Canadian Multistakeholder Process: Enhancing IoT Security

Report on second multistakeholder meeting

Location: Ottawa, Canada
Date: June 21, 2018
In-Person Attendance: ~29
Remote Attendance: ~16
Total Attendance: ~45
Livestream Link: https://bit.ly/2IC8bDV

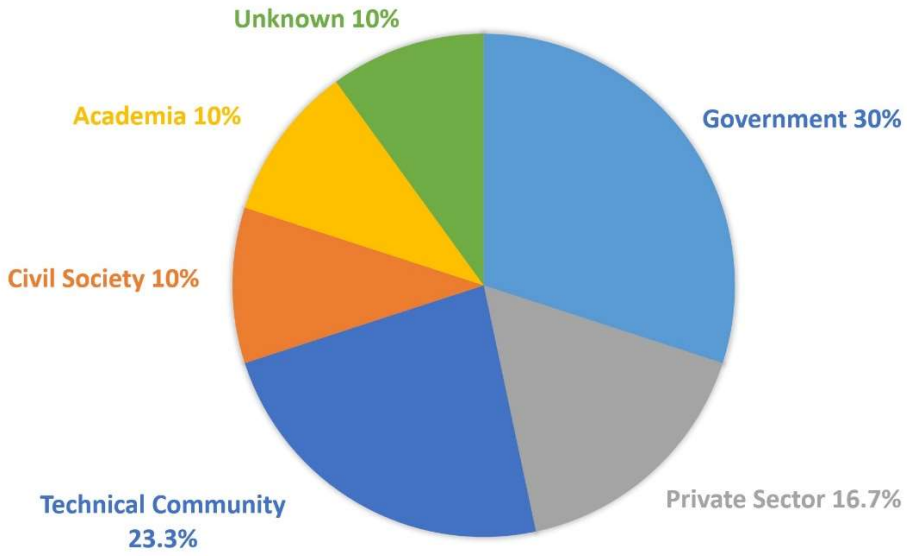
Overview:

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 the year 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 second multistakeholder meeting was to continue building upon the action items and issue areas discussed at the first meeting, as well as develop smaller working groups to conduct research in priority areas. To this end, the bulk of the afternoon was devoted to creating charters for three working groups, focusing on labelling, consumer education & awareness, and network resiliency. The outputs of these groups will serve as the basis for the agenda at the third multistakeholder meeting, tentatively scheduled for August 2018. This was also an opportunity to provide updates on the project and discuss ways of optimizing collaboration through online platforms.

At this meeting, the following stakeholders were represented:



Discussion Regarding Prioritization:

Andrew Sullivan, the meeting facilitator, began the meeting by prompting participants to select the top two or three issues discussed at the first multistakeholder meeting that ought to be given priority (7:00 – 12:45 in session #1 video). The list from the first meeting consisted of the following 10 items:

1. How to create/use existing privacy/security certification labels for devices
2. How to empower consumers through education and public awareness campaigns
3. Researching which standards body could oversee IoT. If none exist, create one
4. Identifying threats and how to use security “trolls” to mitigate them
5. How to use the MS process to determine best practices and standards
6. Determining what the outputs of this MS process will be (white paper, etc.)
7. How to test and evaluate existing devices at scale
8. How to lobby manufacturers of IoT devices
9. Ways of showcasing ‘IoT Stars’ with an award and feature in a research paper
10. Highlighting use cases and promoting joint solutions

Throughout the plenary session, numbers 1, 2, 7, and 8 were given the most attention. There was rough consensus that another item be included, focusing on the technical side of IoT security. After some deliberation, the group decided three items ought to be given priority over the others, namely labelling, consumer education & awareness, and network resiliency (12:45 – 1:15:10).

Establishing the Scope of Working Groups:

The afternoon session consisted of developing charters for working groups that will examine the top three priority items. The following is a list of those charters, as agreed upon by the multistakeholder group:

Labelling (4:00 – 27:35 in session #2 video):
The goal of this group is to scope out possible labelling regimes that could be applied and/or enhanced in the Canadian landscape. In doing that, various questions ought to be considered, including:

1. Should we develop a label, **use an existing label**, or collaborate with others to develop a label? There was rough consensus that there is already a mass of labels/standards out there which ought to be leveraged instead of developing a new one. However, this needs to be researched more.
2. How does the multistakeholder group expect this label to interact with providers (manufacturers, resellers, open-source, and others)?
3. Where will the testing live? Will the organization who administers the label also conduct the tests, or will this process merely identify what tests ought to be conducted? Do we need to develop a new test? Do we have any recommendations regarding who should test?
4. What are the technical aspects of each label meaning?
5. We should not develop a new standard, but rather hone in on the requirements for a label: Who is the label for? What is important for the Canadian consumer? What is important to Canadian business? What is important for the Canadian government? Those requirements then show us what standards and standards groups ought to be considered. (~20:00 in session #2 video)
6. How do we re-use existing work done in this area?

As a potential first step, it was proposed that the group develop a conceptual map of existing standards and identify if there are there any gaps. Faud Kahn, CEO TwelveDot, offered to provide existing research TwelveDot has done in this area, as his organization has catalogued many of the existing standards.

- Stakeholders who ought to be involved (1:30:26 – 1:33:50):
    - Manufacturers
    - Vendors
    - People who are familiar with the standards making process
    - Consumer Protection Professionals
    - IoT Alliances
    - UX Professionals
    - Citizen/Public Interest Group
    - Trusted Certification Bodies/ Industry Standards Orgs.

Consumer Education & Awareness (27:35 – 1:08:00):
The aim of this working group is to establish an education and awareness framework to create a more security-conscious public. The multistakeholder group agreed that this group will not developing campaigns, but rather high-level suggestions. The outputs might include:

1. A toolkit for decision-making
2. A communication plan that outlines resource requirements, the intended audience, the kinds of "things" that ought to be talked about, delivery mechanisms, and in-kind content that has already been developed.
3. A gap analysis, showing where improvements in IoT security education campaigns could be made.

The group agreed that whatever direction they decide to take, the output ought to be structured in a way that could be easily implemented by other actors (*SMART Goals*).

- Stakeholders who ought to be involved (1:33:50 - 1:38:38):
    - Communications Professionals
    - Consumer Protection Professionals
    - Citizen/Public Interest Groups
    - Ministry of Education Representatives/ Educators
    - Civil Society Groups
    - Partners who could implement/deliver
    - Vulnerable Groups (Youth, Senior, Marginalized, Etc.)
    - Municipalities
    - Research/Polling Agencies

Network Resiliency (1:08:00 – 1:30:07):
The overarching goal of this group is to develop a set of recommendations to protect the Internet from things and protect things from the Internet. The outputs of this process could include:

1. A white paper outlining networking operation and management guidance. It was generally accepted that this will not include developing industry networking standards. In terms of a methodology, it was proposed that this working group outline requirements for standards so that if there are gaps, we can make recommendations to standards development organizations (SDOs) to mitigate and/or minimize the issue through some sort of intervention.

2. A prototype and/or proof of concept code to show how labels and other things would work for networks of different scales.

3. The development of a definition of network resilience. Will the scope be narrow or broad? IoT devices are part of cyberphysical systems. They are mediated by the human touch, and that needs to be recognized for any intervention to be successful. With that in mind, we must be clear about where resilience starts and ends. On the user end, this will be covered, in part, by the consumer education component.

- Stakeholders who ought to be involved (1:38:38 – 1:40:00):
    - Network Operators
    - Manufacturers
    - Software Developers
    - Standards Development Organizations

Communication Platforms:

Given that discussion on the listservs has been stagnant, our facilitator asked whether a better mode of communication could be adopted. There was consensus that a blend of platforms, including social media, cloud drives, Slack, and webinars, might be more conducive to discussion. As such, ISOC will assume responsibility for creating accounts and setting up platforms as requested by each working group.

Action Items:

1. ISOC to establish communication platforms for working groups.
2. Working groups to begin addressing items outlined in their respective charters.
3. Working groups will establish among themselves how to communicate with other working groups, the planning committee, and the greater stakeholder group.

APPENDIX A: Agenda

12:30 p.m.	**Registration Opens**
1 pm	**Welcome and overview of the Securing the Internet of Things Canada Project** Mark Buell, Regional Bureau Director, North America, Internet Society
1:05 pm	**Facilitated Discussion** Review of rules of engagement and discussion about last meeting's action items, including: 1. How to create/use existing privacy/security certification labels for devices. 2. How to empower consumers through education and public awareness campaigns. 3. Researching which standards body could oversee IoT. If none exist, create one. 4. Identifying threats and how to use security "trolls" to mitigate them. 5. How to use the MS process to determine best practices and standards. 6. Determining what the outputs of this MS process will be (white paper, etc.). 7. How to test and evaluate existing devices at scale. 8. How to lobby manufacturers of IoT devices. 9. Ways of showcasing 'IoT Stars' with an award and feature in a research paper. 10. Highlighting use cases and promoting joint solutions. Pick 2 items (suggestion: 1 and 2) from the list that ought to be given priority. We will form working groups around these in the afternoon. Andrew Sullivan, Fellow, Oracle/Dyn
2:30 pm	**Break**
3:00 pm	**Facilitated Discussion Resumes**
4:30 pm	**Establishment of Working Groups** Based on the two items selected by attendees, working groups will be formed to conduct further research.
4:45 pm	**Discussion About Communication Platform(s)** How will the larger MS group members and working groups communicate? What platform(s) ought to be created or enhanced to facilitate discussion?
5:00 pm	**Adjourn** Reception at *Sidedoor - 18 York St B* from 5 to 7 p.m.