19 April 2018

IoT Security for Policymakers

"Cybersecurity will be the most pressing challenge of the next decade, and IoT will play a critical role in it."

Internet Society 2017 Global Internet Report

Internet Society

Introduction

The open nature of the Internet creates the ability to connect devices, applications and services on a scale that transforms the way we interact with our environment and our society. The Internet of Things (IoT) carries enormous potential to change our world for the better. Projections for the impact of IoT on the Internet and the global economy are impressive, forecasting explosive growth in the number of IoT devices and their use in a wide variety of new and exciting applications. According to one estimate, "connected devices will number 38.5 billion in 2020, up from 13.4 billion in 2015."[1]

At the same time, with billions of IoT devices, applications and services already in use, and greater numbers coming online, IoT security is of utmost importance. Poorly secured IoT devices and services can serve as entry points for cyber attacks, compromising sensitive data and threatening the safety of individual users. Attacks on infrastructure and other users, fueled by networks of poorly secured IoT devices, can affect the delivery of essential services such as healthcare and basic utilities, put the security and privacy of others at risk, and threaten the resilience of the Internet globally.

IoT also presents important privacy challenges. They will be addressed in a complementary paper on privacy and IoT.

What is the Internet of Things (IoT)? [2]

The term "Internet of Things" refers to **"scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention."** [3] IoT includes consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and more. It presents a new way for users to interact with the network, using devices that are not limited to traditional computers, smartphones, and laptops. IoT brings unparalleled new opportunities for industrial applications and critical infrastructure, but significant challenges as well. Many of the challenges and recommendations addressed in this paper are focused on consumer-grade IoT but are also applicable to industrial and critical infrastructure applications of IoT. While local communication protocols used for IoT, such as Zigbee[4], LORA[5], Z-Wave[6], or Bluetooth[7], present interesting challenges of their own, the Internet Society's primary focus is how IoT systems interact with, and impact, the Internet and its users.

Compromised IoT devices, such as webcams or even lightbulbs, can be used to form "botnets", networks of Internet-connected externally controlled devices. These devices, referred to in this context as "bots", are often infected with malicious software and used for disruptive or criminal

1 https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020
2 For more Internet Society resources on IoT, see our IoT landing page (https://www.internetsociety.org/iot/) and the document "The Internet of Things (IoT): An Overview"
3 https://www.internetsociety.org/doc/iot-overview
4 http://www.zigbee.org/what-is-zigbee/
5 https://www.lora-alliance.org/what-is-lora
6 http://www.z-wave.com/about
7 https://www.bluetooth.com/

purposes, such as attacking other networks, other users, and Internet infrastructure.[8] In 2016, a botnet of compromised IoT devices performed a distributed denial of service (DDoS) attack against Dyn[9], a major Domain Name System (DNS) service provider. The attack made major websites, including Twitter, Amazon and Netflix, temporarily inaccessible for Internet users in some parts of the world.

As greater numbers of vulnerable IoT systems come online, they create a bigger "attack surface" and increase the potential scale and severity of IoT-based DDoS attacks.

Understanding the growing impact that IoT security has on the Internet and its users is critical for safeguarding the future of the Internet. IoT manufacturers, IoT service providers, users, standards developing organizations (SDOs), policymakers, and regulators will all need to take action to protect against threats to Internet infrastructure, such as IoT-based DDoS attacks. It is also important to understand the influence that IoT security has on user trust and online use.[10] Trust is a key ingredient for a sustainable, evolving and global Internet. Without trust, users feel vulnerable and marginalized and are reluctant to take advantage of the many legitimate benefits that the Internet offers. Among those who distrust the Internet, the leading reason is because they believe it is not secure."[11] That being said, many users of IoT devices may not realize that they are interacting with the Internet. Building a secure IoT ecosystem that reduces risks and guards against threats while still realizing the vast potential that IoT presents for society, is crucial, urgent, and needs to be a high priority for all stakeholders.

The challenges presented by IoT make a collaborative security approach[12] more important than ever. As the IoT ecosystem grows, the number of potentially vulnerable connected devices grows with it. These devices do not have to be vulnerable. Alongside individual actors taking responsibility in their respective roles, together we need to take action to reduce the likelihood of vulnerable devices being produced, while reducing the impact of vulnerable devices when they do find their way onto the network.

Policymakers have important choices to make to help shape the future of IoT security. This paper is intended for regulators, policymakers, and anyone interested in the development and implementation of policy tools regarding IoT security.

8 https://www.internetsociety.org/policybriefs/botnets/

9 https://www.internetsociety.org/blog/2016/10/trust-isnt-easy-drawing-an-agenda-from-fridays-ddos-attack-and-the-internet-of-things/

10 https://www.internetsociety.org/resources/doc/2016/policy-framework-for-an-open-and-trusted-internet/

11 https://www.cigionline.org/internet-survey

12 https://www.internetsociety.org/collaborativesecurity

Key Considerations

There are several factors to consider when approaching IoT security. Among them:

1. **IoT is an evolving area and is changing rapidly and organically.** New capabilities are added and new security weaknesses are discovered almost every day. Best practices and standards for IoT security are still emerging and being addressed by numerous organizations worldwide.[13]

The **Internet Society's Online Trust Alliance (OTA) IoT Trust Framework** is a comprehensive set of strategic principles to help secure IoT devices and their data. The result of a collaborative process, the Framework provides recommendations that we believe all IoT manufacturers should adopt to improve security and enhance transparency and communication of the devices' ability to be updated as well as data privacy related issues.[14]

2. **IoT is not just devices. IoT systems are inter-connected and complex.** They include software, devices, sensors, platforms, the transmission of data via the Internet, as well as services, including analysis and storage of data in the cloud (and potentially by third parties). As every part of an IoT system must be secured to provide security to its users and other users of the Internet, a layered and continuous approach to security is required.

3. **Inward security and outward security are distinct but equally important**. An IoT system can be attacked, impacting the privacy and security of its user (e.g., exposing the "private" video feed from a baby monitor, controlling "smart" home systems, causing home appliances to behave in unwanted (and potentially dangerous) ways, tracking when homeowners are away); that is an "inward security" issue. But a compromised IoT system can also be used to launch attacks against third parties or systems (e.g. vulnerable home appliances being infected with "malware" (malicious software) and then becoming part of a botnet used in a DDoS attack on networks, users, or infrastructure); that is an "outward security" issue. IoT systems must be secured against risks to other networks and users (outward security) as well as risks to their users and assets (inward security).

13 https://www.internetsociety.org/blog/2014/04/permissionless-innovation-openness-not-anarchy/

14 The Online Trust Alliance (OTA) is an initiative of the Internet Society. Also, of interest are the OTA documents Securing the Internet of Things and Internet of Things, a Vision for the Future.
https://otalliance.org/iot
https://otalliance.org/system/files/files/initiative/documents/iot_sharedrolesv1.pdf
https://otalliance.org/system/files/files/initiative/documents/iot_visionforthefuture_0.pdf

4. **The security of IoT is a global concern.** The Internet is an interconnected and interdependent network of networks and the security of one impacts the security of anyone else on the network. Vulnerable IoT systems could be compromised from anywhere and used to target anyone.

5. **Security-by-design is essential.** IoT security is most effective when it is included in the design process from the beginning and all the way through to implementation and after-sale support. Security cannot be effective when added as an afterthought.

6. **Security is an ongoing process.** IoT systems need to be maintained to remain secure. Currently, this is primarily the responsibility of IoT manufacturers and service providers. Timely, verifiable, and effective patches and updates to address vulnerabilities are a critical aspect of security. Product and service lifecycles are a vital security component (e.g. how long will support and updates be available, and what happens after they cease?). It is not uncommon for devices to remain in service long after their officially supported lifespan.

7. **Vulnerability research and reporting are important.** Security researchers play an important role in testing the security of devices and alerting manufacturers and service providers to discovered vulnerabilities.

8. **Platforms are significant market players.** IoT platforms (e.g., Apple's Homekit[15] and Google's Weave[16]) some of which have considerable and growing market penetration, enable the control of a host of devices using the same protocol, exchanging data to make informed decisions. Those that have been installed in our "smart" homes, controlling our temperature, lighting, sound systems, and security, use cohesive designs to easily interoperate with other supported devices and simplify our user experience, hiding the complexity and scale of automation. Platform characteristics can greatly impact the IoT market.[17] Platforms with strong security requirements push participating manufacturers and vendors to improve the security of their devices and associated services. However, platform vulnerabilities can affect all connected IoT systems. Also, platforms vary in their privacy practices, with some being better than others.

15 https://www.apple.com/ios/home/ ; https://developer.apple.com/homekit/

16 https://nest.com/weave/

17 https://www.internetsociety.org/blog/2017/09/can-iot-platforms-apple-google-samsung-make-home-automation-systems-secure/

Challenges

When approaching IoT security, one must recognize many challenges. These include:

- **Economics favor weak security.** Competitive pressures for shorter times to market and cheaper products drive many designers and manufacturers of IoT systems, including devices, applications and services, to devote less time and resources to security. Strong security can be expensive to design and implement, and it lengthens the time it takes to get a product to market. The commercial value of user data also means that there is an incentive to hoard as much data for as long as possible, which runs counter to good data security practices. Additionally, there is currently a shortage of credible and well-known ways for suppliers to signal their level of security to consumers (e.g., certifications and trustmarks[18]). This makes it difficult for consumers to compare the security of competing IoT systems, which results in lower consumer pressures for strong security and makes it challenging for suppliers to use security as a competitive differentiator. Further, the cost and impact of poor security tend to fall on the consumer and other Internet users, rather than on the producers of the vulnerable IoT system. For example, if your plumbing freezes when the heat is turned off, or if Internet services are adversely impacted by an attack that your compromised devices participate in, the effects are not directly felt by the producers.

- **Security requires particular expertise.** Implementing strong security in IoT systems takes expertise. New players in the IoT ecosystem may have little or no previous experience with Internet security. For example, a manufacturer may know how to make a refrigerator safe for its intended primary use (electrical wiring, chemicals), but may not understand Internet security. In particular, it may not understand the potential global impact of a compromised system in a "smart" refrigerator.

- **IoT systems are complex and each part must be secured.** The security of a system is only as good as its weakest link. In IoT systems, different components may be under the control of different actors in different jurisdictions (e.g. a server may be located in one country, while the device may be manufactured in another, and in use in yet another), making it difficult to cooperatively solve IoT security problems and making cross-border enforcement challenges particularly problematic. Complex supply chains make security evaluations challenging, requiring systems to be secured holistically with coordination among different parties and parts of the system. Increasingly, IoT systems are managed and/or controlled by (or at least heavily interact with) remotely managed "cloud" services, rather than being controlled locally. Lack of transparency and control for the end-user can also be particularly problematic.

- **Security support must be maintained.** IoT devices, applications, and related services commonly require security patches and updates to protect against known vulnerabilities. Consumers typically do not have the technical ability, or in many cases even the user interfaces, to effectively and safely implement patches. To further complicate matters, when the choice is available, users may choose not to patch their devices or simply not know how.[19] Also, in some cases, users are contractually prevented from updating or repairing the systems themselves or having them repaired by independent specialists, e.g.,

18 A trustmark is a visible indicator of conformance to a well-designed set of trust, security, privacy and/or interoperability requirements.

19 See the US Department of Commerce NTIA Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching. https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security

farm equipment.[20] Despite the fact that supporting IoT systems over time is an expensive and resource-consuming task for IoT service providers and developers, it is often insufficiently prioritized.

- **Consumer knowledge of IoT security is low.** Generally, consumers have limited knowledge of IoT security, impacting their ability to factor security into their buying habits or to configure and maintain the security of their IoT systems. Consumer groups often have budget constraints, making consumer outreach and education particularly challenging.

- **Security incidents may be difficult for users to detect or address.** In many cases, the effects of a poorly secured IoT system will not be evident to the user (e.g. your baby monitor may continue to function well as a remote audio and video monitoring device, despite having been compromised and being part of a botnet performing DDoS attacks or having been modified to relay sound and images to unauthorised parties). It is also often difficult to detect when personal data is being leaked by IoT cloud systems. In addition, many IoT devices lack a user interface altogether or have one that is severely limited. In these cases (as above), it may be difficult or impossible for a user to directly interact with the device to confirm or perform updates, make configuration changes, etc.

- **Existing legal liability mechanisms can be unclear**. Responsibility for harm caused by inadequate IoT security may be hard to pinpoint. This leads to uncertainty among victims when seeking to assign responsibility or obtain compensation for harm. Clear liability can be an incentive for stronger security. In the absence of strong liability regimes, users are ultimately the ones who pay the price of security breaches.

Recommendations and Guiding Principles for Governments on IoT Security

Governments have an important role to play in securing IoT. By using their formidable market power and carefully creating and implementing policies and regulations, governments can encourage better outcomes for IoT security. Governments hold a number of important levers that, if utilized properly, can effectively push industry towards effective industry self regulation with clear accountability and strengthened information sharing among IoT manufacturers, retailers, resellers, integrators, service providers, and individual consumers. Increased transparency benefits all stakeholders.

The following are guiding principles and recommendations for governments to consider when addressing IoT security:

Strengthen accountability

Principle: Strengthen accountability for IoT security and privacy by providing well-defined responsibilities and consequences for inadequate protection.

Recommendations:

- **Ensure legal certainty:** Provide clear, predictable, and enforceable rules requiring IoT providers, developers, and manufacturers to protect against known vulnerabilities by

20 https://motherboard.vice.com/en_us/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware

ensuring reporting mechanisms are in place, supporting their products and systems[21] with security patches and updates, and having clearly defined security patch and update policies, including an end date. Especially in the consumer IoT market, security protections should be opt-out,
not opt-in.

- **Strengthen consumer protection:** Personal data collected or used by IoT, especially sensor data, should be protected by privacy and data protection laws. Governments can facilitate better security and privacy by clarifying how existing privacy, data protection and consumer protection laws apply to IoT. Similar to the prohibition of misleading representations about product safety, companies should also be prohibited from making misleading or deceptive representations about the security of their IoT products or services. Retailers should also share the responsibility and not sell IoT products with known critical safety and security defects.

- **Clearly assign liability:** To address uncertainty, governments should clearly assign liability on those that are most able to exercise control over the security of a product or service. IoT manufacturers and importers should be liable for safety and security defects in their products.

Promote the use of security signals

Principle: Increase incentives to invest in security by fostering a market for trusted independent assessment of IoT security.

Recommendations:

- **Encourage credible security certification schemes:** Certification, by which an organization signals that a product, service, or system has passed a set of quality or performance tests, can be a powerful and visible signal of compliance to know whether an IoT device uses best practices or standards. They can also be an effective tool for assigning and demonstrating accountability. (Note that compliance may be self-asserted or externally validated.) Improving the quality of testing and certification efforts, viewing them as part of a process instead of a snapshot in time, and increasing the visibility of associated trustmarks would apply market pressure on manufacturers to improve security, and help make better security a competitive differentiator.

- **Reviews and Ratings:** Recognize the useful role that consumer ratings and reviews play in highlighting the privacy and security (or lack thereof) of IoT.

Encourage a culture of security among IoT stakeholders

Principle: Encourage security as a component of all stages of the product lifecycle, including design, production and deployment. Strengthen the ability of stakeholders to respond and mitigate IoT-based threats.

Recommendations*:*

[21] "Systems" not only refers to the IoT systems that are installed by the user, but also to the remote (or "backend") systems involved in collecting, storing and processing data. These systems may not be under the users' control or even within their jurisdiction.

- **Support security risk analysis:** Promote the use of industry-accepted security risk assessment techniques before IoT products and services reach the market. Encourage IoT manufacturers and suppliers to use independent security experts to undertake the assessment. Where possible, governments can also support the development of tools and processes to strengthen security risk analyses (e.g., through funding research). They can work with government funding agencies and industry to encourage publicly available research, including security and policy mechanisms.

- **Promote best practices and guiding principles:** Promote on a global level the use of frequently reviewed and commonly accepted security best practices and guiding principles to guide the design, deployment, and use of IoT devices and services.[22] Include these requirements in procurement policies.

- **Encourage a culture of security:** Foster a culture of security among key stakeholders, including Internet service providers (ISPs), that extends beyond their own interests, to the Internet and its users. For example, it is helpful to encourage information sharing, including about threat mitigation techniques. In addition, providing support for computer security incident response teams (CSIRTs) and cybersecurity training and reference resources for new players in the IoT market can be very effective.

- **Strengthen legal protections for security researchers:** Ensure that security researchers are not at legal risk for their investigation of security vulnerabilities.

Provide strong incentives for better security practices

Principle: Governments can use their policy tools, significant resources, and market power to make security a competitive differentiator.

Recommendations:

- **Improve public procurement practices for IoT:** Develop stronger procurement practices for IoT devices, platforms, and services that emphasize adherence to best practices in security and privacy. When governments provide a market for best practices in IoT security, companies respond to meet the demand, influencing the public and private IoT market. Where available, require IoT suppliers to obtain third party certifications or trustmarks as part of procurement policies. Governments should also use industry-accepted tools for testing IoT in their evaluation processes for procurement.

- **Support consumer education:** Support and engage in consumer education and awareness campaigns to stimulate consumer demand for IoT security. When better security is viewed by consumers as a market differentiator, a credible case can be made to potential buyers that higher pricing is justified.

- **Promote a greater role for consumer groups:** There is a greater role for consumer groups in the development, implementation, public education, and evaluation of IoT security. (Currently, consumer groups are largely absent from relevant discussions, and this

22 For example, the Internet Society's OTA IoT Trust Framework and the Internet Society policy brief on the Internet Invariants. https://otalliance.org/iot/ https://www.internetsociety.org/policybriefs/internetinvariants
Also see ENISA's "Baseline Security Recommendations for the Internet of Things in the context of critical information infrastructures." https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

contributes significantly to the extent of the problem.) Recognize that a lack of funding is often a barrier for consumer groups to engage in relevant policy discussions about IoT security.

- **Partner with insurance industry:** The insurance industry can prioritize better privacy and security requirements as a condition of their underwriting. By looking at the security of the IoT devices and related applications and services used by companies, insurance agencies can factor the risk they present into determining insurance premiums and prices.

Foster technology and vendor neutral solutions

Principle: Security solutions should not be based on specific technical standards or vendor products, but instead based on desired outcomes such as better security, privacy, and interoperability. These goals will not likely change frequently, but the means to achieve them will.

Recommendations:

- **Policies and procurement requirements for IoT security should specify outcomes, not methods:** As IoT is a rapidly evolving area, new threats and security methods and technologies are constantly emerging. By specifying outcomes rather than technologies, IoT developers, manufacturers, and service providers are free to innovate. This helps to ensure the policies are more "future proof" and will not need to be significantly changed with new technologies. An example of this would be procurement requirements that specify devices, applications, and services should be fully updated and patched as applicable. They should also include the ability to cryptographically validate and test an update or patch, without requiring a particular means of doing so.

- **Encourage data portability:** Support for interoperable open standards enables users to have more control over their data because it will be more readily portable to other services. Governments are best served by not binding government data or their citizens' data to specific proprietary solutions, also known as "vendor lock-in".

Make smart use of any policy or regulatory tools

Principle: As security is expensive and users may have difficulty recognizing or valuing security, policy and law can have an important role to play in shaping security practices in the IoT industry. Policies can be developed with a goal of influencing the IoT ecosystem to promote better security practices, rather than to mandate specific technical solutions.

Recommendations:

- **Policies or regulations should be developed in a transparent manner and prioritize the interests of users:** To strengthen outcomes, all affected stakeholders (including but not limited to vendors, manufacturers, users, and consumer organizations) should benefit from the development of policies and laws. By representing consumer interests, consumer organizations can play a very important role in policy development. Policymakers should ensure that laws applicable to consumer-grade IoT place the interests of users first. Further, the effects of insecure IoT systems on other network users, not just the direct users, should be factored into developing IoT policies.

- **Regulating by industry sector may lead to better outcomes:** Core principles, such as data protection, should apply across all sectors. However, IoT systems are developed and used in a wide range of industry sectors and applications; therefore, a sectoral approach to regulation, complementary to core principles, may result in stronger security outcomes. In some industry sectors, strong market incentives or existing regulations may make new regulation less necessary than in others. For example, regulatory tools that may be appropriate to the health care sector may not be as useful in the consumer device sector, where attributes like fault tolerance may not be as crucial to developing a safe product.

IoT is poised to transform economies and societies worldwide. The technology brings enormous opportunities but also enormous risks. We are at a critical moment when we need to take steps to ensure that the benefits of IoT outweigh the security risks. Many organizations are working hard on these issues, but there is a need for all stakeholders, including policymakers, manufacturers, and consumers, to make good choices about the future of IoT and security.