Canadian Multistakeholder Process: Enhancing IoT Security

Report on Labelling Webinar

Location: Online
Date: August 1, 2018
Remote Attendance: ~25
Video Link: https://bit.ly/2Ld05fs

Overview:

The Canadian Multistakeholder Process – Enhancing IoT Security is a year-long process to develop recommendations for a set of norms and/or policies to secure IoT in Canada. Throughout the year, various events will serve as an opportunity to begin planning and implementing a bottomup, organic process to remedy existing and potential security challenges in Canada's IoT ecosystem.

This initiative is a partnership between the Internet Society, Innovation, Science and Economic Development, the Canadian Internet Registration Authority, CANARIE, and CIPPIC. The Canadian Chapter of the Internet Society is also assisting in this effort.

On August 1, 2018, the Planning Committee organized a webinar to further the discussion on Labelling. It was set up as an open discussion considering current practice in labelling methods and techniques, as used in multiple jurisdictions around the world. The aim was to set out a way forward for Canada that will help to create labels that usefully inform consumers about important aspects of IoT devices for purchase and use, and to ensure that these labels can be backed by an assurance/guarantee system possibly including legal and/or contractual obligations or a duty of care.

The discussion was informed by a multidisciplinary panel of experts familiar with current practice in Canada, the USA and Europe, including:

- Jonathan Cave – ECO-Labelling Experience
- Jacques Kruze Brandao – European Cybersecurity Act and AIOTI Perspective On Labels
- Faud Khan – ISO/IEC standards, Cybersecurity and the Canadian Experience
- Maarten Botterman – Moderator

Key Messages

Label Usage:

The webinar began with a discussion about how labels are used in practice. At different points in a device lifecycle, labels and/or trustmarks have different functions, including:

- *Prior to purchase* - Labels could be used to inform consumer decisions, by enabling, or making sure that the demand that consumers express, which firms seek to fill, captures their preferences, and their levels of understanding. This includes both concrete, or functional preferences, and ethical principles, technical compatibility, and various other things. They can also be used to highlight and encourage innovation by highlighting gaps based on consumer demand.

- *After purchase* – Primarily, labels serve three primary purposes after purchase:

    - Labels help ensure that devices operate based on how consumers and designers intended them to. In this sense, labels ought to provide information as to how the devices can or ought to be used.
    - They can document accountability trails for the supply chain and function of devices
    - They could also help speak to compatibility and interoperability between devices via software, firmware versions, and other factors

- *End of Life/Usage* – The label could also help provide queues as to how these devices could be disposed of in an environmentally and security-conscious way. It might also provide information regarding how to migrate information/data to a new device and/or how to change users.

Key Design Elements:

Throughout the webinar, the presenters alluded to some key design elements that ought to be part of a robust and respectable labelling regime, including:

- *Accessibility* – Labels ought to be designed to be simple and directly convey relevant information to consumers. They also ought to be placed on a prominent place on packaging, be accessible in multiple languages, and be easy to find information about *(See ISO 14000 and Eco-labelling Standards as a Potential Guideline)*.

- *Machine Readability* – Given that many purchase decisions are often made online, speakers noted that it could be useful to have labels that are machine readable, allowing third parties to conduct independent searches and/or assessments. This information could then be leveraged by search engines, checking for features and/or compatibility across devices and software platforms. Personal information could also be overlaid to help tailor information to the user's preferences or needs, as was the case with personalized energy tariffs in the EU.

- *Visual Features and Branding that Compliment Marketing Efforts* – Much like the eco-labelling efforts that have taken off around the world, IoT device labels ought to work in parallel with marketing campaigns focused on highlighting key features and/or attributes of devices that consumers demand. With respect to the IoT, the assumption is that either there is a demand or emerging demand for increased security and/or privacy features, which could be leveraged by retailers if expressed through a label.

Standardization:

A key reason why labels become commonplace in the market is so that consumers can make comparisons of similar products. If there are multiple options for a label/trustmark, this can frustrate rather than support comparisons of device features. As such, having one or a small number of labels would be favorable from a market and consumer standpoint, allowing consumers to make choices based on a defined set of attributes. Whether or not devices ought to have a label/trustmark will depend legal and/or regulatory requirements and other factors. However, what is clear is that if IoT devices labels are an option, there should be efforts to streamline and standardize labels/trustmarks rather than encourage many to be deployed.

Case Studies/Options:

Apart from the key design elements that ought to be incorporated into a label, there also ought to be regulatory frameworks, management standards, electrical and safety standards, and/or security standards which work together to make device and organizational assessment and enforcement possible. To illustrate how this could occur, the following are two examples of how labelling/trustmark regimes are being developed by different organizations and/or authorities:

1. From a regulation standpoint, the European Commission included articles in its cybersecurity legislation on what IoT devices should adhere to and how it is established. The existing Cyber Security Act, currently under development, includes:

    - Article 45: Security objectives (data confidentiality, data integrity, data/services right management, data/services access/logs, incident response, patch management)
    - Article 46: Assurance levels (basic: limited degree of confidence, substantial: certificate with a substantial decrease of the risk, high: certificate to prevent cybersecurity incidents)
    - Article 47: Certification schemes defining evaluation criteria depending on security objectives

    To ensure this regulation is not only legally viable but also implementable from a practical standpoint, the European Commission has invited industry leaders to reflect and assist on the matter. European Cyber Security Organization (ECSO), an association of over 230 organizations, brings together industry views on the matter through various reports, highlighting that there may be different levels of assurances required to ensure scalability.

    ECSO's position is that a mix of self-assessment and third-party assessment/accreditation is the answer. It is crucial that in a fast-moving market, the assessment processes are structured such that third-party organizations only validate and audit necessary criteria, while embracing a trust-based model for other criteria to make the process as affordable as possible. *(more information can be found at 13:25-29:00 on the livestream video)*

2. The Canadian Standards Association (CSA) is in the process of creating a Cyber Verification Program, which aims to fix the issues previously mentioned. The CSA label would be issued if an organization submits a request to be verified and then complies to certain management and product maturity levels, which are assessed by looking at organizational security processes, product/software development lifecycles, product design attributes, and product vulnerabilities via penetration testing and scans. This is currently in the pilot phase and more information will be known in the coming months. *(more information can be found at 29:08 - 38:20 on the livestream video)*

Some Questions Moving Forward:

- What is the role of government in developing this process or standard? What laws that should be considered (ranging from International Law to local law, from consumer protection to trade agreements);
- How to handle certification of devices that are manufactured outside the country? (Mutual recognition? Legal trade restraints?)
- Do we need different certification or labelling procedures for things developed for export?

- On a different level: should labels aim to *inform* about functionalities, or provide a level of *assurances* regarding certain build and operating quality?
- How do we ensure labels continue to be up-to-date after purchase? What is the consideration for interconnected things?
- What happens after a patch/update is provided?

Conclusions:

There was broad consensus among participants on the webinar that labels/trustmarks are one method of ensuring certain security standards are embedded into the organization and product from the beginning of the product design process. Since product design has increased in complexity, the organization building the device must take on the responsibility of ensuring user safety. However, when consumer device is labeled and certified for safety, then the certifier becomes at least partially responsible for the harms incurred when something goes wrong. Certainly, a level of accountability from both industry and users is to be expected – and perhaps enforced through various mechanisms. However, understanding how responsibility is divided when users suffer harm and seek redress through various authorities in Canada is unclear. Labels/trustmarks seem to be one of the more promising options to delineate expectations and liability between stakeholders when it comes to issues related to the IoT. However, they are not without risks, and the *Canadian Multistakeholder Process* ought to evaluate if the potential security benefits from labels are worth the extra cost to manufacturers in particular.