Microsoft

CYBERSECURITY POLICY FOR THE INTERNET OF THINGS

Authors

Benedikt Abendroth
Aaron Kleiner
Paul Nicholas

Contributors

Erin English
Jim Pinter
Arjmand Samuel
Ron Zahavi

Contents

Executive summary 4

Introduction 5

What exactly is the Internet of Things? 6

Security concerns about the Internet of Things from a user perspective 7

Consumers 7
Enterprises 8
Governments 9

Industry: Enhancing IoT security through a role-based approach 10

IoT hardware manufacturers or integrators 10
IoT solution developers 11
IoT solution deployers 11
IoT solution operators 12

Government: Advancing IoT security through policy 13

Encourage the use of good IoT security practices 13
What about certifying or labeling IoT devices based on security? 15
Build cross-disciplinary partnerships to enhance IoT security 16
Support initiatives that improve IoT security across borders 17

Conclusion 18

Executive summary

This paper addresses the critical task of developing cybersecurity policies for IoT, which has particular urgency because the merger of physical and digital domains in IoT can heighten the consequence of cyber attacks.

Around the world, organizations and individuals are experiencing a fundamental shift in their relationship with technology. This transformation, often called the Fourth Industrial Revolution, has been characterized by the World Economic Forum as a fusion of the physical, digital and biological worlds, with far-reaching implications for economies and industries, and even humankind.[1] These changes create new opportunities and challenges for public policymakers, as traditional governance frameworks and models will have to be reconsidered for a different world.

The Internet of Things (IoT) is a key element of global digital transformation. There is no universally agreed-on definition of IoT, perhaps in part because the term IoT does not simply describe a new type of technical architecture, but a new concept that defines how we interact with the physical world. At a high level, IoT has been described as a decentralized network of devices, applications, and services that can sense, process, communicate, and take action based on data inputs, including control of elements of the physical world.

This paper addresses the critical task of developing cybersecurity policies for IoT, which has particular urgency because the merger of physical and digital domains in IoT can heighten the consequences of cyber attacks. The cybersecurity concerns of IoT user communities—whether consumer, enterprise, or government—provide a convenient lens for identifying and exploring IoT security issues. For example, enterprises and governments may identify data integrity as a primary concern, while consumers may be most concerned about protecting personal information. Acknowledging these perspectives is just the start; the real question is what industry actors and government authorities can do to improve IoT security.

Industry can build security into the development and implementation of IoT devices and infrastructure. However, the number of IoT devices, the scale of their deployments, the heterogeneity of systems, and the technical challenges of deployment into new scenarios require an approach specific to IoT. Because this complex ecosystem depends on many players with a broad and diverse range of security concerns—manufacturers and integrators, developers, deployers, and operators—there are emerging security best practices appropriate for each of these roles.

Government can support those efforts through the development of sound policies and guidelines. As stewards of societal well-being and the public interest, governments are in a unique position to serve as catalysts for the development of good IoT security practices, build cross-disciplinary partnerships that encourage public-private collaboration and inter agency cooperation, and support initiatives that improve IoT security across borders. There is broad evidence that this is well underway as demonstrated by supporting examples of government initiatives from around the world as reference points.

[1] "The Fourth Industrial Revolution, by Klaus Schwab," World Economic Forum, https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab (last accessed April 2017).

Introduction

Digitization and the increasing connectivity between devices, citizens, and their governments continue to transform many aspects of our societies and economies in meaningful ways. Smart cities benefit from sensors that can measure air quality, traffic flow, and energy consumption. Smart manufacturing becomes the norm in Industry 4.0, where intelligent machines are networked so they can exchange and respond to data to independently manage industrial production. The Internet of Things is a transformational concept.

In 1999, Kevin Ashton, co-founder of the Auto-ID Center at the Massachusetts Institute of Technology, envisioned an Internet of Things based on RFID chips that could enable "things" to communicate with each other.[2] Since that time, declining hardware costs, miniaturization of sensors, the emergence of hyper-scale cloud computing, and the proliferation of Internet connectivity have created an environment where IoT usage can grow at a geometric rate. Estimates vary, but some have projected that they will nearly double in the next three years from about 28 billion devices today, to more than 50 billion by 2020.[3]

It is not just the sheer number of IoT devices that will have an impact, but how they connect the physical and cyberworlds. IoT breaks the confines of traditional computer networks and establishes connections directly with objects in the physical world. The core concept of this phenomenon is that IoT allows for "things" to connect to the Internet, ranging from the significant—airplanes, elevators, solar panels, medical equipment—to the mundane—toys, soap dispensers, and porch lights.

To the extent that IoT is an extension of current platforms and networks, many of the same risks to the confidentiality, integrity, and availability of data still apply. However, many connected devices will be deployed into environments with older legacy systems that cannot be easily managed and updated, or they may fall under multiple regulatory jurisdictions with different requirements, or into consumer environments with fewer resources for significant security management.[4]

These challenges provide ample reason to bring governments and the technology industry together to increase the security of IoT networks and devices generally, and to ensure an adequate security baseline that addresses all IoT elements. This paper offers an overview of the security challenges related to IoT and provides guidance on the roles that both industry and government can play in ensuring its security and building a foundation of trust in the Internet of Things.

---

[2] Kevin Ashton, "The 'Internet of Things' Thing," *RFID Journal* (June 22, 2009), http://www.rfidjournal.com/articles/view?4986

[3] "Internet of Things (IoT): number of connected devices worldwide from 2012 to 2020 (in billions)," Statista, accessed April 2017, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide

[4] The President's National Security Telecommunications Advisory Committee (NSTAC) Report to the President on the Internet of Things, Nov. 19, 2014, Appendix E, https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf

What exactly is the Internet of Things?

There is no universally agreed-on definition of IoT, perhaps in part because the term IoT does not simply describe a new type of technical architecture, but a new concept that defines how we interact with the physical world.

The US National Security and Telecommunications Advisory Committee (NSTAC) has defined IoT based on three shared common principles: [5]

Devices
Devices within a network are instrumented so they can be addressed individually.

Platform
Devices are interconnected by way of a shared platform, such as a cloud service.

Intelligence
Devices may perform functions adaptively, on their own or with other devices and applications, based on programming and inputs from the physical world.

[5] NSTAC Report, page 3.

Security concerns about the Internet of Things from a user perspective

The cybersecurity concerns of IoT user communities will differ. But these concerns provide a convenient lens for making sense of the IoT security issues, and can help policymakers develop an understanding of how different users frame and express their IoT security concerns. Empathizing with the user's perspective enables more responsive policy approaches, and helps calibrate guidance and requirements so that they effectively address security concerns without limiting IoT innovation.

Therefore, we propose a framework organized by the three core groups of users—consumers, enterprises, and governments—and provide an illustrative (though not exhaustive) view into how they use IoT.

Consumers

Consumer IoT users may use connected devices in their homes, automobiles, clothing and accessories, and other aspects of their daily lives. Typically, consumer-level IoT uses are characterized by:

- Individuals or groups of users that use shared hardware with relatively limited computing power. For example, several members of a family may share the same Internet-connected device, such as a television or a security system where people share a common account or might have their own accounts.
- Engagement with user-generated data and machine-generated insights through a cloud-based application delivered on websites and small-screen devices. Users may, for instance, track their physical activities through wearable sensors and then use an application for insights into their fitness gleaned from the sensors.
- Sensitive data shared by the user to generate value out of the connected devices. For example, putting an Internet-connected video camera at home can help people monitor for burglars or watch their pet, even though the camera may also capture personal moments that users would not want others to see.

Security concerns in these scenarios often focus on the exposure of private activity or sensitive personal information. In some cases, governments have intervened to ensure that manufacturers implement a reasonable level of cybersecurity defense and truthfully represent security practices.

For example, in 2013 the US Federal Trade Commission (FTC) settled a complaint against a manufacturer of home video cameras that had misrepresented the products' security posture. According to the FTC, "The cameras had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet address." The FTC noted that, among other poor security design choices, the manufacturer had "failed to use reasonable security to design and test its software, including a setting for the cameras' password requirement. As a result of this failure, hundreds of consumers' private camera feeds were made public on the Internet."[6]

---

[6] "Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy," Federal Trade Commission, last modified on September 4, 2013, https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles

Enterprises

Enterprises leverage IoT to improve business processes (supply chain, inventory, maintenance), enhance customer experiences (retail, delivery), and take innumerable other innovative approaches to resolving business challenges. The concept of Industry 4.0, also referred to as a technology-powered Fourth Industrial Revolution, is evidence of this trend.

For example, Rockwell Automation, a firm that provides industrial automation solutions, automated the collection and analysis of data from remote installations across the supply chain of petroleum companies.[7] Similarly, elevator company thyssenkrupp worked with Microsoft to create a line of connected intelligent sensors that monitor millions of elevators around the world in real time, enabling the company to improve their reliability and cut maintenance costs.[8]

Like consumers, enterprises are concerned with vulnerabilities and threats that could lead to compromises of privacy. But they also have other concerns, many of which stem from the challenge of managing IoT security at enterprise scale:

- Operations depend on data integrity and availability, therefore potential for data corruption by attackers can have severe consequences. For instance, a medical device could be hacked to provide false information to the doctor, or a car could receive sensor data indicating that there is no car in the adjoining lane. In addition, ransomware can be particularly damaging to enterprises with its resulting denial of access to data.
- Traditional cybersecurity threats can be significantly more powerful because of IoT, such as distributed denial of service (DDoS) attacks that can make an online service unavailable by overwhelming it with traffic from multiple sources. For example, when an IoT deployment on a college campus was compromised, thousands of connected devices were turned against the campus's own network in a DDoS attack.[9]
- Managing security updates in always-on scenarios such as production environments that operate around the clock 365 days a year, where temporary shutdowns for security updates may cause significant disruptions to system availability.
- Whether the cloud services supporting IoT can demonstrate compliance with international standards, such as ISO 22301 for business continuity management, ISO/IEC 27001 for information security management, and ISO/IEC 27018 for data privacy in the cloud.[10]

As IoT continues to gain traction in the enterprises, questions of security are top of mind for business decision makers. Many enterprises are struggling to determine how secure their end-to-end IoT infrastructure is, and some of them even delay the implementation of IoT technologies until best practices and standards can be established and confirmed. One method to move forward with an IoT deployment is to conduct security evaluations of an entire IoT stack, including the security capabilities of connected devices, to gain insights into potential vulnerabilities.[11]

---

[7] "Fueling the Oil and Gas Industry wih IoT," Microsoft Corporation, last modified on December 4, 2014, https://blogs.microsoft.com/iot/2014/12/04/fueling-the-oil-and-gas-industry-with-iot

[8] "Microsoft HoloLens enables thyssenkrupp to transform the global elevator industry," Microsoft Corporation, last modified on September 15, 2016, https://blogs.windows.com/devices/2016/09/15/microsoft-hololens-enables-thyssenkrupp-to-transform-the-global-elevator-industry/#xULXoLwKMCjvkm2J.97

Governments

Given the breadth of societal roles that governments fulfill, their uses for IoT may be even more diverse than those of enterprises. The many areas in which governments see potential applications of IoT span from e-governance that uses technology to improve services for citizens to environmental protection using sensors to monitor the bacterial levels of rivers and lakes. Smart cities have given rise to a broad range of IoT-powered scenarios that rely on connected devices and sensors—for example, connected street lamps that not only provide light but also measure environmental factors —that will change how city officials deliver services, and how municipal government and citizens interact in the physical world.

Governmental concerns about IoT security are likely to be similar to those of enterprises, but with particular scrutiny given to key areas:

- Meeting baseline security requirements for government through standardized processes, like FedRAMP, the US federal government's program to authorize cloud services for US government agencies.
- Resilience against threats directed at government infrastructure, such as nation-state attacks that rely on deep network penetration to undermine functionality, compromise data, and cause other negative impacts.
- The duration of security support for IoT products and services, ensuring that a product's end of support (or end of life) is sufficiently predictable for long-range planning.

Government reliance on IoT has already been tested in high-profile situations. For example, the San Francisco Municipal Transit Agency experienced a ransomware attack in November 2016 that shut down its ability to collect fares. Fortunately, because the agency had backed up its data, no ransom was paid and the systems were quickly restored to normal.[12]

As these examples demonstrate, the IoT is subject to an array of security challenges that could limit development and slow progress toward broad usability. Both industry and government have roles to play in addressing these challenges. Industry can build security into the development and implementation of IoT devices and infrastructure, and government can support those efforts through the development of sound policies and guidelines.

---

[9] "IoT Calamity: the Panda Monium," Data Breach Digest, Verizon, 2017, http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-sneak-peek_xg_en.pdf

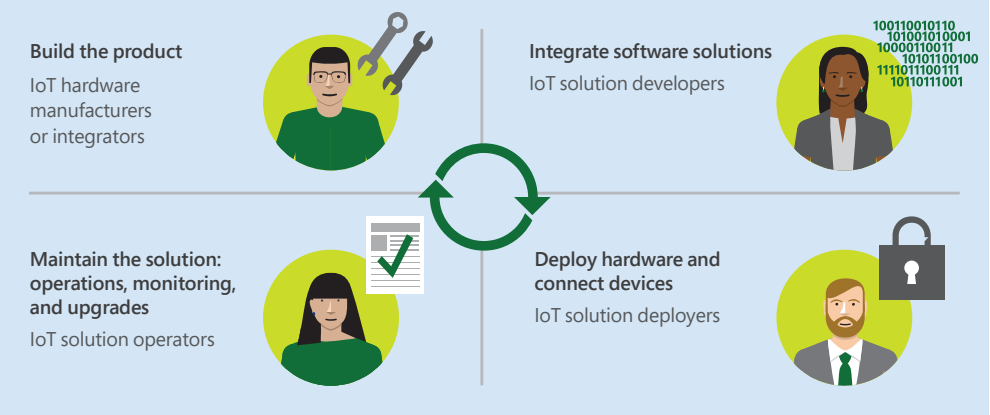
[10] For example, the Microsoft Azure IoT Hub was recently awarded nine industry-leading certifications to demonstrate the company's commitment to supporting users with their compliance needs. https://blogs.microsoft.com/iot/2016/12/07/azure-iot-hub-awarded-9-industry-certifications-for-public-cloud-computing/

[11] For instance, Microsoft announced the Security Program for Azure IoT, which brings together a curated set of security auditors customers can choose from to perform a security audit on their IoT solutions. https://blogs.microsoft.com/microsoftsecure/2016/10/26/securing-the-internet-of-things-introducing-the-security-program-for-azure-iot/

[12] "San Francisco Rail System Hacker Hacked," Krebs on Security, last modified on November 16, 2016, https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked

Industry: Enhancing IoT security through a role-based approach

The IoT ecosystem depends on several key roles - manufacturers and integrators, developers, deployers, and operators. The graphic below outlines these roles and their contribution to the IoT ecosystem.



One way to grasp the security issues each role must address is to examine appropriate security practices for each one. At Microsoft, our experience with IoT networks has helped us identify best practices relevant to each of these roles. While they are not intended as direct recommendations for policy initiatives, they can help policymakers understand the complexity of the IoT ecosystem and how security responsibilities can be distributed across it.

IoT hardware manufacturers or integrators

These are the manufacturers of IoT hardware, integrators assembling hardware from various manufacturers, or suppliers providing hardware for an IoT deployment manufactured or integrated by other suppliers. Microsoft recommends several practices to secure IoT hardware:

- **Scope hardware design to minimum requirements.** To avoid opening the device to unwanted attack vectors, hardware design should include the minimum features required for operation of the hardware and nothing more. For example, include USB ports only if necessary for the operation of the device as unnecessary access points can enable attackers.
- **Make hardware tamper-proof.** Build mechanisms that can detect physical tampering, such as opening the device cover or removing a part of the device, and send an alert as part of the data stream uploaded to the cloud.
- **Build security into hardware.** Build security features such as encrypted storage or integration of cryptographic keys into devices.
- **Make upgrades secure.** Firmware upgrades during the lifetime of the device are inevitable. Building devices with secure upgrade paths and cryptographic assurance of new firmware versions will help ensure device security during and after upgrades.

IoT solution developers

Developers of IoT solutions are typically either part of an in-house team or a system integrator who specializes in this activity. They may develop various components of the solution from scratch, integrate off-the-shelf or open-source components, or adopt preconfigured solutions with minor adaptations. To secure IoT solutions, Microsoft recommends the following practices:

- **Follow secure software development methodology.** Development of secure software requires end-to-end thinking about security from the inception of the project, including choice of platform, language, and tools, to its implementation, testing, and deployment. For example, the Microsoft Security Development Lifecycle provides a step-by-step approach to building secure software.[13]
- **Choose open-source software judiciously.** Open-source software can enable quick development of solutions. However, when choosing open-source software, consider the activity level of the community for each component. Look for an established community that actively supports its software and is responsive to addressing vulnerabilities and other issues that are uncovered.
- **Integrate with care.** Many software security flaws exist at the boundary of libraries and application program interfaces (APIs). Functionality that may not be required for the current deployment might still be available via an API layer, so make sure to check for security flaws at all interfaces of components being integrated.

IoT solution deployers

Deployment involves setting up hardware, connecting devices, and installing software in devices or in the cloud. Use these best practices for more secure deployments:

- **Install hardware securely.** IoT deployments may require hardware to be installed in unsecure or unsupervised locations such as public spaces. In those situations, the deployer must ensure the hardware is protected from tampering. For example, if USB or other ports are available on the hardware, make sure that they are covered securely to keep attackers from using them as entry points.
- **Keep authentication keys safe.** Each device requires an ID and associated authentication keys generated by the cloud service. Keep these keys physically safe even after deployment; a criminal can use a compromised key to impersonate an existing device andsend false data to the operator.

[13] Microsoft Security Development Lifecycle, https://aka.ms/msSDL

IoT solution operators

Once deployed, IoT solutions require monitoring, upgrades, and maintenance. This is most often done by an in-house team of IT specialists, hardware operations and maintenance teams, and domain specialists who monitor the behavior of the overall infrastructure. These best practices will help maintain the security of devices over the long term:

- **Keep the IoT system up to date.** Ensure that device operating systems and all device drivers are upgraded to the latest versions. Microsoft provides automatic updates for its operating systems including Windows 10; other operating systems, such as Linux, may offer this service, or organizations may need to schedule updates themselves.
- **Protect against malicious activity.** If the operating system permits, install the latest anti-virus and antimalware software on each device to help protect against external threats. Make sure that these are updated regularly.
- **Audit frequently.** Audit IoT infrastructure for security-related issues on a regular basis. Most operating systems build in event-logging that must be reviewed frequently to assess the state of the network, including whether security incidents have occurred.
- **Protect the physical IoT infrastructure.** Security attacks against IoT infrastructure can be launched using physical access to devices, for example, the malicious use of USB ports. Logging physical access is a key way to help uncover these physical breaches.
- **Protect cloud credentials.** Cloud authentication credentials used for configuring and operating an IoT deployment can also be a way for a bad actor to gain access and compromise an IoT system. Secure and user-friendly authentication for the user can mitigate the risk of credential theft and account compromise, such as multi-factor authentication or biometrics.

Government: Advancing IoT security through policy

As stewards of societal well-being and the public interest, governments have a special role to play in delivering the vision of a secure IoT and supporting its development. Governments also have unique capabilities to convene stakeholders to address shared challenges, promote best practices through guidance, and intervene as regulators. Indeed, governments around the world have leveraged these capabilities in different ways to address the growth of IoT.

Microsoft offers several recommendations to help governments develop policies that advance IoT security. Governments can:

- Serve as catalysts for the development of good IoT security practices.
- Build cross-disciplinary partnerships that encourage public-private collaboration and inter-agency cooperation.
- Support initiatives that improve IoT security across borders.

We also include supporting examples of government initiatives from around the world as reference points. Given the nascent state of IoT policy development, this will help governments learn from each others' approaches and perspectives as their IoT initiatives move forward.

Encourage the use of good IoT security practices

Raise awareness of best security practices and guidelines

Not every business has the knowledge and expertise to make smart decisions about security when developing and deploying IoT devices and services. Governments can enable better security outcomes by promoting best practices that range from security-by-design principles to sector-specific product development and risk assessment guides.

Examples

- The US Department of Homeland Security offers broad guidance on improving security in the design, manufacture, and deployment of IoT devices. This guidance is not limited to a particular sector and is not regulatory in nature, which makes it accessible to audiences across the IoT ecosystem.[14]
- The Internet and Security Agency of the Government of Korea published a guide that identifies 15 security principles for the development of IoT devices. They cover the whole lifecycle from their design and development to their installation and operation (and ever retirement). The government plans to update this security guidance as IoT technology evolves. [15]

---

[14] Strategic Principles for Securing the Internet of Things, US Department of Homeland Security, November 15, 2016, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

[15] "IoT Common Security Guide," Korea Internet Security Agency, last modified on October 6, 2016, https://www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=1&mode=view&p_No=259&b_No=259&d_No=80&ST=&SV (Korean).

Develop enhanced guidance for safety critical sectors

Greater investments in cybersecurity and system resilience apply in particular to devices that support human life, critical infrastructure, transportation, and other essential functions, whose inability to function and lack of resilience could have dire consequences.

Examples

- The US Food and Drug Administration has issued guidance to encourage management of cybersecurity vulnerabilities for medical devices that are already on the market.[16] In particular, it supports limiting the impact of cybersecurity incidents on devices, thereby reducing patient risk by applying the NIST Framework for Improving Critical Infrastructure Cybersecurity.[17]
- In Japan, the National Center of Incident Readiness and Strategy for Cybersecurity recommends measures to protect against the physical consequences of compromises in or breaches of IoT security, such as when safety concerns flow as potential consequences from cybersecurity concerns. It highlights that IoT security incidents can have impact in the physical world, for instance through large machines that could harm workers operating them, and should be addressed appropriately.[18]

Invest in IoT security training, education, and raise public awareness

Government investments in workforce development and awareness-raising campaigns can help increase the scale and impact of industry-led efforts.

Examples

- Building the IoT ecosystem will depend on a knowledgeable workforce. There are a number of steps that governments can take to encourage schools, universities, and training programs to adopt curricula that advance the knowledge of information security in general and IoT security specifically. The UK Government Office for Science, as one of is ten recommendations for government policymakers, includes promoting the integration of computational thinking in the curricula of schools and training programs.[19]
- The US Federal Trade Commission, drawing on lessons learned from its own data security cases, has developed a business education initiative, "Start with Security," which gives enterprises of all sizes ten effective security measures they can take to protect their data.[20]

---

[16] Postmarket Management of Cybersecurity in Medical Devices, US Food and Drug Administration, December 28, 2016, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[17] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology (NIST), February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[18] General Framework for Secure IoT Systems, National Center of Incident Readiness and Strategy for Cybersecurity, Government of Japan, August 26, 2016 https://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf

[19] The Internet of Things: making the most of the Second Digital Revolution, UK Government Office for Science, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

What about certifying or labeling IoT devices based on security?

The primary goal of a certification program should be to improve security by providing more information to consumers and incentivizing the broader IoT marketplace. Organizations have called for a certification or product labeling approach to IoT device security. The U.S. Presidential Commission on Enhancing National Cybersecurity called for the creation of a cybersecurity "nutritional label" to inform consumer purchasing decisions.[21] Similarly, the European Commission has contemplated a Trusted IoT Label and the establishment of minimum security baselines for IoT devices.[22]

An effective IoT device security certification or labeling program should embrace three key principles:

- **Informed by a robust multistakeholder consultative process.** Stakeholders from across the IoT ecosystem should be integrated into an open and transparent process for developing a certification program. Device manufacturers, software providers, user advocates, and security researchers are among those who should be included along with government representatives.
- **Aligned with international standards.** Certification programs should align with international standards and standardization efforts, not duplicate or contradict them. For example, the OPC Foundation already operates a certification process for its industrial interoperability standard.
- **Flexible implementation.** IoT deployments vary widely. There should be flexibility in how adherence to a certification program is communicated to consumers, whether on a box, website, or other means.

[20] "Start with Security: A Guide for Business," US Federal Trade Commission, June 2015, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[21] Report on Securing and Growing the Digital Economy, Commission on Enhancing National Cybersecurity, 2016, https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

[22] "Commission Staff Working Document, Advancing the Internet of Things in Europe," European Commission, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0110

Build cross-disciplinary partnerships to enhance IoT security

Encourage collaboration between the public and private sector

IoT policy issues are often driven by IoT's unprecedented scale, which can impact a diverse range of stakeholder groups in new ways. For example, realtors may face new challenges in marketing and selling a smart home if its connected elements cannot easily be transferred over to a new owner, while retailers may grapple with how compromised IoT devices impact customer satisfaction and loyalty. Including a broadly representative group of stakeholders can be particularly useful in developing, updating, and maintaining IoT security guidance.

Examples

- The German Plattform Industrie 4.0 convened more than 100 private and several public-sector organizations to create a framework and recommendations for how to implement and manage the digitization of industrial manufacturing, including its security. As part of the network, one working group on the security of networked systems is addressing the implications of cyber attacks on the production process, and offering guidance for small and medium-sized companies on how to secure their infrastructure.[23]
- The US Department of Commerce has created a multi-stakeholder process to address the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things. Their goal is to foster a more security-focused IoT market, particularly with respect to support for security updates and product patching.[24]

Create an interagency task force to coordinate security efforts

The impact of breakdowns in cybersecurity cuts across organizational boundaries, so creating an interagency or inter-ministerial IoT task force can balance perspectives on security and risk management. Such a task force could develop policies and coordination efforts that address these cross-organization security issues.

---

[23] "The background to Plattform Industrie 4," Germany Federal Ministry for Economic Affairs and Energy, 2017, http://www.plattform-i40.de/I40/Redaktion/EN/Standardartikel/plattform.html

[24] Multistakeholder Process on Internet of Things Security Upgradability and Patching, US National Telecommunications and Information Administration, September 2016, https://www.ntia.doc.gov/files/ntia/publications/2016-22459.pdf

[25] Eric Wood, "The Internet of Things can't work without cooperation," Microsoft Corporation, January 29, 2015, https://blogs.microsoft.com/work/2015/01/29/internet-things-cant-work-without-cooperation/#sm.0011nu14713g1fjexb2137e347suk

[26] Industrial Internet of Things: Unleashing the Potential of Connected Products and Services, World Economic Forum, January 2016, http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

[27] "What is OPC?," OPC Foundation, last accessed April 2017, https://opcfoundation.org/about/what-is-opc

[28] "Security Check Performed by German Federal Office for Information Security," OPC Foundation, June, 2016 http://opcconnect.opcfoundation.org/2016/06/bsi-security-check

[29] "About ENISA," European Union Agency for Network and Information Security, last accessed April 2017, https://www.enisa.europa.eu/about-enisa

Support initiatives that improve IoT security across borders

Promote the development of secure, open, consensus-based standards

As new IoT technologies develop, there will be an increasing need to ensure interoperability between new IoT systems and legacy technology systems. Without commonly accepted standards, IoT could potentially fall short of the promise of a connected world.[25]

The World Economic Forum reports that one of the greatest barriers to IoT adoption by many businesses is a lack of interoperability, which can significantly increase complexity and cost.[26] While some Internet protocols can be adopted from existing standards, IoT has specific security requirements that must be addressed separately. Governments can encourage the development of open, voluntary, consensus-based, and globally relevant standards that foster greater interoperability.

Examples

- In the manufacturing sector, the OPC Foundation developed the open-source OPC Standard that companies can follow to help enable the secure exchange of data in automated industrial settings.[27] (The OPC Foundation includes many of the world's largest automation and industrial suppliers, including Microsoft.) After performing a check of the OPC Unified Architecture's (UA) security functions, the German Federal Office for Information Security confirmed it was designed with security in mind and no systemic security vulnerabilities were found.[28]

Harmonize approaches to IoT security across national borders

Manufacturers of IoT devices want to market their devices worldwide, no matter where the underlying code was developed or the devices were manufactured. Governments are in a position to reduce the possible costs for small and medium-size IoT manufacturers to meet IoT security requirements by harmonizing them across countries.

Examples

- The European Union Agency for Network and Information Security (ENISA), a center of expertise for cybersecurity in the EU, is advising member states, countries outside the EU, and the private sector on cybersecurity issues.[29] Based on recent trends of critical infrastructures implementing an increasing number of IoT technologies, ENISA also offers guidance for specific user groups, such as Smart Cars, Smart Homes, Smart Airports and Smart Cities across the EU.[30]
- The Alliance for Internet of Things Innovation, launched by the European Commission and several IoT players, is facilitating the dialogue between several IoT stakeholders to establish a thriving IoT ecosystem across the EU. In its report on policy issues, working group four provides recommendations on how governments can leverage existing efforts, such as the Network and Information Security Platform or the NIST Cyber Physical System Public Working group, as well as security-by-design and best development practices amongst others.[31]

---

[30] "IOT and Smart Infrastructures," ENISA, last accessed April 2017, https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures

[31] Report AIOTI Working Group 4 - Policy, Alliance for Internet of Things Innovation (AIOTI), October 15, 2015, https://aioti-space.org/wp-content/uploads/2017/03/AIOTIWG04Report2015-Policy-Issues.pdf

Conclusion

Securing IoT requires collaboration – across borders, sectors, and organizations – with a sense of urgency. However, the relevant stakeholders, implications of potential policies, and indeed, the relevant technologies themselves are still evolving. Policymakers must therefore take a long-range view of problems and solutions, while moving with agility in the face of a changing landscape.

Dialogue is the most important ingredient for meaningful progress in IoT cybersecurity policy. Policymakers have significant opportunities to create spaces where challenges can be explored and solutions identified, whether through public consultations led by governments or non-governmental organizations, collaboration across stakeholders towards common frameworks or standardized approaches, or other forums. These processes can increase understanding of different perspectives and ultimately lead to policy proposals that are relevant to key constituencies and supported by them.

Looking forward, cybersecurity policy for IoT will only increase in importance as the world grows more connected. The IoT user communities noted in this paper – consumers, enterprises, and governments – will face new security challenges stemming from IoT, including situations where users may not even be aware that they are interacting with a connected device. Addressing these scenarios requires careful consideration of how to balance security needs with opportunities for innovation.

Microsoft looks forward to supporting the growth of a secure IoT ecosystem through advancements in technology and policy, in partnership with stakeholders from across the public and private sectors.


Microsoft