Internet Society

CANADIAN MULTISTAKEHOLDER PROCESS

ENHANCING IOT SECURITY

Final Outcomes and Recommendations Report

Innovation, Science and Economic Development Canada

cira

canarie

cippic Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt publique et de politique d'Internet du Canada Samuelson-Glushko

Table of Contents

Definitions

ccTLD: Country Code Top-Level Domain

CEAWG: Consumer Education and Awareness Working Group

CIPPIC: Canadian Internet Policy and Public Interest Clinic

CIRA: Canadian Internet Registration Authority

CSA: Canadian Standards Association

CSIRT: Computer Security Incident Response Team

CTIA: Cellular Telecommunications and Internet Association, USA

CVP: Cyber Verification Program

DCMS: UK Department of Digital, Culture Media and Sport

DLWG: Device Labeling Working Group

DNSSEC: Domain Name System Security Extensions

DOTS: DDoS Open Threat Signaling

ENISA: European Union Agency for Network and Information Security

IETF: Internet Engineering Task Force

ISED: Ministry of Innovation Science and Economic Development

ISO/IEC: International Organization for Standardization/International Electrotechnical Commission

ISOC: Internet Society

ISP: Internet Service Provider

ITU: International Telecommunications Union

MUD: Manufacturer Usage Description

NCCoE: National Cybersecurity Center of Excellence

NIST: National Institute of Standards and Technology

NRWG: Network Resilience Working Group

OC: Oversight Committee

OSMUD: Open Source Manufacturer Usage Description

OWASP: Open Web Application Security Project

PIPEDA: Personal Information Protection and Electronic Documents Act

SDO: Standards Development Organizations

SIDN: *Stichting Internet Domain Namen* (registry for .NL)

SPIN: Security and Privacy for In-home Networks by SIDN

UPnP: Universal Plug and Play

Executive Summary

The Internet of Things (IoT) carries enormous potential to change the 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.

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 cyberattacks, compromising sensitive data, weaponizing data, and threatening the safety of individual users.

These risks and rewards are being carefully considered by many governments and global organizations. However, given the Internet's global reach and impact, it is critical that its security be addressed collaboratively. That is why the *Canadian Multistakeholder Process: Enhancing IoT Security* initiative was launched.

Recognizing the complexity of mitigating cyber security risks from the global proliferation of IoT and the resulting necessity for a made-in-Canada policy to address these risks, the Internet Society, in partnership with the Ministry of Innovation Science and Economic Development (ISED), the Canadian Internet Registration Authority (CIRA), Canadian Internet Policy and Public Interest Clinic (CIPPIC), and CANARIE, undertook a voluntary multistakeholder process for the development of broad-reaching recommendations to enhance IoT security in Canada.

This initiative brought together a multistakeholder group — drawn from the Canadian Internet community — to explore both the scope of challenges and the range of promising solutions that could be pursued further to address them, guided by the following principles:

1. The complexity of IoT security necessitates a bottom-up, organic process to ensure the outcomes address all existing and potential challenges and issues.[1] The approach should be fluid in nature, defined and refined through discussion with stakeholders.
2. Internationally harmonized technical standards are key to enhancing IoT security in the long-term, but they are hard to get right and take time. It is reasonable for approaches to IoT security to start at a national level while working in collaboration with other national, regional, and international bodies.
3. Because of the immediacy of the risks and the extended time frame of long-term developments, such as improvements to framework policies and the development of international standards, it is important to start work on educating consumers and for businesses to begin adopting best practices that will reduce the risks of consumer IoT device adoption.

Within this context, the initiative was focused on consumer-level devices as opposed to those that are being utilized at the enterprise level.[2] Throughout 2018 and early 2019, the *Enhancing IoT Security* multistakeholder group engaged in a series of in-person multistakeholder meetings, focus groups, and webinars and conducted research to develop the following:

1. A shared set of definitions and benchmarks around the security of Internet-connected devices.
2. Shared guidelines to ensure the security of Internet-connected devices over their lifespan, including the development, manufacturing, communications, and management processes.
3. Recommendations to inform national policy related to IoT security in Canada.

A defining feature of the *Canadian Multistakeholder Process: Enhancing IoT Security* initiative was the use of the multistakeholder approach in its organization, governance, and decision-making. Oversight and guidance were provided by the initiative partners (the Oversight Committee3) and management was provided by the Internet Society. Appendix II explores the role the multistakeholder model played in this work and outlines key learnings from the process.

Three thematic working groups, Network Resilience, Device Labeling, and Consumer Education and Awareness, were established to inform the process and to develop specific recommendations. The recommendations of these Working Groups cover the technical, policy, and behavioural aspects of IoT security.

1 A multistakeholder process is particularly well adapted to discovering insights when the dimensions of the issue are not clear; when the solutions are undetermined; and when in general people do not have the answers, there is no consensus around the possible answers, or approach is lacking.

2 Participants reached near consensus to define IoT as "any network-exposed device not historically accessible, or any device transmitting data, via the Internet, which generally lack sufficient built-in security to protect themselves from causing or becoming a source of harm."

3 See Appendix I

Best Practices, Recommendations, and Next Steps:

Certain aspects of IoT security are so well-established that they were asserted as baseline actions that must be taken to enhance IoT security, including the following:

1. No universal or easily guessed pre-set passwords.
2. Data should be transmitted and stored securely using strong encryption.
3. Data collection should be minimized to only what is necessary for a device to function.
4. Devices should be capable of receiving security updates and patches.
5. Device manufacturers should notify consumers if there is a security breach.
6. Device manufacturers should ensure consumers are able to reset a device to factory settings in the event of a sale or transfer of the device.

Over the course of a year, the multistakeholder group and the Working Groups worked together to develop the following over-arching recommendations:

1. Elevate the focus on international-level standards. Standards can provide clear, testable, and credible guidance on implementing security and privacy by design across all jurisdictions.
2. Continue development and deployment of the Secured Home Gateway at CIRA and the Manufacturer Usage Description (MUD) standard at the Internet Engineering Taskforce (IETF) in order to provide network-level approaches to resiliency that can address the challenge of low-cost, foreign-made devices that do not adhere to security standards (which are designed for specific devices and firms).
3. Continue to develop a consumer friendly label alongside international-level standards. It is recommended that a label combine static "trustmarks" (such as for CE in Europe, Kitemark in the UK, CSA in Canada) with a live component such as a QR Code that can convey advanced and up-to-date product security information.
4. Leverage the multistakeholder group's core content for consumer education and awareness (the Shared Responsibility Framework). This could be used in efforts or campaigns to raise consumer and industry awareness. With funding, a consumer education campaign could be organized by a multistakeholder group that leverages the network created by this Canadian IoT initiative. The Working Groups also developed more granular recommendations for specific stakeholder groups, identified in the following sections.

On Internet-connected device labeling

Recommendations:

1. Develop a security label for Internet of Things (IoT) and other digital products.
2. Adopt standards for testing and evaluation of IoT products to assist purchasing decision.
3. Promote consumer awareness programs for both product labels and testing.
4. Enact a regulatory framework that requires formal testing and evaluation of products.
5. Create a flowchart that could be used by manufacturers to determine requirements, and by users to determine label expectations.

An effective security label should combine the consumer trust factor of known "trust marks" (such as CE in Europe, Kitemark in the UK, and CSA in Canada) with advanced and critical product security information that can be updated. The label should convey the key information that formal testing and certification has been performed on the product, and how to access up-to-date critical information on product security features and installation/deployment considerations. Examples of security labels can be found in Section 3.3.

Recommended Next Steps:

1. Approach and collaborate with organizations focusing on IoT security and privacy in an attempt to reduce the amount of fragmentation in the market for initiatives and labels to avoid consumer confusion.
2. Continue to influence the standards effort through the International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) for international standards and standards developing organizations with similar projects and interests.
3. Collaborate with the Online Trust Alliance (OTA) to approach key vendors and solution providers to raise awareness on the need for security certification and device labels.
4. Determine the best organization to provide a formal specification of the "live label." This could be Internet Engineering Taskforce (IETF) or similar, and includes further developing the live label (QR Codes) proposal through collaborating with other organizations such as OTA.
5. Elevate the proposed voluntary labeling framework as a model for consumer IoT device manufacturers to demonstrate their compliance with existing Canadian law and regulations in this space.
6. Further assess the certification and testing of applications that control devices and backend support services, in addition to focusing on the devices themselves.
7. The development of labeling concept should continue. Labeling can be incorporated as a 'control' as part of IoT security-related standards being developed at the national/regional (T200) and international (SC27030) level.
8. There is a need for a regulatory framework for required formal testing of standards and mutual recognition options between IoT standards, similar to the type of agreements that govern telecommunications equipment.

The Device Labeling Working Group proposes that a security product label should include the following:

1. Identification of the organization overseeing/authorizing the certification and formal testing (e.g. BSI Kitemark, CE mark, CSA mark).
2. A machine-readable code that is linked to a website providing up-to-date product information (i.e., a live label). The website should include the following:
    a. Product model and/or version number
    b. Latest product firmware version number
    c. Recent vulnerability information
    d. Certification/testing framework
    e. Security configuration guide
    f. Information on data collection and sharing
3. Key information to be conveyed by the label:
    a. Formal testing and certification have been performed on the product.
    b. Where to get up-to-date critical information on product security features and installation/ deployment considerations.

The next steps for implementation must be carried out by many stakeholders, including, but not limited to:

4. IEEE Data Port (free resource of large datasets to be fed into the process).
5. Vendors, security experts, consultants.
6. Civil society, to add consumer perspectives to the standards discussion.
7. ISED and government technical experts who can influence the standards discussion to provide public policy considerations, including implication legislation and enforcement.

On consumer education and awareness

The Consumer Education and Awareness Working Group developed a Shared Responsibility Framework which recommends behaviours for consumers and industry. The Working Group recommends that the Implementation Working Group focus on how to take the content of the Framework, as well as related messaging in the other working groups, to further develop and ultimately raise consumers and industry awareness.

SHARED RESPONSIBILITY FRAMEWORK

DEVICE STAGE	DEMAND SIDE: Consumers	SUPPLY SIDE: Manufacturers/Retailers/Government/ Civil Society/Educational Institutions
Before Purchasing	Understand and consent to how the device is collecting, using, and sharing your data.	Improve accessibility and content of privacy policies (i.e., provide clear answers on how the device is collecting, using, and sharing data).
	Ensure that the device comes from reputable/ certified manufacturers (i.e., low cost devices typically come with greater risks. Any smart devices that are connected to the Internet carries a risk of breach).	Clearly lay out the shared responsibility regarding the device's security (i.e., convey expectations of consumers' awareness/ responsibility in the instructions/ToS/warning leaflet of the device).
	Check if there are any extra functionalities (i.e., is the device collecting unnecessary data that could create unnecessary risk? Can you opt out of future features without opting out of security updates?)	Clearly indicate/disclose all functionalities of the device and how to minimize unnecessary functions (i.e., develop a list of sensors in the device, provide information on how to turn off video and audio recording, clearly indicate if new/extra functionalities have been included in updates, and if/how it is possible to opt out of these functionalities).
	Check for user reviews, labels, and certifications (i.e., label and certification indicate that the device has been tested).	Use certification/adherence to laws, standards, and non-binding best practices as a publicized selling feature.
	Consider the lifecycle of the device and the support available to keep your device in use for as long as possible (i.e., verify availability and duration of security upgrades and patches).	Use availability/duration of patches, updates, and support as a publicized selling feature.
	Check that the device works even without Internet connection, and assess functionality in the event the device outlives the company (i.e., smart lock, camera, fridge still function even if the Internet is down or the company no longer exists).	Ensure the devices can still function without Internet connection, and if the company ceases to exist.

SHARED RESPONSIBILITY FRAMEWORK

DEVICE STAGE	DEMAND SIDE: Consumers	SUPPLY SIDE: Manufacturers/Retailers/Government/ Civil Society/Educational Institutions
At Use/Issue	Know where to seek redress and address technical problems, including if your device has been compromised, and keep record of your purchase.	Provide transparent and accessible instructions on seeking redress.
	Follow best practices for network setup and configuration to help mitigate risk when using IoT devices.	Assist consumers to set up their IoT networks consistent with best practices (i.e., make the default setting consistent with best practices).
	Be considerate of the implications or impacts on guests or others who are in the vicinity of your device (i.e., consider notifying your guests when in proximity to your smart home devices, or turning devices off).	Remind consumers about the effects of their IoT devices on their guests (i.e., audio or video recording).
	Be aware that the security of your device is constantly being updated. Ensure that the device is able to receive updates.	Remind consumers to follow recommended security best practices (i.e., follow recommended upgrading and patching recommendations from the NTIA Multistakeholder Process).[4]
	Ensure that each device in your home is secured. The security of your home network is only as good as its weakest link.	Consider providing mechanisms to warn consumers when issues arise (i.e., assist consumers in monitoring their traffic to detect anomalies).
End of Life/Use	Remove data from your device before disposing or moving. Many guides are available to assist users with specific IoT devices (i.e., Nest Thermostat[5]).	Clearly indicate the best method or provide consumer assistance to permanently remove data from device.
	Do not forget to revert back to factory default settings. Many guides are available to assist users with specific IoT devices.	Clearly indicate the best method or provide consumer assistance to revert the device to factory default settings.
	Check the resources that are available to help dispose of IoT devices responsibly. Retailers may provide this information.	Provide resources to help consumers dispose of their IoT devices responsibly.

4 https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf
5 http://www.imove.com/blog/how-to-switch-nest-thermostat-accounts-when-you-move/

Recommended Next Steps:

1. Task the Implementation Working Group with focusing on the delivery of these messages—i.e. convene interested civil society, consumer advocacy, educational institutions, outward-facing Canadian government departments such as the Office of Consumer Affairs (OCA), Canadian Centre for Cyber Security (CCSE), Public Safety Canada, and the Office of the Privacy Commissioner (OPC).
2. Task the Implementation Working Group with providing a multifaceted coordination function, including providing a network where stakeholders could:
    a. Continue dialogue and networking to ensure consistency of messaging.
    b. Share opportunities to input into relevant government processes (e.g., consultations, legislative reviews etc.).
    c. Share their own ongoing IoT-related educational efforts.
    d. Seek support on how to engage their own membership.
    e. Coordinate engagement with industry.
    f. Collaboratively develop an educational campaign (including pooling resources and distribution channels).

On enhancing network resilience

Recommendations:

1. The Secure Home Gateway code should be accepted by the core openWRT[6] project. Furthermore, the openWRT should be bundled by default with its IoT security framework, and/or that when manufacturers upgrade their openWRT software, it comes equipped with this framework.
2. Future work is needed regarding network resilience with regard to IoT security, including:
    a. Security evaluation of any new security/user interaction mechanisms. New MUD-based access controls represent significant new attack surface and must be analyzed and tested.
    b. Continued implementation of a security framework and the integration and development of:
        i. Device fingerprinting
        ii. Automated MUD profile generation
        iii. MUD clearinghouse
        iv. Access controls
        v. User controls (visibility, permissions, notifications)
        vi. Unified onboarding
        vii. DDoS Open Threat Signaling (DOTS)-based DDoS filtering
        viii. Quarantine and un-quarantine procedures
    c. Standards development
        i. Live labels: integration of live label with network onboarding, MUD, user-interaction
        ii. Out of support notification/device management
        iii. Credential management on IoT devices
        iv. Quarantine/unquarantine
        v. (MANRS[7]-inspired) MARIS: Mutually Agreed Norms for Internet Security
    d. Continued global coordination towards standardization, implementation, and adoption.

6 "OpenWrt is an open source project for embedded operating system based on Linux, primarily used on embedded devices to route network traffic." From Wikipedia: https://en.wikipedia.org/wiki/OpenWrt

7 https://www.manrs.org/

Recommended Next Steps:

1. In collaboration with partners, CIRA will continue developing a functional Secure Home Gateway prototype initiative and standard APIs on:
    a. SHG onboarding
    b. IoT device onboarding/management
    c. Device quarantining
    d. Device un-quarantining
2. In collaboration with partners, CIRA will attempt to get two distinct "running code implementations" that are based on the standard APIs.
3. CIRA, in collaboration with the two other Working Groups, will submit Internet drafts for MUD extension to support live labels, privacy notification, user space, IoT device management framework, instant management, and credential management.
4. CIRA's Secure Home Gateway initiative will assess integration with Mozilla's Web of Things initiative.
5. Ensure CIRA's Secure Home Gateway code is available on GitHub, is open source and freely available to all.
6. Integrate the work of this group with the Labeling and Consumer Education and Awareness Working Groups.
7. This working group will reconvene to assess feasibility, new partners, resources required, and to adjust the plan as needed. It will create a mailing list for notification of updates to this work.
8. Raise awareness of stakeholder group recommendations and demonstrate to gateway developers, through the Secure Home Gateway initiative, that these recommendations are achievable, thus providing the larger industry with a framework for secure device development.

Youth-focused recommendations and areas for further research

1. **Education:** For youth in particular, education policy is critical. Provincial/territorial and federal governments should work together with civil society organizations on curricula and programs that can offer forums for discussion and awareness of IoT and other tech-related issues across Canadian educational institutions.

2. **Conversation:** One of the strengths of social media as a medium of engagement is its ability to bring people into a conversation and generate widespread interest in specific topics or events through the multiplying effects of personal networks. Catalyzing authentic personal interest and curiosity through open dialogue which connects a specific issue like IoT security to broader social narratives or concerns is the most effective means of spreading awareness and inspiring action.

3. **Exploration:** Effective engagement and capacity building will also require a deeper dive into assessing the current state of young people's interaction with digital platforms and their knowledge of them.

4. **Improving diversity and multistakeholder access:** Engagement opportunities should be promoted, and not skewed to certain types of organizations over others.

5. **Embed participation:** Avoid requiring significant amounts of additional time from people by incorporating opportunities to learn about and engage with IoT and other emerging technologies, as well as to participate in policy making, into regular education or training activities.

6. **Policy changes:** Policymakers from around the world can use the best practices of existing and proposed regulation to inform and inspire the basis for an approach to data protection for IoT devices.

7. **Collaboration:** Internet governance and policy involves a variety of organizations from a myriad of backgrounds. The topic of IoT security spans multiple interrelated issue areas, each serving as the focus of a number of these groups. In order to prevent duplication of efforts, collaboration and harmonization must increase between these groups at both the community and international level.

The Enhancing IoT Security Implementation Working Group

An Implementation Working Group, made up of members of the OC, WGs, and multistakeholder group, was formed at the sixth and final multistakeholder meeting to ensure the recommendations are implemented and to carry out next steps. Stakeholders will leverage this group to coordinate and contribute to:

1. A coordinated education and awareness campaign on consumer IoT that uses the Shared Responsibility Framework.
2. Canadian participation in national and international standards processes—with specific emphasis on engaging and facilitating the contributions of consumer organizations, civil society, and youth — in particular the development of T200 into a binational standard, the ISO/IEC 27000 series, and the IETF MUD standard.
3. Canadian participation in international IoT security initiatives, integrating or adapting the trajectory set out by the recommendations and input on the final report. This includes the Internet Society IoT Policy Platform,[8] IoXT,[9] IoT Alliance Australia (IoTAA),[10] EU's Cybersecurity Act implementation, etc.
4. The development of the Secure Home Gateway, binary security label, and related standards.

8 https://www.internetsociety.org/iot/iot-security-policy-platform/
9 https://www.ioxtalliance.org/
10 https://www.iot.org.au/

Introduction

IoT carries enormous potential to change the 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.

1.1 Problem Statement

According to one estimate, "connected devices will number 38.5 billion in 2020, up from 13.4 billion in 2015." [11] At the same time, with billions of IoT devices, applications and services already in use and greater numbers coming online every day, securing IoT is of utmost importance. Poorly secured IoT devices and services can serve as entry points for cyberattacks, compromising sensitive data, weaponization, and threatening the safety of individual users. Various studies have used empirical data to show that poorly secured IoT devices have been weaponized to assist perpetrators of domestic abuse to monitor and psychologically abuse their victims.[12] The use of poorly secured IoT devices in this manner poses human rights concerns, particularly for women and other vulnerable groups that are more likely to be victims of domestic abuse.[13]

These risks and rewards are being carefully considered by many governments and global organizations, but given the Internet's global reach and impact, it is critical that its security be addressed collaboratively. That is why the *Canadian Multistakeholder Process: Enhancing IoT Security initiative* was launched.

For more than a year, this initiative convened six in-person, multistakeholder meetings and over a dozen virtual meetings in order to develop recommendations for a set of norms and/or policies to secure IoT in Canada. These events, as well as a comment period on the initial Draft Outcomes Report from this group[14], served as an opportunity to begin planning and implementing a bottom-up, organic process to remedy existing and potential security challenges in Canada's national IoT ecosystem.

11 https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020
12 The Implications of the Internet of Things (IoT) on Victims of Gender-Based Domestic Violence and Abuse (G-IoT) - ucl.ac.uk
13 https://www.canada.ca/en/public-health/services/health-promotion/stop-family-violence/problem-canada.html
14 The comment period was open from February 27, 2019 until March 29, 2019 and ultimately resulted in the submission of comments from eight organizations representing five stakeholder groups.

The *Canadian Multistakeholder Process: Enhancing IoT Security* group reached near consensus to define IoT as "any network-exposed device not historically accessible, or any device transmitting data, via the Internet, which generally lack sufficient built-in security to protect themselves from causing or becoming a source of harm." Within this context, the IoT group focused its activities on consumer devices as opposed to those that are being utilized at the enterprise level.

Though complete consensus was not achieved on a definition of IoT, participants agreed that any definition should be continuously updated as the technology develops. The group also agreed there is value in relying on the existing definitions rather than spending additional time reaching total consensus on its own.

At the first meeting of the *Canadian Multistakeholder Process: Enhancing IoT Security* and throughout subsequent meetings, participants frequently reiterated that there are some aspects of IoT security so well established that this group need not focus its attention on them. Those items included, but were not limited to, the following:

1. No universal or easily guessed pre-set passwords.
2. Data should be transmitted and stored securely using strong encryption.
3. Data collection should be minimized to only what is necessary for a device to function.
4. Devices should be capable of receiving security updates and patches.
5. Device manufacturers should notify consumers if there is a security breach.
6. Device manufacturers should ensure consumers are able to reset a device to factory settings in the event of a sale or transfer of the device.

The objective of this report is to summarize the work of the multistakeholder group, provide insights gained throughout the process, and provide recommendations for policy on IoT security for Canada.

1.2 Methodology

The methodology used for this multistakeholder project was as follows:

1. An Oversight Committee (OC) was created to set the overall goals of the process, review outputs of individual working groups, oversee the development of reports and requests for comments, and approve any external communications. The OC includes representatives from Innovation, Science and Economic Development (ISED), the Internet Society (ISOC), the Canadian Internet Registration Authority (CIRA), Canadian Internet Policy and Public Interest Clinic (CIPPIC), and CANARIE.
2. Decision-making within the Oversight Committee was based on consensus and norms established at the beginning of the process.[15]
3. A transparent multistakeholder group, drawn from government, civil society, academia, technical and security community, the private sector, and other relevant stakeholders was also convened to inform the process, identify appropriate working group members, select areas for research, review documents, and provide guidance to the development of the policy recommendations. Meetings of the multistakeholder group were open, public, and live streamed, with the live stream posted online following each meeting.
4. Reporting to the OC, the Internet Society managed the process.
5. The process was informed by three Working Groups, including on Network Resilience, Device Labeling, and Consumer Education and Awareness, as well as a report submitted to the process on Youth and IoT, focus groups, and research. The subject areas of the respective Working Groups were selected by the multistakeholder group.
6. Primary research was conducted through the expertise from members of the Working Groups and insights gained from participating in various forums.
7. Government participation in the multistakeholder process included activity across a dozen federal departments and agencies.
8. All resources from this project were posted on the initiative website in both English and French.

Efforts were also made to include individuals in these conversations from a variety of regions, languages, and backgrounds. Focus groups were held in both English and French, as well as those targeted at specific demographics, such as youth and Indigenous individuals.

For example, at the 2018 Indigenous Connectivity Summit[16], the Internet Society hosted a roundtable on IoT security with participants of the conference. The roundtable discussion resulted in several insights including the view that devices should be built with security at the forefront, they should be tested, and they should utilize labeling similar to those for organic foods.

Participants further asserted that security training should be tied into digital literacy training and for many users, security and privacy are viewed as the same. Participants in this roundtable also suggested that messaging on a lack of security can lead to fear, which, in turn, leads the public to avoid using such devices without realizing their benefits. These and other insights from the focus groups held throughout the process were a valuable part of the initiative and directly contributed to the final outcomes of the process.

15 See Annex IV for more information.
16 https://www.Internetsociety.org/events/indigenous-connectivity-summit/2018/

Network Resilience Working Group (NRWG)

Large-scale attacks from consumer IoT botnets are one of the largest risks to many Internet-based organizations, including ones that provide critical Internet infrastructure.

2.1 Summary/Problem Statement

IoT devices are both the largest and fastest-growing type of Internet hosts. They are produced by a very wide range of vendors, most of whom have limited cyber-security experience. Many of these devices are, by their nature, likely to have life spans that exceed their software support. For example, many first-generation Smart TVs are no longer provided with security patches by vendors. Though IoT devices generally do not generate high volumes of Internet traffic, the proliferation of gigabit-class home and business Internet provides IoT devices access to high throughput connections.

Given that IoT devices are vulnerable to compromise, rapidly proliferating, and have access to high speed Internet connections, they are attractive weapons for a multitude of uses by bad actors.[17]

The NRWG's central question was how to defend Internet infrastructure from this intensifying threat. While many initiatives address IoT security at a device level or address attack mitigation at the target end, the Working Group contends that, as valuable as these approaches are, they do not sufficiently address the threat. The group's central thesis was that, in order to effectively address IoT-based attacks, the network should protect IoT devices from compromise. Ultimately, the main goal of the group was to develop an IoT security framework for the network to protect devices from being compromised, and to limit, from the network's edge, attacks from compromised devices.

The more limited connectivity needs of IoT devices, as opposed to the extensive connectivity needs of personal devices, provides a route for their protection: they facilitate deployment of fine-grained network-based security controls. The group's work explores how proactively protecting IoT devices can counterbalance the increase in scale of threat from IoT. This group worked to develop a set of recommendations and standards to protect the Internet from things and protect things from the Internet.

The NRWG focused on WiFi-enabled IoT devices. These include home devices, which connect to the home network via WiFi but do not support Internet-browsing by the user, such as phones, tablets, or personal computers. The NRWG calls the device that connects

17 https://www.Internetsociety.org/blog/2017/02/the-Internet-of-things-as-an-attack-tool/

the Internet Service Provider's (ISP) access network to the home network the "home gateway." While the home gateway falls within its definition of an IoT device, its work focuses on protecting other IoT devices.

Appendix III outlines the research the NRWG carried out in their work.

2.2 Discussion

IoT devices are the fastest growing and largest class of consumer Internet-connected devices, eclipsing personal computers and smartphones. While the majority of smartphones and PCs feature a narrow range of operating systems, chip architectures, brands, and form-factors, IoT devices are built from hundreds of different software stacks and chip families, by thousands of manufacturers, in almost every shape and size imaginable. The number of manufacturers contributing to a single product is also raising concern over the security of the supply chain. While most smartphones and computers support many applications, most IoT devices serve a single purpose. These differences, and the scale of IoT device deployment, suggest that there is a need to re-examine how to mitigate threats to and connect consumer devices.

The physicality of IoT has elevated concerns around security in a range of domains. This concern and responses to it are documented in popular books (i.e. Bruce Schneier's "Click Here to Kill Everyone") as well as in domain-specific policy documents (i.e. NISTIR 8228) and standards (i.e. IETF MUD), with the focus on critical infrastructure, government systems, and, increasingly, enterprise users.

While IoT touches sensitive cyber-physical systems from medical devices to power infrastructure, a large portion of connected devices and device types are aimed at the consumer market and found within homes and small businesses. These devices pose privacy, if not safety, risks to their owners. Moreover, the scale and vulnerability of these consumer devices pose risks beyond the homes in which they are found. Large groups of compromised devices have been used together to attack and disable Internet-facing services by forging large volumes of traffic; the most publicized case is the then-record-setting Mirai IoT botnet.[18] In 2016, Mirai exploited unsecure CCTVs whose default passwords had not been changed. The scale of such attacks continues to increase. The increasing scale of consumer IoT prompted the NRWG to be primarily concerned with the risk that such weaponization of IoT devices brings, both to the core infrastructure that provides Internet services, as well as to organizations that depend on maintaining an online presence.

The central question posed by the NRWG is how to defend against this threat. The group identified three approaches to defense that different actors can deploy and that are most valuable in combination. The first approach is to scale existing Distributed Denial of Service (DDoS) mitigation mechanisms. For core Internet infrastructure providers, this generally means scaling up infrastructure spending, but with IoT proliferation in the market outstripping revenue growth, scaling up for attacks is economically problematic.

While cloud service providers, content distribution networks, and DDoS mitigation specialists offer services able to protect a range of service types from a range of attacks, not every Internet organization is able to rent scale—or to afford it. While there are certain to be advances in DDoS mitigation approaches, there are no guarantees that they will keep pace. A qualitatively more dangerous Internet poses a real threat.

The second approach that the group identified is to directly address the insecurity of IoT devices through improved security design and lifecycle management practices, encouraged via standards, awareness, examples, and regulation. There was consensus within the Working Group that this was important, and members identified a range of initiatives aimed at promoting IoT security practices to manufacturers and the market, from security frameworks such as ETSI TS 103 645 to assurance programs such as a UL CAP[19] to IoT security-focused legislation.[20]

18 https://www.Internetsociety.org/blog/2018/11/we-need-to-do-something-about-iot-security/
19 https://industries.ul.com/cybersecurity
20 http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327

Promoting improvements in practices is central to the Consumer Education and Awareness and Device Labeling Working Groups of the multistakeholder process, and endorsed by all participants. As necessary and vibrant as these efforts are, the challenge to this approach is the diversity of manufacturers. For general computing and smart- phones, the relatively small vendor pool (Apple, Google, Microsoft) that produces the bulk of the software for the industry has developed, over many years, excellent software lifecycle practices. With thousands of manufacturers of IoT devices with diverse backgrounds and pervasive pressure to get products to market, many manufacturers will ship products with little consideration or diligence placed on security and lifecycle management.

The third direction the group identified is network-based defenses for IoT. While some of the vulnerability of connected devices may come from software flaws, these flaws require access to be exploited. The central thesis of the NRWG is that networks can protect IoT devices from compromise and weaponization to, in turn, protect themselves. Working Group members have active initiatives to develop these defenses, and identified and connected with those involved in a range of other network-based defenses.

To begin to develop a framework for defense, the group examined the threats against home IoT devices. These threats and the proposed mitigations are summarized as follows:

Pre-compromise threats (high to low)	Mitigation	Notes
Home gateway compromise.	Secure-by-design.	Home gateways are most-compromised "IoT" devices.
IoT device compromise via services exposed to Internet.	Prevent IoT devices from opening static ports in firewall without user approval.	UPnP-based firewall bypass allows device to act as Internet server. Needed by some games and P2P networks, but poses very high risk.
IoT device compromise via services exposed to home LAN.	Policy enforced at gateway limiting LAN access.	Policy can be signaled via IETF MUD or derived implicitly.
Backend compromise.	Private/limited access to backend.	Reduce reachability of backend to ISP domain or ISP and device class.
Post-compromise mitigation	**Method**	**Notes**
Reduce attack size.	Rate-limit policies.	Rate-limiting reduces total attack volume without requiring knowledge of which devices are or are not compromised.
Block in-progress attacks.	Identify and quarantine specific attacker device across NAT (IETF DOTS).	Denial of service attacks are most visible upstream, towards the victim. ISPs which identify attacks in progress can use assistance from the home gateway to identify the specific compromised devices within the home and quarantine them without affecting other home services.
Prevent "ID" theft: access control evasion & rogue AP attacks.	Provide each device with unique WiFi credential.	Provides cryptographically strong identity to facilitate access control. Also allows credential revocation.

The most exposed IoT device in the home is the device that connects the home to the access network: the residential gateway. This residential gateway is open to attacks directly from the Internet as well as from connected devices in the home. Due to their ubiquity, complexity, and exposure, residential gateways have compromised large proportion of the devices within IoT botnets, including Mirai. Hardening these devices is a first step towards hardening the home.

While the NRWG is not aware of security guidelines that are specific to residential gateways, general IoT-focused security considerations, such as those identified by the OWASP IoT project[21] and ETSI TS 103 645[22], apply to these devices. Top threats to residential gateways include guessable passwords, insecure network services, insecure APIs, and poor software lifecycle practices.

Residential Gateways

Residential gateways often act as firewalls (and for IPv4, Network Address Translators) for devices within the home, blocking inbound traffic that is not associated with an outbound connection and providing an important layer of defense between the untrusted public Internet and nominally more trusted home LAN.[23] The Universal Plug and Play (UPnP) framework includes a protocol that devices may use to tell the residential gateway to forward inbound traffic on particular ports to them. The second-largest category of IoT devices recruited to botnets have been those that have exposed open ports to the Internet as a whole—generally leveraging this feature.

IoT devices may also be attacked from other devices or applications on the local area network, including Internet browsers, or from Internet-based services to which they connect. Presently, these are seen as lesser threats, but as the number of devices in the home grows, so too does the importance of in-home segmentation. These attack vectors should be addressed within a comprehensive framework.

The NRWG also identified existing network-based defenses. Some Internet Service Providers (ISPs) scan their customers for open ports to detect vulnerabilities and look for connections between their customers and known command and control addresses to detect compromise. These ISPs are able to proactively notify customers of their security threats or breaches. Without cooperation from the home gateway, however, an ISP is not able to identify which device within the customer premises is affected, or to put in place protective controls.

The core of the NRWG's work centered on protecting IoT devices via the home gateway. The main tool is access control: preventing or allowing particular devices from reaching other devices on defined TCP or UDP ports. For example, if instead of allowing any device on the Internet to connect to an IoT device, the gateway only allows the device manufacturer's cloud service to connect to that IoT device, the threat to that device can be reduced while preserving all of its functionality. Similarly, if a gateway enforces that a home device may only talk to a particular service on the Internet with a maximum daily traffic volume, the home gateway can limit the capacity of that device to attack Internet-based services should it become compromised.

21 https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
22 https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
23 Though usually placed in the home, there are alternate models where firewalling and other residential gateway features are provided by ISPs upstream from the home. Though there are different implementation considerations between the two models, most of the threats and mitigations are similar between them.

Access Control Solution Prototypes

Access control is a mature security tool, but historically it has had limited application within the home, because PCs and smartphones support a rich application set with very few limitations. As the bulk of IoT devices are single-purpose devices, access controls around them should be tightened.

Fine-grained access controls are, however, challenging to specify for thousands of diverse IoT devices, and it wasn't immediately clear to the group how to do so. An emerging protocol for describing access controls is the IETF Manufacturer Usage Description (MUD) RFC 8520[24]. MUD provides a data-model for specifying access controls. In the original MUD concept, devices indicate to the network a URL to a MUD file describing the access profile for a device. The network may retrieve the file, validate its contents, and apply the profile.

This protocol is being proposed as a new way to signal the networking and security control characteristics of an IoT device in order to appropriately apply the correct security controls to ensure its safe operation.

MUD is useful in a world where an IoT device manufacturer takes time and care to define and manage MUD profiles. The challenge with MUD is its adoption: we live in a world where time to market requirements often take priority over security by design requirements. To address the case where manufacturers do not provide reasonable device profiles, an IoT device profiling/fingerprinting mechanism could be developed whereby MUD-like profiles are created for IoT devices and security controls are applied based on these discovered profiles.

However MUD profiles are created, if an IoT device's behavior deviates from its profile[25], a gateway may presume it has been compromised and place it under quarantine to mitigate its potential malicious activities.

There are no current best practices for taking an IoT device out of quarantine mode. Further work is required to develop a best current practice (BCP) to define the processes for quarantining an IoT device and to restoring that IoT device back to normal operations. This remedy needs to address the 'who do we call' (the ISP, the gateway manufacturer, the IoT device manufacturer, the country CSIRT) as well as the mechanism to restore the IoT device back to a normal state.

Fine-grained access controls are, however, challenging to specify for thousands of diverse IoT devices, and it was not immediately clear to the group how to resolve this problem. Again, MUD could be useful for describing access controls, as it provides a data-model for specifying access controls. In the original MUD concept, devices indicate to the network a URL to a MUD file describing the access profile for a device. The network may retrieve the file, validate its contents, and apply the profile.

Within an enterprise setting, MUD provides a way to automate access controls. The enterprise purchases large quantities of a limited set of device models, enterprise IT staff customize MUD files for each device type and have flexibility in choosing how the network associates a device to a MUD file—it can be through explicit signaling or by pre-associating device MAC addresses before deployment.

Within the home, there are no IT staff able to customize device profiles and deployment. MUD files may be maintained by the device manufacturer or by a third party the user trusts. To give the device's user control over permissions, software applying permissions from MUD files may allow a user to grant or revoke each permission present in the MUD file, much as smartphones provide a user the opportunity to deny permissions and app requests. As MUD file adoption by manufacturers is nascent, the NRWG examined options for signaling MUD URLs, generating MUD files, and curating manufacturer files: validating them, maintaining historical files should a manufacturer stop providing one, comparing versions to detect tampering, or allowing community or user-driven modifications.

As part of its Secure Home Gateway project, CIRA and its collaborators within the group demonstrated using a QR Code to deliver a MUD URL for a device to a home gateway and applying the access controls within that file to the device. Ideally, a single QR Code on a device would serve multiple roles, acting as a "live label" that guides the user to information and support for their device, as provisioning material for WiFi Easy Connect to

24 https://datatracker.ietf.org/doc/rfc8520/

25 There are many initiatives on IoT device profiling and fingerprinting. Netherland (.NL) SIDN.NL and Italy IIT CNR (.IT) are examples of country code top-level domains (ccTLDs) developing technology to profile, fingerprint, and detect anomalies in IoT devices.

allow the device to be on-boarded onto a network with a unique credential, and for MUD signaling.

To try to address the larger problem of creating and curating MUD files, CIRA and the group have been in discussions with a wide set of global collaborators, including authors of MUD and DOTS, SIDN (the .NL registrar) lab's SPIN team—who have built IoT connectivity surveillance and visualization tools as well as their own implementation of MUD access controls, the Canadian Centre for Cyber Security, and participants at NIST's MUD Open House– on working cooperatively to develop a full set of tools to deploy MUD and related threat mitigations at the residential gateway.

Many participants and collaborators suggested that when high quality MUD files are not available for a device from its manufacturer, machine learning might be used to construct one. To do this, the gateway may actively probe or passively observe a device in order to develop a large enough body of observations to (optionally: cluster that device with identical or similar models and, for that cluster) build a compact representation of normal behavior which may be used to build MUD files as well as to detect indications of compromise or other anomalies. The IoT Analytics Project at the University of New South Wales provides an implementation of such an automatic MUD-file generator.[26] There is an important user-interaction component to the Secure Home Gateway effort, as light cooperation with the user is viewed as critical for onboarding and incident response.

A second prototyping effort was aimed at onboarding and the shared key problem. For physical security, keys and badges are used for access control, and users with different sets of keys can be allowed into or locked out of different areas. In a hotel, for example, guests renting different rooms are given different keys. In the home, there is generally one WiFi password—one cryptographic key.

Granting the same key to different devices prevents the gateway from enforcing differential access control. To overcome this, TELUS and Algonquin College illustrated giving each device in the home a different password, locked to its MAC address, while still having all home devices share a single WiFi network (SSID) and use the normal WPA2-PSK authentication that all consumer devices support. Handing out different keys facilitates applying access control, and pairing keys with MAC addresses provides a cryptographic root to conventional MAC-based filtering techniques.

The participants validated the technique on a single home gateway using the popular HostAPd open source WiFi Access Point software, in a multiple access point setting with RADIUS authentication from HostAPd to a FreeRadius backend, and with web and app-based user interfaces to hand out passwords and assist in device onboarding.

The main outcome of this work is that popular existing tools are able to support device on- boarding techniques which facilitate applying access controls at the home gateway. The new Wifi Device Provisioning Protocol and Wifi Easy Connect certification offers a streamlined process for onboarding compliant IoT devices and provisioning them with unique credentials. The group has investigated ways to integrate Easy Connect and MUD provisioning, and believes that a single QR Code may function as a live label while performing Easy Connect onboarding and MUD provisioning.

2.3 Conclusions

The NRWG believes that insecure home IoT devices pose a large present and future threat to Internet-based services as well as to home users. This threat should be partially addressed by improvements to existing denial of service mitigations and maturation of IoT device security practices, but may also be partially addressed by improved security frameworks within the home that can place appropriate access controls onto IoT devices and allow users visibility into and control over IoT device behavior. The NRWG has outlined such a framework, and continues to work with global partners to develop, implement and standardize it.

26 https://GitHub.com/ayyoob/mudgee

2.4 Recommendations

The goal of the NRWG was to develop a security framework, running code that implements that framework, and to develop and refine user-centered onboarding and support tools for that framework.

The key outputs of the group to date are:

1. A high-level threat list against IoT devices in the home.
2. A high-level framework for protecting IoT devices against these threats.
3. A demonstration of discovering and applying access controls using MUD.
4. A demonstration of onboarding WiFi devices with unique credentials in a way that strengthens the application of access control rules.
5. Work in progress to design and implement a fuller demonstration of the protection framework.
6. Global collaborations towards this work.

The NRWG's primary recommendation is that the Secure Home Gateway code be accepted by the core openWRT project. In the future, the NRWG aims to ensure openWRT is bundled by default with its IoT security framework, and/or that when manufacturers upgrade their openWRT software, it comes equipped with this framework. Having this group's framework as a standard means it is core to the base openWRT package.

The NRWG also created a set of recommendations for future work, including:

1. Security evaluation of any new security/user interaction mechanisms. New MUD-based access controls represent significant new attack surface and must be analyzed and tested.
2. Continued implementation of a security framework. Integration/development of:
    a. Device fingerprinting.
    b. Automated MUD profile generation.
    c. MUD clearing house.
    d. Access controls.
    e. User controls (visibility, permissions, notifications).
    f. Unified onboarding.
    g. DOTS-based DDoS filtering.
    h. Quarantine and un-quarantine procedures.
3. Standards development
    a. Live label and their integration with network onboarding, MUD, and user-interaction.
    b. Out of support notification/device management.
    c. Credential management on IoT devices.
    d. Quarantining/un-quarantining.
    e. (MANRS[27]-inspired) MARIS: Mutually Agreed Norms for Internet Security.
4. Continued global coordination towards standardization, implementation, and adoption.

27 https://www.manrs.org/

Device Labeling Working Group (DLWG)

The Device Labeling Working Group's objective was to ensure the safe use of connected devices and associated data streams through labeling that clarifies how they will protect privacy and mitigate against cyber threats.

3.1 Summary/Problem Statement

Labels can help consumers make smart choices when it comes to acquiring, using, and disposing of IoT devices. Consumers need to be able to rely on the information provided through a product security label, and the information needs to cover the key aspects for buyers to consider. An effective label should provide information to help consumers make well-informed decisions when purchasing and using an IoT device.

This working group asserted that through consumers making smart choices, the Canadian IoT environment will develop in a safer, more secure way, taking privacy and security into account from the outset. Consumers making smart choices results in manufacturers and businesses offering better and more secure solutions. Ultimately, this process will lead to a higher level of network resilience, both from a societal and from a personal perspective. Consumer education at all levels will need to empower consumers to make the best use of the information provided through the labels. As such, the Device Labeling Working Group worked closely with the Consumer Education and Awareness Working Group to ensure their work was complementary.

This section of the report presents the primary findings for product labeling and the need for more joint efforts, not just in Canada, but globally on security and privacy requirements for IoT. This work included cooperation and evidence sharing between the Canadian multistakeholder process and the UK Department for Digital, Culture, Media and Sport (DCMS).

When a buyer, either consumer or business, purchases an IoT product or solution, they must consider specific characteristics, including at a minimum aspects of user functionality, security, privacy, and safety. The key aspects of effective labeling are as follows:

1. **Content**: providing reliable, relevant, and useful information when it is needed.
2. **Coverage:** ensuring that all consumers of all competing products see the information.
3. **Uniformity**: using a single simple and recognizable design to facilitate comparison.

Appendix IV outlines the research into existing labeling formats and standards carried out by the DLWG.

3.2 Discussion

The Need for a Labeling Scheme for Consumer IoT devices

In October 2018, PETRAS IoT Hub, the Dawes Centre for Future Crime at UCL, and the United Kingdom as part of its "Secure by Design Review" for consumer Internet of Things products, published the report "Rapid evidence assessment on labeling schemes and implications for consumer security."[28]

The report found that consumers cannot distinguish between devices that offer good and inadequate security when making purchasing decisions. Instead, they must investigate the security features and capabilities of the product themselves before purchasing. This would involve evaluating technical information such as security standards compliance, what data is collected by the device and how it is shared, the length of support, and default password configuration. Default passwords can often be easily obtained from vendor sites and other sources, and therefore must be changed by the consumer.

Awareness campaigns and behavior change interventions can encourage consumer behavior and motivate consumers to routinely assess the security of IoT devices they consider purchasing. Research has shown, however, that such intervention will not be sufficient to have a real impact on consumer decisions when buying an IoT product.[29] A key reason is that manufacturers do not systematically communicate information about the security features that devices possess and need to be evaluated to assess their level of security. The average consumer does not have the expertise required to evaluate this information, and typically is inclined to avoid such demanding tasks, as per relevant research.[30] A label that consumers can relate to and that would inform their decision- making in a meaningful way is a more achievable intervention that could influence their choices.

As mentioned, manufacturers often do not currently provide correct or accessible information to inform consumers and retailers about the level of security their devices offer. A labeling scheme would encourage manufacturers to compete on security as a form of market differentiation. It would also hold manufacturers to account by directing their attention to the security of devices according to clear criteria and guidelines. Finally, a labeling scheme would allow market oversight and consumer protection authorities to assess compliance to IoT security in a more consistent and transparent approach.[31]

Labeling Formats

This group considered three primary varieties of labeling formats:

1. Descriptive information label, which details security-related information.
2. Binary seal of approval labels in which a product is certified to a certain standard.
3. Graded scheme labels that allow more critical comparisons of security-related compliance.

In order to provide more insight into the relative merits of the different types of labeling, the Device Labeling Working Group referred to critical research performed on established labeling schemes, particularly on food and energy efficiency labels.[32]

28 PETRAS IoT Hub, Rapid evidence assessment on labeling schemes and implications for consumer IoT security, October 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf

29 PETRAS IoT Hub, Rapid evidence assessment on labeling schemes and implications for consumer IoT security, October 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf

30 Kahneman D, Egan P. Thinking fast and slow. New York: Farrar, Straus and Giroux. 2011.

31 PETRAS IoT Hub, Rapid evidence assessment on labeling schemes and implications for consumer IoT security, October 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf

32 See Appendix VI for more information and background research.

IoT Device Security Labeling

As possible IoT device security label formats, each of the dominant three labeling schemes has its strengths and weaknesses:[33]

1. The colored graded scheme would attract the attention of consumers and help them compare the security of different devices. For this implementation to be effective, the display of the graded label must be mandatory for manufacturers.
2. The binary or "seal of approval" label is typically preferred by consumers due to its simplicity, but is less effective in guiding attention and informing consumer choice.[34] The use of the binary label may lead consumers into a false sense of security or to assume that no intervention is required to keep them secure.
3. The descriptive information label communicates critical information to consumers and may provide helpful indicators of a device's security readiness. The label needs to communicate the most relevant information only and not burden consumers with unnecessary information. This type of label is more suitable for the voluntary label introduction.

Mandatory versus Voluntary Labels

The Department of Digital, Culture Media and Sport (DCMS) of the UK released their policy review for Secure by Design for consumer IoT products in March 2018[35] as well as a final report in October 2018.[36] A key measure in the report is a voluntary code of practice for manufacturers to ship products with features that make them "Secure by Design." The report also proposed exploring the role of a voluntary labeling scheme to communicate important information to consumers that is otherwise invisible to them, or difficult to find, such as how data collected by devices is shared and the support period for the product.[37]

More recently, the DCMS announced a consultation process on the government's regulatory proposals regarding consumer IoT security.[38] In this consultation process, initiated in May 2019, a proposal was made for the "top three" guidelines of the Code of Practice, to become mandatory in the UK. These critical guidelines are: all IoT device passwords shall be unique and not be resettable to any universal factory default value; that the manufacturer shall provide a public point of contact as part of a vulnerability disclosure policy; that manufacturers will explicitly state the minimum length of time for which the product will receive security updates.

A voluntary labeling scheme would be useful as an initial step. However, for sustainable market growth and to ensure manufacturers' adherence, as well as to maintain consumer awareness, the label must be mandatory in order to be effective, especially given some manufacturers unwillingness to display a label that indicates poor security of a product.

QR Codes

A Quick Response (QR) code is a type of matrix bar code or two-dimensional code that can store data and is designed to be read by smartphones. The code consists of black modules arranged in a square pattern on a white background. The information encoded may be text, a URL, or other data.[39, 40] The popularity of QR Codes is growing all around the world. Now, mobile phones with a built-in camera are widely able to recognize the QR Codes.

---

33 PETRAS IoT Hub, Rapid evidence assessment on labeling schemes and implications for consumer IoT security, October 2018,
34 Koenigstorfer J, Wasowicz-Kiryło G, Styśko-Kunkowska M, Groeppel-Klein A. Behavioural effects of directive cues on front-of-package nutrition information: The combination matters! Public Health Nutr. 2014;17:2115–21.
35 Department of Digital, Culture, Media and Sport (DCMS), Secure by Design Report, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf
36 https://www.gov.uk/government/collections/secure-by-design
37 Id.
38 https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security
39 Dong-Hee Shin, Jaemin Jung, Byeng-Hee Chang "The psychology behind QR Codes: User experience perspective", Science Direct, Computers in Human Behaviour 28 (2012) pp 1417-1426.
40 Phaisarn Sutheebanjard, Wichian Premchaiswadi, "QR Code Generator", IEEE 2010 8th International Conference on ICT and Knowledge Engineering (24-25 Nov. 2010) pp 89-92.

QR Code Usage Statistics

The use of code scanning has increased during the past few years as awareness and adoption of QR Codes has grown exponentially. QR Code stats done by ScanLife show that 23 million QR Codes were scanned during the first quarter of 2015, which is nearly 10 million more than during the first quarter of 2012. Moreover, the first quarter of 2012 had posted a 157 per cent increase as compared to the first quarter of 2011.[41]

The age group with the highest percentage of people scanning QR Codes was 34 to 44 years in 2015. Since then, apps popular with the younger generation, such as Snapchat, Pinterest, and WeChat, have added QR Code scanning features. Therefore, the age distribution is likely to shift towards the younger generation moving forward.[42]

Twenty-seven million Canadians are online, representing eighty per cent of the population. Ninety-three per cent of them go online to view and verify product information. These figures have changed the way Canadian marketers and retailers engage their audience. To strike a chord with the young generation, marketers, retailers, manufacturers, and even the police have adopted QR Codes in Canada.

Code of Practice for Consumer IoT Security

Recent research, including research by the Internet of Things Security Foundation,[43] as well as the UK's Department for DCMS report titled "Code of Practice for Consumer IoT Security",[44] have identified critical information and best practices to be followed and documented by manufacturers, service providers, retailers, and consumers. The DLWG considered each of these inputs in the development of its labeling schema.[45]

Certification

Currently, there is no one single standard or recommendation that can provide product or solution assurance to security. However, there are some that will indicate that a product has undergone some evaluation and testing to get a mark. The DLWG carefully considered these schemes when evaluating its proposed solution.[46] Regional efforts currently underway in the UK, EU, Australia, USA, and Canada were also considered.

41 ScanLife.com, "QR Code Adoption: Trends and Statistics", www.scanlife.com
42 QR Code Statistics 2018: Latest Numbers On Global QR Code Usage, (https://scanova.io/blog)
43 IoT Security Foundation, Establishing principles for IoT Security, https://iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf
44 Department of Digital, Culture, Media and Sport (DCMS), Code of Practice for Consumer IoT Security, 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747977/Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf
45 See Appendix VI for more information.
46 See Appendix VI for more information.

3.3 Conclusions

Comparison of Types of Labels for IoT Device Security

This table provides a comparison between the different types of labels, focusing on their suitability as a label for IoT device security:

Type of Label	Pros	Cons	Notes
Graded/ Color Graded	• Attracts the attention of consumers. • Helps consumers compare the security of different devices.	• To be effective, the display needs to be mandatory for manufacturers.	• Could be introduced at a later stage in a mature IoT Security market.
Binary (Seal of Approval)	• Easy for customers to interpret. • Preferred by consumers.	• Less effective in guiding consumer choice. • Gives (false) sense of security and belief that no additional action from consumer is needed. • Does not automatically reflect current security status or new product vulnerabilities.	• Example is BSI Kitemark in the UK. • Combine binary/seal of approval label with another informative label (e.g. live label).
Informative	• Communicates critical information to consumers. • Provides helpful indicators of a device's security readiness. • More suitable for voluntary label introduction.	• Need to limit display to most relevant information.	• Suitable for market introduction and to help build consumer understanding and trust.
Live label (e.g. QR Code)	• A form of informative label. • QR Codes are gaining adoption from manufacturers as marketing tools • Provides link to current information on product security. • Allows consumer to get information beyond security compliance, e.g. deployment recommendations, data collection/sharing information, latest vulnerabilities.	• Requires consumer to scan QR Code and spend time going through relevant information.	• Suitable for market introduction and to help build consumer understanding and trust.

Live Label Requirements and Structure

As many of the labels represent a static view of a product at a specific time within the product lifecycle, there is a need to ensure that a dynamic view of the product is available to users. The concept of a "live label" is not new; however, based on the discussions within the multistakeholder process, it became clear that a different approach to labeling is required.

A live label will provide a near real-time view of any product's security risks. As many products undergo formal testing and evaluation, there will be aspects of the software components that could provide no risks one day but, due to a zero-day discovery and/or malware, the components and possibly the product will be prone to compromise. The need to be able to provide a single source of information for product buyers is becoming more critical. As many vendors do currently offer support sites, the additional elements recommended are not a far reach to meet the necessary requirements to offer a comprehensive view of an IoT product's risks.

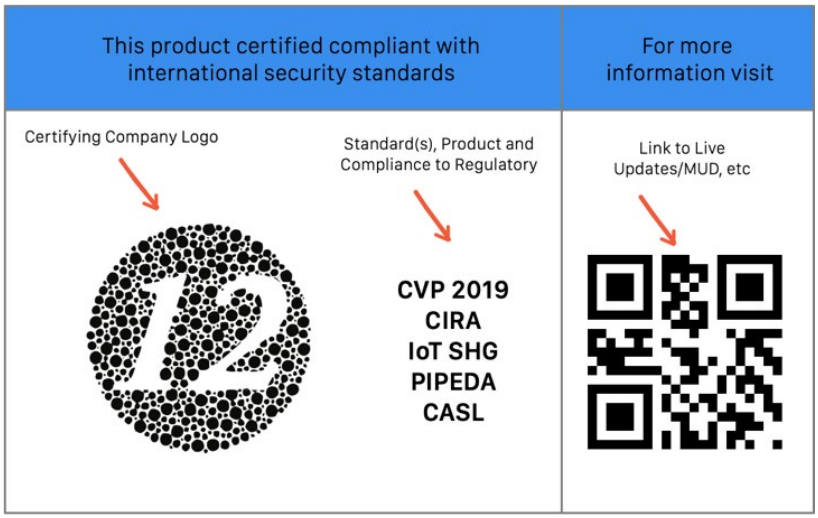
Requirements:

1. A web page accessible by secure means (such as https and encryption) containing specific details of each product or a group of products provided by the vendor, including:
    a. Product firmware updates.
    b. Product security alerts and announcements, including any CVEs and CVSS registrations.
    c. Policies for privacy and vulnerability disclosures, including any recent changes to data collection policies or practices.
    d. Contact details for either phone, web, or email support that will result in a minimum response of seventy-two hours.
2. The web page should contain additional details, such as:
    a. "How To" and user guides for secure setup and configuring the IoT device(s).
    b. References to updated certifications and/or attestations obtained.
3. The web page may contain supporting details, including:
    a. Third party organizations who conducted formal testing and assessment to recognized standards and attestations.
    b. Alert levels for cloud hosting and online system availability.
4. Use an electronic coding scheme that will allow users to quickly find the "live label" website.
5. Additional fail safes that will prevent the counterfeiting of labels placed on products.

A security product label should also have the following structure:

1. Clearly identify the organization that performed the formal testing and assessment.
2. Clearly identify the standard and product being tested and assessed.
3. Include a holographic, embedded RFID tag or other means to prevent counterfeiting.
4. Provide a machine-readable code that can be used to provide updates to date and live information on the specific instance of the product. This can be hosted on the current company or product website and should include the following:
5. Product model and/or version number.
6. Latest product firmware version number.
7. CVEs or CVSS references.
8. Security configuration guide.
9. Proposals for IoT Device Labeling

Proposal One of IoT Device Security Label



Reference Sample ONLY

Label Proposal One

The reference example above indicates what a proposed "live label" might look like. This indicates the three key elements, including the name of certifying company, product, standard, compliance, and link to live site. While not completely fool-proof, it does provide additional information that a user can use to validate a label. If the vendor attempts to falsify all of these details it would clearly indicate a liability situation.

Proposal Two of IoT Device Security Label

Label Proposal Two

Following the comparison between the benefits of the different label formats, the proposed approach is to combine the consumer trust factor of known "trust marks" such as for CE in Europe, Kitemark in the UK, or CSA in Canada, with advanced and critical product security information that is difficult to display on a label, and have the nature to change over time.

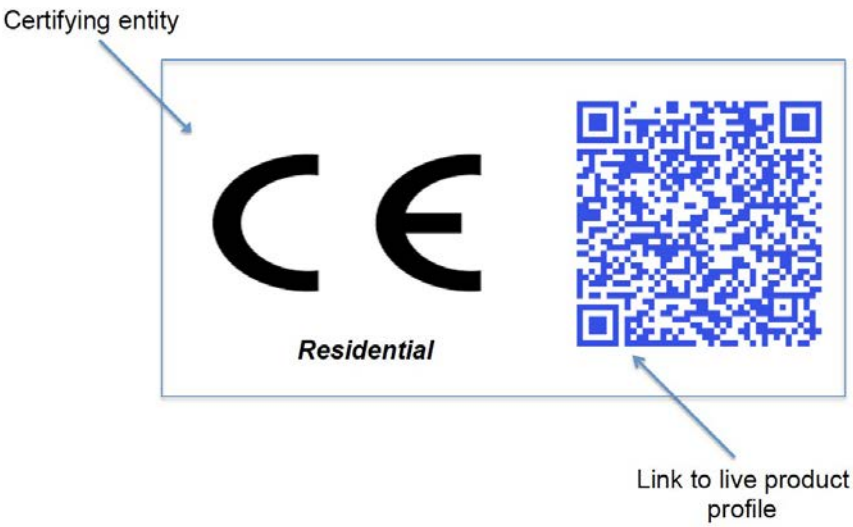
Key information to be conveyed by the label should include:

1. Formal testing and certification have been performed on the product.
2. Where to get up-to-date critical information on product security features and installation/deployment considerations.

Main aspects to be covered by a security product label are:

1. Identification of the organization overseeing/authorizing the certification and formal testing (e.g. BSI Kitemark, CE mark, CSA mark).
2. A machine-readable code that is linked to a URL providing up-to-date product information (i.e. a live label). The website should include the following:
    a. Product model and/or version number.
    b. Latest product firmware version number.
    c. Recent vulnerability information.
    d. Certification/testing framework.
    e. Security configuration guide.
    f. Information on what data is collected and how it is shared.

Proposal Three of IoT Device Security Label



Label Proposal Three

In the Label Proposal Two, the entity overseeing/authorizing the product certification and testing is the CTIA, while the device tested is the Amazon Alexa smart home assistant. The testing and assessment are performed against the Online Trust Alliance (OTA) framework v2.5.[47] The QR Code (i.e. live label) points to the product site with up-to-date product information.

The Label Proposal Three presents a simpler label format, focusing on the CE label[48] (the European Certification) and the QR Code of the product being certified (e.g. Amazon Alexa). Information regarding the standard used in the testing and certification is available on the product site, accessed by scanning the QR Code, instead of being explicitly mentioned on the label. Potentially the word "Residential" could be added in the label to indicate the intended usage of the product.

We believe Label Proposal Three qualifies as a simpler and easier to understand label.

47 https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

48 It should be noted that in the UK DCMS "Consultation process on the government's regulatory proposals regarding consumer IoT security", a proposal for a labeling scheme is introduced. The label is based on a combination of a binary label that indicates if "Essential security features are included", and a label for the length of time security updates are provided by the manufacturer.

3.4 Recommendations

3. Approach and collaborate with other organizations focusing on IoT security and privacy such as the NIST, ENISA, IoT Security Foundation, IoXT, IoTAA, UK DCMS, ETSI and EU in an attempt to reduce the amount of fragmentation in the market for initiatives and labels to avoid consumer confusion.
4. Continue to influence the standards effort through the ISO/IEC for international standards and SDOs with similar projects and interests.
5. Collaborate with the Online Trust Alliance (OTA) to approach key vendors and solution providers to raise awareness on the need for security certification and device labels.
6. Determine the best organization to provide a formal specification of the "live label." This could be IETF or similar, and includes further developing the live label (QR Codes) proposal through collaborating with other organizations such as the OTA.
7. Elevate the proposed voluntary labeling framework as a model for consumer IoT device manufacturers to demonstrate their compliance with existing Canadian law and regulations in this space, including but not limited to the *Canada Consumer Product Safety Act,* the *Personal Information Protection and Electronic Documents Act (PIPEDA),* and the *Canadian Anti-Spam Legislation (CASL).* This also reveals that the 'gap' is the lack of a clear and consistent way for manufacturers to indicate that they complete the certification with certain standards, and provide additional information that makes them compliant with these laws. This in turn situations the proposed voluntary labeling framework as a flexible, user-friendly framework to apply in order to advertise their compliance and effort put towards reducing risks associated with IoT devices.
8. Further assess the certification and testing of applications that control devices and backend support services, in addition to focusing on the devices themselves.

The key findings for this working group include:

1. Security labels need rules for appearance and what information to include.
2. Consumers need more education on types of labels and what they actually mean for security and privacy implications.
3. Canada needs to find ways to work globally to eliminate duplication of effort for security and privacy labeling.
4. We need to consider compliance to Canada laws for PIPEDA and CASL for vendors and how this is reported to consumers or integrated into a label.
5. While labeling for most products should be voluntary, in some sectors it should be mandatory where personal safety could be at risk.

National and international standards will continue to be improved by members of this group, including the T200 and the SC27030.

Consumer Education and Awareness Working Group (CEAWG)

As more consumers adopt IoT solutions in the home, their role in the overall security and privacy of IoT increases. Consumers are also required to take a more active role in purchasing and in their home security and privacy.

4.1 Summary/Problem Statement

Well-informed and empowered consumers are more likely to trust and engage with the IoT industry; demanding consumers also place pressure on businesses to be more innovative and competitive in order to earn their business. Educating consumers about IoT risks and opportunities has the potential to be beneficial for consumers, businesses, and the economy.

The focus of the Consumer Education and Awareness Working Group (CEAWG) is on household and business IoT devices. Systems that include many connected devices and complex systems, such as autonomous vehicles and smart cities, were not included in its analysis.

Shared Responsibility Framework

A Shared Responsibility Framework (below) is used to illustrate how demand and supply sides of IoT devices can collaborate to bridge the gap between the ideal situation/behaviours that are outlined for consumers and the status quo by engaging the diversity of actors (expertise/stakeholders/forces/incentives/trusted authorities). This Shared Responsibility Framework broadly organizes the ideas into the demand side and the supply side, which can work collaboratively over the lifecycle of the device:

1. Demand side: The expectations of the consumers who are active users of the IoT device.
2. Supply side: A broader category of stakeholders who are either directly or indirectly involved in the supply chain of the device.

Appendix V includes an evaluation of existing educational resources carried out by the CEAWG.

4.2 Discussion

The approach taken by the working group was to involve all stakeholder groups, including consumers. IoT consumer device manufacturers are the main targets of the CEAWG. The principal output of this working group is the Shared Responsibility Framework of key messages about behaviours and recommendations that need to be communicated to consumers, manufacturers, retailers, service providers, governments, civil society, educational institutions, and others. A list and evaluation of existing educational products is included in Appendix V.

A website/repository with the information below and relevant links will be available on the Enhancing IoT Security initiative website.[49]

The CEAWG first focused on reaching consensus on the content of key messages, then turned its attention to how this content will be translated into a full-scale Consumer Education and Awareness Campaign. Throughout the process of creating the content, several issues and considerations arose. In rough chronological order, the considerations for future work are as follows:

Evaluating the Varying Elements of Key Messages[50]

1. **Scope of application:** General messaging was adopted instead of instructions for specific device/systems. The impact of this scoping of the content of the messages needs to be further considered.
2. **Product range:** How do the messages differ when applied to high-security products (i.e. vehicles) vs. low-security (home appliances)?
3. **Audience:** Target seniors, youth, newcomers, low tech literacy, or all IoT consumers? One approach to consider the audience perspective is to run a thought exercise for a consumer's use of devices (i.e., imagine scenario of device setup and assess which key messages will be most relevant and salient).
4. **Link to Smart Cities:** Consider the application of the WG's conclusions/key messages to educate citizens on smart cities (i.e. traffic lights, smart sidewalk, etc.)

Linking Consumer Education and Awareness Messaging with Labeling Options[51]

How does the message promote use of the label by businesses and consumers and how can the label serve as a link to the content? For example, if the delivery of these messages relies on the QR Code model as proposed by the labeling WG, this assumes the users have access to a smartphone, which may affect use.

Options for Information Dissemination

Awareness activities will largely need to be tailored to various audiences (e.g., youth, elderly, etc.), recognizing how to best convey the content to them. Resource requirements and delivery mechanisms (e.g., social media campaigns vs. traditional advertising, etc.) also need to be tailored to each audience.

---

49 The Consumer Education and Awareness Working Group will provide links and relevant information for inclusion on this webpage, which will be maintained by the Internet Society: https://iotsecurity2018.ca/consumer-education-and-awareness/

50 We wish to note that the CEAWG agreed that initial messaging will be developed using all consumers as the intended audience. Future efforts may take place to develop messages aimed at specific groups of consumers such as youth, seniors, and more tech-savvy demographics.

51 See also the information in the Device Labeling Working Group section above.

Campaign Evaluation

In order to properly assess the effectiveness of the campaign message, a process must identify and validate consumer behaviour and reaction to key messages. Indicators of impact will be important to consider, including changes to consumer behaviour, complaints, the impact on purchasing (brands, types of devices, and devices with labels vs. devices without labels). Metrics showing the popularity of websites or other channels that deliver the content of the key messages will also be important.

Additional tools that can be explored to support consumers include a) redress mechanisms and consumer support beyond this educational campaign and b) ongoing development of the Canadian Cyber Centre's one stop shop and point of contact for reporting cybercrime.[52]

52 https://www.cyber.gc.ca/en/

4.3 Recommendations

All the messaging contained in the Shared Responsibility Framework (below) are considered recommended behaviours for consumers and industry:

SHARED RESPONSIBILITY FRAMEWORK

DEVICE STAGE	DEMAND SIDE: Consumers	SUPPLY SIDE: Manufacturers/Retailers/Government/ Civil Society/Educational Institutions
Before Purchasing	Understand and consent to how the device is collecting, using, and sharing your data.	Improve accessibility and content of privacy policies (i.e., provide clear answers on how the device is collecting, using, and sharing data).
	Ensure that the device comes from reputable/ certified manufacturers (i.e., low cost devices typically come with greater risks. Any smart devices that are connected to the Internet carries a risk of breach).	Clearly lay out the shared responsibility regarding the device's security (i.e., convey expectations of consumers' awareness/ responsibility in the instructions/ToS/warning leaflet of the device).
	Check if there are any extra functionalities (i.e., is the device collecting unnecessary data that could create unnecessary risk? Can you opt out of future features without opting out of security updates?)	Clearly indicate/disclose all functionalities of the device and how to minimize unnecessary functions (i.e., develop a list of sensors in the device, provide information on how to turn off video and audio recording, clearly indicate if new/extra functionalities have been included in updates, and if/how it is possible to opt out of these functionalities).
	Check for user reviews, labels, and certifications (i.e., label and certification indicate that the device has been tested).	Use certification/adherence to laws, standards, and non-binding best practices as a publicized selling feature.
	Consider the lifecycle of the device and the support available to keep your device in use for as long as possible (i.e., verify availability and duration of security upgrades and patches).	Use availability/duration of patches, updates, and support as a publicized selling feature.
	Check that the device works even without Internet connection, and assess functionality in the event the device outlives the company (i.e., smart lock, camera, fridge still function even if the Internet is down or the company no longer exists).	Ensure the devices can still function without Internet connection, and if the company ceases to exist.

DEVICE STAGE	DEMAND SIDE: Consumers	SUPPLY SIDE: Manufacturers/Retailers/Government/ Civil Society/Educational Institutions
At Use/Issue	Know where to seek redress and address technical problems, including if your device has been compromised, and keep record of your purchase.	Provide transparent and accessible instructions on seeking redress.
	Follow best practices for network setup and configuration to help mitigate risk when using IoT devices.	Assist consumers to set up their IoT networks consistent with best practices (i.e., make the default setting consistent with best practices).
	Be considerate of the implications or impacts on guests or others who are in the vicinity of your device (i.e., consider notifying your guests when in proximity to your smart home devices, or turning devices off).	Remind consumers about the effects of their IoT devices on their guests (i.e., audio or video recording).
	Be aware that the security of your device is constantly being updated. Ensure that the device is able to receive updates.	Remind consumers to follow recommended security best practices (i.e., follow recommended upgrading and patching recommendations from the NTIA Multistakeholder Process).[53]
	Ensure that each device in your home is secured. The security of your home network is only as good as its weakest link.	Consider providing mechanisms to warn consumers when issues arise (i.e., assist consumers in monitoring their traffic to detect anomalies).
End of Life/Use	Remove data from your device before disposing or moving. Many guides are available to assist users with specific IoT devices (i.e., Nest Thermostat[54]).	Clearly indicate the best method or provide consumer assistance to permanently remove data from device.
	Do not forget to revert back to factory default settings. Many guides are available to assist users with specific IoT devices.	Clearly indicate the best method or provide consumer assistance to revert the device to factory default settings.
	Check the resources that are available to help dispose of IoT devices responsibly. Retailers may provide this information.	Provide resources to help consumers dispose of their IoT devices responsibly.

Additional information

For more information on the Consumer Education and Awareness Working Group, please see their draft report on the Enhancing IoT Security website.[55]

53 https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_capabilities_oct31.pdf
54 http://www.imove.com/blog/how-to-switch-nest-thermostat-accounts-when-you-move/
55 https://iotsecurity2018.ca/consumer-education-and-awareness/

Inter-Group Collaboration

When the multistakeholder group first selected its three working groups—Consumer Education and Awareness, Device Labeling, and Network Resilience—they were treated as separate, but interrelated, entities.

As the project moved forward and the working groups developed their resources and outputs, they also became more tightly interwoven. Continuing to foster the ties between all three groups and encourage their collaboration will be critical.

The Network Resilience Working Group's primary recommendation is to ensure that all home gateway open source software has a Secure Home Gateway (SHG) framework as part of the core software. The SHG is made up of two parts: (1) the secure router and (2) an application on users' phones or tablets that allows them to see the MUD files of all the IoT devices connected to that router. If and when an IoT device begins to malfunction by sending unusual amounts of data, or sending data to unusual places, or another security breach indicator, the application will notify the user and allow them to simply quarantine the device through their application until the problem is resolved.

The SHG is an excellent step toward a more secure network of things. However, when the SHG is produced, users will need a way to understand whether the devices they have already connected to the router are secure.

If a certification label were included in or alongside the MUD files in the user's application, even the most basic users would understand whether the devices they have connected in their homes are secure. A label that meets both national/regional (T200) and international (SC27030) levels will allow users to easily understand the impact their devices may have on their network and which devices are most or least likely to have a security problem.

Together, the Network Resilience Working Group's SHG and the Device Labeling Working Group's label and standards development can create a more secure, easier to understand landscape for consumers, which will directly affect the way they interact with the devices in their homes.

However, without consumer education about the importance of SHG and labeling, it will be significantly more challenging for these to be widely adopted. That is why the Consumer Education and Awareness Working Group will need to focus their attention on supporting the other two Working Groups by sharing the message of the work they have carried out and the impact it can have on consumers in the context of the Shared Responsibility Framework.

Through the creation of their dynamic coalition in the implementation phase of this process, the Consumer Education and Awareness Working Group will be able to rapidly respond to new developments from both the Network Resilience and Device Labeling Working Groups and assist in all public-facing outputs. They will have a direct window to consumer needs and can also report back to the other two groups if any developments are inaccessible or difficult for consumers to understand.

Though all three working groups are independently focused on their own priorities, they all have an intertwined role to play in securing the Internet of Things. Without any one group, the other two would limit their success.

Youth Perspectives

This report explores the IoT security and privacy climate by examining existing digital literacy pedagogies and interventions as well as youth attitudes, beliefs, and behaviours toward IoT and privacy.

EXCERPT IS DRAWN FROM "YOUTH AND THE INTERNET OF THINGS IN CANADA: PERSPECTIVES ON PRIVACY, SECURITY, AND ENGAGEMENT IN THE DIGITAL AGE." [56]

While the survey conducted for this report has a limited scope, the work is important because it is the first of its kind. It lays the groundwork and offers recommendations for a future survey engaging Canadians with IoT security issues, and features a lengthy discussion section on this particular area. The youth report authors believe that policy should be backed by evidence, and thus they advocate for a large-scale, representative, and nationwide survey, building upon their findings and limitations, in order to adequately assess attitudes toward IoT and how best to engage youth in understanding its implications.

56 "Youth and the Internet of Things in Canada: Perspectives on Privacy, Security, and Engagement in the Digital Age," prepared by the Youth Internet Governance Forum for the Canadian Multistakeholder Process of Enhancing IoT Security. https://iotsecurity2018.ca/wp-content/uploads/2019/01/Youth-and-IoT-in-Canada-Report-1.pdf.

6.1 Methodology

Survey

The aim of this online survey was to provide an overview of IoT device usage by young people in the context of both at-home and wearable use; to document youth awareness of IoT security issues; and to understand how individuals in this demographic consume media. In order to achieve this, the youth reporters circulated a survey through their networks, as well as through social media channels to garner responses from youth internationally. The data obtained from the survey was supplemented by insights from the 13th Internet Governance Forum (IGF), the ICANN63 Public Meeting, and the 2018 GovTech Summit.

Survey Development and Pilot Testing

The survey was developed with the intention of collecting both quantitative and qualitative responses, as the researcheres were interested in acquiring both statistical understandings and more subjective exploratory perspectives. To this end, the survey is comprised of a variety of question types including multiple choice questions, open-ended written responses, and Likert scales. To build the survey, they used Google Forms, primarily for its simplicity, ease of use, and visualizations. In developing the survey, careful attention was paid to the verbiage and wording in order to minimize bias and ensure neutrality. This process involved consulting members of the Youth IGF at an IGF session, and revising aspects of the survey based on their feedback. Data was anonymized as much as possible so that participants would feel comfortable providing truthful responses. Further, the length and time to complete the survey were carefully considered in order to ensure participants would complete it. Overall, thirteen questions were included, with the survey taking roughly two to three minutes to complete.

6.2 Summary of Findings

IoT Use

The survey generated some novel insights into the use of IoT technologies by young people. Perhaps unsurprisingly, wearable devices such as smartwatches and fitness trackers (e.g. Apple Watch or Fitbit) and smart speakers (e.g. Amazon Alexa or Google Home) are the two leading IoT uses among youth. Several individuals stated that they interacted with multiple IoT devices, due to both their own ownership and their family's usage of IoT devices at home. However, the majority of youth do not identify themselves as frequent IoT users. About one-third considered themselves to be daily or weekly users; nearly one-third stated that they used it occasionally; and over one-third of youth indicated that they 'rarely' use IoT. Interestingly, these results match those of a 2017 survey by the Association of Energy Services Professionals (AESP) and Essense Partners which showed that millennials do not use IoT as much as older age groups.[57]

Awareness of Security and Privacy Issues

On a scale of one to five, with five being 'Completely Aware,' the majority of respondents identified as having a mid-range (three or four) awareness of security and privacy issues related to IoT devices. But when asked to identify their level of concern, with five being 'Very Concerned,' the majority indicated a higher range (four or five). Despite enjoying the benefits of IoT usage that the majority of responses seem to exhibit, the attitudes towards IoT devices are decidedly more mixed. Many responses showed awareness of the security and privacy issues around these devices across a variety of contexts, specifically surveillance and tracking and associated data (mis)use.

Participants demonstrated a high-level of awareness regarding the ecosystem of these devices and their functions, but admitted that they lacked specific knowledge of the technical considerations of IoT device insecurities.

57 Research, Navigant. "IoT and Millennials." Forbes. March 24, 2017. Access January 1, 2019

Engagement

Much like engaging other groups, engaging youth requires not only understanding where they are most reachable but also how best to reach them. It is no surprise that engagement is now often digital by default, leveraging the reach of various platforms online to enable more widespread information dissemination and interactivity.

6.3 Areas for Additional Research and Recommendations

1. **Education:** For youth especially, education policy is critical. Provincial and federal governments should work together with civil society organizations on curricula and programs that can offer forums for discussion and awareness of IoT and other tech-related issues across Canadian educational institutions.
2. **Conversation:** One of the strengths of social media as a medium of engagement is its ability to bring people into a conversation and generate widespread interest in specific topics or events through the multiplying effects of personal networks. Catalyzing authentic personal interest and curiosity through open dialogue which connects a specific issue like IoT security to broader social narratives or concerns is the most effective means of spreading awareness and inspiring action.
3. **Exploration:** Effective engagement and capacity building will also require a deeper dive into assessing the current state of young people's interaction with digital platforms and their knowledge when it comes to not only IoT security but other topics in the tech sphere such as data and privacy rights.
4. **Improving diversity and multistakeholder access:** Engagement opportunities should be promoted, and not skewed to certain types of organizations over others.
5. **Embed participation:** Avoid requiring significant amounts of additional time from young people by incorporating opportunities to learn about and engage with IoT and other emerging technologies, as well as to participate in policy making, into regular education or training activities.
6. **Policy changes:** European-style privacy laws such as the General Data Protections Regulation (GDPR) can inform and inspire the basis for regulatory and legislative approaches towards data protection reform with respect to IoT devices.
7. **Collaboration:** Internet governance involves a variety of organizations from a myriad of backgrounds. The topic of IoT security spans multiple interrelated issue areas, each serving as the focus of a number of these groups. In order to prevent duplication of efforts, collaboration and harmonization must increase between these groups at both the community and international level.

CANADIAN MULTISTAKEHOLDER PROCESS

ENHANCING IOT SECURITY

Final Outcomes and Recommendations Report

Appendices

Appendix I

7.1 Partners and Working Group Leads

Partnering Organizations:

- Internet Society
- Ministry of Innovation, Science and Economic Development Canada (ISED)
- Canadian Internet Registry Authority (CIRA)
- Canadian Internet Policy and Public Interest Clinic (CIPPIC)
- CANARIE

Working Group Leads:

- Network Resilience: Jacques Latour, CIRA and Jordan Melzer, Telus
- Labeling: Faud Khan, TwelveDot and Hosein Badran, Badran Digital Consulting
- Consumer Education: Rouba Alfattal, ISED

Appendix II

7.2 Timeline of Meetings, Workshops, Focus Groups

April 4, 2018: Launch of the Enhancing IoT Security initiative and first multistakeholder meeting

May 17, 2018: Youth focus group

May 22, 2018: Virtual multistakeholder meeting

June 14, 2018: Network Resilience webinar

June 21, 2018: Second multistakeholder meeting

July 12, 2018: Ranking Digital Rights webinar with Tatevik Sargsyan

July 17, 2018: French language round table

August 1, 2018: Labeling webinar with Maarten Botterman

August 15, 2018: Consumer Education and Awareness Working Group meeting

August 29, 2018: Network Resilience webinar with Jacques Latour

September 5, 2018: Third multistakeholder meeting

October 11-12, 2019: Focus group at the Indigenous Connectivity Summit

October 22, 2018: Consumer Education and Awareness webinar

October 30, 2018: Network Resilience virtual roundtable

November 4, 2018: Fourth multistakeholder meeting

January 3, 2019: Consumer Education and Awareness and Labeling joint working group meeting

January 15, 2019: Consumer Education and Awareness Working Group meeting

February 27, 2019: Fifth multistakeholder meeting and launch of Draft Outcomes Report. Public comment period begins.

March 29, 2019: Public comment period on Draft Outcomes Report closes

April 18, 2019: Final multistakeholder meeting

May 28, 2019: Launch of Final Outcomes Report

Appendix III

7.3 The Role and Importance of the Multistakeholder Approach

A defining feature of the *Canadian Multistakeholder Process: Enhancing IoT Security* has been its use of the multistakeholder approach in its organization, governance, and decision-making. But what is meant by 'the multistakeholder process'? 'The multistakeholder model' is sometimes referred to as if it were a single solution. But in reality, there is no single model that works everywhere or for every issue. Instead, the multistakeholder approach is an agile set of tools or practices that all share one basis:

> Individuals and organizations from different realms participating alongside each other to share ideas or develop consensus policy.[58]

The Internet Society has characterized the multistakeholder approach as transparent, accountable, sustainable, and—above all—effective. The better the inputs and the more inclusive the process, the better the outputs and the more likely their implementation.[59]

Some characteristics of multistakeholder processes include:

1. All stakeholders have equal permission to speak.
2. Stakeholders self-identify.
3. Stakeholders self-represent.
4. Lack of formal legal procedures.
5. Lack of precedent.
6. Discussion addresses various stakeholders, not just the government.
7. The audience is a participant.
8. State-based entities do not have higher status.
9. Transparency is fundamental.
10. The organization is fluid, but not without structure.

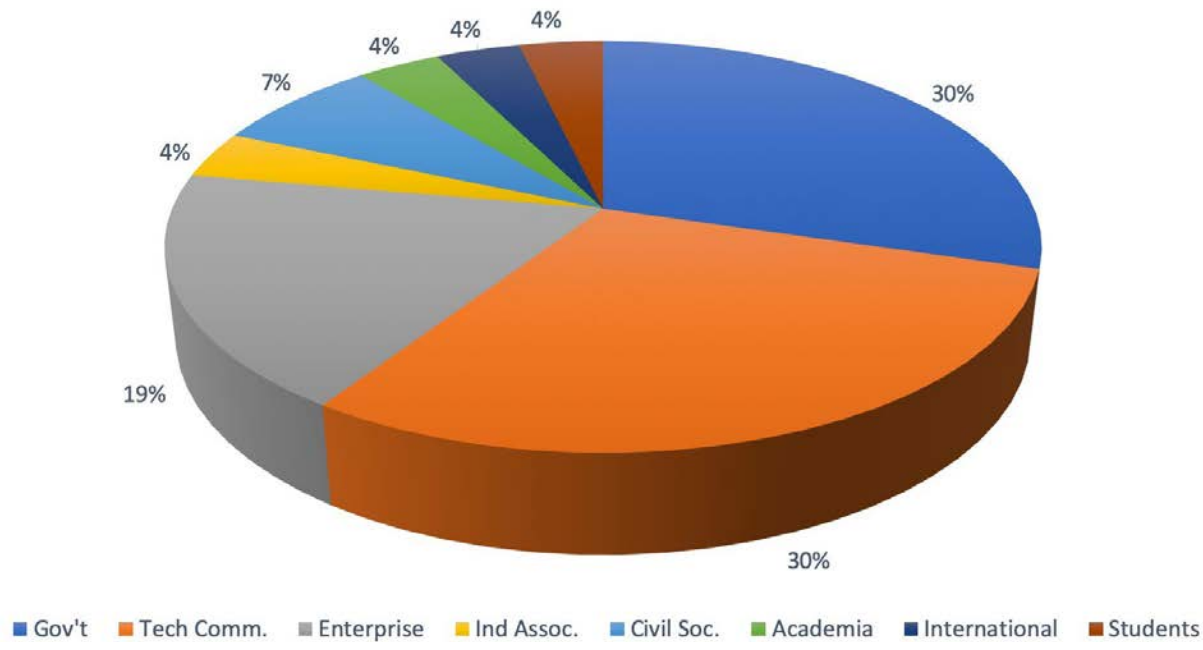
For more than two decades, the Internet Society has been a strong advocate of the use of multistakeholder approaches to policy development and decision-making. Therefore, when it considered the growth and complexity of mitigating cyber security risks from the global proliferation of the Internet of Things (IoT) and the resulting necessity for a "made-in-Canada" policy, it was predisposed to using the multistakeholder model in both the policy development and decision-making process.

One of the tenets of this model is to engage all stakeholder communities throughout the process, including the technical community, industry, government, consumers, academia, and civil society.

58 Internet Society, "Internet Governance: Why the Multistakeholder Approach Works". https://www.Internetsociety.org/resources/doc/2016/Internet-governance-why-the-multistakeholder-approach-works/

59 Ibid.

As the participants in the process engaged in their research, a broader and more diverse group became involved in the process, as indicated below.



This breadth of attendance can be directly linked to the group's openness, its acceptance of new contributors, and its respect of new ideas. Specifically, how did the multistakeholder approach used in this IoT security initiative affect the organization, process, and decision-making?

Organization

The Internet Society convened the process, assuming initial responsibility for setting goals and the agenda, bringing stakeholders together, and ensuring transparency and accessibility. In partnership with the Ministry of Innovation, Science and Economic Development (ISED), they took the initial steps in the process by reaching out to a diverse group of stakeholders from industry, the technical community, government, and civil society. Together, ISED and the Internet Society asked these stakeholders to come together as an Oversight Committee (OC) to structure and support the rest of the process.

The OC included ISED, the Canadian Internet Registration Authority (CIRA), Canadian Internet Policy and Public Interest Clinic (CIPPIC), CANARIE, along with the Internet Society. These primary organizations developed the Enhancing IoT Security initiative and were instrumental in bringing together a much larger multistakeholder group for participation and contribution to the process.

Community Engagement

A transparent multistakeholder group, drawn from the technical community, industry, government, consumers, academia, civil society, and other relevant stakeholders was convened to inform the process, select areas for research, identify appropriate working group members, review documents, and provide guidance to the development of the policy recommendations. Meetings of the Multistakeholder Group were open, public, and livestreamed, with the livestream posted online following each meeting. Reporting to the OC, the convening Internet Society was responsible for managing the process.

Three thematic areas were identified by the larger multistakeholder group and working groups were created for each:

Network Resilience: To develop a set of recommendations to protect the Internet from things and protect things from the Internet.

Device Labeling: To scope out possible labeling regimes that could be applied and/or enhanced in the Canadian landscape.

Consumer Education and Awareness: To establish an education and awareness framework to create a more security-conscious public.

Primary research was conducted through the expertise of members of the Working Groups and insights gained from participating in various fora. All resources from this project were posted on the initiative website in both English and French.

Process

The overall process included moderated, in-person meetings with the larger stakeholder group (half-day and full-day); in between those sessions, there were smaller workshops with special interest groups, virtual roundtables, and bi-weekly webinars. This was supplemented by online communication platforms (Slack, listservs, etc.) for general discussion.

One notable aspect of this process was the contribution from other ongoing and transparent concurrent processes, including the following:

Canadian Internet Governance Forum February 27, 2019

Because many of the IoT security groups were also involved in the organization of the Canadian IGF,[60] one of the panels at this meeting was devoted to "Considerations for Effective Internet of Things Labels." The aim of this panel was to discuss the proposed IoT security framework and how different stakeholder groups can support its implementation, and many of the speakers were participants in the Device Labeling Working Group of the Enhancing IoT Security process. The larger IoT process held one of its face-to-face sessions at the same venue the next day, February 28, and many of the participants in the Canadian IGF participated.

Youth IGF

Youth IGF in Canada,[61] established in 2017, worked with the Internet Society to better engage youth in Internet of Things security and amplify their voices in global and national policy making. As a part of this work, they developed a survey to learn about youth knowledge of IoT security and their opinions are about its future. Results of the survey were used to inform the development of the *Canadian Multistakeholder Process*.

Indigenous Connectivity Summit

The 2018 Indigenous Connectivity Summit[62] (ICS) was held in Inuvik, Northwest Territories on October 11-12, 2018 with the objective of finding solutions to ensure that Indigenous communities across North America can connect to fast, affordable, and reliable Internet. It drew nearly 140 delegates to Canada's Arctic Circle (and included more than 700 virtual participants) for a two-day series of panels and presentations themed on connecting the first 1,000 miles out of communities with a focus on rural and remote northern communities. One of the focus groups at the summit dealt with "Securing the Internet of Things," which was facilitated by Natalie Campbell and Katie Watson Jordan of the Internet Society.

The roundtable discussion resulted in several insights including the view that devices should be built with security at forefront and should be tested and utilize labeling similar to those for organic foods. Security training should be tied into digital literacy training and for many users, security and privacy are viewed as the same. These insights were important both as contributions to the process, and insight into consumers' understanding of the issues at hand.

60 https://canadianigf.ca/
61 https://www.facebook.com/YIGFCanada/
62 https://www.Internetsociety.org/events/indigenous-connectivity-summit/2018/

Norms and Decision-making

At the kick-off meeting of the initiative, Larry Strickling, then Executive Director of the Collaborative Governance Project at the Internet Society and former Assistant Secretary for Communications and Information at the United States' Department of Commerce, began by leading a discussion on the multistakeholder process, including the establishment of ground rules for participation, future discussion, and consensus-building for the group. Participants, both in-person and online, developed the following rules for engagement:

1. Treat people with respect: make sure everyone has a chance to express their ideas, and commit to thinking through and discussing all ideas expressed.
2. Introverts: be proactive. Extroverts: use active listening skills.
3. Stay on topic and be concise and clear.
4. Use "yes, and" instead of "no, but."
5. Raise your hand to speak and do not interrupt.
6. Declare conflicts of interest in advance.
7. Views matter more than numbers.
8. Stick with decisions unless/until new information is brought to the table.

The participants also determined how consensus would be met, with the following criteria:

1. No one is arguing anymore.
2. All dissenting views have been discussed.
3. The majority agrees on a decision, a few can live with it, and none or almost none of the participants cannot live with it.

International Linkages and Outputs

Another important aspect of the Canadian IoT process was the ability of some of the participants to bring the experience of the process to the international community. Examples include:

1. Maarten Botterman, of GNKS Consult BV, in the Netherlands, is also an active participant in the IGF Dynamic Coalition on IoT Security[63] and provided an update on the process at the IGF in Paris in November 2018.
2. Byron Holland, of CIRA, and Taylor Bentley, from ISED, also provided their perspective on the Canadian process at a different panel at the 2018 IGF: Global Alignment for Improving the Security of the Security of IoT Devices.[64]
3. ISED has agreed to participate on the IoT Security Policy Platform to share best practices and harmonize the IoT security landscape along with representatives from the United States, United Kingdom, Netherlands, France, Senegal, Uruguay, Mozilla, ENISA, and others.

International Processes Inspired by the Canadian IoT Process

Senegal – A delegation from Senegal came to Canada[65] in July to meet with members of the *Enhancing IoT Security* oversight committee. The group was comprised of government officials, Internet Society Senegal Chapter members, and staff from the Internet Society's African Bureau. The delegation met with Canadian government officials, technologists, public interest groups, and North American Bureau staff to learn more about how and why the IoT security project was initiated, and what the group had accomplished to date. The group discussed the significant successes the Canadian multistakeholder group had already achieved, the challenges it faced, and goals for the project. These conversations ultimately aided the delegation in its decision to replicate the Canadian process to enhance IoT security in Senegal. On November 28-29, the inaugural Senegalese *Multistakeholder Process: Enhancing IoT Security*[66] was held and a representative from the Canadian initiative presented on the best practices and lessons learned to date in Canada.

France – In January 2019, the Internet Society announced the creation of the IoT Security Working Group.[67] Its founding members include AFNIC (French Association for Internet Naming and Cooperation), ANSSI (National Agency for the Security of Information Systems), ARCEP (Regulatory Authority for Electronic Communications and Posts), CINOV-IT (Professional Chamber of Small and Medium-sized Digital Enterprises), Conseil National du Numérique (National Digital Council), La Quadrature du Net (Squaring of the Net advocacy group), Nokia, and Pôle Systematic Paris-Région (Ile-de-France business cluster).

The Working Group leads are now actively consulting members of the Canadian OC as they develop their best practices and recommendations.

63 https://www.iot-dynamic-coalition.org/dc-iot-meetings-at-igf/13th-igf-paris/
64 https://www.intgovforum.org/multilingual/content/igf-2018-of-25-global-alignment-for-improving-the-security-of-iot-devices
65 https://www.Internetsociety.org/blog/2018/07/collaborative-governance-leaders-canada-and-senegal-exchange-notes-on-iot-security-frameworks/
66 https://www.iotsecurity.sn/2018/12/senegal-kicks-off-enhancing-iot-security-project/
67 https://www.Internetsociety.org/news/press-releases/2019/Internet-society-advances-iot-security-in-france/

Lessons Learned

For all of the multistakeholder process' advantages, it also poses challenges. Over the course of this project, the group developed best practices based on what it learned that it will incorporate into future initiatives.

These lessons included:

1. **Scope:** Defined by participants, and if gaps appear, they can only be addressed by the group as a whole in agreement.
2. **Time:** Because multistakeholder projects can move very slowly, adding extra contingency time is prudent.
3. **Stakeholder identification:** Use as many resources as possible to assist with identification and outreach, including the Oversight Committee, newly recruited stakeholders, and the influence of champions within your own organization.
4. **Stakeholder engagement:** Multistakeholder projects demand much commitment from stakeholders.
5. **Facilitation:** The most critical component to this initiative's success has been using a facilitator who is both a subject-matter expert and has experience with the multistakeholder process. In the case of the *Enhancing IoT Security* initiative, that was Andrew Sullivan, President and CEO of the Internet Society.
6. **Maintaining momentum:** After pivoting to more webinars and many more communication platforms, engagement increased between multistakeholder meetings.

Appendix IV

7.4 NRWG Research

The goal of the NRWG was to develop a security framework, run code that implements that framework, and develop and refine user-centered onboarding and support tools for that framework.

The NRWG considered the following aligned activities in consideration of this project:

1. Manufacturer Usage Description (MUD)

An important element that the working group discovered at the outset was the existence of a new Internet Engineering Task Force (IETF) protocol in development named Manufacturer Usage Description (MUD). This protocol is proposed as a new way to signal the networking and security control characteristics of an IoT device in order to appropriately apply the correct security controls to ensure its safe operation.

2. The National Cybersecurity Center of Excellence and National Institute of Standards and Technology

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is also working on "Mitigating IoT-Based Automated Distributed Threats".[68] Both CIRA and NIST initiatives have similar architecture and seem to be aligned with a different scope.[69]

3. Open Source Manufacturer Usage Description (OSMUD) @ osmud.org

OSMUD is an open source Manufacturer Usage Description project (osMUD for short). osMUD is working to improve the security of connected things and their networks. osMUD implements the MUD specification, and is therefore another reference implementation for MUD. At this stage of development, having multiple reference implementations (running code) is an important aspect of standard development. The Network Resilience Working Group is closely tracking their work.

4. IoT Analytics Project At University of New South Wales

A research project which for six months instrumented a smart environment with more than twenty-eight different IoT devices spanning cameras, lights, plugs, motion sensors, appliances, and health-monitors. The project created a tool for generating MUD files from network traces, and hosts generated MUD and trace files, as well as research papers.

68 https://www.nccoe.nist.gov/projects/building-blocks/mitigating-iot-based-ddos

69 See also: https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

5. **OpenWRT @ openwrt.org**

The ultimate goal of this project is to have our Secure Home Gateway code included and accepted by the core openWRT project. In the future, the NRWG aims to ensure openWRT is bundled by default with its IoT security framework, and/or that manufacturers' upgrades to their openWRT software come equipped with this framework. Having this group's framework as the standard would mean that it is core to the base openWRT package.

6. **PRPL Foundation (prplWRT) @ prplfoundation.org**

The mission for PRPL is to develop, support, and promote an open-source, community-driven consortium with a focus on enabling the security and interoperability of embedded devices for the IoT and smart society of the future. PRPL strives to support, align, and complement major community initiatives such as OpenWrt to drive carrier grade features to the next level.

Including the Secure Home Gateway framework as part of the PRPL initiative would help the NRWG's code to become part of the core openWRT base platform, but the major opportunity is the potential reach and impact of PRPL. In order to take advantage of this opportunity, a member of this working group would need to join as a member and participate in the prplSecurity workgroup.

7. **Project home base @ GitHub.com/CIRALabs/Secure-IoT-Home-Gateway**

The CIRA Secure Home Gateway project consists of a functional prototype, open source software and the implementation of new standards. Its major components are the Turris Omnia Home Gateway from CZ.NIC, which is a secure home gateway that leverages the OpenWRT operating system; IoT device provisioning based on the IETF Manufacturer Usage Description (MUD) standard; and a Home Gateway smart phone app that runs on Android and iOS.

The Secure Home Gateway secures the IoT devices in the network using a Per Device Access Policy (PDAP). The device onboarding process includes three steps. First, the home gateway identifies any new IoT device that's been added to the network. Then it places a policy around the IoT device restricting it to performing a specific function. Finally, while the device is in operation, the home gateway constantly monitors and quarantines it at the first sign of any behavioural changes.

8. **Standard for an Architectural Framework (IEEE P2413)**

This standard defines an architectural framework for IoT, including descriptions of various IoT domains, definitions of IoT domain abstractions, and identification of commonalities between different IoT domains. The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements. It also provides a blueprint for data abstraction and the quality "quadruple" trust that includes protection, security, privacy, and safety. Furthermore, this standard provides a reference architecture that builds upon the reference model. The reference architecture covers the definition of basic architectural building blocks and their ability to be integrated into multi-tiered systems. The reference architecture also addresses how to document and, if strived for, mitigate architecture divergence. This standard leverages existing applicable standards and identifies planned or ongoing projects with a similar or overlapping scope.

9. **ETSI Technical Specification 103 645ETSI Technical Specification 103 645**

ETSI's specifications are also consumer IoT-centric. The objective of the present document[70] is to support all parties involved in the development and manufacturing of consumer IoT with guidance on securing their

70 https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

products. The provisions are outcome-focused, rather than prescriptive, giving organizations the flexibility to innovate and implement security solutions appropriate for their products. The focus is on the technical controls and organizational policies that matter most in addressing the most significant and widespread security shortcomings, including ensuring compliance with the General Data Protection Regulation (GDPR), the Cybersecurity Act, and the proposed IoT Cybersecurity Improvement Act of 2019[71] in the United States.

10. CableLabs MicroNets

CableLabs has recently begun prototyping a similar framework for limiting and tailoring IoT connectivity. Because it is conceptually based around network segmentation, they call it MicroNets.

11. Scalability, Control, and Isolation on Next Generation Networks (SCION)

SCION "provides route control, failure isolation, and explicit trust information for end-to-end communication." This architecture "organizes existing ASes into groups of independent routing planes, called isolation domains, which interconnect to provide global connectivity".[72] It was recommended[73] through the open comment period for the Draft Outcomes Report that SCION be considered by the NRWG, but the group ultimately did not reach consensus on its use for the purposes of this project.

NRWG conducted outreach and collected feedback from the following events:

1. Many IoT security 2018 multistakeholder meetings: https://iotsecurity2018.ca/
2. Amsterdam RIPE77: https://ripe77.ripe.net/archives/video/2309/
3. ICANN60: Abu Dhabi – https://ccnso.icann.org/sites/default/files/field-attached/presentation-home-network-registry-idea-30oct17-en.pdf
4. ICANN61: Puerto Rico – https://static.ptbl.co/static/attachments/169252/1520883903.pdf?1520883903
5. ICANN63: Barcelona – https://static.ptbl.co/static/attachments/191684/1540208530.pdf?1540208530
6. CENTR Tech38/R&D12 – Moscow Presentation

Specifications NRWG is leveraging:

1. https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/
2. https://datatracker.ietf.org/doc/draft-ietf-netmod-acl-model
3. RFC 7368
4. RFC 8375
5. https://datatracker.ietf.org/doc/draft-ietf-homenet-simple-naming
    a. https://datatracker.ietf.org/doc/draft-ietf-homenet-front-end-naming-delegation
    b. RFC 4033,4034,4035 (DNSSEC)
    c. https://datatracker.ietf.org/doc/rfc5011/
    d. RFC 4795

71 https://www.scribd.com/document/401616402/Internet-of-Things-IoT-Cybersecurity-Improvement-Act-of-2019
72 https://www.scion-architecture.net/
73 https://iotsecurity2018.ca/wp-content/uploads/2019/04/IoT-Canada.pdf

Specifications NRWG is planning/considering:

1. RFC4301, RFC7296 (IPsec. Considering OpenVPN too)
2. RFC8366, https://datatracker.ietf.org/doc/draft-ietf-anima-bootstrapping-keyinfra/
3. https://datatracker.ietf.org/doc/draft-cheshire-dnssd-roadmap/
4. https://datatracker.ietf.org/doc/draft-ietf-dnssd-hybrid/
5. https://datatracker.ietf.org/doc/draft-cheshire-dnssd-roadmap/
6. https://datatracker.ietf.org/doc/draft-ietf-dnssd-mdns-relay/

Specifications NRWG is developing:

1. draft-richardson-opsawg-securehomegateway-mud-00
2. draft-richardson-anima-smartpledge-00

NRWG Next Steps:

CIRA and the participating NRWG experts expect to meet the following high-level requirements for its Phase 2 Secure Home Gateway demonstrator:

1. Re-develop a reference implementation that is installable, reliable, upgradable, and fully supports daily use through an app.
2. Complete/continue to maintain IETF standards and Best Current Practices.
3. Standardize the API between APP and gateway, MUD, provisioning with new Internet-Draft.
4. Create a process to curate MUD profiles and associated firmware for global access.
5. Internet-Draft, Best Current Practices on how to un-quarantine devices.
6. Address WiFi shared key problem and give unique passwords on shared SSID.
7. Provide traffic visualization through SPIN/nTOP.
8. Include DNS provisioning, a unique domain per SHG to leverage DNSSEC and have legitimate CERTs.
9. Build evaluation units for field testing (aspirational goal).
10. Overall: Run code and follow/improve/create IETF or ISO standards.

A further direction of interest is to apply the framework beyond WiFi to other kinds of IoT gateways based on, e.g.,

1. 4G & 5G cellular networks.
2. LoRa.
3. 802.15.4 (i.e. Zigbee, Thread, 6loWPAN).

The group intends to continue to build partnerships on MUD profile curation/storage/development, and is particularly interested in finding a partner capable of hosting a MUD file clearinghouse.

Appendix V

7.5 DLWG Research and Evaluation of Existing Labeling Formats and Standards

The sections that follow provide the research and information that was identified over the course of the project. These details were discussed and reviewed for applicability to Canada and as discussion points at the meetings that were held over the project period. They are included here as a summary review and consideration for labeling requirements.

In order to provide more insight into the relative merits of the different types of labeling, it is useful to refer to critical research performed on well-established labeling schemes, particularly on the food labels and the energy efficiency labels.

Food and energy labels serve as particularly effective models for labeling schemes.[74] [75]

74 PETRAS IoT Hub, Rapid evidence assessment on labeling schemes and implications for consumer IoT security, October 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf

75 UCL Jill Dando Institute of Security and Crime Science, "Developing a consumer security index for domestic IOT devices (CSI), "17 January 2019.

Refrigerating appliances, as EEI									
A+++	A++	A+	A	B	C	D	E	F	G
<22	<33	<42/44	<55	<75	<95	<110	<125	<150	>150

FIGURE 1. ENERGY EFFICIENCY LABEL

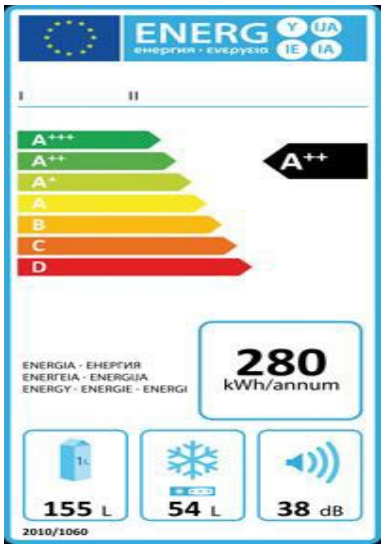


FIGURE 2. LABEL CATEGORIZATION FOR REFRIGERATORS

Energy Efficiency Labels

In 1995, the EU introduced the Directive 92/75/EC that was updated as Directive 2010/30/EU, outlining an energy consumption labeling scheme to be displayed on electronic products (Figure 1). In 2010, a grading scheme (A+, A++, and A+++) was introduced, following developments in energy efficiency standards. It is mandatory for manufacturers to display energy efficiency labels for certain classes of product, including refrigerators, televisions, and dryers.

The EU directive requires manufacturers to provide the labels for free to dealers, and include a performance table in brochures and associated documents.

A challenge for consumers in dealing with the energy efficiency label A+++ to G is that it is quite product dependent and not standardized. For example, television labels encompass from A+ to F, but coffee machines use a scheme from A to G. In 2010, all washing machines that were in label category A were prohibited. Then in order to drive market shift, all future washing machines needed to be in the A+ to A+++ range. These distinctions are generally invisible to the consumer and lead to confusion among product lines.

Also, the introduction of A+ to A+++ grading has undermined the efficacy of the label as it became difficult for consumers to differentiate between A+ to A+++ and A to G. Consumers are generally not willing to make the additional investment to buy an A+ or A++ rated product, and settle for an A product as good enough.

GDA LABEL

GDA LABEL WITH TRAFFIC LIGHT SYSTEM

Food Labels

As per the PETRAS report, food labeling enables consumers to make healthier food choices and reduce levels of obesity in the general public. The European Commission regulates the provision of food labeling, requiring pre-packaged foods to label their nutritional content (EC No. 1169/2011). Labeling on the back of a food package is mandatory for manufacturers, while labeling on the front-of-pack (FOP) is optional. FOP labels must display portion values for key risk areas (sugars, salt, fat, and saturates).

There are three types of FOP labels. The first is the Guideline Daily Amount[76] (GDA) shown below. The other figure shows the GDA scheme with colored traffic light system and is approved by the UK Food Standards Agency.[77] The third FOP type is a health logo, which is a "seal of approval" scheme, granted to a food product that is proven to meet particular nutritional requirements and/or standards (see below). This also shows the European Union organic food logo,[78] which came into effect in 2012, and is compulsory on all pre-packaged organic food products produced in the EU that meet specific standards.

76 https://www.foodlabel.org.uk
77 https://www.food.gov.uk
78 https://www.foodnavigator.com

EUROPEAN UNION ORGANIC FOOD LOGO

European Union organic food logo

Research has shown that the display of FOP labels has increased healthy product choice by eighteen per cent.[79] Little consensus exists on the most effective FOP labeling scheme. Research on GDA has shown that consumers find it difficult to identify the nutrient content, while more recent research has indicated that it helps consumers identify healthier products. On the other hand, a number of studies have shown that the traffic light FOP scheme facilitates more healthy food choices, compared to other FOP labeling schemes.[80] Health "seal of approval" logos are preferred by consumers due to their simplicity[81] and intuitive format, and have been found to reduce the time consumers spend in examining food packages.

In summary, there are clear benefits to a FOP label in aiding consumer choice, with each format offering its own strengths and limitations. Consumers tend to prefer a binary label; however, this may lead to poor decision-making, and research indicates that traffic light systems help consumers make better judgments and are marginally more effective in driving a healthier product choice.

The success of any of the food label schemes will be limited by the consumer's attention at the point of sale. Often, consumers are rushed and focus on trading off the brand, costs, convenience, and taste when making product choices.[82]

79 Cecchini M, Warin L. Impact of food labeling systems on food choices and eating behaviours: a systematic review and meta-analysis of randomized studies. Obes Rev. 2016;17:201–10. doi:10.1111/obr.12364

80 Id.

81 Id.

82 Szanyi JM. Brain food: Bringing psychological insights to bear on modern nutrition labeling efforts. Food and Drug Law Journal. 2010;65. http://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/foodlj65&section=9. Accessed 24 May 2018.

QR CODES USED BY HP

STAPLES MOBILE MARKETING CAMPAIGN USING QR CODES

Relevant Use Cases for QR Codes

The use cases of QR Codes vary widely and cover different areas from marketing, product packaging, advertising, special causes, customer surveys, and much more. Below, three use cases of QR Codes are presented that focus on providing product information particularly in the ICT (information and communications technology) domain.[83]

HP Use Case

HP sought a practical and interactive way for customers to receive details on their products right from the package. They wanted potential customers to more easily understand what they were purchasing, and what accessories, like ink packages, were required for each.

HP used ScanLife activated codes extensively on most of their consumer printer line around the world. The codes told customers more about the products and gave them details on accessories which made it easier for shoppers to buy products, especially during the busy holiday season when retail associates were difficult to find.

Staples Use Case

Staples had a variety of goals for its mobile marketing campaign, including demonstrating value for the consumer while also helping the business achieve key sales milestones. The ultimate objective, however, was to increase overall conversions through the use of an effective in-store campaign. Staples incorporated QR Codes into its in-store displays.

83 Scanbuy, QR Codes Use Cases, http://www.scanlife.com/case-studies/

SELECTING KEURIG COFFEE MACHINES UTILIZING QR CODES

Keurig Use Case

Keurig wanted to give customers more dynamic information on all of their products, from K-Cup brewers to K-Cup flavours. Keurig used QR Codes as a flexible tool and centralized code management platform to work across multiple divisions within the organization. Dynamic codes were generated for Keurig products allowing the experiences to be adapted in real-time. Once scanned, the codes educate consumers on the product of interest: product information, a video tutorial of how the product works, and an explanation of why everyone should have a Keurig in their home or office. The campaign helps shoppers decide which Keurig brewing machine was best for them without interacting with sales associates.

Selecting Keurig coffee machines utilizing QR Codes

Standards and Best Practices

As multiple groups develop standards, the scope and jurisdiction of these documents may create confusion for consumers. Buyers must consider how they will use this product and the potential risks involved before determining the best documents to purchase. Currently, fragmentation and lack of industry wide collaboration on security and privacy across standards development organizations (SDOs) and trade associations is a problem not just in North America, but globally.

In the following table, we have included the key referenced standards by the DCMS report "Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security".[84] They are provided here for reference only as users will need a means to determine risks prior to purchase.[85]

84 Department of Digital, Culture, Media and Sport (DCMS), Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security, 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747977/Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf

85 Other recommendations and standards include NIST's definition of baseline IoT security recommendations, with conclusion expected out by the fall of 2019: https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iot_cybers ecurity_capabilities_baseline_considerations.pdf, and the legislation passed by California and other states in the United States, most of which are focused on minimum guidelines.

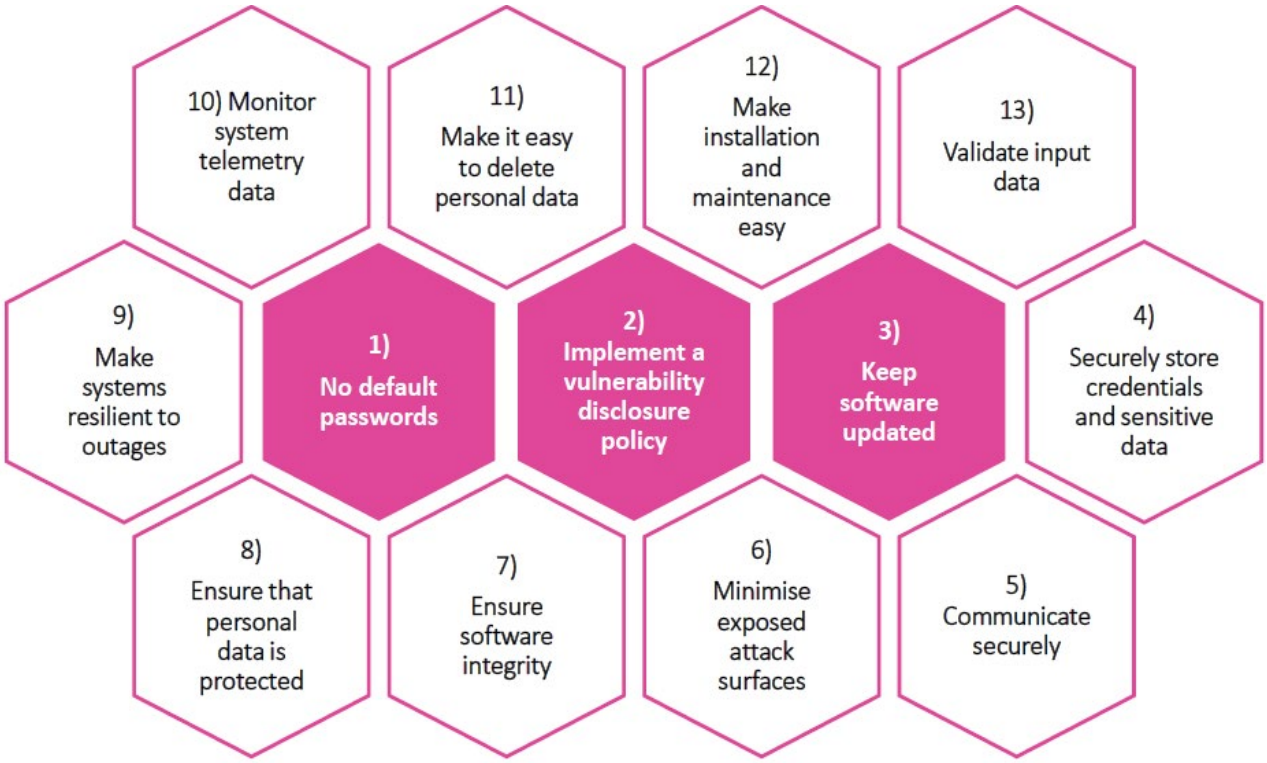
Organization	Standard/Recommendation
ETSI Technical Specification	Globally-applicable industry standard containing normative provisions for consumer IoT
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT
GSMA	IoT Security Guidelines for Service Ecosystems
IEEE	IoT Security Principles and Best Practices
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices
IoT Security Foundation	IoT Security Compliance Framework 1.1
IoT Security Initiative	Security Design Best Practices
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5
U.S. Department of Homeland Security	Strategic Principles for Securing the Internet of Things (IoT)
U.S. House of Representatives	HR 1668 – Internet of Things (IoT) Cybersecurity Improvement Act of 2019 (Bill)
Alliance for Internet of Things Innovation (AIOTI)	Report on Workshop on Security and Privacy in the Hyper connected World
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations
CableLabs	A Vision for Secure IoT
IoT Security Foundation	Vulnerability Disclosure Best Practice Guidelines, IoT Security Compliance Framework 1.1
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations

Organization	Standard/Recommendation
Cloud Safety Alliance	Future-proofing the connected world: thirteen steps to Developing Secure IoT
European Commission and AIOTI	Report on Workshop on Security & Privacy in IoT
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0
IoT Security Initiative	CyberSecurity Principles of IoT
Internet Research Task Force (IRTF) Thing-to-Thing Research Group (T2TRG)	State-of-the-Art and Challenges for the Internet of Things Security
Microsoft	IoT Security Best Practices
Open Connectivity Foundation (OCF)	OIC Security Specification v1.1.1
Open Web Application Security Project (OWASP)	IoT Security Guidance
Symantec	Strategic Principles for Securing the Internet of Things (IoT)
oneM2M	TR-0008-V2.0.1 Security (Technical Report)

The principles identified in the Code of Practice for Consumer IoT Security[86] are shown below.

Similar guidelines have been provided by the U.S. Department of Homeland Security in the "Strategic Principles for Securing the Internet of Things" report.[87] The IoT Alliance Australia (IoTAA) published a comprehensive report titled "Internet of Things Security Guidelines".[88] The IoTAA report identifies "the Trust Framework," whose requirements form the basis for evaluating an IoT system for best practices in security and privacy, and the basis of the IoTAA Security and Privacy Trustmark.

UK IOT CONSUMER CODE OF PRACTICE



86 Department of Digital, Culture, Media and Sport (DCMS), Code of Practice for Consumer IoT Security, 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747977/Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf

87 [17] U.S. Department of Homeland Security, Strategic Principles for Securing the Internet of Things, 2016, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

88 IoT Alliance Australia, Internet of Things Security Guideline, 2017, http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf

BSI Kitemark for IoT Devices in the United Kingdom

In March 2018, the United Kingdom Government's Secure by Design review announced a series of measures to make connected devices safer to use.[89] The British Standards Institution (BSI) Kitemark builds on these guidelines by providing ongoing rigorous and independent assessments to make sure the device both functions and communicates as it should, and that it has the appropriate security controls in place. Manufacturers of Internet connected devices will be able to reassure consumers by displaying the Kitemark on their product and in their marketing materials.

There are three different types of BSI Kitemark for IoT Devices, which will be awarded following assessment according to the device's intended use: residential, for use in residential applications; commercial, for use in commercial applications; and enhanced, for use in residential or commercial high value and high-risk applications.[90]

The assessment process involves a series of tests that help ensure the device is fully compliant to the requirements. Before being awarded the Kitemark, the manufacturer is assessed against ISO 9001, and the product is required to pass both an assessment of functionality and interoperability, as well as penetration testing that scans for vulnerabilities and security flaws. Once the BSI Kitemark is achieved, the product will undergo regular monitoring and assessment including functional and interoperability testing, further penetration testing, and an audit to review any necessary remedial action. Importantly, if security levels and product quality are not maintained, the BSI Kitemark will be revoked until any flaws are rectified.

BSI Kitemark[91] provides comfort and confidence to users of products or services across a whole range of sectors. Recognition of the BSI Kitemark is high. Two thirds of all UK consumers associate it with quality, assurance, reliability, and trust. Ninety-three per cent of adults believe BSI Kitemark products are safer and seventy-five per cent say the BSI Kitemark will help make choosing between products easier.

Other Labeling Programs

It should be noted that other labeling programs are currently in development, such as Trustable Technology Mark a self-asserted mark covering broad aspects of IoT security and privacy.[92] The DLWG's research is not meant to be exhaustive, but rather to paint a picture of the existing IoT security labeling market.

89 UCL Jill Dando Institute of Security and Crime Science, "Developing a consumer security index for domestic IOT devices (CSI), "17 January 2019
90 British Standards Institution. BSI launches Kitemark for Internet of Things devices, 2018. https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2018/may/bsi-launches-kitemark-for-Internet-of-things-devices/.
91 Id.
92 https://trustabletech.org/

IoT Product Testing in Australia

Another example of IoT product testing and certification is the process identified in Australia. IoT product manufacturers may wish to submit their products for testing by an accredited test laboratory, either under the National Association of Testing Authority (NATA) scheme or under the Australian Government in the Australasian Information Security Evaluation Program (AISEP). Formal testing will, if successful, result in the award of a test certificate and provide evidence of independent security assurance to customers.

Currently, there is no mandated requirement for security testing, but the high profile of cyber-attacks involving IoT devices makes this a key area of consideration for users. Having evidence that a device has been security tested will be a competitive advantage.

In order to provide security and privacy confidence in IoT devices designed, manufactured, or deployed in Australia, the IoTAA will release a security testing procedure based on the Online Trust Alliance Framework[93] which will be available for accredited organizations to use to recommend the issue of an IoTAA Security and Privacy Trustmark. There are currently three sets of published criteria that can be used for testing IoT devices:

1. The IoT Security Foundation has proposed a compliance scheme based on evaluation against their Security Compliance Framework. This is based on the DCMS code of practice. In addition, the IoT Security Foundation has proposed a compliance regime for demonstrating security in IoT devices and systems. This categorizes an IoT product into one of five classes: Class 0 to Class 4. Additionally, the ETSI TS 103 645 has been written so that manufacturers can test against the thirteen steps.

Class	Impact of Compromise	Confidentiality	Integrity	Availability
0	Minimal	Basic	Basic	Basic
1	Limited impact on an individual or organization	Basic	Medium	Medium
2	Significant impact on one or more individuals or organizations	Medium	Medium	High
3	Significant impact to sensitive data	High	Medium	High
4	Personal injury or damage to critical infrastructure	High	High	High

2. The Open Web Application Security Project (OWASP)[94] has developed a testing guide for IoT products. It covers sixteen IoT Principles of Security and provides a framework for testing ten different vulnerabilities.
3. The Online Trust Alliance (OTA) framework provides measurable requirements, which can be used as a starting point for selecting security-testing requirements.[95] The framework consists of eight categories of actionable principles: authentication, encryption, security, updates, privacy, disclosures, control, and communications. It also considers stakeholders who will have a collective responsibility for developing a secure solution.

IoT device manufacturers could select the relevant criteria for their device from these three documents, in addition to any device specific functionality not otherwise covered. These criteria will then form the Initial Claims Document for the security testing.

93 https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

94 Open Web Application Security Project (OWASP), Principles of Security, www.owasp.org/index.php/Principles_of_IoT_Security

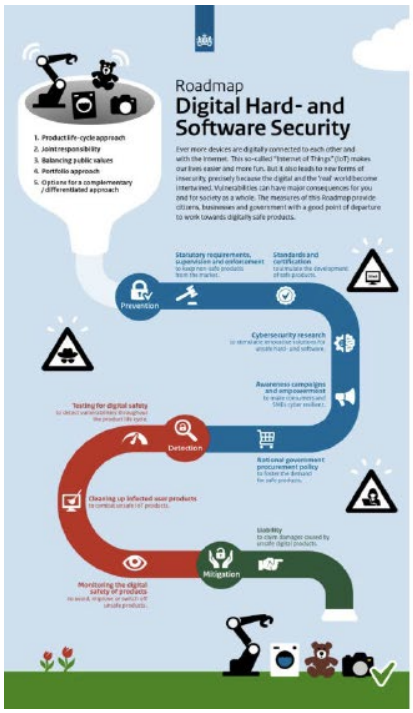
95 Online Trust Alliance (OAT), IoT Trust Framework, https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

IoT Product Certification in The Netherlands/European Union

As part of EU negotiations, the Netherlands is strongly promoting the rapid adoption of the Cybersecurity Act (CSA) and the active development of a European Cybersecurity Certification framework for ICT products and services.[96]

Moreover, the Dutch government supports the swift adoption of mandatory certification for specific product groups, i.e. products that present the greatest risk or the most problems in practice. In the long term, mandatory certification or compliance with a CE marking for all products with Internet connectivity should be implemented through gradual expansion.

ROADMAP FOR HARDWARE AND SOFTWARE SECURITY – THE NETHERLANDS



Product life cycle approach

Balancing public interest

Joint responsibility

Portfolio approach

EU Framework: Security Certification of ICT Products and Services

The proposed Cybersecurity Act (CSA) is the European Commission's attempt to create, amongst others, a harmonized framework for the cybersecurity certification of ICT products and services within the EU. The absence of reciprocal agreements on standards and certification systems forms a barrier to creating a European market for cybersecurity products and services because it limits the scale for providers, reduces choice, and creates increasing uncertainty for procurers.

Common European certification of products and services will indicate that they are resilient (at a specified security level) to threats to their availability, authenticity, integrity, and reliability of data or of the functionalities and services being offered. The CSA aims to target fragmentation and foster the harmonization and mutual acknowledgment of cybersecurity certification at the European level.

Once a European certification framework has been adopted for a product or service, national government schemes will become redundant, and the Member States will no longer need to develop their own certification programs.

96 Ministry of Economic Affairs and Climate Policy, The Netherlands, Roadmap for Digital Hard-and Software Security, 2018, https://www.government.nl/documents/reports/2018/04/02/roadmap-for-digital-hard--and-software-security

ETSI Cyber Security for Consumer Internet of Things Standard

The European Telecommunications Standards Institute (ETSI) published the "Cyber Security for Consumer Internet of Things" or the TS 103 645 V1.1.1 standard, in Feb. 2019.[97] This is certainly a major development into the direction of specifying globally applicable high-level provisions for the security of consumer devices that are connected network infrastructure such as the Internet or home network.

The standard document provides basic guidance for manufacturers involved in the development and manufacturing of consumer IoT on how to implement those provisions.

The thirteen high-level provisions identified in the standard document closely follow the principles identified in the Code of Practice for Consumer IoT Security.[98]

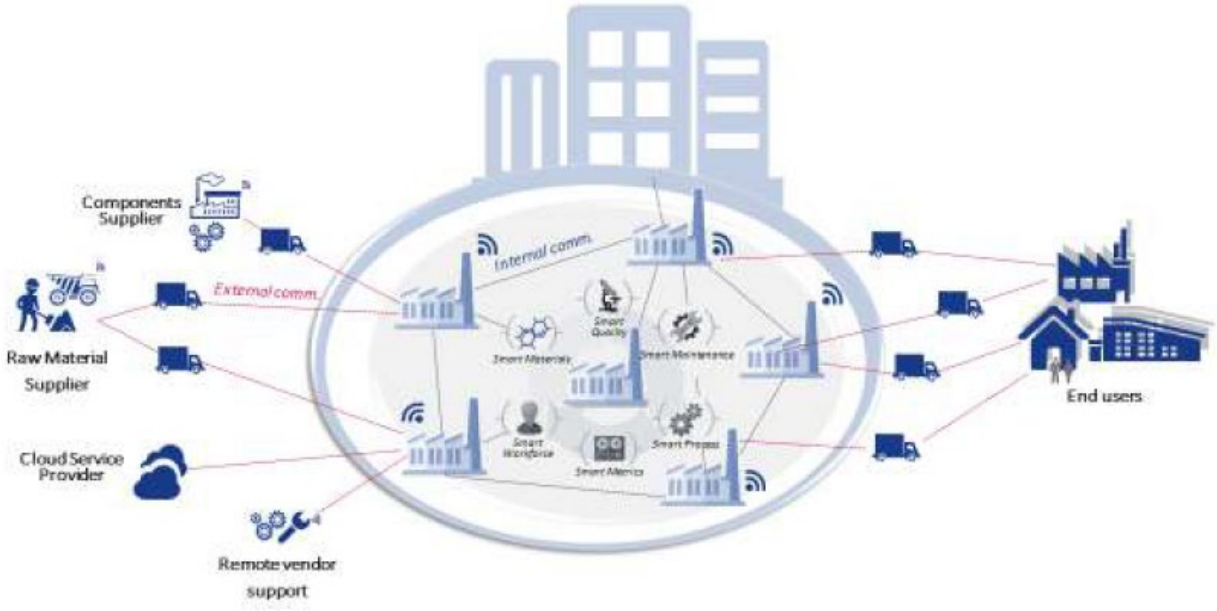
ENISA "Good Practices for Security of Internet of Things"

Towards the end of 2018, the European Union Agency for Network and Information Security (ENISA), which is a center of network and information security expertise for the EU, published a comprehensive report on "Good Practices for Security of Internet of Things," focusing on the context of Smart Manufacturing (Industry 4.0.).[99]

ENISA defines Industry 4.0 as "a paradigm shift towards digitalized, integrated and smart value chains enabling distributed decision-making in production by incorporating new cyber-physical technologies such as IoT".

Industry 4.0 is gaining acceptance and is rapidly becoming a reality, making use of intelligent, interconnected cyber-physical systems to automate all phases of industrial operations. This evolution is spanning phases of design, manufacturing, and operations, with a great impact on consumers' and citizens' safety, security, and privacy due the extremely wide threat landscape, resulting from the cyber-nature and the inherent autonomy of Industry 4.0 and IoT.

COMMUNICATIONS RELATIONSHIPS IN INDUSTRY 4.0



97 ETSI, Cyber Security for Consumer Internet of Things, TS 103 645 V1.1.1, https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

98 Department of Digital, Culture, Media and Sport (DCMS), Code of Practice for Consumer IoT Security, 2018, https://www.gov.uk/government/publications/secure-by-design

99 ENISA, Good Practices for Security of Internet of Things, 2018, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

A key focal point of the ENISA report is the development of Security Measures for IoT in Smart manufacturing. The approach is to provide guidelines and recommendations for Operators, Manufacturers, and Users of Industrial IoT (IIoT). Applying these guidelines can help prevent or properly respond to potential cyber-attacks and ensure overall security and safety of the industrial IoT environment.

The recommendations and guidelines are classified into three main groups: Policies, Organizational Practices, and Technical Practices.

GOOD PRACTICES OVERVIEW

CTIA Cybersecurity Certification for IoT Devices in the U.S.

In 2018, the U.S. Cellular and Telecommunications and Internet Association (CTIA) published its Cybersecurity test Plan for IoT Devices.[100] This plan identifies testing requirements for CTIA Cybersecurity Certification of managed Internet of Things devices. In this case, an IoT device contains an IoT application layer that provides identity and authentication functionality and at least one communications module supporting either LTE or WiFi connectivity.

The test plan defines the Cybersecurity test that will be conducted by CTIA Authorized test labs (CATLs) on devices submitted for CTIA Cybersecurity Certification. An IoT device connects to at least one network to exchange data with other devices, vehicles, home appliances, infrastructure elements, etc. The device might include hardware, software, sensors, actuators, and network connectivity.

CTIA Cybersecurity Certification is defined in three categories. The first category identifies core IoT device security features, and the second and third categories identify security elements of increasing sophistication, complexity, and manageability.

While the test plan aims at ensuring compatibility across Cybersecurity systems through using the most widely adopted standards, it mandates a number of critical standards including: AES key size standards, end-to-end encryption standards, syslog standards, etc. An AES with a minimum of 128-bit key is expected by the test plan, to ensure interoperable cryptographic capability among all devices tested. However, devices may also support other algorithms and key sizes that provide the same or more cryptographic security.

100 CTIA, CTIA Cyber Security Certification Test Plan for IoT Devices, 2018, https://api.ctia.org/wp-content/uploads/2018/08/CTIA-IoT-Cybersecurity-Certification-Test-Plan-V1_0.pdf

The table below provides an overview of the cybersecurity test cases per IoT device category:

CTIA IOT CYBERSECURITY TEST CASES

CATEGORY 1 IoT security features	Terms of Service and Privacy Policies
	Password Management
	Authentication
	Access Controls
	Patch Management
	Software Updates
CATEGORY 2 IoT security features	Cat. 1 IoT security features
	Audit Log
	Encryption of Data in Transit
	Multifactor Authentication
	Remote Deactivation
	Secure Boot
	Threat Monitoring
	IoT Device Identity
CATEGORY 3 IoT security features	Cat. 1 and Cat. 2 IoT security features
	Encryption of Data at Rest
	Digital Signature Generation and Validation
	Tamper Evidence
	Design-in Features

Canadian Standards Association (CSA) Group Cyber Verification Program

The CSA Group is currently developing a program and national standard that is aiming to address the product and organization security aspects. The Cyber Certification Program (CVP) consists of several aspects including a self-assessment, onsite audit, and formal product testing and evaluation. This program is built on the premise that an insecure organization cannot build a secure product. Security practices must be embedded into the organization's operations and development processes.

The assessment aspects consider six domains and eighteen practice areas within these domains. The current self-assessment consists of 198 binary questions that, once completed in connection with an audit, will provide a maturity rating for the organization.

The program has been field testing and has resulted in filing of a bi-national standard under Standards Council of Canada and the American National Standards Institute. This standard currently titled T-200 in Canada is currently under development. This will include the ability for vendor organizations to perform an attestation to this standard and as a maturity-based model it can use any recognized standard or best practice as the control for assessment.

Underwriters Laboratories (UL) 2900

UL has a series of standards that will formally evaluate a product against specific criteria to determine that the vendor is following and has correctly implemented the list of controls. These currently include medical products and devices. The testing and evaluation process is stringent and will provide buyers the assurance that formal testing, including penetration testing, has been conducted against a product.

ISO/IEC Standards

There are several standards that may be considered for products and organizations to determine their security posture. These may not necessary result in a label but a certificate of product or organizational testing and evaluation.

ISO/IEC 27001: A standard and certification process that will indicate that an organization has formally implemented and maintains an information security management system or ISMS. An ISMS is a formal system of process, procedures, and controls that identify and mitigate the risks associated with the organization. The controls are defined in the standard and guidance is provided on how to implement the necessary risk management framework within an organization.

ISO/IEC 9001: A standard and certification process that will indicate the process maturity of an organization in order to deliver a product or service. This includes an approach that states what they do, do what they say, and be able to prove it by creating process artifacts.

ISO/IEC 15408: Common Criteria is a formal product assessment methodology that provides assurance to product based on confidentiality, integrity, and availability. It can assess both hardware and software and is typically a requirement for government and higher security technology deployments. Objective testing uses an evaluation process that considers either the Evaluation Assurance Level (EAL) or Security Assurance Requirements (SAR) to provide the buyer with a rating that indicates whether the vendor meets a specific target level.

ISO/IEC 62443: This family of standards is focused on industrial and embedded systems. Organizations can target either assessing their products individually or having their entire SDLC program certified for any product/service being developed. With global recognition it does provide a means for a single level of assessment for a vendor to provide assurance of the security design practices. Given the complexity of this standard it is not necessary positioned for SMBs or start-ups but for more mature organizations with products. Due to the inherent costs of implementation and the required expertise it might be very difficult for SMBs to consider this standard.

CyberNB Cyber Essentials: This program is built on the UK program with the same title and objectives. The province of New Brunswick and several partners have adopted this framework as a means to validate that organizations have a minimum set of security requirements that they can demonstrate have been deployed. The focus is on IT controls within the organization and targets SMBs for deployment of these controls.

Potential labels by function

The list that follows provides some product categories and product labels that currently exist. While not foolproof, the labeling does provide a level of assurance that the vendor takes assessment and evaluation seriously. As such, these vendors have decided to obtain formal certification which indicates a level of business, process, and product maturity. These certifications are not a guarantee of security and privacy safety, but that the product has undergone a certain level of evaluation.

1. Home appliances
    a. Electrical certification: multiple CAN, US, and IEC standards.
    b. Security testing and evaluation: UL 2900 or equivalent.
    c. Attestation to CSA, CVP, or equivalent.
    d. Consumer Reports, BSI Kitemark, or equivalent.
    e. 62443-3-1 or 62443-4-1 for embedded systems and vendor SDLC.
2. Security and safety
    a. Functional safety certification to IEC 61508.
    b. Security testing to ISO 15408 *for mission critical environments.
    c. Security testing and evaluation UL 2900 or equivalent.
    d. Attestation to CSA, CVP, or equivalent.
    e. Consumer Reports, BSI Kitemark, or equivalent.
3. Lighting
    a. Electrical certification: multiple CAN, US, and IEC standards.
    b. Security testing and evaluation UL 2900 or equivalent.
    c. Attestation to CSA, CVP, or equivalent.
    d. 62443-3-1 or 62443-4-1 for embedded systems and vendor SDLC.
4. Entertainment
    a. Electrical certification: multiple CAN, US, and IEC standards.
    b. Security testing and evaluation UL 2900 or equivalent.
    c. Attestation to CSA, CVP, or equivalent.
    d. Consumer Reports, BSI Kitemark, or equivalent.
5. HVAC
    a. Electrical certification multiple CAN, US, and IEC standards.
    b. Functional safety certification to IEC 61508.
    c. Security testing and evaluation UL 2900 or similar.
    d. Attestation to CSA, CVP, or similar.
    e. 62443-3-1 or 62443-4-1 for embedded systems and vendor SDLC.

6. Utility
    a. Functional safety certification to IEC 61508.
    b. Electrical certification: multiple CAN, US, and IEC standards.
    c. Security testing and evaluation UL 2900 or similar.
    d. Attestation to CSA, CVP, or similar.
    e. 62443-3-1 or 62443-4-1 for embedded systems and vendor SDLC.

Regardless of the sector or product, there are two standards that an organization can target which will provide a level of process maturity for product quality and security management. These are ISO 9001 for a quality management system and ISO 27001 for an information security management system. A vendor that has one or both of these standards provides a higher level of assurance to a product with the necessary security controls deployed. An organization will have to balance business decisions and ensure full understanding of options and benefits to each standard.

Enforcement of Standards

Certification is neither a guarantee of product security nor privacy. Certification of any product or organization is based on a standard, usually international in context, which is used to conduct formal testing on a product or organization.

While under development, no standard for IoT controls currently exists that can be used to definitively address IoT security and privacy issues. As a result, other aspects can be evaluated under formal audit and product testing to validate whether both a company and product are being securely developed.

In addition, a company can falsify a label, and therefore buyers need to determine if a label has been counterfeited. This issue might be a bigger problem for consumers who are now being educated to trust labeling as an accepted means to determine assurance. The motivations for counterfeiting include costs, attempting to gain market share, or grey market goods. To better protect the buyer, labeling requirements should include a "live" portion to allow a potential buyer to determine the following:

1. A machine-readable code that will redirect the user to a live Internet portal (i.e. QR Code).
2. The Internet portal should contain the following as a minimum:
    a. Company name.
    b. Product.
    c. Current model version.
    d. Current firmware version.
    e. Current MUD file or equivalent version.
    f. Certifying company.
    g. Date of certification or last assessment.

Appendix VI

7.6 CEAWG Evaluation of Existing Educational Resources

Canada:

1. Wearable devices and your privacy
    a. Some proposals are unrealistic and a consumer will likely make tradeoffs in favor of convenience/functionality.
    b. Too broad to be applicable.
    c. Steps are easy to follow and content actionable.
2. Privacy and the Internet of Things
    a. Same as first.
3. Get Cyber Safe Blog
    a. Navigation is poor and material is unclear.
4. The Internet of Things
    a. Cites specific incidents.
    b. Graphically presented and easy to follow.
    c. Succinct enough that people may share it with friends and family.
    d. Links to many other resources at the bottom.
    e. Video format allows for distributing via playback in public spaces.

International:

1. Online Trust Alliance resources for smart home users
    a. IoT Security & Privacy Checklist – Press Release
    b. Smart Home Checklist, Advice for Buyers, Sellers & Renters (Updated March 2017, PDF)
    c. Considerations When Buying & Setting Up A Connected Device (PDF)
    d. Enterprise IoT Security Checklist
2. Stop Think Connect (Department of Homeland Security)
3. OnGuard Online – Set of consumer-friendly resources and videos (Federal Trade Commission)
4. What To Do After A Data Breach (Federal Trade Commission)
5. Tax Payer Guide To Identity Theft (IRS)
6. Protect Your Privacy Online; Educating Washington Residents On Privacy In The Digital Age (State of Washington)
7. Online Tips & Advice (Washington State Attorney General)
8. Consumer Federation of America
9. Consumerman
10. Better Business Bureau – Consumer Resources

11. Identity Theft Risk Calculator (LifeLock)
12. Field Guide To Home Automation (National Association of Realtors)
13. Identity Theft Resources (Identity Guard Resource Center)
14. Top Tips for Consumers: Internet of Things Security and Privacy (Internet Society)
15. StaySafeOnline

General Feedback

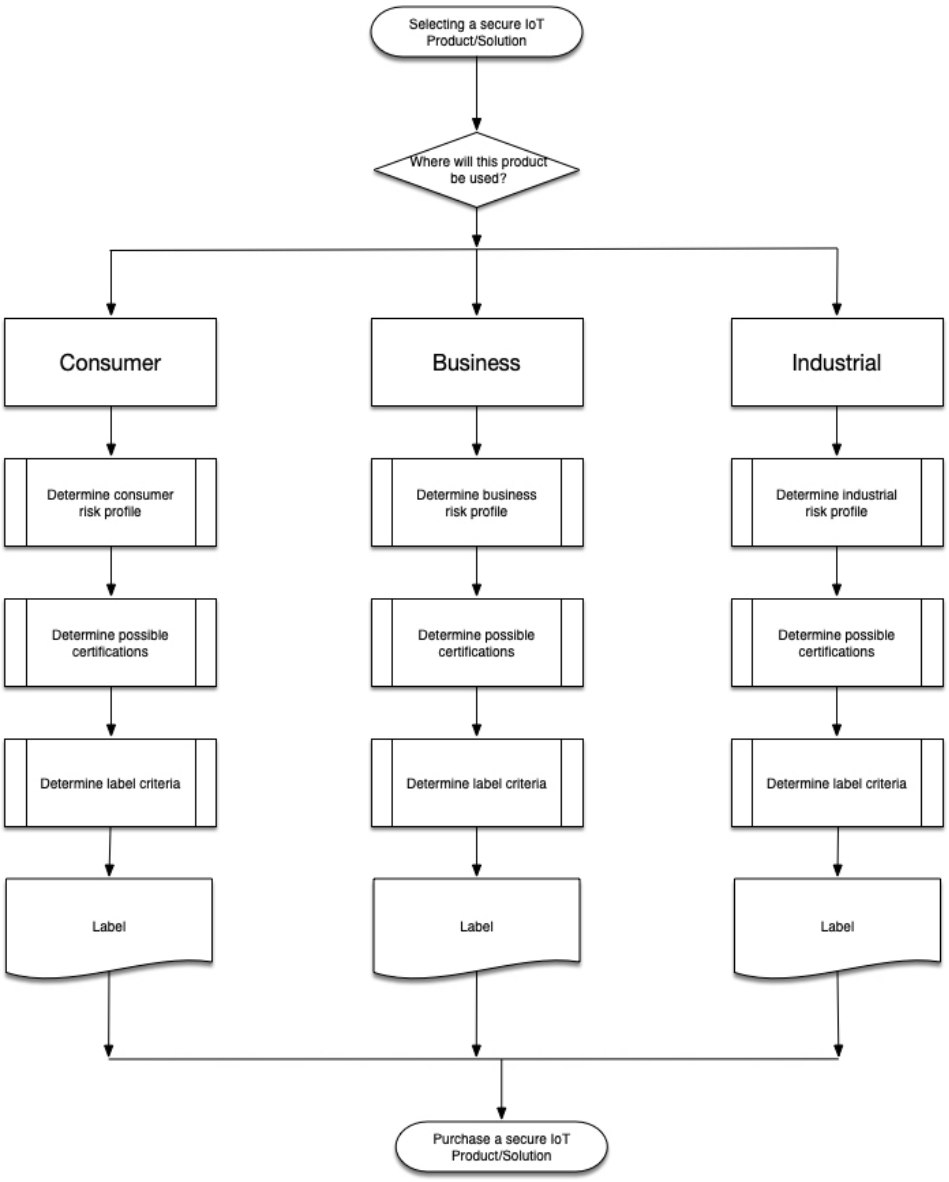
1. Accessibility
    a. Do we know how many people actually seek these resources and read them?
    b. Are there active efforts to promote this information?
2. Framing
    a. Much of the content takes the approach of "these are the steps that a user can take and devices will be magically secure," versus "this is how device security works and the user can start asking what should be done". The former is simple because it requires minimal effort, but the latter is more engaging: rather than carrying out some steps to feel a little more secure, the consumer develops a security mindset that is more likely to go viral, as they are more likely to share this knowledge and have discussions with friends about security.

The Device Labeling Working Group also collected some information on the way consumers interact with IoT devices and how specific labels may better inform their decision making. That research is included below.

Users are increasingly attentive to the handling and use of their data across all devices, especially consumer IoT products that have not traditionally been Internet-enabled (appliances, HVAC, lighting, etc.). However, users are faced with a volume of available conflicting information. Therefore, a decision-making model can be provided to help users and businesses identify and assess any labeling used on an IoT device. The model also illustrates that there are different risk aspects of IoT devices in other sectors. The following diagram provides the necessary guidance for each user group to best determine the labels that should be considered.

Where will the product be used?

Many IoT solutions target three separate sectors: consumer, business, and industrial. These three sectors represent three very distinct risk profiles for the end user. Recognizing that these risks exist and must be used as differentiators will help the vendor and buyer of these solutions to meet label requirements. While this report considers the industrial sector, the focus is on the consumer and business sectors.



Risk Profiles

In order to make informed buying choices, consumers should be able to consider and evaluate the risks of an IoT solution as opposed to a non-connected alternative. Consumers should be able to develop a 'risk profile' for any device.

The following criteria consider some of the high-level risks that are associated with each level of product category. The only way to fully quantify the risk of an IoT solution would be to conduct a formal security assessment or Threat and Risk Assessment (TRA) against the solution for each sector.

Buyers should, at a minimum, attempt to answer the following questions to determine the risk of exposure. Lack of details from a vendor should be considered as not implemented. Buyers should never assume that security and privacy have been implemented to protect their interests and/or data.

Security attributes that need to be considered when evaluating a product:

1. **Confidentiality:** Can the vendor provide details of how the design of the solution or product will protect the confidentiality of the data being collected, processed, and stored?
2. **Integrity:** Can the vendor provide details of how the design of the solution or product will protect the integrity of data being collected, processed, and stored? This includes integrity of the device or solution when under attack or potentially compromised.
3. **Availability:** Can the vendor provide details of how the design of the solution or product will protect or ensure that device or solution will be available when and how the consumer wants to access and use it?
4. **Safety:** Can the vendor ensure the product will function as anticipated and not become a hazard due to a device failure that may cause fire, electrocution, burning, melting, emitting of harmful vapor, or emitting harmful radio signals?
5. **Reliability:** Can the vendor provide details of how the device or solution will ensure that it will provide a specific or targeted state of being reliable?

These attributes of the features implemented in a device or solution provide a context or approach for consumers to evaluate and select IoT products, as outlined below.

Minimum attributes that a vendor should have regardless of product and service:

1. **No default user accounts and passwords:** Upon the setup and configuration of a new device, the device should force the setting of a new password for the device. This password should follow best practices for strong passwords.
2. **The device should be secure out-of-the-box:** New devices should be configured in a state that protects the consumers from having to learn to configure how best to secure the device.
3. **Vendor should clearly outline their privacy practices:** The vendor should provide details of data being collected, processed, and stored for service users. This includes data breach protocols and third parties that are provided this data for free or as a revenue stream for the organization.
4. **Devices and solutions should be formally tested prior to release:** The solution including the device should be tested for the presence of known and potential vulnerabilities.
5. **Vendor should have a vulnerability disclosure process:** The vendor should have a process within the organization that will permit the reception of a potential vulnerability and the ability to perform a vulnerability disclosure in the event a vulnerability is confirmed in their solution.
6. **Encryption technology should be peer reviewed and based on standards:** Vendors should not be developing proprietary encryption technologies but use those that have been peer reviewed and based on standards to ensure interoperability. This may include solutions for protecting data communications but also the boot process and data storage.
7. **Solution should have a secure update method:** The vendor should provide a secure method to provide updates to the device. This may include checks to ensure that the firmware has not been tampered with prior to installation.
8. **Vendor should provide specific dates for product support:** The vendor should be clear and concise about the date or period that a product will be supported with software updates. When possible, users should be notified that a product has reached it end-of-life for software support.

These attributes will guide customers to make better informed decisions when buying an IoT product or solution. The following table outlines potential threats and additional considerations that will help to determine if a product or vendor might pose a cyber risk.

Profile	Category and Threats	Considerations
Consumer	Data breach, device compromises, account compromises, and weaponizing of devices.	• Lack of security and privacy requirements and considerations for the solution. • Implementation errors for SSL and other crypto-related technologies due to lack of expertise. • Lack of a formal SDLC that mitigates risks to acceptable levels. • Lack of formal security testing and evaluation including third party assessments and attestations. • Vendor's lack of governance for security and privacy. • Vendor's failure to knowingly report a data breach. • Privacy policy not clear on data aspects collected, processed, and stored by the vendor, including the selling of this data collected to third parties.
Business	Data breach of infrastructure, account compromises for users and administrators, weaponizing of infrastructure and devices, source code and firmware compromises.	• Failure to risk assess the IoT solution both at design and implementation stages. • Failure to correctly define the security and privacy requirements for IoT solution. • Lack of governance to oversee the implementation of a solution. • Policies and procedures that do not include incident handling during data breach situations. • Failure to identify either a data breach, device compromise, or user account compromise.
Industrial	Secure operation of device in-field and compromises of management infrastructure.	• Lack of SDLC that includes security and safety testing. • Lack of governance to oversee the secure design of a solution. • Threat modeling for both green field and brown field implementations. • Real-time monitoring of management and control infrastructure, including incident handling.

Possible Certifications, Marks, and Testing

Currently, there are no formal testing standards specifically for IoT products/solutions. Buyers are left to determine the security of a product typically based on vendor reputation or the recommendation of friends. Consumers typically care about the usability, not the security and privacy aspects of these solutions. However, once a data breach or device compromise has occurred, they are usually left to figure out the situation on their own. Providing the following details will hopefully help consumers purchase a product that meets both security, privacy, and functionality needs.

Sector	Certification	Considerations
Consumer	Electrical	• Where was the device manufactured? Some regions require products to undergo electrical certification, which may include the CE mark. • The CE Mark is used in the EU to illustrate products that have been formally evaluated to the EU requirements for electrically powered products. While not security focused, it provides a means to show the vendor has undergone formal assessment by a regulatory framework and does have a minimum level of maturity for organizational processes.
	Safety	• If this device were to have a failure such as overheating, not turn off, not turn on, accessible remotely without authority, have connection ports that allow modifications, does not provide load protection or surges, would these have an impact on the buyer? • Look for IEC 15208 to ensure that the product has been assessed for safety.
	Quality	• Do you want to purchase a product that has been produced by an organization that has been evaluated for having a quality management process in place? • Look for ISO 9001 or ISO 14001. These symbols indicate formal assessment for process and manufacturing assurance for the vendor.
	Security	• Do you want to purchase a product that has undergone security and product testing? • Look for the BSI Kitemark to represent organizations whose product has undergone formal testing and assessment for security and other attributes. It also includes an ISO 9001 audit to ensure the vendor meets certain criteria prior to attaining this accreditation for a product. • UL 2900 also provides a means to determine that a product has undergone a formal product assessment. While the vendor's processes other than development are not considered, it still provides a means to determine that a minimal level of assessment has been completed for a product. The current standard does not have any requirements for privacy.
	Security Penetration Testing	• Do you want to purchase a product that has been security stress tested? • Look for indications either on the website or product documentation that penetration tests have been conducted. • Note of caution: Not all penetration tests are equal as there are no formal standards on methodology or tools. As such, it can be a one-and-done approach versus a continuous improvement program within the organization.

Sector	Certification	Considerations
Business	Electrical	• Same as consumer
	Safety	• Same as consumer
	Security	• Do you need to have a product that will provide a level of assurance for operating environments, such as government, telecommunications, or high-risk operating environments? • Look for Common Criteria ISO 15408 with protection profiles that align to the product base functionality. • UL 2900 Series can also be used to determine if a product has been assessed for specific security design features and flaws. Privacy is not included in this assessment.