Canadian Multistakeholder Process: Enhancing IoT Security

Report on Montreal Focus Group

Date: July 17, 2018
Location: W Hotel, Montreal, Quebec

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 bottomup, 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.

On 17 July, the Internet Society, in partnership with the Internet Society's Quebec Chapter, hosted a focus group in Montreal to gain an understanding of how to best engage the Internet community in Quebec, and to begin planning a full multistakeholder event in the province later in 2018.

Discussion at the focus group in Montreal centred on who is responsible for IoT security, the challenges of securing consumer-level IoT devices, what aspects of IoT need to be addressed most urgently, and on a potential full meeting of a multistakeholder group in the Province of Quebec. The focus group was conducted in both English and French.

Who is responsible for IoT security?
The group recognized the necessity for a collaborative approach to secure the Internet of Things, however, they also identified that there are different degrees of responsibility for each stakeholder group, including:

- End users need to know that they could become part of a global army of devices (botnet) if they are not secure. However, many in the group felt that it is hard to engage average citizens in that discussion. Therefore, public education on IoT security may be challenging. Other believed that a security breach would rarely be the fault of the user, as it's the vendor who lets insecure devices on the market.
- It was generally recognized that the private sector (device manufacturers, service providers, etc.) needs to be central to the security discussion as end users may not advocate for their own security. Some participants argued that this may be difficult, as companies will adopt standards only if there is a reason to do so; that is, if there are financial consequences in cases of security or data breaches. Currently, IoT

development and adoption are driven by economics. The lowering time-to-market for IoT devices has become so accelerated it is negatively impacting device security.
- The group proposed the "20/80 rule" be used: 20 per cent of the time and resources to secure IoT be put towards end users, the remaining 80 per cent of time and resources be put toward vendors.
- There are numerous ethical questions that need to be discussed. Therefore, multiple levels of government, universities, privacy advocates, and law makers need to be a part of the framework for securing IoT. Furthermore, there are academics and civil society that are already demanding transparency around data collection.
- Some participants felt that governments need to regulate minimum security. There was no consensus on how this could be developed and implemented, but one idea was for governments to require the adoption of standards among service providers and device manufacturers for IoT. Other participants stated that governments are not responsible for the standards of IoT devices or Internet.

Challenges to securing IoT

A number of challenges to enhancing IoT security in Canada were identified by the group, including:

- It is not enough to address IoT security in just Canada or any other country as the IoT ecosystem is global therefore it must be addressed as a global issue. Even if security is implemented in Canada, what about the devices in other parts of the world that, if they are compromised, could affect Canadians?
- Standards will be important for IoT security; however, device manufacturers have no reason to create interoperability between devices. In fact, there is an economic disincentive for standards as they could enable consumers to operate multiple devices from different manufacturers on the same system.
- It's important to remember that we have faced security and safety challenges in the past when new technologies are introduced. Often, these technologies were developed by engineers who understand how the device works and the risks of using it. With IoT, we are trying to take a complex technology and market it to end users who may not have the skills or interest to ensure it is secure. It will take time for end users to adapt to new technologies and gain an understanding of the security risks.

What is important:

A number of facets of securing IoT were identified by the group:

- Upgradability is important for IoT security. However, there will be a large number of 'simple' devices that cannot be upgraded, so a containment strategy needs to be part of the solution.
- There was a robust discussion on liability when there is a security or data breach, as it could move vendors to secure their devices. It was pointed out that liability would have to be implemented globally, as the impact of insecure IoT devices can affect any other region.
- Labeling devices to identify them as conforming to some set of security standards (such as the ability to be upgraded) was identified as a potentially effective way to enhance IoT security. Related to labeling was a discussion on insurance for device manufacturers, as it was assumed that insurance companies would require proof – i.e. a label – that devices meet a certain security standard.

Holding a multistakeholder meeting in Quebec

There was consensus that a full multistakeholder meeting for the Securing IoT Process in Canada was important. There is a large start-up community in Montreal, many of which are working on IoT-related products and services, and there are a lot of "deep tech" people in the province. It was also mentioned that there are a lot of venture capitalists in the province, and that they need to be part of the process.

A potential venue in Montreal, Norman House (http://notman.org), was identified, as were libraries and university campuses if an event were to be held outside of Montreal. Finally, it was recommended that the Cyberjustice Laboratory (http://www.cyberjustice.ca) be approached to participate in future events.