Canadian Multistakeholder Process: Enhancing IoT Security

Report on Fourth Multistakeholder Meeting

Location: Ottawa, Canada
Date: November 20, 2018
In-Person Attendance: ~30
Remote Attendance: ~40
Total Attendance: ~70
Livestream Link: https://livestream.com/internetsociety/iotsecurity2018-3

Overview:

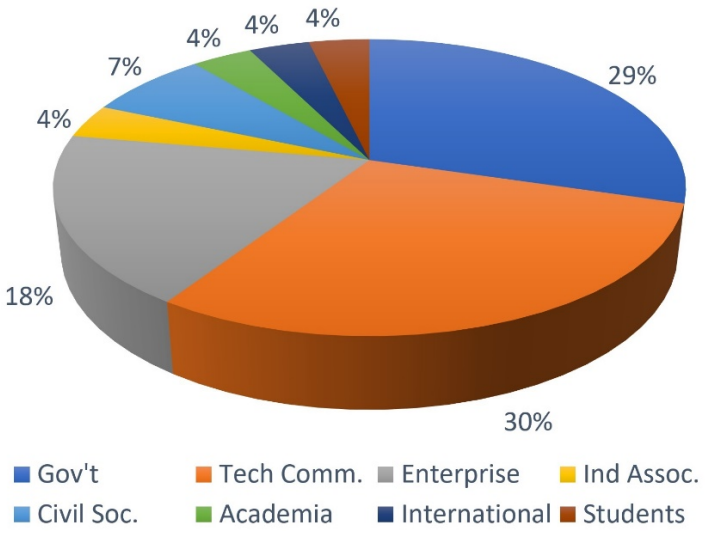
The Canadian Multistakeholder Process – Enhancing IoT Security is a year-long process to develop recommendations for a set of norms and/or policies to secure the Internet of Things (IoT) in Canada. Events throughout 2018 and early 2019 will serve as an opportunity to begin planning and implementing a 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 (ISED); the Canadian Internet Registration Authority (CIRA); CANARIE, and CIPPIC. The Canadian Chapter of the Internet Society is also assisting in this effort.

The goal of the fourth multistakeholder meeting was to receive reports from the Labelling, Consumer Education, and Network Resiliency working groups, followed by a longer discussion aimed at identifying and refining key messaging within the groups' research objectives. The results of this discussion will serve as the basis for a draft report being developed by early 2019.

This report details the meetings, evolving research, and points of consensus arrived at by the multistakeholder group, herein known as the *Shared Responsibility Approach for IoT Security*.

At this meeting, the following stakeholders were represented:



Stakeholder Rules & Reminders (1:04 – 5:24):

Facilitator Andrew Sullivan reviewed the multistakeholder rules of engagement as established at the first multistakeholder meeting on April 4.

Labelling Working Group Presentation (5:24 – 1:08:31):

The Previous Working Group Mandate: https://iotsecurity2018.ca/wp-content/uploads/2018/09/Multistakeholder-Meeting-3-Report.pdf (Page 5 - 7)

Presentation Link: https://iotsecurity2018.ca/wp-content/uploads/2018/12/IoT-Security-Label-v1.1.pdf

Introduction:

Volunteer leaders Dr. Hosein Badran (Badran Digital Consulting) and Mr. 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. Badran and Khan then outlined three goals to achieve this aim:

1. To provide consumers with the ability to understand the security and privacy features embedded into their IoT devices at the time of purchase.
2. To provide manufacturers, vendors, and service providers with a clear and concise way of displaying both security features and their compliance to related standards.
3. To provide a mechanism that market oversight authorities could use to transparently and consistently assess compliance with future IoT security guidelines.

Their presentation broadly covered five areas: Label Formats, Standards, Certification, Enforcement, and Example Label Requirements and Structure.

Label Formats and Examples:
There are a variety of different styles of labels, each of which conveys different types of information to the consumer. The first format examined by this group was a graded format scheme. These types of labels highlight different features or attributes in products and assign them a number or grade. This is commonly found in the food sector and/or on appliances as an indicator of energy efficiency. The conclusion of the Labelling group was that this type of label would need to be mandatory in order to be effective.

The second format is the binary scheme, colloquially known as a *Seal of Approval* scheme, where a product is tested against a known standard and if it passes that test, it is given a seal of approval. In terms of existing certifications, the British Standards Institute, which is the national standards body in the United Kingdom, has developed the Kitemark. This mark merely denotes where a device is acceptable to use, either in residences, businesses, or environments that require enhanced security measures. The Canadian Standards Authority – Cyber Verification Program, which has been discussed at other meetings, would also fall into this category as well. While this format of label/trustmark is often the preferred type for consumers, it could lead to a false sense of security that would cause consumers to mistakenly believe that no further security actions were needed to keep their device secure.

The third format is a descriptive information label, which is a list of capabilities or features. This provides the highest degree of information to consumers, but it would require a certain degree of technical and security knowledge to be meaningful. However, the working group believes that this would be a worthwhile format to consider if a voluntary label were to be deployed in the Canadian marketspace.

Recommended Specifications:
Graphically, any label would have three elements:

a. It would have a label and/or trustmark that would signify that the label has gone through a formal testing and evaluation scheme.
b. Next to the label, there would be a code which denotes what evaluation scheme and/or standards the IoT device has been evaluated against and its official product code.
c. On each device and package, there would also be a quick response (QR) code which would allow consumers to efficiently access an information repository that would provide a real-time security view of a product. This could also serve as a means of pairing the device with a secure home gateway using IETF-MUD[1].

Discussion Input:

- During the discussion, it was clear that participants were interested in the tension between two labels with high bars for consumer education—a binary label which is easier for consumers to understand or one which provides information about features and/or grading. While the current suggestion trends towards the latter, many participants wondered if an easier to comprehend component could also be added.
- There was a recommendation to add the words "Security of this device certified by [company]" next to the evaluation scheme and a product code to help consumers understand the label more clearly. There was also a recommendation to add "For more information about this device's security features, scan this label" above a QR code.
- A participant asked if there was data available on consumer uptake of QR codes. (The working group has not researched this yet.)
- A participant also asked whether adoption of a label can be based on existing data about other labels and/or trustmarks currently deployed for the IoT. The group answered that this data does not yet exist.
- At the end of the presentation, Sullivan facilitated an exercise to gauge participants' responses to what was developed. It seemed that there was more of an appetite to roll out a label as a mandatory mechanism, while leveraging a non-binary label. It was also clear that the content will need to evolve and develop further.

Action Items:

- Develop a white paper with three components, with sections for policymakers, consumers, and manufacturers.
- Conduct a feasibility analysis of consumer usage of QR codes to determine whether this is viable for stemming the issues related to IoT security. This could include an index of current use cases.

[1] Internet Engineering Task Force's manufacturer usage descriptions: https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/

- Initiate collaboration discussions with international efforts.

Consumer Education & Awareness Presentation (1:08:31 – 2:28:40):

The Previous Working Group Mandate: https://iotsecurity2018.ca/wp-content/uploads/2018/09/Multistakeholder-Meeting-3-Report.pdf (Pages 3 - 5)

Presentation Link: https://iotsecurity2018.ca/wp-content/uploads/2018/12/Consumer-Education.pdf

Introduction:

Volunteer leader Ms. Rouba Alfattal (Office of Consumer Affairs [OCA]—ISED) presented on the Consumer Education & Awareness working group's current status. She outlined how the working group has elaborated on their messaging framework since the September 5 meeting. The group had created a high-level framework of the top six recommendations for security, privacy, and functionality for both consumers and manufacturers. The framework further divides up messaging into different phases in a device's lifecycle, which includes prior to purchase, after purchase, and end of use (by original owner). These tips are not intended to serve as a finished product, but rather as something to be further refined and tailored for specific audiences.

The format of the working group's presentation was to walk through the matrix and make live edits to the framework's language.

Action Items:

- There was a high-level recommendation to add service providers to the "supply" side of recommendations. This will require that the working group assesses if their messaging is still relevant and applies appropriately.
- On the "before purchase" side, there were suggestions to merge points #4 and #5. In terms of point #6 , which refers to labelling, the Consumer Education and Labelling groups will need to coordinate to establish the best way to educate consumers about the label. This will likely be an activity which will come after the Labelling group has finalized its basic requirements.
- There have been multiple suggestions to aggregate various studies and best practices related to label adoption and behavioral science which could support efforts in both working groups. Information from advertisers could also be incorporated as well.
- During the discussion about the at use/at issue messaging, there was a suggestion to emphasize the notion that security is an ongoing process so that consumers are aware that what is secure today might not be secure tomorrow.
- There was also a suggestion to combine points #2 and #3, indicating that there will be automatic patches and that all the various parts of a network are secure.
- At the end of the day, Mr. Maarten Botterman (GNKS Consult) gave a presentation on various initiatives in Europe which have significant messaging similarities. There were some suggestions from participants that the group could adopt messaging from those initiatives.

Network Resiliency Group Presentation (2:28:40 – 3:33:28):

The Previous Working Group Mandate: https://iotsecurity2018.ca/wp-content/uploads/2018/09/Multistakeholder-Meeting-3-Report.pdf (Pages 7 - 9)

Presentation Links:

- https://iotsecurity2018.ca/wp-content/uploads/2018/12/Network-Resiliency-Nov-20th-presentation.pdf
- https://iotsecurity2018.ca/wp-content/uploads/2018/12/shg201811.pdf

Introduction:

Volunteer leaders Dr. Jordan Melzer (TELUS Communications) and Mr. Michael Richardson (CIRALabs) presented on the working group's current status. First, they outlined the working group's core mandates, which are to reduce the vulnerability of consumer IoT devices and decrease the threat of large-scale attacks posed by compromised devices. These would be prevented through security measures implemented in the home gateway or by the Internet service provider (ISP). Then they outlined threats and mitigations, summarized below:

Pre-compromise threats (high to low):	**Mitigation**	**Notes**
Home gateway threat	Security by design	Home gateways are the most-compromised "IoT" devices
IoT device threat via services exposed to Internet	Prevent IoT devices from opening static ports in firewalls without user approval	UPnP[2]-based firewall bypass allows devices to act as Internet servers. Required by some games and P2P[3] networks, but poses a very high risk
IoT device threat via services exposed to home LAN[4]	Policy enforced at gateway limiting LAN access.	Policy can be signaled via IETF MUD or derived implicitly
Backend threat	Private / limited access to backend.	Reduce reachability of backend to ISP domain or ISP and device class
Post-compromise mitigation:	**Strategy**	**Notes**
Reducing attack size	Rate-limit policies	Rate-limiting reduces total attack volume without requiring knowledge of which devices are or are not compromised
Blocking in-progress attacks	Identify and quarantine specific attacker device across NAT[5]	Denial of service attacks are most visible upstream, towards the victim. ISPs which identify attacks in progress can use

[2] Universal Plug and Play
[3] Peer-to-peer
[4] Local area network
[5] Network Address Translation

		assistance from the home gateway to isolate and quarantine the specific compromised devices without affecting other home services
Using shared WiFi credentials to evade access control policy or setup as rogue AP	Providing each device with a unique WiFi credential	Provides cryptographically strong identity to facilitate access control. Also allows credential revocation

The group noted that lessons learned from the gateway and their broader research could be divided into four categories and compiled into white papers for specific audiences, as follows:

1. Secure Gateway Overall Design:
    - Output – Whitepaper for Standards
    - Audiences – Broadband Forum (BBF), Cablelabs
2. Unique WiFi Keys for Legacy Devices:
    - Output – Open Code/Configuration & Whitepaper for Standards
    - Audiences – TELUS/ Algonquin College, Wifi Alliance, WBA
3. MUD / Permissions App Demo:
    - Outputs – OpenWrt & app demo/Open Code
    - Audiences – CIRA, IETF
4. Private IoT Deployment:
    - Outputs – Whitepaper (Informational Request for Comments [RFC]) & Demo
    - Audiences – ISP and/or Cloud Provider[6]

Richardson closed by giving a video demonstration of the secure home gateway prototype and outlining various outstanding issues related to the gateway specifically[7].

Discussion Input:

- Richardson noted that there may be some issues associated with how a gateway or mobile device is set up in circumstances where there is not any connectivity. He noted that he has developed a specification which may help with this problem. However, it needs further refinement testing before it is ready to be introduced to the group.
- As part of Richardson's presentation, the notion of liability was discussed – specifically, who would be liable for cheap home routers if they were to be weaponized for some sort of attack. Consensus was not reached on this point, but Richardson stated that the answer would reveal who would be responsible for deploying a device like the secure home gateway.

Action Items:

- Develop the white paper in accordance with the framework outlined by Melzer.

Broader Discussion (3:33:28 – 4:03:52):

[6] More information can be found in the slide deck.
[7] Action items can be found in the slides provided on behalf of CIRALabs.

Action Items:

- Develop a taxonomy of processes and/or standards to which a label could refer.
- Botterman provided an outline of various initiatives happening within the European Union. His presentation focused mainly on what is happening in the Netherlands and the United Kingdom (UK). In both cases, there is a nexus between what is being examined with the *Canadian Multistakeholder Process* and what has been developed in those countries. From the Dutch approach, Botterman suggested that the group could also include elements of:
    - Liability
    - Government procurement
    - Legislation
    - How to clean up infected or legacy products

  Botterman suggested that it might be prudent to adopt the UK's Code of Practice or at the very least, use it as a point of discussion on the value of something similar for Canada[8].
- One participant commented that part of the issue with IoT security is that each stakeholder group is being pulled in multiple directions to undertake activities to mitigate problems associated with the IoT. Therefore, the purpose of this initiative is in part to clarify what the expectations are from each group.

[8] Mr. Botterman's slides can be found here: https://iotsecurity2018.ca/wp-content/uploads/2018/12/UK-NL-approach-4.pdf

Appendix A: Agenda

12:30 p.m.	**Registration Opens**
1 p.m.	**Welcome and overview of the Securing the Internet of Things Canada Project** Tom Stark, Internet Society
1:05 p.m.	**Review of rules of engagement and project recap** Andrew Sullivan, Internet Society
1:10 p.m	**Labelling Working Group Discussion** • Presentation of Group Progress (10 mins) – Faud Khan, TwelveDot • Questions and Facilitated Discussion (~50 mins)
2:10 p.m	**Consumer Education Working Group Discussion** • Presentation of Group Progress (10 mins) – Rouba Alfattal, OCA • Questions and Facilitated Discussion (~50 mins)
3:15 p.m.	**Break**
3:30 p.m.	**Network Resiliency Working Group Discussion** • Demonstration of Gateway – Michael Richardson, CIRA Labs (10 mins) • Presentation of Group Progress (10 mins) – Jordan Melzer, Telus • Questions and Facilitated Discussion (~ 40 mins)
4:30 p.m.	**Broader Discussion** Does the group believe we are still addressing priority areas? In the context of what has been happening in the three working groups, does anyone have any outstanding issues they would like to discuss?
4:55 p.m	**Any Other Business** Are there any needs that ISOC and the Planning Committee can provide support for?
5:00 p.m.	**Adjourn** Reception from 5 to 7 p.m.