] support was dropped after less than 2 years. (Fortunately, there are technical instructions from third parties that show how to compromise the device and manually alter the operating system.[18])

With the IoT, we should expect to have a wide range of vulnerable devices that remain in use years after manufacturers drop support. These devices may be used to compromise the device itself, or use the device as a jumping-off point to compromise other devices on the network.

Unfortunately, the refrigerator example is not a worst-case scenario. Many consumers installed smart-home devices that controlled everything from the thermostat and lighting to the alarm system and home theaters. One smart-home manufacturer, Nest, was purchased by Google's parent company, Alphabet. In 2016, Alphabet decided to drop support for Nest smart-homes. As reported by Business Insider, this move "will make customers' existing devices completely useless."[19] As consumer Arlo Gilbert noted:[20]

> I don't mean that the Nest product will reach end-of-life for support and updates. No, I mean that on May 15th they will *actually turn off the device* and disable your ability to use the hardware that you paid for.
>
> …

[15] http://www.netmarketshare.com/ May 2016, distribution by Operating System Version.
[16] http://www.wired.com/2015/12/the-year-we-started-buying-phones-like-cars/
[17] http://www.lg.com/us/refrigerators/lg-LFX31995ST-french-3-door-refrigerator
[18] https://www.exploitee.rs/index.php/LG_Smart_Refrigerator_%28LFX31995ST%29%E2%80%8B and http://hackaday.com/2014/08/09/defcon-22-hack-all-the-things/
[19] http://www.businessinsider.com/googles-nest-closing-smart-home-company-revolv-bricking-devices-2016-4
[20] https://arlogilbert.com/the-time-that-tony-fadell-sold-me-a-container-of-hummus-cb0941c762c1

> On May 15th, my house will stop working. My landscape lighting will stop turning on and off, my security lights will stop reacting to motion, and my home made vacation burglar deterrent will stop working. This is a conscious intentional decision by Google/Nest.

With the IoT, we can expect manufacturers to intentionally disable some devices when support is not considered to be a desirable option -- even if consumers are dependent on the devices. With Nest smart-home devices, disabling them could impact people who are disabled, or facilities that use the automation in mission-critical environments, such as long-term care homes or manufacturing facilities.

Personal Information

Issues #17 and #18 in the NTIA RFC asked about privacy and consumer protection issues that are raised specifically by the IoT.

As electronic devices become more prevalent in society, they are increasingly used to store personal information. As the cost to manufacture IoT capabilities decreases, more devices will become interconnected and more devices will branch out to include personal information. Once single purpose devices, cellphones have branched out to include applications for banking, shopping, email, cameras, social media, and GPS-related services.

Even toilets, whose only prior integration in the last 50 years was the inclusion of electronic bidets, are not safe from the influence of innovation.[21] Toilets can now link directly to doctors offices detailing frequency of use, weight, and may one day report key indicators of health including blood sugar levels, cholesterol, bacteria levels, early pregnancy, PSA levels, and alcohol levels.[22,23]

An insecure, lost, stolen, or compromised electronic device may divulge personal information to neighbors, landlords, identity thieves, undesirable advertisers, and criminals. As the IoT expands, the attack surface will also increase, giving malicious individuals new opportunities to affect more people. In 2014, 7% of all U.S. residents 16 years or older were the victim of identity theft,[24] and with an increased attack surface, this number will likely rise. In addition to identity theft, exposed personal information can result in blackmail and corruption at all levels of business and government.

[21] http://www.huffingtonpost.com/2012/05/07/high-tech-toilet-takes-urine-sample_n_1479348.html

[22] http://www.wired.com/insights/2014/04/toilet-role-internet-things/

[23] http://www.yankodesign.com/2012/05/04/the-value-of-pee/

[24] http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408

Recycling and Safe Disposal

While there is plenty of documentation focusing on replicating personal information onto a new phone, there is very little guidance on properly sanitizing an old phone and the procedure can be inconsistent between manufacturers.

A recommendation from FTC includes erasing personal information before disposing electronic devices.[25] In fact, the FTC recommends deleting, checking the device, and possibly deleting a second time: “After you’ve deleted your personal information, it’s good to double-check to make sure it’s gone.” Unfortunately, many personal devices do not delete all personal information. For example, many Android devices do not delete personal information after a factory reset.[26,27] Moreover, deleting data does not necessarily mean that the data is permanently gone; many types of deleted personal files can be recovered with free and commercial off-the-shelf (COTS) tools and services.[28,29]

Disposable electronics and planned obsolescence leads to a growing problem with electronic waste.[30] Many consumers recycle their phones by donating to charities that repurpose old phones to those in need, or consumers resell their phones on digital marketplaces like eBay or CraigsList. These phones end up in the hands of other consumers, who may use any preserved data for malicious purposes. As Consumer Reports noted, “Erasing data isn’t enough to prevent identity theft when recycling gadgets.”[31]

Disposable Electronics

Every two years, approximately 44% of Americans upgrade their cellphones.[32] This leads to a significant amount of electronic waste. While some devices are recycled, many end up in landfills. Steve Manning, CEO of cellphone reseller ReCellular, described the problem in simple terms:[33]

[25] https://www.consumer.ftc.gov/articles/0200-disposing-your-mobile-device
[26] http://www.ubergizmo.com/how-to/wipe-android-phone-tablet/
[27] http://www.techtimes.com/articles/55837/20150527/androids-factory-reset-does-not-wipe-your-data-heres-the-solution.htm
[28] http://www.file-recovery.com/android_recovery.htm
[29] http://www.geek.com/apple/how-to-recover-deleted-files-from-your-pc-or-mobile-device-1537610/
[30] http://www.recyclingtoday.com/article/survey-examines-consumer-mobile-device-recycling-habits/
[31] http://www.consumerreports.org/cro/news/2014/08/erasing-data-is-not-enough-to-prevent-identity-theft/index.htm
[32] http://www.gallup.com/poll/184043/americans-split-often-upgrade-smartphones.aspx
[33] http://www.cnet.com/news/your-smartphones-secret-afterlife-smartphones-unlocked/

> "One cell phone in the trash isn't a big deal," said Steve Manning, CEO of cell phone reseller ReCellular. "100 million in the trash is an environmental disaster."

The Guardian also noted this sentiment:[34]

> Consumers aren’t the only losers here, the environment is too. Due to a lack of clear economic incentives and methods, globally only 12% of smartphone upgrades involve older devices being sold or traded for the new one. This means ecologically damaging devices end up languishing in drawers and eventually landfills.

The IoT will result in more electronic devices being disposed over time. Without clear guidance and direction, this will lead to global environmental problems.

Insecure Design

Issue #16 in the NTIA RFC relates to IoT and cybersecurity concerns.

Administrators and developers are quick to invent and adopt new technologies when they may not fully understand the security implications related to that technology. Consulting outside experts can be time consuming and may increase the time it takes to deliver a product. Even if there is time for a security review, experts may be hard to find for newer technologies. As a result, IoT products are often designed without the proper security controls. A few recent examples include:

- iKettle: This IoT teapot revealed the local Wi-Fi password to attackers.[35]

- LIFX light bulbs: These Wi-Fi enabled multicolor LED light bulbs permit remote control from a smartphone. However, researchers discovered that the control protocol was vulnerable to data injection, replay attacks, and unencrypted transmissions.[36]

- SanDisk Cruzer: This USB memory stick contains a static data set (called the U3 partition) that stores manufacturer-specific files. These files cannot be easily deleted; removing the files and reinserting the USB stick into a Windows

[34] http://www.theguardian.com/sustainable-business/2015/mar/23/were-are-all-losers-to-gadget-industry-built-on-planned-obsolescence
[35] http://www.theregister.co.uk/2015/10/19/bods_brew_ikettle_20_hack_plot_vulnerable_london_pots/
[36] http://www.contextis.com/resources/blog/hacking-internet-connected-light-bulbs/

computer recreates the deleted files. Attackers can use this U3 partition to install malware onto computers.[37,38]

- Webcams: Most network-configurable devices contain default login credentials. Unfortunately, many consumers never perform basic steps, like changing the default passwords. In 2014, Sophos' Naked Security reported on Insecam.com -- a site that linked to over 13,000 publicly accessible webcams and baby monitors that used default passwords.[39] Although a few devices use random default passwords (usually printed as stickers on the device) or require changing the default password prior to full activation, most permit access by anyone who knows the default settings. Unfortunately for those consumers who do not change the default settings, lists of default passwords for devices are publicly available.[40,41]

- Routers, modems, IP cameras, VoIP phones and other embedded devices: In 2015, security firm SEC Consult evaluated the firmware from 70 major manufacturers and found that SSH and HTTPS keys are often reused.[42] The keys were readily retrieved from firmware and create a break-one-get-all situation. SEC Consult estimated than 150 HTTPS server certificates were used by 3.2 million devices, and 80 SSH host keys were used by 900,000 devices. In general, if a manufacturer creates devices that all have the same encryption key, then compromising one device means the other devices can be compromised.

- Heinz and Fitbit: In 2015, The Guardian reported on a Heinz Ketchup online contest.[43] The contest was accessed by QR codes (barcodes) on select ketchup bottles. Scanning the code opened a web page to a contest web site. After the contest ended, Heinz allowed the contest's domain to expire. Unfortunately, the newly available domain name was re-registered by someone else and linked to a German porn site, impacting all consumers who scanned in the ketchup contest code. Fortunately, the situation was not worse. The popular wearable biometric tracker, Fitbit, also uses a hard-coded domain name. If the domain is ever

[37] https://www.ifixit.com/Answers/View/13735/I+can%27t+erase+file
[38] http://wiki.robotz.com/index.php/Sandisk_U3_Flash_Drive_Virus
[39] https://nakedsecurity.sophos.com/2014/11/10/is-your-webcam-or-baby-monitor-video-feed-being-streamed-to-this-website/
[40] http://www.defaultpassword.com/
[41] https://cirt.net/passwords
[42] http://www.pcworld.com/article/3009143/security/millions-of-embedded-devices-use-the-same-hard-coded-ssh-and-tls-private-keys.html
[43] https://www.theguardian.com/technology/2015/jun/19/heinz-ketchup-qr-code-links-porn

acquired by another entity, then the new owner will begin receiving personal biometric information from all Fitbit users.

The security issues are not limited to explicit vulnerabilities. Products developed securely for the average consumer may be deployed in an environment that requires stricter controls. For example, a hospital may use a non-HIPAA compliant device, or a military sensitive compartmented information facility (SCIF) may unknowingly utilize a device with integrated technology that can transmit outside of the facility.

In 2008, the US Government forbid the use of USB devices in government computers, and some secure facilities forbid unapproved USB devices.[44] These restrictions impact many IoT devices include Timex Datalink watches,[45] Google Glass,[46] Fitbit activity tracker, and Lechal haptic footwear.[47] The ubiquitousness of IoT devices may lead to consumers forgetting that they are Internet-enabled when they enter a restricted facility, putting the facility's information at risk.

All USB ports have been disabled
on this computer for security reasons.

Photo by Michael Sauers, https://www.flickr.com/photos/travelinlibrarian/144297435

[44] http://www.stripes.com/news/dod-bans-the-use-of-removable-flash-type-drives-on-all-government-computers-1.85514
[45] https://en.wikipedia.org/wiki/Timex_Datalink
[46] https://en.wikipedia.org/wiki/Google_Glass
[47] http://lechal.com/

Even if an IoT device currently has no known vulnerabilities and is used in an appropriate environment, this does not mean it will always be secure. New exploits may be identified as time progresses.

Inherent Vulnerabilities

Issue #16 in the NTIA RFC relates to IoT and cybersecurity concerns.

Many IoT devices are based on computationally weak hardware, minimal operating systems, and limited memory. These systems either lack the resources needed to run full antivirus and intrusion detection systems, or lack the resources necessary for continuously employing them in real time.

Limited resources make IoT devices more vulnerable to denial-of-service and stack-smashing attacks. As one commentator remarked, “to be fair, trying to respond to a 64k ping when you only have 30k of RAM left kinda is a futile task.”[48] As a result, many IoT devices are vulnerable to common exploits.

For example, the Ping of Death (CVE-1999-0128) has been well known for over a decade.[49] Major desktop operating systems are no longer vulnerable, but this simple fragmentated ICMP packet can still hang many IoT devices. This includes devices that support bluetooth and IPv6.[50,51]

Less powerful hardware and limited system resources also reduces the developer’s ability to use widely deployed and publicly reviewed software libraries. Without access to public cryptographic libraries, systems may end up using cryptographically weak solutions. For example, Hewlett-Packard released a small network device called the “Secure Web Console” that provides remote access to server consoles. However, researcher Michael Shaffer noted that the security came from XOR’ing all data packets with a single character (0x37).[52] XOR encoding is trivial to detect and trivial to reverse; it offers no more security than pig-latin does for disguising English. In effect, the HP Secure Web Console was *secure* in name alone.

These same hardware and resource limitations may also restrict developer tools. Programmers may end up creating vulnerable functionality because common libraries

[48] http://forums.channelregister.co.uk/forum/1/2014/07/30/each_internetofthings_thing_contains_25_vulnerabilities/
[49] https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0128
[50] http://arxiv.org/pdf/1206.1482.pdf
[51] http://ccent.syr.edu/wp-content/uploads/2014/06/Study_of_IPv6_Security_Vulnerabilities.pdf
[52] https://www.giac.org/paper/gsec/172/cracking-hp-secure-web-console/100647

may not exist for the specific IoT platform. In addition, programming languages that check for common overflow conditions may be too resource intensive for some IoT devices. This results in development being performed with languages that pose higher risks to all but highly experienced security-oriented programmers.

Intentional Backdoors

Issue #16 in the NTIA RFC relates to IoT and cybersecurity concerns.

IoT devices are often inexpensive and single-purpose (or limited purpose) items that are readily introduced into the local network. Unlike applications that are downloaded or installed from removable media, IoT devices are never scanned with sophisticated antivirus tools or checked for malicious software. IoT devices with backdoors permit remote attackers to access the device and use them as a staging areas for attacking the rest of the network.

Some remote access backdoors are intentional. For example, it is common for developers to create devices with remote access for testing purposes. Unfortunately, these undocumented remote access methods are often included in the final product and not disabled before shipping. In 2014, Eloi Vanderbeken identified an intentional backdoor that impacted Cisco, Linksys, NetGear, and Diamond routers.[53] And in 2015, Bernardo Rodrigues identified 600,000 cable routers that had a backdoor within a backdoor.[54]

In contrast, some backdoors are unauthorized. In 2015, researchers identified unauthorized code in Juniper NetScreen firewalls that permitted remote access.[55] It is believed that nation-state actors inserted these code changes. Similarly, a warning this month stated that some Chinese microcomputers (used in IoT devices like the Raspberry Pi, tablets, and set-top boxes) contain a modified firmware that permits privilege escalations.[56] And in 2008 and 2009, digital picture frames were found to ship with malware that installed keyloggers and backdoor software.[57]

[53] http://www.synacktiv.com/ressources/TCP32764_backdoor_again.pdf

[54] http://www.scmagazine.com/600000-cable-routers-found-to-have-a-backdoor-within-a-backdoor/article/456352/

[55] https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/

[56] http://arstechnica.com/security/2016/05/chinese-arm-vendor-left-developer-backdoor-in-kernel-for-android- pi-devices/

[57] http://www.cnet.com/news/latest-problem-import-infected-digital-photo-frames/

In contrast to Juniper, where the unauthorized code was surreptitiously inserted, the FBI explicitly asked Apple to insert a backdoor into iPhones.[58] The main concerns are that (1) any backdoor that exists on these devices can be used to compromise any of these devices, and (2) if law enforcement can use a backdoor, then so can attackers.

A key issue with IoT devices concerns trust: vendors are not checking their products to ensure that they are shipping what they think they are shipping, and consumers are trusting manufacturers to not provide clandestine functionality. IoT devices are vulnerable to altered hardware, firmware, and software during production, and these exploits can be used to compromise home and office networks.

Network and Infrastructure

NTIA RFC issue #6 inquires about technological issues that may hinder the development of IoT devices.

There are three types of network addressing used by devices on the internet: MAC, IPv4, and IPv6. Unfortunately, each of these addressing mechanisms will negatively impact IoT development.

The media access control address (MAC address) is used for local network packet routing. MAC addresses are not typically transmitted across the Internet, but are used for directing traffic from the last router to the local computer system.[59] (If the Internet works like the postal service, then the MAC address is how the letter goes from the street address and mailbox delivery to the intended recipient named on the letter.) Every device on the local network needs a unique MAC address.

The MAC address consists of 6 bytes (48 bits). Two bits determine whether the address is locally or globally administered; virtually no devices are currently locally administered. For globally administered addresses (the vast majority of devices), the IEEE uses 22 bits to identify specific vendors (called the OUI, or Organizationally Unique Identifier). The remaining three bytes (24 bits) represent up to 16 million unique IDs that can be assigned by the manufacturer.

Unfortunately, there is not enough address space for every networked device to have a unique MAC address.[60,61] For example, in 2015 Apple reported that they sold 74.5

[58] http://www.apple.com/customer-letter/

[59] The purpose of the MAC address is a little more complicated than this, but for this paper, we are keeping the description at a high level.

[60] https://securityledger.com/2015/11/will-a-reliance-on-mac-address-pose-a-privacy-risk-for-iot/

million iPhones, which is more than a single OUI allocation. (Fortunately for Apple, they have currently been allocated 471 OUI ranges, which is more than any other vendor except Cisco.) That same year, Apple's iOS 8 introduced randomized MAC addresses for wireless connections.[62] However, this is not enough to ensure uniqueness.[63] Many vendors already reuse MAC addresses across products.[64] While reuse is only a problem when two devices are attached to the same local network, it is becoming increasingly more likely that a network will have multiple devices with the same MAC address.

Along with the MAC address is the Internet address, which permits routing beyond the local network. The older Internet Protocol, called IP or IPv4, consists of four bytes of address space, or approximately 4.3 billion addresses. Unfortunately, the primary allocating bodies have already depleted their allocation supply of IPv4 address ranges.[65] Although IPv4 is still in use, there is a push toward the next generation of Internet addressing, IPv6, which offers more address space.

Unlike IPv4, which was relatively simple to implement, IPv6 is more complicated. Many IoT devices do not fully implement IPv6. These incomplete implementations are vulnerable to network attacks and malware.[66]

The exponential growth of Internet enabled devices will further tax both MAC address allocation and Internet address allocation.[67] Devices that only support IPv4 will become obsolete in the very near future. And devices that do not fully implement IPv6 pose support and vulnerability issues.

Economic Impact

NTIA RFC issue #12 inquires about methods to measure the economic impact of IoT and issue #13 focuses on the impact IoT will have on industrial practices, including manufacturing and supply chains.

Gartner, a leading research and advisory firm, predicts that IoT will generate revenue exceeding $300 billion in 2020.[68] In the next decade, the World Economic Forum

[61] http://www.computing.co.uk/ctg/news/2433827/mac-addresses-the-privacy-achilles-heel-of-the-internet-of-things
[62] http://www.mathyvanhoef.com/2016/03/how-mac-address-randomization-works-on.html
[63] http://papers.mathyvanhoef.com/asiaccs2016.pdf
[64] https://jira.iotivity.org/browse/IOT-381
[65] https://en.wikipedia.org/wiki/IPv4_address_exhaustion
[66] https://www.us-cert.gov/sites/default/files/publications/IPv6Malware-Tunneling.pdf
[67] http://cloudtimes.org/2013/12/20/gartner-the-internet-of-things-will-grow-30-times-to-26-billion-by-2020/
[68] http://www.cips.org/supply-management/opinion/2015/february/the-internet-of-things-offers-vast-potential-for-supply-chains-but-also-risks/

expects 10% of cars on the road to be driverless, the first robotic pharmacist will be deployed, and one trillion sensors will be connected to the Internet.[69]

In commercial applications, IoT sensors can be applied to track inventory, transportation, temperature, and quality. As an example, ambient sensors installed throughout GM's manufacturing plants allow GM to avoid painting cars during overly humid conditions, which can adversely impact paint quality.[70] In the pharmaceutical industry, serialization is mandatory and driving chain of custody tracking to identify counterfeit products.[71] Similar applications exist for the food industry, which is increasingly concerned with tracking product and its sources for product safety, labeling, freshness, and recall purposes. Within agriculture, satellite images, weather tracking, sensors for farm equipment, fertilizer, and water can be measured and tracked for each individual plant.[72]

The IoT is being studied throughout the industry, including by groups like the Open Interconnect Consortium -- an organization working to develop standards and certifications. The economic impact of IoT is currently being measured across NGO's and private institutions like Gartner, ABI Research, and McKinsey, whose work can assist in benchmarking this trend.

Labor is one of the highest components of cost offsetting revenues and is even more pronounced for smaller businesses. The U.S. Department of Labor estimates 10-20% labor costs for the retail industry and perhaps 30% for industries such as food and hospitality.[73] Companies seeking labor saving opportunities have already extracted significant benefits by offshoring labor to lower cost countries.

As technology becomes more connected, IoT devices can be used to automatically trigger process adjustments that previously were handled manually. As a result, the IoT will create new job opportunities while also rendering other manual jobs obsolete. Gartner, in its most conservative estimates, predicts that there will be “persistent and higher unemployment” and, by 2020, the impact of labor reduction "will cause social unrest and a quest for new economic models in several mature economies”.[74] Having

[69] http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf
[70] http://www.enterpriseappstoday.com/supply-chain-management/internet-of-things-adds-intelligence-to-supply-chain-1.html
[71] http://www.forbes.com/sites/sungardas/2015/07/27/balancing-the-internet-of-things-iot-in-the-supply-chain/
[72] http://bits.blogs.nytimes.com/2015/08/03/the-internet-of-things-and-the-future-of-farming/
[73] http://wheniwork.com/blog/are-your-labor-costs-out-of-control/
[74] http://www.computerworld.com/article/2485967/emerging-technology/gartner-s-dark-vision-for-tech--jobs.html

worked directly with several companies who offshore office and factory labor and then further reduce the need for this labor with automation and machine learning, we have seen this trend firsthand and believe them to be a significant source of income disparities. Although these technologies will benefit the economic community as a whole, particularly in the form of cheaper goods and services, it has a natural tendency to skew the greatest geometric benefits toward the highest earners.

Industry Recommendations

NTIA RFC issue #3 asks about current or planned laws, regulations, and/or policies. Unfortunately, there are no standards. Currently, policies are limited to ad hoc recommendations. For example:

- The Open Web Application Security Project (OWASP) is currently developing a draft document that discusses issues and common problems related to IoT devices (https://www.owasp.org/index.php/IoT_Security_Guidance). This document includes security recommendations for manufacturers, developers, and consumers, and it covers topics such as encrypted network communications and secure user interfaces. The current draft focuses on common bad practices, such interfaces that permit weak passwords or devices that do not use encryption for sensitive communications.

- Microsoft provides high-level guidelines for securing IoT devices: https://azure.microsoft.com/en-us/documentation/articles/iot-security-best-practices/. These recommendations include general statements like “make hardware tamper proof” and “keep authentication keys safe”. While these platitudes sound helpful, Microsoft offers no details other than stating that bad things can happen. For example, Microsoft’s recommendation for “Protect against malicious activity” states:

  > **Protect against malicious activity**: if the operating system permits, place the latest anti-virus and anti-malware capabilities on each device operating system. This can help mitigate most external threats. Most modern operating systems, such as Windows 10 IoT and Linux, can be protected against this threat by taking appropriate steps.

  This advices does not mention what steps should be taken beyond running an antivirus scanner. It does not mention what is “appropriate” or options for operating systems that do not support antivirus software. Moreover, antivirus software only catches about 25% of the most common malware,[75] so this advice is not very effective.

Surprisingly, the best recommendations for security and privacy are not explicitly focused on security and privacy:

1. **Public standards**. Currently, most specialized IoT devices have their own proprietary interfaces for communication, authentication, authorization, patch management, and command and control (C&C). Well-defined open standards for these interfaces reduce the need for custom protocols. Consistent, peer-reviewed, and established protocols reduce the risk from oversight in proprietary interfaces.

2. **Open application interfaces**. The current proprietary interfaces deter interoperability with other systems and devices. Open application interfaces (APIs) that use well-defined standards improve interoperability and removes the dependency on any single resource. For example, if the Nest smart-home system was not explicitly linked to Alphabet/Google's resources, then the device would not need to be turned off when the service goes away.[76] Instead, other providers could step up and offer compatible functionality. Similarly, if the LG Wi-Fi enabled refrigerator used open standards, then it could still receive patches and updates even after LG dropped product support.[77]

Public standards and open interfaces permit public vetting. As a result, inherent issues related to security and privacy should be readily identified and addressed. In addition, the use of well-defined public standards for these interfaces does not preclude the use of proprietary technology within an IoT device.

Unfortunately, well-defined and vetted public standards for communication, authentication, authorization, patch management, and C&C do not currently exist. Ideally, these specifications would be publicly available, simple to understand, and easy to implement in low-resource environments such as IoT devices. They should not be vendor specific, tied to proprietary requirements, or hyper-focused on specific functionality.[78]

[75] http://www.computerworld.com/article/2472120/security0/how-useful-is-antivirus-software-.html
[76] http://www.businessinsider.com/googles-nest-closing-smart-home-company-revolv-bricking-devices-2016-4
[77] http://www.lg.com/us/refrigerators/lg-LFX31995ST-french-3-door-refrigerator
[78] Because we cannot predict what functionality or hardware requirement a future IoT device may require, the open standards should not define or restrict the set of required or permitted functionality.

Governmental Role

Issues #3, #25, and #26 in the NTIA RFC inquired about potential laws, regulations, and policies related to the IoT.

Governmental policy has fallen behind current technology. While this may be advantageous to manufacturers, it can leave businesses and consumers exposed. To help protect all members of society, the government should:

- Increase its participation,
- Update and publish its regulations, policies, best practices and guidelines,
- Advocate for consumer education and awareness,
- Increase its enforcement and accountability, and
- Increase incentives for manufacturers to meet and exceed regulations related to security and privacy.

Current Government Policies

NTIA RFC issues #16, #17, #26, and #27 inquire about existing government recommendations and policies.

In January 2015, the Federal Telecommunication Commission (FTC) issued a staff report titled “Internet of Things: Privacy & Security in a Connected World”.[79] This 71-page report details some of the risks and concerns mentioned in this RFC response and offers recommendations regarding privacy and security. These recommendations include:

- **Security by design**. Manufacturers should build in security processes rather than augmenting an insecure design with generic security solutions.

- **Train employees**. Educate product developers in good security practices.

- **Data minimization**. Reducing the data collected by IoT devices mitigates the risk of personal information loss.

- **Limit legislation**. We are at the beginning of the IoT era. As the report recommended, “IoT-specific legislation at this stage would be premature” and could hinder future product designs.

[79] https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

The FTC's recommendations mirror conventional wisdom regarding software and online security. However, these suggestions are easier said than done. Moreover, while the FTC offers good, generalized recommendations, they lack completeness, enforcement, and incentives. For example:

- **Security by design** and **training employees** to be security conscious may seem like a good idea. However, they are actually impractical. Microsoft implemented mandatory security training for all of its engineers,[80] but their products still contain vulnerabilities. Training and best practices help mitigate the risk of vulnerabilities, but it does not completely neutralize the threat.

- **Minimizing data collection** is not the same as no data collection or offering the user a way to reset the system and wipe all data prior to disposal. Moreover, any data that a product and company collects may not have an obvious third-party value to the company, but may nonetheless be valuable to an identity thief or attacker; any collected data, even if only a minimal amount, may pose a risk to consumer privacy and security. In contrast, if the data is never collected then it cannot be stolen.

- **Limiting legislation** to virtually nothing beyond HIPAA, SOX, PCI, and other established legal requirements provides no enforcement and no incentive for companies to follow even these minimal best practices.

The FTC recommendations sound good as high-level offerings, but provide no real security or privacy, ignore practicality, and lack foresight.

Recommended Government Policies

NTIA RFC issues #20-#27 request recommendations for government policies as well as defining a role for the Department of Commerce.

There is an important role for government and legislation in the IoT. The government should provide regulations and enforcement related to consumer protections, including:

- **Mandatory support**. Regulations should mandate product support, including updates and patches related to security and privacy. The duration of the support should be consistent with the product's retail price and role. For example, a

[80] https://www.microsoft.com/security/sir/strategy/default.aspx#!section_4

non-critical and inexpensive IoT device may only need one year of support, but a $4,000 IoT refrigerator should be supported for the life of the refrigerator.

- **Mandate patches and updates** for existing IoT devices when solutions to vulnerabilities related to security and/or privacy are available. This requires developers to design long-term support mechanisms. For technologies that are predetermined to not have long-term support, the duration of the support must be specified prior to the purchase. Consumers should know what they are buying and not be surprised when product support is unexpectedly terminated.

- **No personal registration**. It is likely that companies will view product support as an opportunity to collect personal information in the form of mandatory product registration. Simply being in possession of the IoT device should be enough to demonstrate ownership and receive required support; additional personal information for product registration should not be required.

- **Delete personal information**. Regulations should mandate methods to completely and securely delete all personal information from an IoT device prior to disposal. This should be initiated by the consumer, and not at a remote reclamation facility, in order to minimize the risk from any personal information disclosure.

- **End-of-life planning**. Regulations should specify that reclamation and environmentally friendly disposal must be explicitly designed into the product's lifecycle.

- **Continuity and risk management**. The government should take an active, collaborative interest in ensuring businesses that rely on these technologies have adequate business continuity and risk planning. In particular, this applies to cases of national security such as oil, gas, aerospace, transportation, agriculture, and companies that are economically deemed too big to fail or that deploy IoT technologies across these industries.

Along with each of these laws or regulations should be enforcement requirements and penalties for non-compliance. This should include:

- **Defined terms of liability**, similar to HIPAA-violations.

- **Explicit penalties** and/or **remediation options** when expensive or critical IoT devices become unusable or indefinitely vulnerable through no fault of the consumer.

Most devices offer a limited liability warranty (1- to 3-year terms are common). However, there is an established precedence for holding manufacturers liable for essential devices after the limited warranty expires. For example, in 2013 Toyota issued a recall for vehicles with Takata airbags, impacting 2.14 million vehicles manufactured between 2000 and 2004.[81] Each of these vehicles were more than a decade old and all were beyond their original warranties.[82] The vehicles were recalled due to safety issues.

These recommended regulations and associated enforcement will provide an incentive for manufacturers to limit electronic waste, protect consumer information, and develop effective means for updating products as new vulnerabilities and issues are discovered. This will directly impact the current practice of “disposable electronics”.

With regards to IoT growth (NTIA RFC issue #24): An effective role for the federal government would be to:

1. Better track jobs lost due to IoT and automation. This may require relying more heavily on external benchmarking and trending than on Bureau of Labor Statistics measurements,[83] which can miss underemployed populations and wage reduction trends.

2. Re-evaluate taxation and lobby congress to favor a more consumption-based tax code. Bill Gates and several Washington policymakers also support this recommendation.[84]

3. Given skills gap trends in the job market, which includes the technology sector,[85] evaluate the impact of prioritizing federal government support including student loans and educational institution subsidies to those professions where demand for qualified labor outpaces supply.

[81] http://www.reuters.com/article/us-toyota-recall-idUSKBN0EM0F620140611
[82] Toyota’s basic warranty is for 36 months or 36,000 miles. (http://www.cavatoyota.com/blog/what-is-covered-under-toyota-warranty/). Toyota’s extended warranty plans typically last a maximum of 8 years. For a 2000 Toyota to still be under warranty in 2013, it would require a minimum of a basic warranty, an extended warranty, and a renewed extended warranty. (http://www.copelandtoyota.com/ExtendedWarranties.aspx)
[83] http://www.bls.gov/lau/stalt.htm
[84] http://fortune.com/2014/10/15/bill-gates-income-inequality/
[85] http://money.cnn.com/2015/08/07/news/economy/us-economy-job-skills-gap/

Proposed Role for NTIA

It is our understanding that NTIA is not a law-making or enforcement body. NTIA cannot pass laws, cannot enforce requirements, and cannot make standards. However, NTIA can get the necessary stakeholders together to discuss these issues and determine the future direction.

As noted in this response's section "Industry Recommendations", well-defined and vetted public standards and open interfaces do not currently exist. NTIA could facilitate the creation of working groups that are focused on developing these public standards.

Similarly, NTIA could coordinate discussions between knowledgeable technology experts, lawmakers, and regulatory organizations in order to define the recommended government policies mentioned in this response.

Contributors

This DoC NTIA RFC response is provided by Dr. Neal Krawetz of Hacker Factor, Eric Schultz of the National Software Security Association, Valerie Kaminski of i2i Business Engineering, Bill Tucker, two anonymous contributors, and feedback from members of the Northern Virginia Hackers (NoVaHa) and Fort Collins Internet Professionals (FCIP) groups.

If you have questions, please contact:

Neal Krawetz, Ph.D.
Hacker Factor Solutions
PO Box 270033
Fort Collins, CO 80527-0033
http://www.hackerfactor.com/