BITAG

Broadband Internet Technical Advisory Group

Internet of Things (IoT) Security and Privacy Recommendations

A BROADBAND INTERNET TECHNICAL ADVISORY GROUP
TECHNICAL WORKING GROUP REPORT

A Uniform Agreement Report

Issued:

November 2016

Copyright / Legal Notice

This document and the information contained herein is provided on an "AS IS" basis and BITAG AND THE CONTRIBUTORS TO THIS REPORT MAKE NO (AND HEREBY EXPRESSLY DISCLAIM ANY) WARRANTIES (EXPRESS, IMPLIED OR OTHERWISE), INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, FITNESS FOR A PARTICULAR PURPOSE, OR TITLE, RELATED TO THIS REPORT, AND THE ENTIRE RISK OF RELYING UPON THIS REPORT OR IMPLEMENTING OR USING THE TECHNOLOGY DESCRIBED IN THIS REPORT IS ASSUMED BY THE USER OR IMPLEMENTER.

The information contained in this Report was made available from contributions from various sources, including members of Broadband Internet Technical Advisory Group, Inc.'s Technical Working Group and others. Broadband Internet Technical Advisory Group, Inc. takes no position regarding the validity or scope of any intellectual property rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this Report or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights.

About the BITAG

The Broadband Internet Technical Advisory Group (BITAG) is a non-profit, multi-stakeholder organization focused on bringing together engineers and technologists in a Technical Working Group (TWG) to develop consensus on broadband network management practices and other related technical issues that can affect users' Internet experience, including the impact to and from applications, content and devices that utilize the Internet.

The BITAG's mission includes: (a) educating policymakers on such technical issues; (b) addressing specific technical matters in an effort to minimize related policy disputes; and (c) serving as a sounding board for new ideas and network management practices. Specific TWG functions also may include: (i) identifying "best practices" by broadband providers and other entities; (ii) interpreting and applying "safe harbor" practices; (iii) otherwise providing technical guidance to industry and to the public; and/or (iv) issuing advisory opinions on the technical issues germane to the TWG's mission that may underlie disputes concerning broadband network management practices.

The BITAG Technical Working Group and its individual Committees make decisions through a consensus process, with the corresponding levels of agreement represented on the cover of each report. Each TWG Representative works towards achieving consensus around recommendations their respective organizations support, although even at the highest level of agreement, BITAG consensus does not require that all TWG member organizations agree with each and every sentence of a document. The Chair of each TWG Committee determines if consensus has been reached. In the case there is disagreement within a Committee as to whether there is consensus, BITAG has a voting process with which various levels of agreement may be more formally achieved and indicated. For more information please see the BITAG Technical Working Group Manual, available on the BITAG website at www.bitag.org.

BITAG TWG reports focus primarily on technical issues, especially those with the potential to be construed as anti-competitive, discriminatory, or otherwise motivated by non-technical factors. While the reports may touch on a broad range of questions associated with a particular network management practice, the reports are not intended to address or analyze in a comprehensive fashion the economic, legal, regulatory or public policy issues that the practice may raise. BITAG welcomes public comment. Please feel free to submit comments in writing via email at comments@bitag.org.

Executive Summary

In the past few years, many of the new devices connected to the Internet have not been personal computers, but rather a variety of devices embedded with Internet connectivity and functions. This class of devices has generally been described as the *Internet of Things* (IoT) and has brought with it new security and privacy risks.

The term "IoT" has potentially broad scope. IoT can refer to deployments in homes, businesses, manufacturing facilities, transportation industries, and elsewhere. Thus, IoT can refer to much more than simply consumer-oriented devices. For the purposes of this report, we use the term IoT to refer solely to consumer-oriented devices and their associated local and remote software systems, though some or all of our recommendations may be more broadly applicable. This report is concerned with scenarios where consumers are installing, configuring, and administering devices that they lease or own.

The number and diversity of consumer IoT devices is growing rapidly; these devices offer many new applications for end users, and in the future will likely offer even more. Many IoT devices are either already available or are being developed for deployment in the near future, including:

- sensors to better understand patterns of daily life and monitor health
- monitors and controls for home functions, from locks to heating and water systems
- devices and appliances that anticipate a consumer's needs and can take action to address them (e.g., devices that monitor inventory and automatically re-order products for a consumer)

These devices typically interact with software running elsewhere on the network and often function autonomously, without requiring human intervention. In addition, when coupled with data analysis and machine learning, IoT devices may be able to take more proactive actions, reveal interesting and useful data patterns, or make suggestions to end users that may improve their health, environment, finances, and other aspects of their lives.

Although consumers face general security and privacy threats as a result of *any* Internet-connected device, the nature of consumer IoT is unique in that it can involve non-technical or uninterested consumers, challenging device discovery and inventory on consumer home networks as the number and variety of devices proliferate, impacts on the Internet access service of both the consumer and others that run on shared network links, and effects on other services in that when IoT devices are compromised by malware they can become a platform for unwanted data traffic – such as spam and denial of service attacks – which can interfere with the provision of these other services.

Several recent reports have shown that some devices do not abide by rudimentary security and privacy best practices. In some cases, devices have been compromised and allowed unauthorized users to perform surveillance and monitoring, gain access or control, induce device or system failures, and disturb or harass authorized users or device owners.

Potential issues contributing to the lack of security and privacy best practices include: lack of IoT supply chain experience with security and privacy, lack of incentives to develop and deploy updates after the initial sale, difficulty of secure over-the-network software updates, devices with constrained or limited hardware resources (precluding certain basic or "common-sense" security measures), devices with constrained or limited user-interfaces (which if present, may have only minimal functionality), and devices with malware inserted during the manufacturing process.

The emergence of IoT presents opportunities for significant innovation, from smart homes to smart cities. In many cases, straightforward changes to device development, distribution, and maintenance processes can prevent the distribution of IoT devices that suffer from significant security and privacy issues. BITAG believes that following the guidelines outlined in this report may dramatically improve the security and privacy of IoT devices and minimize the costs associated with the collateral damage that would otherwise affect both end users and ISPs. In addition, unless the IoT device sector—the sector of the industry that manufactures and distributes these devices—improves device security and privacy, consumer backlash may impede the growth of the IoT marketplace and ultimately limit the promise IoT holds.

Observations. From the analysis made in this report and the combined experience of its members when it comes to Internet of Things devices, the BITAG Technical Working Group makes the following *observations*:

- **Security Vulnerabilities:** Some IoT devices ship "from the factory" with software that either is outdated or becomes outdated over time. Other IoT devices may ship with more current software, but vulnerabilities may be discovered in the future. Vulnerabilities that are discovered throughout a device's lifespan may make a device less secure over time unless it has a mechanism to subsequently update its software.

- **Insecure Communications:** Many of the security functions designed for more general-purpose computing devices are difficult to implement on IoT devices and a number of security flaws have been identified in the field, including unencrypted communications and data leaks from IoT devices.
    - **Unauthenticated Communications:** Some IoT devices provide automatic software updates. Without authentication and encryption, however, this approach is insufficient because the update mechanism could be compromised or disabled. In addition, many IoT devices do not use authentication in the course of communicating.
    - **Unencrypted Communications:** Many IoT devices send some or all data in cleartext, rather than in an encrypted form. Communications in cleartext can be observed by other devices or by an attacker.

    - **Lack of Mutual Authentication and Authorization:** A device that allows an unknown or unauthorized party to change its code or configuration, or to access its data, is a threat. The device can reveal that its owner is present or absent, facilitate the installation or operation of malware, or cause its core IoT function to be fundamentally compromised.
    - **Lack of Network Isolation:** These devices also create new risks and are susceptible to attacks *inside* the home. Because many home networks do not, by default, isolate different parts of the network from each other, a network-connected device may be able to observe or exchange traffic with other devices on the same home network, thus making it possible for one device to observe or affect the behavior of unrelated devices.

- **Data Leaks:** IoT devices may leak private user data, both from the cloud (where data is stored) and between IoT devices themselves.
    - **Leaks from the Cloud:** Cloud services could experience a data breach due to an external attack or an insider threat. Additionally, if users rely on weak authentication or encryption methods for these cloud-hosted services, user data may also be compromised.
    - **Leaks from and between Devices:** In some cases, devices on the same network or on neighboring networks may be able to observe data from other devices such as the names of people in a home, the precise geographic location of a home, or even the products that a consumer purchases.

- **Susceptibility to Malware Infection and Other Abuse:** Malware and other forms of abuse can disrupt IoT device operations, gain unauthorized access, or launch attacks.

- **Potential for Service Disruption:** The potential loss of availability or connectivity not only diminishes the functionality of IoT devices, but also may degrade the security of devices in some cases, such as when an IoT device can no longer function without such connectivity (e.g., a home alarm system deactivating if connectivity is lost).

- **Potential That Device Security and Privacy Problems Will Persist:** IoT device security issues are likely to persist because many devices may never receive a software update, either because the manufacturer (or other party in the IoT supply chain, or IoT service provider) may not provide updates or because consumers may not apply the updates that are already available.
    - **Many IoT Devices Will Never Be Fixed:** Deploying software updates that patch critical security vulnerabilities is difficult in general. Many device vendors and manufacturers do not have systems or processes to deploy software updates to thousands of devices, and deploying over-the-network

updates to devices that are operating in consumer homes is difficult, as updates can sometimes interrupt service and sometimes have the potential to "brick" the device, if done improperly. Additionally, some devices may not even be capable of software updates.

  - **Software Updates Address More Than Just Bugs:** Software updates are not simply intended to fix security or privacy bugs. They may also be intended to introduce major new functions, or improve performance and security.
  - **Consumers Are Unlikely to Update IoT Device Software:** Few end users consistently update device software of their own accord; it is best to assume that most end users will never take action on their own to update software.

- **Device Replacement May be an Alternative to Software Updates – for Inexpensive or "Disposable" Devices:** In some cases, replacing a device entirely may be an alternative to software updates. Certain IoT devices may be so inexpensive that updating software may be impractical or not cost-effective.

<u>Recommendations.</u> The BITAG Technical Working Group also has the following *recommendations*:

- **IoT Devices Should Use Best Current Software Practices:**
  - **IoT Devices Should Ship with Reasonably Current Software:** BITAG recommends that IoT devices should ship to customers or retail outlets with reasonably current software that does not contain severe, known vulnerabilities.
  - **IoT Devices Should Have a Mechanism for Automated, Secure Software Updates:** Software bugs should be minimized, but they are inevitable. Thus, it is critical for an IoT device to have a mechanism for automatic, secure software updates. BITAG recommends that manufacturers of IoT devices or IoT service providers should therefore design their devices and systems based on the assumption that new bugs and vulnerabilities will be discovered over time. They should design systems and processes to ensure the automatic update of IoT device software, without requiring or expecting any type of user action or even user opt-in.
  - **IoT Devices Should Use Strong Authentication by Default:** BITAG recommends that IoT devices be secured by default (e.g. password protected) and not use common or easily guessable user names and passwords (e.g., "admin", "password").
  - **IoT Device Configurations Should Be Tested and Hardened:** Some IoT devices allow a user to customize the behavior of the device. BITAG recommends that manufacturers test the security of each device with a range of possible configurations, as opposed to simply the default configuration.

- **IoT Devices Should Follow Security & Cryptography Best Practices:** BITAG recommends that IoT device manufacturers secure communications using Transport Layer Security (TLS) or Lightweight Cryptography (LWC). If devices rely on a public key infrastructure (PKI), then an authorized entity must be able to revoke certificates when they become compromised, and manufacturers should take care to avoid encryption methods, protocols, and key sizes with known weaknesses. Additional encryption best practices include:
    - Encrypt Configuration (Command & Control) Communications By Default
    - Secure Communications To and From IoT Controllers
    - Encrypt Local Storage of Sensitive Data
    - Authenticate Communications, Software Changes, and Requests for Data
    - Use Unique Credentials for Each Device
    - Use Credentials That Can Be Updated
    - Close Unnecessary Ports and Disable Unnecessary Services
    - Use Libraries That Are Actively Maintained and Supported

- **IoT Devices Should Be Restrictive Rather Than Permissive in Communicating:** When possible, devices should not be reachable via inbound connections by default. IoT devices should not rely on the network firewall alone to restrict communication, as some communication between devices within the home may not traverse the firewall.

- **IoT Devices Should Continue to Function if Internet Connectivity is Disrupted:** BITAG recommends that an IoT device should be able to perform its primary function or functions (e.g., a light switch or a thermostat should continue to function with manual controls), even if it is not connected to the Internet because Internet connectivity may be disrupted due to causes ranging from accidental misconfiguration to intentional attack. IoT devices that have implications for user safety should continue to function under disconnected operation to protect the safety of consumers.

- **IoT Devices Should Continue to Function If the Cloud Back-End Fails:** Many services that depend on or use a cloud back-end can continue to function, even if in a degraded or partially functional state, when connectivity to the cloud back-end is interrupted or the service itself fails.

- **IoT Devices Should Support Addressing and Naming Best Practices:** Many IoT devices may remain deployed for a number of years after they are installed. Supporting the latest protocols for addressing and naming will ensure that these devices remain functional for years to come.
    - **IPv6:** BITAG recommends that IoT devices support the most recent version of the Internet Protocol, IPv6.

  - **DNSSEC:** BITAG recommends that IoT devices support the use or validation of DNS Security Extensions (DNSSEC) when domain names are used.

- **IoT Devices Should Ship with a Privacy Policy That is Easy to Find & Understand:** BITAG recommends that IoT devices ship with a privacy policy, but that policy must be easy for a typical user to find and understand.

- **Disclose Rights to Remotely Decrease IoT Device Functionality:** BITAG recommends that if the functionality of an IoT device can be remotely decreased by a third party, such as by the manufacturer or IoT service provider, this possibility should be made clear to the user at the time of purchase.

- **The IoT Device Industry Should Consider an Industry Cybersecurity Program:** BITAG recommends that the IoT device industry or a related consumer electronics group consider the creation of an industry-backed program under which some kind of "Secure IoT Device" logo or notation could be carried on IoT retail packaging. An industry-backed set of best practices seems to be the most pragmatic means of balancing innovation in IoT against the security challenges associated with the fluid nature of cybersecurity, and avoiding the "checklist mentality" that can occur with certification processes.

- **The IoT Supply Chain Should Play Their Part In Addressing IoT Security and Privacy Issues:** End users of IoT devices depend upon the IoT supply chain, from manufacturer to retailer, to protect their security and privacy, and some or all parts of that IoT supply chain play a critical role throughout the entire lifecycle of the product. In addition to other recommendations in this section, BITAG recommends that the IoT supply chain takes the following steps:
  - **Privacy Policy:** Devices should have a privacy policy that is clear and understandable, particularly where a device is sold in conjunction with an ongoing service.
  - **Reset Mechanism:** Devices should have a reset mechanism for IoT devices that clears all configuration for use when a consumer returns or resells the device. The device manufacturers should also provide a mechanism to delete or reset any data that the respective device stores in the cloud.
  - **Bug Reporting System:** Manufacturers should provide a bug reporting system with a well-defined bug submission mechanisms and documented response policy.
  - **Secure Software Supply Chain:** Manufacturers should protect the secure software supply chain to prevent introduction of malware during the manufacturing process; vendors and manufacturers should take appropriate measures to secure their software supply chain.

- **Support IoT Device for Entire Lifespan:** Manufacturers should support an IoT device throughout the course of its lifespan, from design to the time when a device is retired, including transparency about the timespan over which they plan to provide continued support for a device, and what the consumer should expect from the device's function at the end of the device's lifespan.

- **Clear Contact Methods:** Manufacturers should provide clear methods for consumers to determine who they can contact for support and methods to contact consumers to disseminate information about software vulnerabilities or other issues.

- **Report Discovery and Remediation of Vulnerabilities:** Manufacturers should report discovery and remediation of software vulnerabilities that pose security or privacy threats to consumers.

- **Clear Vulnerability Reporting Process:** Manufacturers should provide a vulnerability reporting process with a well-defined, easy-to-locate, and secure vulnerability reporting form, as well as a documented response policy.

Table of Contents

1 Introduction

In the past few years, many of the new devices connected to the Internet have not been personal computers, but rather a variety of devices embedded with Internet connectivity and functions. Examples of such devices include thermostats, smart plugs, and networked cameras. This class of devices has generally been described as the *Internet of Things* (IoT), and it is clear that this new class of device will see strong growth in the coming years, with varying estimates from different sources, but all forecasting many billions of such devices by 2020 [1].

The number and diversity of IoT devices is growing rapidly; these devices offer many new applications for end users, and in the future will offer even more. Many IoT solutions are either already available or are being developed for deployment in the near future, including:

- sensors to better understand patterns of daily life and monitor health
- monitors and controls for home functions, from locks to heating and water systems
- devices and appliances that anticipate a consumer's needs and can take action to address them (e.g., devices that monitor inventory and automatically re-order products for a consumer)

In addition, when coupled with data analysis and machine learning, IoT devices may be able to take more proactive actions, expose interesting data patterns, or make suggestions to end users that may improve their health, environment, finances, and other aspects of their lives.

The emergence of IoT presents opportunities for significant innovation, from smart homes to smart cities. Unfortunately, many IoT devices have shipped with serious security and privacy flaws [2]; Section 3 discusses many recent examples in detail. These flaws put end users that purchase the devices at risk in a number of ways and can affect the Internet access service of both the user of the devices and other users whose traffic runs over the same shared Internet links. The flaws also create broader security and mitigation issues for targets of attacks, Internet Service Providers (ISPs), as well as other service providers —for example search engine services, web-based email, and gaming sites—and importantly introduce new support and mitigation costs (which are typically passed onto end users) [3]. Additional costs may also be imposed on the device makers themselves, who may need to take steps to mitigate these problems.

In many cases, straightforward changes to device development, distribution, and maintenance processes can prevent the distribution of IoT devices that suffer from significant security and privacy issues. BITAG believes that following the guidelines outlined in this report may dramatically improve the security and privacy of IoT devices and minimize the costs associated with the collateral damage that would otherwise affect both end users and ISPs. In addition, unless the IoT device sector—the sector of the industry that manufactures and distributes these devices—improves device security and privacy, consumer backlash may impede the growth of the IoT marketplace and ultimately limit the promise IoT holds for end users.

2 What is The Internet of Things?

The Internet of Things (IoT) comprises devices that function as sensors, actuators, controllers, and activity recorders. These devices typically interact with software running elsewhere on the network, such as on a mobile phone, a general purpose computing device (e.g., a laptop), a machine on the public Internet (e.g., in "the cloud"), or a combination of these. IoT devices often function autonomously, without requiring human intervention.

The term "IoT" has potentially broad scope. IoT can refer to deployments in homes, businesses, manufacturing facilities, transportation industries, and elsewhere. Thus, IoT can refer to much more than simply consumer-oriented devices.

For the purposes of this report, the term IoT is used to refer solely to consumer-oriented devices and their associated local and remote software[1] systems, though some or all of our recommendations may be more broadly applicable. This report is concerned with scenarios where consumers are installing, configuring, and administering devices that they lease or own.

2.1 Scope Limitations

The report does not directly consider devices intended for industrial or business-to-business settings, such as sensors in hotels or airport networks, smart cities, industrial automation, commercial building control, or manufacturing inventory control. In these settings, customers often have the resources and incentives to specify and manage the security and privacy features of the products they purchase. In addition, many of these devices use commercial wireless connections that do not provide full access to and from the Internet. That being said, some of the same issues addressed in this report may be present in those environments as well.

The scope of this report is also limited to IoT devices that either originate or terminate a data flow. More specifically, the report does not focus on devices that pass through traffic that may happen to contain data going to or coming from IoT devices, among other traffic, such as a home gateway, wireless access point, or router.

Additionally, the report focuses only on devices and systems that use the Internet Protocol (IP), whether IPv4 or IPv6 or both. A variety of IoT devices use other transport mechanisms, such as Zigbee 1.0 [4], X10 [5], and so on. These devices cannot be connected to the Internet other than through a device that performs protocol conversion. They operate on an isolated network. However, the recommendations herein still apply to the device that performs the protocol conversion (e.g., home automation hub or gateway).

This report focuses on issues that are specific to devices on a local IP network that can communicate over the Internet. Privacy and security problems that occur on isolated

[1] When BITAG uses the term "software", it is intended to include device firmware, which is a form of software, and all other types of software.

networks that do not have connectivity to the public Internet are out of scope for this report.

2.2 IoT Devices That Users Have Modified

Some devices can have their software updated or replaced with software other than that which the manufacturer intended, in many senses creating a new product. For example, a user may install open-source software on a device, instead of using the vendor-supplied software. The resulting product may be subject to the considerations and recommendations of this report, but in this case the device should be viewed as a distinct product for which the user is responsible.

3 Why IoT Security and Privacy is of Particular Interest

IoT devices face the same types of security and privacy challenges that many conventional end-user devices face. IoT devices, on the other hand, typically offer neither clear controls nor documentation to inform a user about risks introduced when these devices are deployed. Further, studies have shown that relying on the end user for security and privacy decisions is prone to failure [6,7,8].

3.1 Non-technical or uninterested consumers.

End users do not have the technical expertise to evaluate the privacy and security implications of any particular IoT device, or they may lack interest in doing so [9]. Additionally, more often than not, the deployed devices lack automated mechanisms to perform secure updates or enforce security policy [9,10].

3.2 Challenging device discovery and inventory.

Consumers already have difficulty identifying and troubleshooting the devices that are currently connected to their home networks [11]. IoT devices will exacerbate this situation, as consumers connect an increasingly wide variety of devices to their home networks. Users will likely lose track of what devices are connected to the Internet over time, which will make securing them even more challenging. In addition, ISPs will have difficulty helping consumers identify the sources of security problems. Although ISPs may be able to determine that some device on a customer's home network is compromised, they may be unable to identify the specific compromised device, due to technologies such as network address translation (NAT) and other technologies that may obscure the identity of individual devices.

3.3 Effects on Internet access service.

IoT devices compromised by malware (see Sections 4.5 and 5.3) can affect the Internet access service of both the user of such IoT devices and other users whose traffic runs over the same shared Internet links. These devices may also present a threat to the user and other targets of the malware [12]. This malware can be used to launch DDoS attacks [13], send spam, attack other devices on the user's network, or otherwise maliciously interfere with the user's Internet access service.

These problems increase the costs incurred by the ISP, who must spend effort mitigating these attacks, providing help desk support for users who are unable to determine why their Internet access service is behaving poorly or abnormally, and even disabling the Internet access service of users whose devices are performing malicious network activity. The problems also increase costs to the consumer by degrading performance and creating the potential for loss of credentials. Finally, they impose costs on the target of any such attacks and the IoT device manufacturers themselves (or other parts of the IoT supply chain), who may need to take steps to mitigate these problems.

3.4 Effects on other services.

IoT devices that are compromised by malware can become a platform for unwanted traffic, such as spam and denial of service attacks—including reflection and amplification attacks, whereby an attacker sends traffic to a device with the spoofed source address of a victim, causing the device to send large amounts of traffic towards the victim) [14]—which can interfere with a service provider's ability to deliver a service [15]. Compromised devices may also be used to eavesdrop on local network traffic or as "stepping stones" to attack other devices and services on the customer's local network, creating the potential for data leaks. Providers who offer services such as search engines, web-based email, and gaming sites must invest resources to mitigate these attacks. The victims of these attacks will also bear financial and privacy costs. Compromised IoT devices can also occasionally affect the business model of a service provider. One example is the DNSChanger malware, which allowed attackers to insert their own advertisements into victims' webpages [16].

4 Many Devices Do Not Follow Security and Privacy Best Practices

IoT devices have already become a platform for abuse and attacks. Many technologists have uncovered various security and privacy risks associated with IoT devices that are available now [17,18,19,20,21,22,23,24]. Tens of millions more IoT devices will likely be deployed in the next few years, creating the potential to become a large platform for launching attacks—both on other devices in the user's home and on the Internet at large—and for surreptitiously collecting private information about specific end users or groups of users. In addition to the losses that consumers may experience, ISPs may sustain an increase in technical support calls and attack incidences, raising the cost of operations that are passed on to consumers.

Several recent reports have studied the security and privacy characteristics of IoT devices and found that some devices do not abide by rudimentary privacy and security best practices [25,26,27,28,29,30,31]. In some cases, devices have been compromised [32].

Potential issues contributing to this lack of privacy and security best practices include:

4.1 Lack of incentives to develop and deploy updates after the initial sale

For consumer IoT devices sold through retail channels, device vendors may have little incentive to deliver software updates after the initial sale. If the revenue for a device comes solely from the initial sale, then any maintenance of the device erodes that initial revenue, decreasing profit. This structure can encourage planned obsolescence, where vendors prioritize selling new devices over supporting existing ones.

4.2 Difficulty of secure over-the-network software updates

IoT devices may not be designed and configured to receive secure software updates over the network, leading to cumbersome update processes.

4.3 Devices with constrained resources

IoT devices sold in a low-margin consumer environment may be designed with limited hardware resources. As a result, certain basic security measures such as encryption, software signature verification, and secured access control are not feasible. Thus, designs that limit a device's processing and memory capability may preclude running host-based security software or prevent it from being securely upgraded. Section 5.1 discusses this issue in more detail.

4.4 Devices with constrained interfaces

Many types of IoT devices have limited or non-existent user interfaces. Even when a device exposes a user interface via a secondary device (e.g., a smartphone app), its functionality may be minimal. As a result, tasks such as configuring a local firewall or disabling remote services may be impossible. Devices may also lack the capacity to display meaningful error conditions and alerts to those users who may use error information to better protect a device.

4.5 Devices with malware inserted during manufacturing.

Malware can be inserted into devices at time of manufacture or packaging by employees of the manufacturer or others with access to the manufacturing or packaging environment. A compromised device may often appear to be functioning normally, in which case the security or privacy breach may persist until the compromise is detected. Firewalls and network isolation cannot defend against attacks launched by such compromised devices on other devices internal to the isolated network. For known examples of such compromised devices and additional discussion of the effects of malware, see Section 5.3.

4.6 Lack of manufacturer experience with security and privacy

Many IoT device manufacturers (and other parts of the IoT supply chain) have no prior experience designing, developing, or maintaining Internet connected devices or handling consumer data. These manufacturers lack secure development lifecycles, incident response teams, and experience with privacy and security engineering in general.

4.7 Risks due to vulnerable devices

The following examples illustrate the scope and extent of the problems that are possible when IoT devices become vulnerable to attacks on security and privacy. An unauthorized user may be able to:

- **Perform unauthorized surveillance and monitoring.**
    - know whether a specific person is home, what room they occupy, and when they enter the home
    - know what other devices are connected to the home network, and how users are interacting with them
    - remotely activate a microphone or a camera on a device to eavesdrop or spy on someone [33]
    - discover whether a door or garage has recently been opened and closed to determine whether someone is home, to aid in a physical break-in
    - install malware on an IoT camera to access the camera's video feed [34]
- **Gain unauthorized access or control.**
    - turn a thermostat off during winter months to cause water pipes to burst, damaging a home
    - turn lights on or off, such as turning off perimeter lighting to aid in a physical break-in
    - unlock doors to aid in a physical intrusion
    - suppressing an alarm from a door or window sensor
    - repurpose a device for illicit use (e.g., as a Bitcoin miner [35])
- **Induce device or system failures.**
    - activate residential air conditioning systems to create an unexpected surge on a power grid in an attempt to create brownout or blackout conditions
    - subvert health data collection sensors to modify health data such as blood pressure, blood sugar, or weight information that may be transmitted to a health monitoring service or medical device (such as an insulin pump)

  - emulate the device's management software so that it appears to be operating normally, but instead disable important functionality or make other operating changes, resulting in equipment or hardware systems failing in important ways [36]
  - prevent a thermostat from controlling building heating or cooling, resulting in extreme heat or cold

- **Disturb or harass users.**
  - remotely activate a speaker and engage in verbal threats or harassment
  - activate smoke or other security alarms

All of these scenarios create serious privacy and security risks for end users and for the Internet as a whole. Some end user security and privacy risks could also enable a new form of digital harassment. In extreme cases, subversion of health data collection could lead to injury or death. For widely deployed devices, security risks can be compounded across hundreds or thousands of devices to create distributed attacks on critical infrastructure.

Security and privacy problems with IoT devices could ultimately constrain the future growth of the IoT sector. A small number of high-profile incidents may curtail demand for IoT devices or otherwise constrain the growth and potential of IoT. Thus, it is critical these issues be addressed to support the long-term health, vibrancy, and growth of the IoT marketplace.

5 Observations on IoT Security and Privacy Issues

It is unrealistic to expect manufacturers to create software products that are bug-free; all software has bugs, and producing software free of such flaws remains an unsolved problem. As a result, some IoT devices ship "from the factory" with software that either is outdated or becomes outdated over time. This is not a matter of shipping buggy software, which is arguably unavoidable; rather, the concern is that manufacturers may ship devices with obsolete software that contains many significant, documented security vulnerabilities, some of which may be immediately exploitable when the device is first connected to the Internet [37].

Other IoT devices may ship with more current software that contains no major known security vulnerabilities at the time of shipping. Even in these cases, vulnerabilities may be discovered in the future, which may make a device less secure over time unless it has a mechanism to subsequently update its software. Unfortunately, many IoT devices lack secure, automated software update mechanisms that can patch vulnerabilities once devices have been shipped and deployed.[2] Without widespread adoption of secure, automated software update methods, the number of insecure and compromised IoT devices are likely to increase dramatically in the coming years.

IoT devices that ship with security and privacy issues or that develop them over time can create a new population of devices that can be used by malicious hackers, for example to conduct reflection and amplification attacks [41]. Not only do these devices pose risks for the device owners themselves, but they can also be exploited to abuse other parties. The security of IoT devices is thus of interest not only to the manufacturers (and other parts of the IoT supply chain) and customers of IoT devices, but also to the Internet at large.

Finally, although this report provides many examples of IoT devices that either have or previously have had security or privacy issues, in many cases the examples highlighted here may have been addressed by relevant parties prior to publication of this report.

5.1 Insecure Network Communications

IoT devices in general can be quite resource-constrained, lacking the computational power and bandwidth of more conventional computing devices such as mobile phones, laptops, and desktop computers, as discussed in Section 4. As a result, many of the security functions designed for more general-purpose computing devices are more difficult to implement on IoT devices. For example, public key encryption—which underlies modern secure communications based on Transport Layer Security (TLS) [42] and Datagram Transport Layer Security (DTLS)[43]—may be difficult to implement on certain resource-constrained IoT devices. For instance, Arduino and Raspberry Pi devices can take many seconds to perform an asymmetric encryption or decryption operation [44,45].

Beyond the inherent limitations of IoT devices and the IoT platforms on which they run, a number of security flaws have been identified in the field, including unencrypted communications, data leaks from IoT devices, and negative effects to the network where the IoT device is attached [25,26,27,46,47].

For example, certain TLS server implementations are vulnerable to so-called "downgrade" attacks, whereby an attacker can force a server to use an older version of the TLS protocol, which may have known security issues, such as vulnerabilities to man-in-the-middle attacks. In these scenarios, the communication between an IoT device and the cloud-hosted service that supports it could be compromised.

▪ Unauthenticated Communications

Some IoT devices provide automatic software updates. Without authentication and encryption, however, this approach is insufficient, since the update mechanism could be compromised or disabled [48]. The update mechanism itself and any associated command

[2] The IoT camera cited in the recent large-scale DDoS against the krebsonsecurity.com website was made by Dahua Security. That company issued an advisory [38] and suggested device owners download and update their firmware [39], as well as take additional steps to secure their devices (not done by default by Dahua Security) [40].

and control traffic should be authenticated and encrypted, and the integrity of communications between the device and other endpoints should be protected.[3] Unfortunately, many IoT devices do not use authentication in the course of communicating. For example, the Lightwave RF Smart hub sent traffic to a remote server on the network each time it restarted and subsequently every fifteen minutes when checking for software updates [29]. If the connection is not secured, it is not difficult for an attacker with network access to conduct a man-in-the-middle attack.

- **Unencrypted Communications**

Many IoT devices send some or all data in cleartext, rather than in an encrypted form. This means that the data can "leak out" and be observed by other devices or by an attacker.

As a result, some IoT devices leak user information (such as to an observer of the network traffic), and this can identify the IoT device(s) that are being used, as well as reveal current user activity and behavior [17].[4] For example:

- A digital photo frame carries the user's email address in cleartext during when synchronizing photos, and current user activity is also shown in the clear [10].
- A web camera sends video files in cleartext [29].
- An audio personal assistant carries user audio commands, sensor readings, and user email addresses in cleartext [29].
- A thermostat carries local weather data with precise user location information in cleartext, and is clearly identifiable as a specific brand's thermostat based on the ports utilized.[5]
- An IoT device hub has a cleartext traffic profile which is so regular and specific that the device hub can be identified merely by fingerprinting the pattern of cleartext traffic [29].
- Some IoT-enabled pacemakers use unencrypted communication channels [52].

Sending traffic in cleartext is not the recommended model for new deployments and creates issues where personal or other information leaks over a local network, or over the Internet. On this issue, for example, the Internet Architecture Board (IAB) has recently stated, "The IAB urges protocol designers to design for confidential operation by default…[w]e strongly encourage developers to include encryption in their implementations, and to make them encrypted by default."[53]

[3] Message integrity allows an endpoint that receives a message to verify that the message has not been modified in transit between the sender and receiver.

[4] It is not necessarily negative that a device can be identified or that user activity and normal behavior can be identified. There may be legitimate security reasons for this that provide benefits to end users and improve security and privacy generally.

[5] In a recent case involving the Nest thermostat, this bug was fixed after the researchers reported it to Nest. The Nest thermostat can do automatic software updates [49,50]. Unfortunately, automated updates have themselves introduced a different set of issues [51].

- **Lack of Mutual Authentication and Authorization**

Many attacks originate from behind a firewall at a network border, in the home or elsewhere. As a result, communications behind a firewall should not necessarily be considered trustworthy. Thus, a device needs to establish trust between devices, regardless of whether it is on a local area network or the Internet; it should assume that other devices are untrusted by default and should be explicitly authenticated and authorized. A device that allows an unknown or unauthorized party to change its code or configuration, or to access its data, is a threat; the device can reveal that its owner is present or absent, facilitate the installation or operation of malware, or cause its core IoT function to be fundamentally compromised.

Fortunately, in contrast to general-purpose computing devices such as laptops, which may communicate with many Internet destinations, IoT devices often communicate with a small number of well-defined destinations. For example, a device may communicate regularly only with a control or update server that has a well-known DNS name or IP address; substantial communication with other destinations may be cause for concern.

- **Lack of Network Isolation**

In addition to the security and privacy risks that IoT devices introduce outside of the home network where the IoT device itself is installed (see Section 4), these devices also create new risks and are susceptible to attacks *inside* the home. Because many home networks do not, by default, isolate different parts of the network from each other, a network-connected device may be able to observe or exchange traffic with other devices on the same home network, thus making it possible for one device to observe or affect the behavior of unrelated devices.

Although it is common practice to use firewalls to isolate devices on a network from one another, firewalls alone cannot always defend against device compromises or data leaks, and they cannot defend against malware on devices already inside the home network. A typical home network today offers little or no isolation between devices. Section 6 discusses firewalls and other network isolation mechanisms in more detail.

This lack of isolation poses a threat to security and privacy of all devices on the network, both as a result of specific manufacturer actions (or actions by other parties in the IoT supply chain) and as a consequence of device compromise [27,54,55]. Specifically, an attacker may be able to collect intelligence or personal information from other devices on the same network. Typically, each device on a home network can see the traffic from other devices that are on the same network. If devices transmit traffic in cleartext, one device may be able to discover the details of another device's activity. Recent work has shown that even the ability to observe more "coarse" details, such as DNS lookups and changes in traffic volumes, may reveal information about device activity and user behavior [56]. An attacker that compromises one device may thus be able to infer significant information about an end user, such as the times of entry and exit from the home via compromised door sensors or audio and video recordings from microphones and video cameras embedded in IoT devices. The security design of many home wireless networks enable "stepping stone" attacks [57], whereby an attacker may compromise one vulnerable IoT device and use that compromise as a mechanism to gain access to other connected devices from the inside of the network. Examples include:

- A smartwatch product included a functioning DNS server that external attackers could use to attack other devices on the network that the smartwatch was connected to. The same product had a vulnerability that allowed local network traffic to be viewed by external network attackers [27].
- A smart lightbulb could be tricked into sending wireless network credentials which external attackers could then use to control the lights and view local network traffic [54].
- Some device manufacturers and ISPs have exposed insecure remote management interfaces of millions of devices and customer premises equipment (e.g., modems, home routers) that all shared the same known private key, exposing these devices to both passive and active man-in-the-middle attacks [55].
- Vulnerabilities in a certain model of VoIP phone would allow a local network attacker to provide malicious firmware upgrades to the phone [58].
- A manufacturer of Wi-Fi security cameras designed their products with peer-to-peer networking software that would "punch" multiple holes through the local network firewall and could not be easily deactivated. This software allowed attackers to not only compromise the camera itself from a wide variety of endpoints, but also launch attacks on other devices on the local network [31].

5.2 Data Leaks

Installing IoT devices in the home creates the potential for these devices to leak private user data, both from the cloud (where data is stored) and between IoT devices themselves.

- **Leaks From the Cloud**

Much of the data that IoT devices collect is currently stored in cloud services outside the home; these cloud services could experience a data breach due to an external attack or an insider threat.

Additionally, if users rely on weak authentication or encryption methods for these cloud-hosted services, user data may also be compromised.

A few examples include:

- A web application associated with a teddy bear (which contains a small camera on its nose) contained a security vulnerability that left children's identities exposed [59].
- The doll sent encrypted chats between the doll and the cloud-hosted servers using a version of TLS that was vulnerable to a downgrade attack, making it possible to eavesdrop on children's recordings [60].

- A data breach at a children's toymaker exposed the personal data of more than six million children [61].
- Weaknesses in the configuration of the Wi-Fi access point on a motor vehicles resulted in many vehicle locations being tracked on websites that harvest the names of Wi-Fi access points and their locations [62].
- A car maker's system sent fuel economy statistics, precise geographic coordinates, speed, direction, and destination in cleartext to a central server [63].

Many other examples of data breaches from these devices exist [25,28,30,32,64,65,66,67]. Data leaks from the cloud are not new or specific to IoT devices, yet the prevalence of data leak vulnerabilities in cloud-hosted services is especially problematic for consumer IoT devices, which are not only increasingly pervasive but also increasingly collect personal and private data.

- **Leaks From and Between Devices**

IoT devices from a variety of different manufacturers, running many different software applications, may all reside on the same local area network. Although standard Wi-Fi encryption techniques can protect the confidentiality of data transmissions on the local area network, encryption alone does not ensure user privacy.

In some cases, devices on the same network or on neighboring networks may be able to observe data from other devices. For example, a device may "leak" data to nearby devices or users (either on the same local area network, Wi-Fi network, or simply nearby). Even with Wi-Fi encryption, one device can still observe the presence of other devices on the same local area network, and the other device's hardware addresses—which can often reveal the type of device—are also typically visible in cleartext. This level of visibility could, for example, make it possible for software on a digital photo frame to monitor a user's interactions with other devices on the same network.

Data that leaks from one device to another may include information such as the names of people in a home, the precise geographic location of a home, or even the products that a consumer purchases. For example, a recent study discovered that a thermostat was leaking precise geographic information from the home [17]. In another recent study, researchers were able to determine a user's ATM PIN based on accelerometer data leaked over Bluetooth from a fitness-tracking device [68].

5.3 Susceptibility to Malware Infection and Other Abuse

Malware, which is malicious software installed on a user device that typically disrupts operations, gains unauthorized access, or launches attacks, can infect IoT devices through a variety of mechanisms. As well, other forms of abuse can occur. Some examples include:

- The manufacturer may not adequately secure the software supply chain [69] and thereby allow malware to be placed on the initially-shipped software of the IoT device [34], as noted in Section 4.5.

- Devices may ship with out-of-date software that contains known vulnerabilities. When a user connects the device to the network, the device immediately becomes a target for attackers. Past studies demonstrate that the "survival time" (i.e., the time that a device is connected to the network before it is infected) can in some cases be less than ten minutes [70].[6] If a device ships with out-of-date software and does not immediately check for software updates, it risks becoming infected immediately.

- The software update mechanisms may not include authentication of software loads to ensure the software is from a trusted source. Through social engineering, the user can be influenced or induced into loading compromised software onto an IoT device.

- The software may include command-line capabilities or Application Programming Interfaces (APIs) that can be exploited (with or without user involvement) to load malware onto an IoT device.

- The device has unnecessary ports left open and unsecured, such as telnet. These unnecessary ports have been used to compromise a device, for example instructing the device to access a destination in order to download malware [71,72,73]. Unnecessary ports can also be used in amplification attacks.

- The device uses weak default authentication, such as common or easily guessable user names and passwords (e.g., "admin", "password") [74]. In addition, authentication for remote access may not have been secured, enabling others who are not physically present in the home to login to the device and install malware onto it [13,75,76,77,78].

5.4 Potential for Interruption of Service

One important aspect of IoT device security is service availability in the face of device failure and attack. The potential loss of availability or connectivity not only diminishes the functionality of IoT devices, but also may degrade the security of devices in some cases such as when an IoT device can no longer function without such connectivity (e.g. a home alarm system deactivating if connectivity is lost). An IoT device can experience service interruption in several ways.

- **Loss of support from a cloud-hosted application.** If the device depends on communication with a cloud service, the device may fail to function when it loses connectivity with the cloud service. Such disconnection might occur for a variety of reasons, including interruption of Internet connectivity, bugs in the cloud software service, a vendor or manufacturer going out of business, or a consumer's decision to discontinue a service subscription.

[6] The presence of a firewall is not necessarily a defense against this sort of compromise. Section 6 discusses firewalls and other network isolation mechanisms in more detail.

- **Loss of connectivity to the network.** Connectivity within a home network may be interrupted, perhaps due to an unplugged power cable, radio interference with Wi-Fi, or a firewall deciding to restrict access, for example.
- **Damage to the device.** A device could become physically damaged, or its software could become corrupted or otherwise inoperable (sometimes referred to as "bricking" a device).

A "bricked" device—one that is physically or logically damaged—may be unrecoverable, while a device that depends on communication with a cloud-hosted service may become operable again when communication is restored.

Outages to certain services can damage property and place users in danger. For example, a software bug in an IoT thermostat resulted in inoperable home heating systems, and (as a result) frozen pipes in homes [51]. Malfunctioning heating and cooling systems can result in fatalities. When IoT devices are responsible for everything from personal health to home security, the stakes for user safety are high.

5.5 Potential That Device Security and Privacy Problems Will Persist

This section briefly discusses why the security issues outlined in the previous section are likely to persist. One could expect that many such IoT devices may never receive a software update, either because the manufacturer (or other party in the IoT supply chain, or IoT service provider) may not provide updates or because consumers may not apply the updates that are already available. There are many examples of this with similar types of devices [79,80,81,82].

- **Many IoT Devices Will Never Be Fixed**

Deploying software updates that patch critical security vulnerabilities is difficult in general, yet IoT devices pose unique challenges. First, many device vendors and manufacturers do not have systems or processes to deploy software updates to thousands of devices (or more). Second, deploying over-the-network updates to devices that are operating in consumer homes is difficult, as updates can sometimes interrupt service and sometimes have the potential to "brick" the device, if done improperly. Additionally, some devices may not even be capable of software updates [83].

Three software update approaches have emerged in the consumer electronics industry, two of which rely on users to take action (a fundamental flaw) while the third is automatic with no user action required. The effectiveness of each of these varies in practice. These approaches are as follows:

- **User-initiated software updates.** This approach requires the local administrator of the device to manually initiate a check and installation for any software updates to a device. An example of this model is in the typical retail home gateway or router device market. Some of those devices require the user to download a new software image from the manufacturer's website, then access a local device administration webpage, find the interface for software upgrades and upload a file. This process is not only time-consuming but can be daunting for non-technical or casual users for which a device may still be working “well enough.”

- **Automated software update checks, with user approval.** These devices periodically check for new software updates. When an update is available, the device presents the user with a prompt that asks for permission to proceed with the update. Smart TV and console gaming devices often use this approach. In these scenarios, applying any particular software update may take several minutes—or longer—which is why the user is presented with the option of deferring installation.

- **Fully automated software updates.** Some devices will periodically check to see if new software is available; if it is, they will download the software and install it without user intervention [84,85]. In some cases, the device may apply the update at a particular time of day, such as late at night or when there has been no activity pertaining to the device for some period of time, to minimize user disruption. Unfortunately, automated software updates can also pose challenges for some users who have data caps (where applicable), and when the updates themselves introduce new bugs [51].

The common approaches for software updates are either user-initiated or user-approved, both of which tend to lead to relatively low update rates [86]. As a result, millions of Customer Owned And Maintained (COAM) home gateways will likely never receive a software update. For example, some models of NetGear home gateway shipped with a software bug that caused these devices to randomly flood ISP DNS servers with thousands of DNS requests per second, adding up to millions per day, or a flood of NTP queries to NTP servers [87,88,89,90]. While this specific software bug has been reported for many years, network operators nevertheless still observe these devices running older software and misbehaving on the network, inadvertently performing DDoS attacks due to software bugs.

▪ Software Updates Address More Than Just Bugs

It is also worth bearing in mind that software updates are not simply intended to fix security or privacy bugs. They may also be intended to introduce major new functions. In addition, they may be more generally related to performance and security, such as support or bug fixes related to IPv6 addressing, DNS Security Extensions (DNSSEC) validation, and TCP buffer control (e.g., “buffer bloat”) or Active Queue Management (AQM).

▪ Consumers Are Unlikely to Update IoT Device Software

Few end users consistently update device software of their own accord unless they are constantly and obtrusively reminded to do so by the device’s graphical user interface (GUI) (i.e., a regular pop-up window on a PC, a counter in a mobile app store, a bouncing application icon, etc.), a lesson understood well in the discipline of human-computer interaction [86]. Other recent work suggests that users forego applying software updates on both fixed and mobile devices for a variety of reasons, ranging from the disruption of their work cycle to the data costs associated with software updates [86].

Although no in-depth studies on user software updating behavior have been undertaken for IoT devices, the state of affairs is likely worse than for conventional, or non-IoT, devices. Adding to users' already risky behavior with respect to software updates, many IoT devices lack a GUI or other indicator that new software is available or necessary. Additionally, the proliferation of devices—both in number and in diversity—make tracking software updates an unwieldy task for the typical Internet consumer.

Thus, for IoT devices, it is best to assume that most end users will never take action on their own to update the software on the device.

5.6 Device Replacement May Be An Alternative to Software Updates

In some cases, replacing a device entirely may be an alternative to software updates. Certain IoT devices may be so inexpensive that updating software may be impractical or not cost-effective. For example, perhaps a charging adapter that costs $0.99 has some limited IoT function. At that unit cost, updating a device may not be economical; rather, it may make more sense to recycle the device and purchase a replacement. However, this approach requires the following elements to provide a secure alternative to software updates:

- A way to identify when one or more accumulated vulnerabilities in a device have compromised it to the point that it should be replaced.
- A way to disable communication with the device once it is determined to be vulnerable. Examples of potential methods include remotely disabling the device from the network, or blocking access to the device from a home gateway.
- A way to notify users that communication with the device has been disabled.

Even in these cases, of course, users may be reluctant to stop using a device as long as it continues to function in part. As long as the device's ability to communicate has been disabled, however, continued use should not present a security vulnerability.

6 A Possible Role for In-Home Network Technology

Device manufacturers securing their devices by default constitutes an important step for improving IoT security and privacy, but it is by no means sufficient. Even IoT devices that are not infected with malware may still eavesdrop on other home network traffic (e.g., via manufacturer-installed or third-party software), compromising user privacy. A home is often considered a firewalled or isolated environment, and multiple unrelated IoT devices will typically have unrestricted access behind this firewall. Furthermore, as mentioned in Section 3.4 and 5.1, a single insecure or compromised device in the home network may lead to stepping-stone attacks, so "defense in depth" [91] is critical.

Recent studies and reports have suggested that, in the future, there may be some role for a home network appliance to control and manage the traffic that IoT devices exchange with each other and with the rest of the Internet [92]. Possible capabilities for such a network device include:

- Automatic discovery and inventory of in-home Internet connected devices [93].
- Mechanisms for presenting the user with clear information about (1) what data the device is sending to the rest of the Internet and (2) what other devices in the home the device is talking to, as has been done in the past for smartphones and browsers [94,95].
- Mechanisms that provide the user with simple ways to prevent or disable communication of a single device with other IoT devices on the home network, or with storage servers in the cloud, *without impairing the primary functionality of the device.* One recent study was able to achieve this with two example IoT devices, a Philips Hue lightbulb and a Nest thermostat [92].

Network technology to improve security and privacy may ultimately take one of several forms. A home network gateway, either separate (e.g., an IoT hub or separate home router) or integrated with ISP-provided equipment, could perform measurements within the network that help users understand the complex data flows both between IoT devices in the home and between these devices and third-party sites and services outside of the home. In this sense, network technology in the home that monitors device traffic may ultimately help improve the *transparency* of the behavior of these IoT devices.

There is some conflict between monitoring and managing IoT traffic by a hub and the end-to-end security of the traffic itself. It is worth noting that even if network traffic to and from these devices is encrypted end-to-end, certain characteristics, such as the other devices and locations that any particular device is communicating with, will still be evident from this traffic. Standardization to allow cooperative traffic classification and protection with such an IoT hub would allow the device to be a recognized and authenticated part of the ecosystem, providing that management with fine-grained control available to the traffic originator on an opt-in basis.

In addition to simply helping visualize these traffic flows, such a gateway could enforce *reasonable default* settings to improve the security and privacy of the connected IoT devices. For example, recent research suggests that a home network firewall can prevent certain devices from exfiltrating logs and other information to third-party cloud providers without crippling the functionality of the device itself [92]. An open question involves identifying reasonable default firewall settings that could be installed at such a gateway to improve security and privacy. Given that such a home network firewall might instigate a "privacy arms race" (e.g., one could imagine a device manufacturer not providing security updates to a user who blocks the device's tracking capabilities), one aspect of device certification for manufacturers and vendors may ultimately involve ensuring that consumers retain informed *choice* as to how these devices communicate with each other and with third-party sites and services.

Finally, interaction between IoT devices may require more complex mediation. For example, while a user may not generally desire certain devices communicating or interacting with one another, there may be specific use cases that permit communication or interaction between devices for specific tasks. As one possible example, consider a scenario where a user might want to automatically dim the lights when watching a movie in the home. In this case, the application might involve mediated communication between a streaming device (e.g., a Roku or Apple TV) and the smart plugs and switches (e.g., a Belkin WeMo switch). On the other hand, in general, a user may not want these devices to interact, or even to observe each other's traffic. Thus, the network gateway, coupled with the appropriate user interface, may ultimately provide better opportunities for this type of complex mediated interaction.

Recent reports suggest that many of these goals are likely within reach. For example, researchers used a home network firewall to prevent a Nest thermostat from sending its status logs to the cloud, without impairing the device itself [92]. Because the typical user is unlikely to configure firewall rules, however, such firewalling functions must be more usable—and, if possible, automated—before they can be considered practical.

7 Recommendations

This section of the report presents recommendations of the BITAG Technical Working Group (TWG). Although earlier sections of this report have discussed the potential of longer-term, forward-looking solutions (e.g., the role of in-home network technology to mitigate device insecurity), this section focuses on recommendations that BITAG believes are actionable in the short term using existing technology.

7.1 IoT Devices Should Use Best Current Software Practices

- **IoT Devices Should Ship with Reasonably Current Software**

  BITAG recommends that IoT devices should ship to customers or retail outlets with reasonably current software that does not contain severe, known vulnerabilities. However, software bugs are somewhat of a "fact of life" and it is not uncommon for new vulnerabilities to be discovered while devices are on the shelf. Hence it is critical for an IoT device to have a mechanism by which devices receive automatic, secure software updates (see next bullet).

- **IoT Devices Should Have a Mechanism for Automated, Secure Software Updates**

  Software bugs should be minimized, but—as noted above—they are inevitable. Thus, it is critical for an IoT device to have a mechanism for automatic, secure software updates, as discussed in Section 5.5.

  BITAG recommends that manufacturers of IoT devices or IoT service providers should therefore design their devices and systems based on the assumption that new bugs and vulnerabilities will be discovered over time. They should design systems and processes to ensure the automatic update of IoT device software, without requiring or expecting any type of user action or even user opt-in.

Although such updates should be automatic and mandatory for end users, if for some reason the update system must allow for a choice of either opt-out or opt-in, then based on human-computer interaction studies, any such system should be opt-out so that updates will occur automatically by default and without any user intervention, user approval, or other end user action. The ability for a user to configure the nature of software updates may be important to some end-users, such as those running devices in resource-constrained settings (e.g., satellite connections, or other places where data costs are high).

In some cases, in-home network devices might interact with consumers to raise periodic alerts to facilitate meaningfully informed decision-making (e.g., polling the user with questions they can understand about how they want devices to interact). Incorporating this type of function requires extreme care in design, to ensure that these alerts to the user are meaningful and that the volume of updates is not overwhelming. This sort of functionality can be complicated to implement reliably.

- **IoT Devices Should Use Strong Authentication by Default**

  BITAG recommends that IoT devices be secured by default (e.g. password protected) and not use common or easily guessable user names and passwords (e.g., "admin", "password"). Finally, authentication for remote access should be secured, as it potentially allows others who are not physically present in the home to monitor and control aspects within the home (e.g., changing climate controls, monitoring user activity). Authentication credentials should be unique to each device.

  Possible default authentication methods that satisfy these criteria include: (1) shipping each device with a fixed default password but requiring the user to change it as part of the installation process (i.e., before the device will function); and (2) shipping each device with a unique password for each unit and printing the password on a label that is affixed to the device.

- **IoT Device Configurations Should Be Tested and Hardened**

  Some IoT devices allow a user to customize the behavior of the device. BITAG recommends that manufacturers test the security of each device with a range of possible configurations, as opposed to simply the default configuration. A device's interface should prevent—or at least actively discourage—users from configuring the device in a way that makes it less secure.

7.2 IoT Devices Should Follow Security & Cryptography Best Practices

BITAG recommends that IoT device manufacturers secure communications using Transport Layer Security (TLS) or Lightweight Cryptography (LWC) [96,97,98]. Some devices can perform symmetric key encryption in near-real time. In addition, Lightweight Cryptography (LWC) provides additional options for securing traffic to and from resource-constrained devices. If devices rely on a public key infrastructure (PKI), then an authorized entity must be able to revoke certificates when they become compromised, as web browsers and PC operating systems do [99,100,101,102,103,104,105]. Cloud services can strengthen the integrity of certificates issued by certificate authorities through, for example, participating in Certificate Transparency [106]. Finally, manufacturers should take care to avoid encryption methods, protocols, and key sizes with known weaknesses.

Vendors who rely on cloud-hosted support for IoT devices should configure their servers to follow best practices, such as configuring the TLS implementation to only accept the latest TLS protocol versions.

- **Encrypt Configuration (Command & Control) Communications By Default**

  As explained in Section 5.1, using unauthenticated or cleartext communication for managing a device poses a significant security risk. BITAG recommends that all communication for device management take place over an authenticated and secured channel.

- **Secure Communications To and From IoT Controllers**

  If IoT devices use a centralized controller to facilitate over-the-Internet communication with a cloud service, then BITAG recommends this communications channel be secured in both directions.

- **Encrypt Local Storage of Sensitive Data**

  BITAG recommends that any sensitive or confidential data (e.g., private key, pre-shared key, user or facility information) reside in encrypted storage.

- **Authenticate Communications, Software Changes, and Requests for Data**

  BITAG recommends that IoT devices authenticate the endpoints they communicate with. Authenticating communication entails verifying the endpoint's identity, which in turn also involves verifying that the certificate the endpoint is using is signed by a certificate authority that the device trusts and that has not been revoked.

- **Use Unique Credentials for Each Device**

  BITAG recommends that each device have unique credentials. If a device uses public-key cryptography (e.g., to sign messages, exchange a session key, or authenticate itself) each device should have a unique, verifiable certificate. If a device is using symmetric key cryptography, pairs of endpoints should never share the symmetric key with other parties.

- **Use Credentials That Can Be Updated**

  BITAG recommends that device manufacturers support a secure mechanism by which the credentials used by a device can be updated. However, implementing this recommendation securely requires particular care, since an incorrect implementation may itself introduce a new attack vector.

- **Close Unnecessary Ports and Disable Unnecessary Services**

  BITAG recommends that device manufacturers close unnecessary ports, such as telnet, as unnecessary ports may be unsecured or can otherwise become compromised [107]. Devices should close or disable administrative interfaces and functions that are not being used. Devices should also not ship with drivers that the device is not using.

- **Use Libraries That Are Actively Maintained and Supported**

  Many of the recommendations in this report require implementing secure communications channels. Yet, home-grown implementations of cryptographic protocols and secure communications channels can themselves introduce vulnerabilities. BITAG recommends that, when implementing the recommendations in this report, device manufacturers use libraries and frameworks that are actively supported and maintained whenever possible.

7.3 IoT Devices Should Be Restrictive Rather Than Permissive in Communicating

BITAG recommends that IoT devices communicate only with trusted endpoints. When possible, devices should not be reachable via inbound connections by default. IoT devices should not rely on the network firewall alone to restrict communication, as some communication between devices within the home may not necessarily traverse the firewall.

Note that a BITAG recommendation to restrict the *configuration* of IoT device communications should not come at the cost of an open ecosystem. A user should be able to configure communications between arbitrary IoT devices, and devices that trust one another should be allowed to communicate. Secure communications can bootstrap restricted trust lists that reflect the set of devices with which any given device expects to communicate. These inter-device communications should only be permitted through trusted mechanisms and secure communication channels.

7.4 IoT Devices Should Continue to Function if Internet Connectivity is Disrupted

BITAG recommends that an IoT device should be able to perform its primary function or functions (for example, a light switch or a thermostat should continue to function with manual controls), even if it is not connected to the Internet. This is because Internet connectivity may be disrupted due to causes ranging from accidental misconfiguration or intentional attack (e.g., a denial of service attack); device function should be robust in the face of these types of connectivity disruptions.

IoT devices that have implications for user safety should continue to function under disconnected operation to protect the safety of consumers. In these cases, the device or backend system should notify the user about the failure.

When possible, device manufacturers should make it easy for users to disable or block (e.g., with a firewall) various network traffic without hampering the device's primary function.

7.5 IoT Devices Should Continue to Function If the Cloud Back-End Fails

Many services that depend on or use a cloud back-end can continue to function, even if in a degraded or partially-functional state, when connectivity to the cloud back-end is interrupted or the service itself fails. For example, a thermostat whose setting can be altered via a cloud service should in the worst case continue to operate using either last-known or default settings. A cloud-hosted home security camera should be accessible from within the home, even when Internet connectivity fails.

7.6 IoT Devices Should Support Addressing and Naming Best Practices

Many IoT devices may remain deployed for many years after they are installed. As a result, IoT devices should support relatively recent, though current, best practices for IP addressing and the use of the Doman Name System (DNS). Supporting the latest protocols for addressing and naming will ensure that these devices remain functional for years to come, that they perform well, and that they can support important DNS-based security functionality.

- **IPv6**

  BITAG recommends that IoT devices support the most recent version of the Internet Protocol, IPv6.

- **DNSSEC**

  BITAG recommends that IoT devices support the use or validation of DNS Security Extensions (DNSSEC) when domain names are used. For example, if an IoT device communicates with a cloud service using the example.com domain, then the cloud provider should be able to sign the domain, and the IoT device should be able to validate that signature (or ensure that its upstream DNS resolver has done so and indicated this in a DNS response).

7.7 IoT Devices Should Ship with a Privacy Policy That is Easy to Find & Understand

BITAG recommends that IoT devices ship with a privacy policy, but that policy must be easy for a typical user to find and understand.

7.8 Disclose Rights to Remotely Decrease IoT Device Functionality

BITAG recommends that if the functionality of an IoT device can be remotely decreased by a third party, such as by the manufacturer or IoT service provider, this possibility should be made clear to the user at the time of purchase.

7.9 The IoT Device Industry Should Consider an Industry Cybersecurity Program

BITAG recommends that the IoT device industry or a related consumer electronics group consider the creation of an industry-backed program under which some kind of "Secure IoT Device" logo or notation could be carried on IoT retail packaging. Such a program may be analogous to the way that the Wi-Fi Alliance or other groups validate devices are compliant with various standards and/or best practices.

An industry-backed set of best practices seems to be the most pragmatic means of balancing the innovation in IoT against the security challenges associated with the fluid nature of cybersecurity, and avoiding the checklist mentality that can occur with certification processes.

7.10 The IoT Supply Chain Should Play Their Part In Addressing IoT Security and Privacy Issues

In today's factory to retail supply chain, it is often difficult to define the roles that each party plays over time. As such, they are defined here simply as the "IoT supply chain". End users of IoT devices and others depend upon the IoT supply chain to protect their security and privacy, and some or all parts of that IoT supply chain play a critical role throughout the entire lifecycle of the product. In addition to other recommendations in this section, BITAG recommends that the IoT supply chain takes the following steps:

- Devices should have a **privacy policy** that is clear and understandable, particularly where a device is sold in conjunction with an ongoing service.
- Devices should have a **reset mechanism** for IoT devices that clears all configuration for use when a consumer returns or resells the device. The device manufacturers should also provide a mechanism to delete or reset any data that the respective device stores in the cloud.
- Manufacturers should provide a **bug reporting system** with a well-defined bug submission mechanisms and documented response policy.
- Manufacturers should protect the **secure software supply chain** to prevent introduction of malware during the manufacturing process; vendors and manufacturers should take appropriate measures to secure their software supply chain.
- Manufacturers should **support for an IoT device throughout the course of its lifespan**, from design to the time when a device is retired, including transparency about the timespan over which they plan to provide continued support for a device, and what the consumer should expect from the device's function at the end of the device's lifespan.
- Manufacturers should provide **clear methods for consumers to determine who they can contact for support** and **methods to contact consumers** to disseminate information about software vulnerabilities or other issues.

- Manufacturers should **report discovery and remediation of software vulnerabilities** that pose security or privacy threats to consumers.

- Manufacturers should provide a **vulnerability reporting process** with a well-defined, easy-to-locate, and secure vulnerability reporting form, as well as a documented response policy. Manufacturers should consider compliance with ISO 30111 [108], a standard for vulnerability report handling.

8 Other Groups Focused on This Issue

While the BITAG has a unique take on this issue it is worth noting that several other groups are also focused on various aspects of this as well. Those groups include:

- Internet Protocol for Smart Objects Alliance (IPSO) [109]
- Institute of Electrical and Electronics Engineers (IEEE) [110]
- National Institutes of Standards and Technology (NIST) [111]
- Internet Engineering Task Force [112]
  - LWIG (Light-Weight Implementation Guidance) [113]
  - 6Lo (IPv6 over Networks of Resource-constrained Nodes) [114]
  - 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e) [115]
  - ROLL (Routing Over Low power and Lossy networks) [116]
  - CoRE (Constrained RESTful Environments) [117]
  - DICE (DTLS in Constrained Environments) [118]
  - ACE (Authentication and Authorization for Constrained Environments) [119]
  - COSE (CBOR Object Signing and Encryption) [120]
  - 6lowpan IPv6 over Low power WPAN (closed) [121]
- GSMA: Connected Living [122]
- IRTF: Internet Research Task Force [123]
  - T2TRG: Thing-to-Thing Research Group [124]
- W3C: Worldwide Web Consortium [125]
  - WoT: Web of Things Interest Group [126]
- U.S. Federal Trade Commission (FTC) [127,128,129]
- U.S. Department of Commerce, National Telecommunications & Information Administration (NTIA) [130, 131]
- Internet Governance Forum (IGF) [132]
- Online Trust Alliance [133]
- International Organization for Standardization Joint Technical Committee 1 (ISO/IEC JTC1) [134]: Created two Special Working Groups on Management and the Internet of Things; one is administered by ANSI.
  - International Electrotechnical Commission [135]: While the IEC isn't limited only to IoT devices (and works on all electrical/electronic technologies), it has done several research papers on IoT that may have standards in them.
- InterNational Committee for Information Technology Standards (INCITS) [136]: Accredited by ANSI, to "serve as the central U.S. technical advisory group for a global effort."

- TRUSTe Multi-stakeholder IoT Privacy Tech Working Group [137]: Aiming to draw up technical standards to help companies develop solutions needed to protect consumer privacy in IoT.
- Institute of Electrical and Electronic Engineers (IEEE) P2413 [138]: An IEEE project regarding a standard for an architectural framework for the IoT.
- Wireless IoT Forum [139]: "Not a standards organization but aims to deliver requirements… to standards bodies where there are a lack of standards (e.g. long-range wireless connectivity), and drive consensus where there are competing standards (e.g. home device discovery)."
    - Applications group: working group that reviews standard APIs
    - Connectivity group: working group assessing radio access.
    - Regulatory group: working group harmonizing global license-exempt regulations and availability of licensed spectrum.
- Open Connectivity Foundation (previously called the Open Interconnect Consortium) [140]: Organization created by Intel, Cisco, and Samsung to create an open interoperable specification for IoT. Also acquired UPnP Forum.
- Object Management Group (OMG) [141]: An international not-for-profit technology standards consortium, doing major work on industrial IoT.
    - Industrial Internet Consortium [142]: "… is the open membership, international not-for-profit consortium… setting the architectural framework and direction for the Industrial Internet." Working on accelerating adoption of wireless WAN technologies dedicated to the IoT market. Founded by CISCO, includes Accenture, Arkessa, BT Telensa and WSN.
- oneM2M [143]: Developing technical specifications which address the need for a common M2M Service Layer that can be embedded within various hardware and software
- International Society for Automation (ISA) [144]: "Nonprofit professional association that sets standard for those who apply engineering and technology to improve management, safety, and cybersecurity of modern automation and control systems." Has done some research on IoT, though no indications of a working group.
- OASIS [145]: "Nonprofit consortium that drives the development, convergence and adoption of open standards for the global information society."
    - OASIS Advanced Message Queuing Protocol (AMQP) TC: Defining a ubiquitous, secure, reliable and open internet protocol for handling business messaging.
    - OASIS Message Queuing Telemetry Transport (MQTT) TC: Providing a lightweight publish/subscribe reliable messaging transport protocol suitable for communication in M2M/IoT contexts where a small code footprint is required and/or network bandwidth is at a premium.
    - OASIS Open Building Information Exchange (oBIX) TC: Enabling mechanical and electrical control systems in buildings to communicate with enterprise applications.
- Hypercat [146]: A consortium and standard driving secure and interoperable IoT for Industry and cities.
- AllSeen Alliance [147]: Created AllJoyn, which is a "collaborative, open ecosystem".

- Thread Group [148]: Created the Thread protocol, which is a royalty-free networking protocol for the Internet of Things. Offers product certification.

9 References

[1] James Manika et al., The Internet of Things: Mapping the Value Beyond the Hype, McKinsey Global Institute, June 2015, http://www.mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world.

[2] [2] Brian Krebs, “IoT Reality: Smart devices, Dumb defaults,” Krebs on Security, Blog, Feb. 8, 2016, http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/.

[3] Kalev Leetaru, “How the Internet of Things will Turn your Living Room Into The Future Cyber Battleground,” Nov. 6, 2015, Forbes.com, http://www.forbes.com/sites/kalevleetaru/2015/11/06/how-the-internet-of-things-will-turn-your-living-room-into-the-future-cyber-battleground/ (last visited Nov. 18, 2016).

[4] IEEE Standards Association, IEEE 802.15: Wireless Personal Area Networks (PANs), https://standards.ieee.org/about/get/802/802.15.html (last visited Nov. 18, 2016).

[5] X10, https://www.x10.com/ (last visited Nov. 18, 2016).

[6] Hewlett Packard, Internet of Things Research Study: 2015 Report, HP Enterprise, 2015, *available at* https://www.hpe.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

[7] John Pescatore, Securing the Internet of Things Survey, Sans Institute Analyst Survey, Jan. 2014, *available at* https://www.sans.org/reading-room/whitepapers/analyst/securing-internet-things-survey-34785.

[8] Charlie Osborne, “Internet of Things devices lack fundamental security, study finds,” April 8, 2015, ZDNet, http://www.zdnet.com/article/internet-of-things-devices-lack-fundamental-security-study-finds/ (last visited Nov. 18, 2016).

[9] Ka-Ping Yee, "Aligning security and usability." IEEE Security & Privacy 2.5 (2004): 48-55, *available at* http://zesty.ca/pubs/yee-sid-ieeesp2004.pdf.

[10] Veracode, The Internet of Things: Security Research Study, Whitepaper, 2014, *available at* https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf

[11] Rebecca E. Grinter, et al., "The work to make a home network work." *ECSCW 2005*. Springer Netherlands, 2005, *available at* http://www.cc.gatech.edu/~beki/c27.pdf.

[12] Yin Min Pa Pa, et al. “IoTPOT: Analysing the Rise of IoT Compromises.” (2015), *available at* https://www.usenix.org/system/files/conference/woot15/woot15-paper-pa.pdf

[13] Symantec, “IoT devices being increasingly used for DDoS attacks,” Symantec Security Response, September 22, 2016, *available at:* http://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks.

[14] Steve Rogerson, “IoT blamed for denial of service attacks,” IoT MTM Council, April 29, 2015, *available at* http://www.iotm2mcouncil.org/serviceattacks.

[15] Energin Janina, “Distributed denial-of-service (DDoS) attack knocked the file-sharing site Pirate Bay offline,” May 17, 2012, ceoworld.biz, http://ceoworld.biz/ceo/2012/05/17/distributed-denial-of-service-ddos-attack-knocked-the-file-sharing-site-pirate-bay-offline.

[16] Angela Moscaritolo, “FBI arrests six in click-fraud cyber scam that netted $14M,” SC Magazine, Nov. 9, 2011, http://www.scmagazine.com/fbi-arrests-six-in-click-fraud-cyber-scam-that-netted-14m/article/216399/

[17] Sarthak Grover and Nick Feamster, The Internet of Unpatched Things, PrivacyCon 2016, https://www.ftc.gov/system/files/documents/public_comments/2015/10/00071-98118.pdf.

[18] Bruce Schneier, “The Internet of Things Is Wildly Insecure – And Often Unpatchable,” Wired, Jan. 6, 2014, https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html.

[19] Bruce Schneier, “Surveillance and the Internet of Things,” Blog, May 21, 2013, https://www.schneier.com/blog/archives/2013/05/the_eyes_and_ea.html.

[20] Matt Loeb, “Internet of Things Security Issues Require a Rethink on Risk Management,” Wall Street Journal, Oct. 14, 2015, http://blogs.wsj.com/cio/2015/10/14/internet-of-things-security-issues-require-a-rethink-on-risk-management/.

[21] Arik Hesseldahl, “A Hacker’s-Eye View of the Internet of Things,” Recode.net, Apr. 7, 2015, http://recode.net/2015/04/07/a-hackers-eye-view-of-the-internet-of-things/.

[22] Arik Hesseldahl, “The Internet of Things Is the Hackers’ New Playground,” Recode.net, July 29, 2014, http://recode.net/2014/07/29/the-internet-of-things-is-the-hackers-new-playground/.

[23] Julie Knudson, “Security Challenges of the Internet of Things: The IoT’s lack of standardized protocols and new traffic flows complicate administrators’ security efforts,” Enterprise Networking Planet, May 13, 2015, http://www.enterprisenetworkingplanet.com/netsecur/security-challenges-of-the-internet-of-things.html.

[24] Reddit, Discussion List on Privacy, “I bought and returned a set of WiFi connected home security cameras, forgot to delete my account and can now watch the new owner,” https://www.reddit.com/r/privacy/comments/4ortwb/i_bought_and_returned_a_set_of_wifi_connected/ (last visited Nov. 18, 2016).

[25] Christina Cardoza, “Princeton tires to find out if your IoT devices are safe,” SD Times, Jan. 22, 2016, *available at* http://sdtimes.com/princeton-tries-to-find-out-are-your-iot-devices-safe/.

[26] Christian Dancke Tuen, “Security in Internet of Things Systems,” Masters Thesis, Norwegian University of Science and Technology, Department of Telematics, June 2015, *available at* https://brage.bibsys.no/xmlui/bitstream/handle/11250/2352738/12892_FULLTEXT.pdf?sequence=1&isAllowed=y.

[27] Hewlett Packard, Internet of Things Security Study: Smartwatches, IoT Research Series 2014, http://go.saas.hpe.com/l/28912/2015-07-20/325lbm/28912/69038/IoT_Research_Series_Smartwatches.pdf.

[28] Kim Zetter, “Hospital Networks are Leaking Data, Leaving Critical Devices Vulnerable,” June 25, 2014, https://www.wired.com/2014/06/hospital-networks-leaking-data/.

[29] Mario Ballano Barcena & Candid Wueest, Insecurity in the Internet of Things, Mar. 12, 2015, Symantec, https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-insecurity-in-the-internet-of-things-ds.pdf.

[30] Katie Natopoulos, “Somebody’s watching: how a simple exploit lets strangers tap into private security cameras,” Feb. 3, 2012, The Verge, http://www.theverge.com/2012/2/3/2767453/trendnet-ip-camera-exploit-4chan.

[31] Brian Krebs, “This is Why People Fear the Internet of Things,” Feb. 8, 2016, Krebs on Security, https://krebsonsecurity.com/2016/02/this-is-why-people-fear-the-internet-of-things/

[32] Brady Dale, “Eight Internet of Things Security Fails: Change the passwords on your routers when you set them up for goodness sake,” Observer, July 16, 2015, http://observer.com/2015/07/eight-internet-of-things-security-fails/.

[33] Michael Winter, “Calif. youth admits Miss Teen USA ‘sextortion’ plot,” USA Today, Nov. 12, 2013, http://www.usatoday.com/story/news/nation/2013/11/12/miss-teen-usa-sextortion-guilty-plea/3510461/.

[34] Kevin Townsend, “Malware Found in IoT Cameras Sold by Amazon,” Security Week, April 11, 2016, http://www.securityweek.com/malware-found-iot-cameras-sold-amazon.

[35] Johannes Ullrich, “Coin Mining DVRs: A compromise from start to finish,” Internet Storm Center, SANS ISC InfoSec Forums, https://isc.sans.edu/forums/diary/Coin+Mining+DVRs+A+compromise+from+start+to+finish/18071/.

[36] Kim Zetter, “An Unprecedented Look at STUXNET, the World’s First Digital Weapon,” WIRED, Nov. 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[37] Swati Khandelwal, “IoT Botnet – 25,000 CCTV Cameras Hacked to launch DDoS Attack,” The Hacker News, June 28, 2016, http://thehackernews.com/2016/06/cctv-camera-hacking.html.

[38] Dahua, Cyber Security Statement, Press Release, Oct. 1, 2016, *available at* http://www.dahuasecurity.com/en/us/single.php?nid=274.

[39] Dahua, Dahua Support Wiki Main Page, http://www.dahuawiki.com/Main_Page (last visited Nov. 18, 2016).

[40] Dahua, How to Create a More Secure Security System, http://www.dahuasecurity.com/en/us/best-practices.php (last visited Nov. 18, 2016).

[41] Broadband Internet Technical Advisory Group (BITAG), SNMP Reflected Amplification DDoS Attack Mitigation, August 2012, http://bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf.

[42] T. Dierks & E. Rescorla, “The Transport Layer Security (TLS) Protocol 1.2”, RFC 5246, Aug. 2008, https://tools.ietf.org/html/rfc5246.

[43] E. Rescorla & N. Modadugu, “Datagram Transport Layer Security Version 1.2”, RFC 6347, Jan. 2012, https://tools.ietf.org/html/rfc6347.

[44] Aaron Ardiri, “Is it possible to secure micro-controllers used within IoT?”, EVO Things, Blogs/Tutorials, August 27, 2014, https://evothings.com/is-it-possible-to-secure-micro-controllers-used-within-iot/;

[45] Reinhard Seiler, Blog, Truecrypt benchmark for Raspberry Pi, July 20, 2012, http://blog.rseiler.at/2012/07/truecrypt-benchmark-for-raspberry-pi.html.

[46] Darlene Storm, “MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks,” Computerworld, June 8, 2015, http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html.

[47] Kim Zetter, “How Thieves Can Hack and Disable Your Home Alarm System,” WIRED, July 23, 2014, https://www.wired.com/2014/07/hacking-home-alarms/.

[48] Marek Majkowski, “Say Cheese: a snapshot of the massive DDoS attacks coming from IoT cameras,” Oct. 11, 2018, Cloudflare Blog, https://blog.cloudflare.com/say-cheese-a-snapshot-of-the-massive-ddos-attacks-coming-from-iot-cameras/ (last visited Nov. 18, 2016).

[49] Nest, “Nest Learning Thermostat software update history,” Nest Support, https://nest.com/support/article/Nest-Learning-Thermostat-software-update-history (last visited Nov. 18, 2016).

[50] Nest, “How do I update the software on my Nest Learning Thermostat,” Nest Support, https://nest.com/support/article/How-do-I-update-the-software-on-my-Nest-Learning-Thermostat (last visited Nov. 18, 2016).

[51] Nick Bilton, “Nest Thermostat Leaves Users in the Cold,” Jan. 13, 2016, NYTimes, *available at* http://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html.

[52] Catalin Cimpanu, “Security Researcher with Implanted Pacemaker Sounds the Alarm on IoT Medical Devices,” Softpedia, Jan. 5, 2016, http://news.softpedia.com/news/security-researcher-with-implanted-pacemaker-sounds-the-alarm-on-iot-medical-devices-498448.shtml.

[53] Russ Housley, Words from the IAB Chair: IAB Statement on Internet Confidentiality, IETF Journal March 2015, https://www.internetsociety.org/publications/ietf-journal-march-2015/words-iab-chair-12.

[54] Jane Wakefield, “Smart LED light bulbs leak wi-fi passwords,” BBC News, July 8, 2014, http://www.bbc.com/news/technology-28208905.

[55] SEC Consult, “House of Keys: Industry-Wide HTTPS Certificate and SSH Key Reuse Endangers Millions of Devices Worldwide,” Blog, Nov. 25, 2015, http://blog.sec-consult.com/2015/11/house-of-keys-industry-wide-https.html (last visited Nov. 18, 2016).

[56] Erik C. Davis, “Clustering and Outlier Detection: Methods and Applications in Smart Home Networks”, Undergraduate Dissertation, Operations Research and Financial Engineering. Princeton University. June 2016.

[57] Yin Zhang & Vern Paxson, “Detecting Stepping Stones”, *USENIX Security Symposium,* August 2000, https://www.cs.utexas.edu/~yzhang/papers/stepping-sec00.pdf.

[58] Robert Vamosi, “Covert Hacking of IoT Trivial Say Researchers,” Mocana, Feb. 28, 2014, https://www.mocana.com/blog/2014/02/28/covert-hacking-iot-trivial-say-researchers.

[59] Lorenzo Franceschi-Bicchierai, “Internet-Connected Fisher Price Teddy Bear Left Kids’ Identities Exposed,” Motherboard, Feb. 2, 2016, http://motherboard.vice.com/read/internet-connected-fisher-price-teddy-bear-left-kids-identities-exposed.

[60] Lorenzo Franceschi-Bicchierai, “Bugs in ‘Hello Barbie’ Could Have Let Hackers Spy on Children’s Chats,” Motherboard, Dec. 4, 2015, http://motherboard.vice.com/read/bugs-in-hello-barbie-could-have-let-hackers-spy-on-kids-chats.

[61] Lorenzo Franceschi-Bicchierai, “Hacked Toymaker VTech Admits Breach Actually Hit 6.3 Million Children,” Motherboard, Dec. 1, 2015, http://motherboard.vice.com/read/hacked-toymaker-vtech-admits-breach-actually-hit-63-million-children.

[62] BBC, “Mitsubishi Outlander hybrid car alarm ‘hacked’,” BBC News: Technology, June 6, 2016, http://www.bbc.com/news/technology-36444586.

[63] Darlene Storm, “Nissan Leaf secretly leaks driver location, speed to websites,” ComputerWorld, June 14, 2011, http://www.computerworld.com/article/2470123/endpoint-security/nissan-leaf-secretly-leaks-driver-location--speed-to-websites.html.

[64] Leo Kelion, “Nissan Leaf electric cars vulnerability disclosed,” BBC News: Technology, Feb. 24, 2016, http://www.bbc.com/news/technology-35642749.

[65] Colin Neagle, “Smart refrigerator hack exposes credentials,” NetworkWorld, Aug. 26, 2015, http://www.networkworld.com/article/2976270/internet-of-things/smart-refrigerator-hack-exposes-gmail-login-credentials.html.

[66] Newswise, “Georgia Tech Warns of Threats to Cloud Data Storage, Mobile Devices in Latest ‘Emerging Cyber Threats’ Report,” Press Release, Nov. 6, 2013, http://www.newswise.com/articles/georgia-tech-warns-of-threats-to-cloud-data-storage-mobile-devices-in-latest-emerging-cyber-threats-report

[67] Institute for Information Security & Privacy, Georgia Institute of Technology, Emerging Cyber Threats Report 2016, 2016, *available at* http://www.iisp.gatech.edu/sites/default/files/documents/2016_georgiatech_cyberthreatsreport_onlinescroll.pdf.

[68] Phys.Org, “Your smartwatch is giving away your ATM PIN,” July 6, 2016, http://phys.org/news/2016-07-smartwatch-atm-pin.html (last visited Oct. 7, 2016).

[69] Robert J. Ellison et al., “Evaluating and Mitigating Software Supply Chain Security Risks,” Software Engineering Institute, Technical Note, May 2010, *available at* http://www.sei.cmu.edu/reports/10tn016.pdf.

[70] Internet Storm Center, Survival Time: Summary, https://isc.sans.edu//survivaltime.html (last visited Nov. 18, 2016).

[71] Brian Krebs, “KrebsOnSecurity Hit with Record DDoS,” KrebsOnSecurity, Sept. 21, 2016, https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/ (last visited Oct. 3, 2016).

[72] Flashpoint, “Attack of Things!”, Blog Post, Sept. 17, 2016, https://www.flashpoint-intel.com/attack-of-things/ (last visited Nov. 18, 2016).

[73] Drew Fitzgerald, “Hackers Infect Army of Cameras, DVRs for Massive Internet Attacks,” Wall Street Journal, Sept. 30, 2016, http://www.wsj.com/articles/hackers-infect-army-of-cameras-dvrs-for-massive-internet-attacks-1475179428 (last visited Oct. 3, 2016).

[74] Federal Trade Commission, “ASUS Settles FTC Charges That Insecure Home Routers and “Cloud” Services Put Consumers’ Privacy At Risk,” Press Release, Feb. 23, 2016, *available at* https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.

[75] Network World, “KrebsOnSecurity moves to Project Shield for protection against DDoS attack censorship,” Ms. Smith Blog, Sept. 25, 2016, http://www.networkworld.com/article/3123806/security/krebsonsecurity-moves-to-project-shield-for-protection-against-ddos-attack-censorship.html (last visited Oct. 3, 2016).

[76] Brian Krebs, “The Democratization of Censorship,” KrebsOnSecurity, Sept. 16, 2016, https://krebsonsecurity.com/2016/09/the-democratization-of-censorship/ (last visited Oct. 3, 2016).

[77] Tim Greene, “Largest DDoS attack ever delivered by botnet of hijacked IoT devices,” Network World, Sept. 23, 2016, http://www.networkworld.com/article/3123672/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html (last visited Oct. 3, 2016).

[78] Dan Goodin, “Record-breaking DDoS reportedly delivered by >145k hacked cameras,” ArsTechnica, Sept. 28, 2016, http://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/ (last visited Oct. 3, 2016).

[79] David Plonka & Elisa Boschi, The Internet of Old and Unmanaged, 2016, *available at* https://down.dsg.cs.tcd.ie/iotsu/subs/IoTSU_2016_paper_25.pdf.

[80] David Plonka, Measurement and Analysis for the Internet of Things, July 18, 2016, *available at* https://www.ietf.org/proceedings/96/slides/slides-96-maprg-8.pdf.

[81] Lucian Constantin, "Attackers hijack CCTV cameras to launch DDoS attacks, Computerworld," Oct. 22, 2015, http://www.computerworld.com/article/2996079/internet-of-things/attackers-hijack-cctv-cameras-to-launch-ddos-attacks.html.

[82] Kashmir Hill, "This guy's light bulb performed a DoS attack on his entire smart house," Fusion.net, March 3, 2015, http://fusion.net/story/55026/this-guys-light-bulb-ddosed-his-entire-smart-house/.

[83] Tom Spring, "Insecurity: Pinpointing the Problems," ThreatPost, July 21, 2016, https://threatpost.com/iot-insecurity-pinpointing-the-problems/119389/.

[84] DirectTV, User Guide: Genie and Earlier HD DVR Receivers, pg. 107, http://www.directv.com/learn/pdf/System_Manuals/DIRECTV/DIRECTV_HDDVR_HR20-44.pdf.

[85] Roku, "How can I update my software on my Roku player?," https://support.roku.com/hc/en-us/articles/208755668-How-can-I-update-the-software-on-my-Roku-player- (last visited Nov. 18, 2016).

[86] Arunesh Mathur, et al. "They Keep Coming Back Like Zombies': Improving Software Updating Interfaces," *USENIX Symposium on Usable Security and Privacy,* 2016, *available at* https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-mathur.pdf.

[87] David Plonka, Flawed Routers Flood University of Wisconsin Internet Time Server, July 19, 2006, http://pages.cs.wisc.edu/~plonka/netgear-sntp/.

[88] Comcast, "Some NetGear Routers Causing Flood of DNS Queries," Comcast DNS News, May 20, 2013, http://dns.xfinity.com/index.php/entry/some-netgear-routers-causing-flood-of-dns-queries.

[89] NetGear Community Discussion List, "Thousands of DNS Requests Per Second!?", March 2, 2012, https://community.netgear.com/t5/General-WiFi-Routers/Thousands-of-DNS-Requests-Per-Second/td-p/414710.

[90] Benoit Panizzon, DDOS Attack by Netgear Products caused by CNAME instead of A record?, [SWINOG] Discussion List, June 27, 2013, http://lists.swinog.ch/public/swinog/2013-June/005863.html.

[91] National Security Agency, Defense in Depth, Whitepaper, 2010, *available at* https://citadel-information.com/wp-content/uploads/2010/12/nsa-defense-in-depth.pdf.

[92] Vijay Sivaraman et al. "Network-Level Security and Privacy Control for Smart-Home IoT Devices", *IEEE Wireless and Mobile Computing, Networking, and Communications.* 2015, https://www.researchgate.net/publication/281275810_Network-Level_Security_and_Privacy_Control_for_Smart-Home_IoT_Devices.

[93] Konstantinos Grivas & Stelios Zerefos, Augmented Home Inventories, European Conference on Ambient Intelligence, 2015.

[94] William Enck, et al. "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones," In Proc. of the USENIX Symposium on Operating Systems Design and Implementation (OSDI), October 2010, *available at* http://appanalysis.org/tdroid10.pdf.

[95] Disconnect, Disconnect Privacy Tool, https://disconnect.me/ (last visited Nov. 18, 2016).

[96] Masanobu Katagi and Shiho Moriai, Lightweight Cryptography for the Internet of Things, 2011, https://www.iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf.

[97] GitHub, "SSL and TLS Deployment Best Practices," SSL Labs Wiki, https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices (last visited Oct. 3, 2016).

[98] Mozilla, "Security/Server Side TLS," Mozilla Wiki, https://wiki.mozilla.org/Security/Server_Side_TLS (last visited Nov. 18, 2016).

[99] Dan Auerbach, "2011 In Review: Ever-Clearer Vulnerabilities in Certificate Authority System," Electronic Frontier Foundation, Dec. 27, 2011, https://www.eff.org/deeplinks/2011/12/2011-review-ever-clearer-vulnerabilities-certificate-authority-system.

[100] Wikipedia, Revocation List, https://en.wikipedia.org/wiki/Revocation_list (last visited Nov. 18, 2016).

[101] Dennis Fisher, "Final Report on Diginator Hack Shows Total Compromise of CA Servers," ThreatPost, Oct. 31, 2012, https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/.

[102] Eric Mill, "Certificate Authorities are Actually a Tremendous Problem," Blog Post, June 21, 2013, https://konklone.com/post/certificate-authorities-are-actually-a-tremendous-problem (last visited Nov. 18, 2016).

[103] Chester Wisniewski, "Another certificate authority issues dangerous certificates, Naked Security," Nov. 3, 2011, https://nakedsecurity.sophos.com/2011/11/03/another-certificate-authority-issues-dangerous-certficates/ (last visited Nov. 18, 2016).

[104] Glenn Fleishman, "The Huge Web Security Loophole That Most People Don't Know About, And How It's Being Fixed," FastCompany, *available at* http://www.fastcompany.com/3042030/tech-forecast/the-huge-web-security-loophole-that-most-people-dont-know-about-and-how-its-be.

[105] Steve Roosa, "The Flawed Legal Architecture of the Certificate Authority Trust Model," Freedom to Tinker, Dec. 15, 2010, https://freedom-to-tinker.com/blog/sroosa/flawed-legal-architecture-certificate-authority-trust-model/ (last visited Nov. 18, 2016).

[106] Google, Certificate Transparency Project, What is Certificate Transparency?, https://www.certificate-transparency.org/what-is-ct (last visited Nov. 18, 2016).

[107] Level 3 Threat Research Labs, "Attack of Things!", Level 3 Blog, http://blog.level3.com/security/attack-of-things/ (last visited Nov. 18, 2016).

[108] International Organization for Standardization, ISO/IEC 30111:2013: Information Technology – Security techniques – Vulnerability handling processes, 2013, *available at* http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231.

[109] IPSO Alliance, http://www.ipso-alliance.org (last visited Nov. 18, 2016).

[110] Institute of Electrical and Electronics Engineers (IEEE), https://www.ieee.org (last visited Nov. 18, 2016).

[111] US Department of Commerce, National Institute of Standards and Technology, http://nist.gov (last visited Nov. 18, 2016).

[112] Internet Engineering Task Force (IETF), http://www.ietf.org (last visited Nov. 18, 2016).

[113] Internet Engineering Task Force (IETF), Light-Weight Implementation Guideance (lwig) https://datatracker.ietf.org/wg/lwig/ (last visited Nov. 18, 2016).

[114] Internet Engineering Task Force (IETF), IPv6 Over Networks of Resource-Constrained Nodes (6lo), https://datatracker.ietf.org/wg/6lo/ (last visited Nov. 18, 2016).

[115] Internet Engineering Task Force (IETF), IPv6 over the TSCH mode of IEEE 802.15.4e (6tisch), https://datatracker.ietf.org/wg/6tisch/ (last visited Nov. 18, 2016).

[116] Internet Engineering Task Force (IETF), Routing over Low power and Lossy networks (roll), https://datatracker.ietf.org/wg/roll/ (last visited Nov. 18, 2016).

[117] Internet Engineering Task Force (IETF), Constrained RESTful environments (core), https://datatracker.ietf.org/wg/core/ (last visited Nov. 18, 2016).

[118] Internet Engineering Task Force (IETF), DTLS in Constrained Environments (dice), https://datatracker.ietf.org/wg/dice (last visited Nov. 18, 2016).

[119] Internet Engineering Task Force (IETF), Authentication and Authorization for Constrained Environments (ace), https://datatracker.ietf.org/wg/ace/(last visited Nov. 18, 2016).

[120] Internet Engineering Task Force (IETF), CBOR Object Signing and Encryption (cose) https://datatracker.ietf.org/wg/cose/ (last visited Nov. 18, 2016).

[121] Internet Engineering Task Force (IETF), IPv6 over Low power WPAN (6lowpan), https://datatracker.ietf.org/wg/6lowpan (last visited Nov. 18, 2016).

[122] Groupe Speciale Mobile Association (GSMA), GSMA IoT Security Guidelines, http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/ (last visited Nov. 18, 2016).

[123] Internet Research Task Force, http://irtf.org (last visited Nov. 18, 2016).

[124] Internet Research Task Force, Thing-to-Thing Research Group, https://irtf.org/t2trg (last visited Nov. 18, 2016).

[125] World Wide Web Consortium (W3C), http://www.w3c.org (last visited Nov. 18, 2016).

[126] World Wide Web Consortium (W3C), Web of Things Interest Group, https://www.w3.org/WoT/IG/ (last visited Nov. 18, 2016).

[127] Federal Trade Commission, Bureau of Consumer Protection and Office of Policy Planning, In The Matter of The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancemenet of the Internet of Things, Docket No. 160331306-6306-01, Comments of Staff, https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-office-policy-planning-national-telecommunications/160603ntiacomment.pdf.

[128] Federal Trade Commission, Internet of Things: Privacy & Security in a Connected World, Staff Report, January 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[129] Dennis Fisher, FTC Warns of Security and Privacy Risks in IoT Devices, June 3, 2016, https://www.onthewire.io/ftc-warns-of-security-and-privacy-risks-in-iot-devices/ (last visited Nov. 18, 2016).

[130] National Telecommunications & Information Administration, Internet of Things, https://www.ntia.doc.gov/category/internet-things (last visited Nov. 18, 2016).

[131] National Telecommunications & Information Administration, U.S. Department of Commerce Seeks Comment on Potential Policy Issues Related to Internet of Things, Press Release, April 5, 2016, https://www.ntia.doc.gov/press-release/2016/us-department-commerce-seeks-comment-potential-policy-issues-related-internet-thi

[132] Internet Governance Forum, Dynamic Coalition on the Internet of Things, https://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/827-dciot-2015-output-document-1/file.

[133] Online Trust Alliance, Internet of Things, Sept. 19, 2016, https://otalliance.org/initiatives/internet-things (last visited Nov. 18, 2016).

[134] International Organization for Standardization (ISO), ISO/IEC Joint Technical Committee on Information Technology, http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45020 (last visited Nov. 18, 2016).

[135] International Electrotechnical Commission (IEC), http://www.iec.ch/ (last visited Nov. 18, 2016).

[136] International Committee for Information Technology Standards, http://www.incits.org/ (last visited Nov. 18, 2016).

[137] TRUSTe, Privacy Risk Summit 2016, June 8, 2016, http://www.truste.com/events/privacy-risk/

[138] Institute of Electronic and Electrical Engineers (IEEE), P2413 – Standard for an Architectural Framework for the Internet of Things (IoT), https://standards.ieee.org/develop/project/2413.html (last visited Nov. 18, 2016).

[139] Wireless IoT Forum, http://www.wireless-iot.org/ (last visited Nov. 18, 2016).

[140] Open Connectivity Foundation, https://openconnectivity.org/ (last visited Nov. 18, 2016).

[141] Object Management Group, http://www.omg.org/ (last visited Nov. 18, 2016).

[142] Industrial Internet Consortium, http://www.iiconsortium.org/ (last visited Nov. 18, 2016).

[143] oneM2M, http://www.onem2m.org/ (last visited Nov. 18, 2016).

[144] Bill Lydon, "Internet of Things: Industrial automation industry exploring and implementing IoT," InTech Magazine, Mar-Apr 2014, *available at* https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/2014/mar-apr/cover-story-internet-of-things/.

[145] OASIS, OASIS Committee Categories:IoT/M2M, https://www.oasis-open.org/committees/tc_cat.php?cat=iot (last visited Nov. 18, 2016).

[146] HYPERCAT, http://www.hypercat.io/ (last visited Nov. 18, 2016).

[147] AllSeen Alliance, https://allseenalliance.org/ (last visited Nov. 18, 2016).

[148] Thread, http://threadgroup.org/ (last visited Nov. 18, 2016).

10 Document Contributors and Reviewers

- Fred Baker, *CISCO*
- Steven Bauer, *MIT*
- Richard Bennett
- Don Bowman, *Sandvine*
- William Check, *NCTA*
- kc claffy, *UCSD/CAIDA*
- David Clark, *MIT*
- Shaun Cooley, *CISCO*
- Amogh Dhamdhere, *UCSD/CAIDA*
- Nick Feamster, *Princeton University*
- Francis Ferguson, *Level 3*
- Joseph Lorenzo Hall, *Center for Democracy & Technology*
- Ken Ko, *ADTRAN*
- Jason Livingood, *Comcast*
- Patrick McManus, *Mozilla*
- Chris Morrow, *Google*
- Donald Smith, *CenturyLink*
- Barbara Stark, *AT&T*
- Darshak Thakore, *CableLabs*
- Matthew Tooley, *NCTA*
- Jason Weil, *Charter Communications*
- Greg White, *CableLabs*
- Todd Whitenack, *Cellcom*
- David Winner, *Charter Communications*