Canadian Multistakeholder Process: Enhancing IoT Security

Report on Fifth Multistakeholder Meeting

Location: Toronto, Ontario Canada
Date: February 28, 2019
In-Person Attendance: ~24
Remote Attendance: ~35
Total Attendance: ~59
Livestream Link: https://livestream.com/internetsociety/iotsecurity2018-5

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. Events throughout 2018 and early 2019 will serve 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.

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.

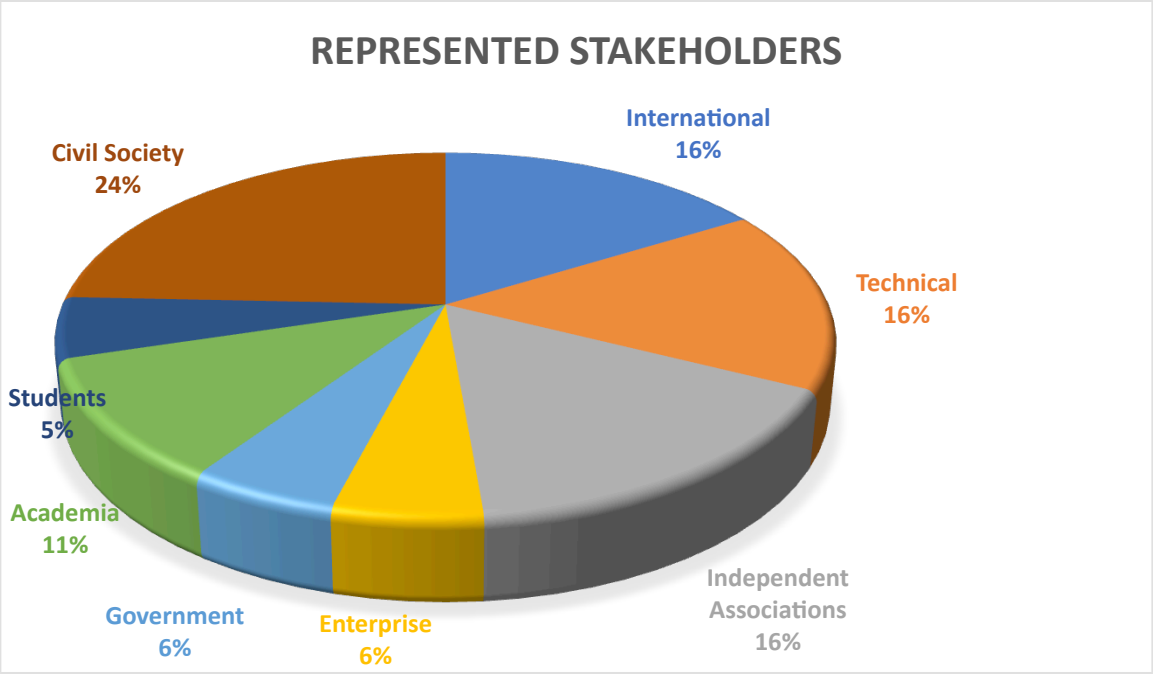
The goal of the fifth multistakeholder meeting was to give an update on the work to date from each working group, finalize the recommendations and best practices from each working group, and launch the Draft Outcomes Report.

This report details the meetings, the evolving research, and points of consensus arrived at by the multistakeholder group.

In particular, this report details the feedback gathered on the *Securing the Internet of Things A Canadian Multistakeholder Process* Draft Report[1] from the Labelling and Consumer Education Working Group and the Network Resiliency Working Group.

At this meeting, the following stakeholders were represented (by registration):

[1] Report available here: http://iotsecurity2018.ca/wp-content/uploads/2019/02/Enhancing-IoT-Security-Draft-Outcomes-Report.pdf



Labelling and Consumer Education Working Group Discussion:

The Previous Working Group Mandate: https://iotsecurity2018.ca/wp-content/uploads/2018/12/IoT-Security-Report-Meeting-4-November-20.pdf (Pages 2 - 4)

Description:

Introduction:

Volunteer leaders Dr. Hosein Badran and Faud Khan (TwelveDot) presented the working group's current status. They began by outlining the key objective of the working group, which is to develop a mechanism by which consumers can educate themselves in order to make smarter, more secure choices.

They gave a brief overview of the draft report and then opened the floor to discussion. They reminded the group about the constraints of their mandate and the need for a final report to be completed in a timely manner, whilst emphasizing that feedback should be action-oriented and directly relevant.

The group first discussed consumer education and creating awareness of labels in a general sense before moving on to a more technical discussion of labels and related standards themselves.

Discussion:

Consumer Education:

It was first noted that it is not the objective of this group to design a consumer education campaign in and of itself. Rather, the underlying messaging, key ideas that are required to be conveyed and how the labeling will relate to consumer education should be the focus. In this sense, it was agreed that the existing draft report should be seen as the "raw materials" for a future campaign directed at consumers, conducted by the government alongside relevant civil society partners. It was also agreed that working with civil society partners would allow the message to reach some audiences who may not trust or engage with traditional government messaging. Multiple stakeholders within the IoT sphere must be encouraged to participate actively in the education process.

There was also broad agreement that the federal and provincial Privacy Commissioners should be engaged more deeply at this stage of the process in order to determine how existing legislation and regulation would play into a consumer education campaign. Further, small and medium businesses, either within the IoT sphere themselves or using IoT products, should be specifically targeted as they are often unaware of their legal obligations in terms of handling of customer data.

Research has shown that security is a concern for consumers, but that they lack both trustworthy advisors on the topic and knowledge about what, exactly, makes a product "safe" versus "unsafe". The labeling should be seen as a concise element of an overall strategy around consumer safety. There was some discussion around a concrete "what to look for/avoid" list that could be easily memorable for consumers. Some participants felt that this would be redundant to existing consumer guides (such as that developed by the Online Trust Alliance), unless it had either a specifically Canadian focus or was more concise and tailored.

The Government of Canada has recently undertaken some initiatives to make information on cybersecurity available to the public, but these have not specifically addressed the question of IoT devices. There has been a shift in what consumers are buying that the government information is not fully caught up with. On this basis, it was agreed that the federal government should review its existing outward-facing materials on cybersecurity and coordinate efforts across the relevant departments (public safety, consumer protection, etc.) to ensure consistency.

There was a further discussion on how to convey to consumers who can be trusted to deliver labels that mean a product has been properly tested. There are currently approximately a dozen companies that have gone through a pilot process to test IoT devices, but they are not known to consumers. This led into the discussion on labeling with agreement that the two issues were intertwined and that as consumers saw security testing labels on the products they are purchasing, active efforts were needed to convey what these labels meant.

Labeling:

It was firstly agreed that the work of this group in terms of labeling is the Canadian contribution to a much larger conversation. There are not yet unified standards for IoT and national-level frameworks diverge in various ways. That said, the Canadian contribution should make an effort to not diverge too heavily from existing frameworks and risk further fracturing of the market and confusion for consumers.

There was broad agreement on the need for standards to preserve flexibility and the ability to innovate whilst also signaling compliance with relevant legislative principles (most obviously the Privacy Act). If the labeling and testing regime is too onerous or confusing, manufacturers may be put-off, particularly if they suggest that older products are not properly tested and secured. This could lead to greater production occurring outside of Canada or the adoption of alternate standards that the government of Canada does not influence. A further danger is that if there are too many independent certifying entities, each with different styles of label, this may confuse consumers and prove counter-productive.

There were also concerns regarding a label providing a degree of false confidence for consumers, particularly in terms of privacy. It was agreed that the federal Privacy Act is in need of updating and that therefore certification of compliance with its provisions is not a total guarantee of good privacy practices. The labels should also not convey the idea that a consumer can be personally reckless when using the device and not themselves practice basic cybersecurity and privacy etiquette.

The average consumer needs a small label that acts as a sign of quality and immediately communicates the basic message that the device meets basic security standards. Consumers interested in learning more in depth should be enabled to have that option. There was some discussion around a QR-code based model for this, though some questioned its relevance in a Canadian context.

There was, finally, broad agreement that cybersecurity testing is likely to become mandatory or effectively mandatory, as opposed to voluntary, over the medium term (this is already somewhat the case in the European Union). Therefore, the labeling regime should be flexible enough that it can merge into a mandatory testing environment when the time comes. A suggestion that was floated was to have company-level labels in addition to product-level labels. For instance, certifying that a particular company practices security-by-design. This was seen as potentially promising but harder to verify.

Network Resiliency Working Group Discussion:

The Previous Working Group Mandate: https://iotsecurity2018.ca/wp-content/uploads/2018/12/IoT-Security-Report-Meeting-4-November-20.pdf (Pages 5 - 7)

Description:

Introduction:

Working group lead, Jordan Melzer, began with an overview of the work done to date by the network resiliency group, including the Secure Home Gateway, the draft report, and ongoing work on the MUD standard within the IETF. Melzer also presented a framework of risks and mitigations for home gateways.

The group discussed how to create recommendations and best practices, considering the technology it would ultimately recommend is still in development and the ways in which consumers can be encouraged to spend more on products (such as a secure home gateway) that would meaningfully enhance network resiliency.

The majority of the time was spent discussing concrete best practices, recommendations, and stakeholders to engage.

Discussion:

Home gateways are in a unique position within networks because they create the connection between devices internal to a network and the broader Internet. Thus, it is very important to develop and implement best practices for security around home gateways, as they are the "first line of defense" against potential cybersecurity threats or other incidents.

At the same time, technologists working in the sector feel that it is more important to figure out how to implement something before a set of best practices and recommendations is developed. Thus, as far as Secure Home Gateways (SHGs) are concerned, there was agreement that the implementation steps were a critical element to get right in the process. In particular, it was agreed that there is a need for device manufacturers to release MUD profiles, ISPs to offer SHGs, and consumers to buy SHGs for the overall strategy to work.

From this, there was a related discussion on liability for when networks are impacted due to security incidents which did not reach a firm consensus. It was generally suggested that this is an area where policymakers need to be active in figuring out a solution which divides liability appropriately. There was agreement that all stakeholders share some degree of liability, but the balance of this was not obvious to the group.

In terms of concrete best practices, it was agreed that the biggest impact could be had if telecoms and other internet service providers offered SHGs by default. A representative from Telus indicated that their company, and likely others in the industry, are interested in policies that encourage this and would not view them as an inappropriate imposition, providing they were properly formulated.

The group did agree on some basic best practices for home gateways themselves and on the consumer side:

Best practices for home gateways:

- Create and offer a Secure Home Gateway (for ISPs, should be the default consumer option)
- Secure-by-design principles must be respected
- Limit in-bound static port access
- Policy enforce at gateway limiting LAN access
- Private / limited access to backend
- Reduce attack size through rate-limit policies
- Block in-progress attacks by identifying and quarantining specific attacker devices across NAT (IEFT and DOTS)
- Prevent "ID" theft (access control evasion and rogue AP attacks) by providing each device with unique WiFi credentials

Best practices for consumers:

- Have SHG in your home

- Use onboarding mechanisms and applications to securely onboard devices
- Follow application guidance to identify and address devices with security flaws
- Make sure to have a modern, reputable home gateway with updated access
- Turn off the ability for your home devices to turn on or access external ports
- Be cautious about the devices you connect
    - Pay attention to the security of the devices you connect and where.
- Don't use the same password on devices as you use on other services (e.g. online banking)

There were also sets of recommended actions for the group in terms of both aspects:

Recommendations for home gateways:

- Continue working on the Secure Home Gateway (with CIRA)

Recommendations for consumers:

- Consumers should be educated about network resiliency and the existing projects or best practices

There was also a discussion on best practices and recommendations for manufacturers. However, it was agreed that this section of the report needed to be fleshed out more and further discussion would occur leading up to the next stakeholder meeting.

Finally, it was agreed that there were some particularly important stakeholders to engage as the process moved forward who may not have been involved thus far. Third party ISPs and "hub" creators were seen by the group as necessary to be engaged with more clearly.

Appendix A: Agenda

Fifth Multistakeholder Meeting: Enhancing IoT Security

February 28, 2019

8:30 am	**Registration opens and breakfast is served**
9:00 am	**Welcome and launch of the Enhancing IoT Security draft report** Katie Watson Jordan, Internet Society
9:05 am	**Panel update from working groups** Taylor Bentley, ISED Faud Khan, TwelveDot Jordan Melzer, Telus
10:00 am	**Break**
10:15 pm	**Breakout group discussions** Main Room: Consumer Education and Awareness and Labeling Facilitators: Taylor Bentley and Faud Khan Breakout Room: Network Resiliency Facilitators: Jordan Melzer and Katie Watson Jordan Topics for discussion: • What stakeholders should be targeted to engage during the comment period, and how will we reach them? • What is the best venue to continue discussing and developing outcomes, and which stakeholders should take the lead? • How should target stakeholders implement the outcomes?
11:30 am	**Reconvene and discussion on international alignment** Katie Watson Jordan, Internet Society
12:00 p.m.	**Adjourn** Reception from 12:00 to 1:30 p.m.