Canadian Multistakeholder Process – Enhancing IoT Security

Report on first multistakeholder meeting

Location: Ottawa, Canada
Date: April 4, 2018
In-Person Attendance: ~60
Remote Attendance: ~20
Total Attendance: ~80
Livestream Link: https://livestream.com/internetsociety/iotsecurity2018

Overview:

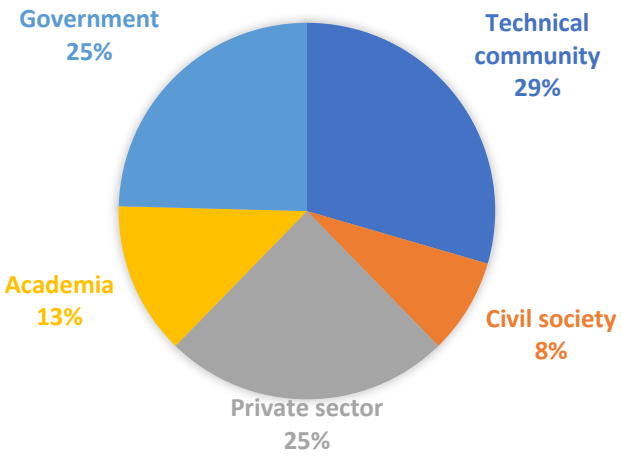
The *Canadian Multistakeholder Process – Enhancing IoT Security* is a year-long process to develop recommendations for a set of norms and/or policies to secure IoT in Canada. Events throughout the year will serve as an opportunity to begin planning and implementing a bottom-up, organic process to remedy 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.

Two thematic areas were identified by the project partners to be addressed in this multistakeholder process:

1. *Consumer Protection* -- Some consumers may not understand what personal information is collected about them through IoT devices, how it is used, or how it is shared. Nor do they trust that the data collected is kept secure. In Canada there are a variety of policies and tools in place to protect consumers from security breaches, such as the *Personal Information Protection and Electronic Documents Act (PIPEDA)*. However, consumers may be unclear of how to take advantage of these protections. Greater transparency could empower consumers to make more informed decisions, better understand the risk of adoption, and to be a more active in their data protection.
2. *Network Resiliency* -- There is a pressing need for greater resilience to be built into the networks, servers, and software that transmit and store data from IoT devices. We ought to consider what steps could be taken to mitigate vulnerabilities in IoT devices in the short-term, and what data protection and transference measures can be put in place to address long-term risks over a device's lifecycle.

At the first multistakeholder meeting in this process, the following stakeholders were represented:



Setting the rules for engagement:

The event kicked-off with a session facilitated by Larry Strickling, Executive Director of the Collaborative Governance Project. Strickling provided an overview of the multistakeholder process and worked with participants to determine ground rules and define what constitutes consensus in a multistakeholder process. Participants, both those remote and in-person, outlined a dozen rules (condensed to the following eight), including the following:

1. Treat people with respect: make sure everyone has a chance to express their ideas, 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 talk and don’t 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.

They 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.

These rules will be used throughout this year-long process.

Setting the stage:

Participants heard from a series of speakers on the following topics[1]:

- Jacque Latour, Chief Technology Officer at the Canadian Internet Registration Authority: IoT security and risks.
- Maarten Botterman, Director of GNKS Consult BV: how network vulnerability can be quantified
- Olaf Kolkman, Chief Internet Technology Officer at the Internet Society: the relationship(s) between IoT and society.
- Faud Khan, Chief Executive Officer of TwelveDot: IoT device standards.

Speakers emphasized the need for developers of IoT devices to consider security concerns from the earliest stages of design so as to avoid making large-scale adjustments once in production.

Breakout discussions:

In order to guide the discussions, the following definition of IoT for the purposes of this project, was presented to the group:

> *"We 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."*

Participants were then divided into eight groups, including one group of remote participants from around the world, to discuss two topics:

1. What are IoT devices, and is our working definition sufficient?
2. What can this group accomplish in a year to diminish the vulnerabilities IoT devices pose to networks?

After two hours of discussion, the full group reconvened to report back. Andrew Sullivan, a Fellow at Oracle Dyn, facilitated. Groups were not limited in the topics or interpretations they could bring forward on the questions. For example, many groups had unique interpretations of how and why we would want to define IoT. Some suggested this group should be limited to only using internationally-agreed upon definitions, such as those written by the European Parliamentary Research Service, Institute of Electrical and Electronics Engineers (IEEE), the National Telecommunications and Information Administration (NTIA), or Electronic Privacy Information Center (EPIC). Others suggested a narrow definition, or 'class' of IoT devices that this initiative could focus on.

Participants had many different suggestions and strategies for moving forward along the two thematic areas (consumer protection and network resilience). Discussions indicated that there are many concrete objectives and products that could be developed that would enhance IoT security. Suggestions for the coming year included the following:

1. Create privacy/security certification labels for devices.

[1] Presenters' presentation slides are available at https://iotsecurity2018.ca.

2. Empower consumers through education and public awareness campaigns.
3. Research which standards body could oversee IoT. If none exist, create one.
4. Identify threats and use security "trolls" to mitigate them.
5. Use the multistakeholder process to determine best practices and standards.
6. Write a white paper.
7. Test and evaluate existing devices.
8. Lobby manufacturers of IoT devices.
9. Showcase 'IoT Stars' with an award and feature in a research paper.
10. Highlight use cases and promote joint solutions.

The thematic area of network resilience was noted as a particularly important subject during both the speakers' presentations and during breakout discussions. However, there was insufficient time to fully discuss and build consensus on the suggestions related to network resilience. Organizers noted this for future meetings and intersessional discussions.

Participants noted that consumer protection and network resiliency may not be two separate issues, but rather a continuum that can be addressed in tandem. This is an important consideration for the initiative's work going forward. In-person meetings can be utilized to identify and work on areas of overlap between the two thematic areas.

Consensus reached:

The group reached consensus to pursue this work and that meaningful outcomes can be accomplished in a year, as long as it is forward-looking and provides a baseline/foundation for future work to enhance IoT security. A specific area of work that participants agreed to was on the need to educate "humans" about IoT; including the creation of an entertaining, educational tool. There was a lengthy discussion regarding what kind of audience this tool would target, and what form it would take.

It was recommended that the group discuss users, consumers, purchasers, developers, service providers, and vendors separately. As such, we will consider three groups: consumers, service providers and creators. Consumers will include users and purchasers, while creators will include developers and vendors. More broadly, anyone who does not have input over how their data is collected and used by an IoT device is a consumer, and anyone who decides how to collect and use data is a creator. Service providers provide connectivity for devices and operate the networks that data is transmitted over. Moving forward, the group's work will address these three categories independently.

Several participants also suggested that when considering an educational tool, we should leverage existing groups with experience creating educational courses, such as ISOC and IEEE. Participants offered many suggestions for how educational tools could be created, including using gamification to reward participants, comedy, and visualization to reach the broadest audience possible.

Suggestions for moving forward:

This group is working towards the creation of a concrete outcome that enhances IoT security and reduces the risk to consumer adoption and use of IoT devices. The exact nature and focus of this document will be the product of the collective efforts of participants across the next year of in-person meetings and intersessional work.

In the near term, the initiative's work is expected to be carried out across several directed working groups interacting primarily through e-mail listservs. The working groups will be fluid, and stakeholder-driven. The secretariat has proposed the below working groups to get the discussions started, but their focus and progress will be stakeholder-driven. Please note that the 'Rules for Engagement' discussed at the first meeting will apply to exchanges in these working groups.

The next in-person meeting can be used to focus on areas of overlap between working groups. For example, work on consumer protection could continue by determining who the appropriate audience is for an educational tool, and what such a tool may look like. Another could be to utilize the discussed classification scheme to create a threat model that could be considered by IoT users and service providers. This will allow us to focus our work and determine ways to mitigate vulnerabilities and threats.

Next Steps:

Create four working groups, supported by listservs for the following efforts:

1. *General*: to share information that relates to the project as a whole. Project leads and partners will share news with participants regarding project progress and upcoming events and meetings.
2. *Classifying IoT*: to create a classification schema to determine what segment of the IoT ecosystem this initiative will focus on, and at what part of the network resilience is needed most.
3. *Buying IoT*: to address what the average consumer, unfamiliar with IoT security issues, needs to know when buying an IoT device. What questions should they be asking when procuring IoT devices for business or personal use?
4. *Interacting with IoT*: to address consumer expectations with how their IoT devices will function and utilize their data. What questions should they be asking service providers regarding how and when data is used, and how to reduce the risk of their devices being compromised to become security threats for networks?

APPENDIX A: Agenda

9:30 a.m.	**Registration opens**
10 a.m.	**Welcome and overview of the Securing the Internet of Things Canada Project** Mark Buell, Regional Bureau Director, North America, Internet Society
10:05 a.m.	**Welcome message** Pamela Miller, Director General, Innovation, Science and Economic Development – Government of Canada
10:15 a.m.	**What are multistakeholder processes?** *Setting the terms of engagement and defining consensus* Larry Strickling, Executive Director, Collaborative Governance Project
11:15 a.m.	**Setting the stage** Andrew Sullivan – Fellow, Oracle Dyn Jacques Latour – Chief Technology Officer, Canadian Internet Registration Authority Maarten Botterman – Director, GNKS Consult BV Olaf Kolkman – Chief Internet Technology Officer, Internet Society Faud Khan – Chief Executive Officer, TwelveDot
12:00 p.m.	**LUNCH + Table Discussions:** With the people at your table, appoint a leader, develop rough consensus and/or talking points around: What are IoT devices? Is our working definition sufficient? What can this group accomplish in a year to diminish vulnerabilities IoT devices pose to networks? *Note: You will be required to report back on the outcomes of these conversations during our group discussion in the afternoon.*
2:00 p.m.	**BREAK**
2:15 p.m.	**Group Discussion: How do we secure the Internet of Things?** *Reporting back on Table Discussions* Andrew Sullivan – Fellow, Oracle Dyn
4 p.m.	**Adjourn/Reception** *Rideau Club – 99 Bank St.*