Canadian Multistakeholder Process: Enhancing IoT Security

Report on Network Resiliency Webinar

Location: Online
Date: June 14, 2018
Remote Attendance:
Video Link: https://bit.ly/2NuUsM3

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.

On 14 June, the Planning Committee organized a webinar to further the discussion on network resiliency. The group came up with four dimensions of network resiliency which could be examined for the purposes of this project:

1. Improving the network's ability to withstand attacks
2. Improving the network's ability to suppress attacks
3. Improving the network's ability to make hosts resilient to compromise (increasing attack costs, and taking a wider view of "network")
4. Improving host ability to continue to operate when network infrastructure is down

Suggestions:

A variety of solutions came up throughout the one-hour conversation, including:

A) Not changing how devices are connected, but attempting to improve infrastructure, techniques, and cooperation for defending against attacks (1&2) and designing IoT devices to more gracefully tolerate Internet failure (4).

B) Elevating the gateway's role in policing device traffic (2), eg by taking some action when devices behave differently from their profile, or by encouraging devices to use non-IP

protocols (implicitly forcing them to connect through a gateway and to be somewhat isolated from the home LAN).

C) Designing a different model for IoT devices to access the Internet, one that provides access only to resources they have requested and not to anything else (3).

An international participant offered a cooperative model for doing 1) and possibly 2), which it might be valuable to have references for.

Another participant discussed an open-source approach to building or testing IoT gateways, particularly for allowing non-IP access.

Yet another participant suggested C), arguing that if our worry is that the Internet will be awash in a tide of compromised devices with very limited purposes but large potential to cause harm, we should reconsider if our assumptions about providing "Internet" to vulnerable devices are appropriate. The more challenging we can make it to gain sufficient access to IoT devices to compromise them, the smaller a problem we'll face, and the more success we'll see through other resiliency approaches. While any-to-any reachability is part of the success of the Internet, it doesn't have to be what a device and the network negotiate. If IETF can engineer tailored access that is compelling for "IoT" implementers, we may have an opportunity to stop a large proportion of IoT devices from being soft targets.

There was a question raised about whether or not C) was really necessary, or if a single gateway model using MUD or some other means to baseline devices should be sufficient for the network to police traffic. It was suggested that a device that was already compromised would likely be able to change its identity to the network (eg, MAC), leaving the network with very little to go on to contain it. There appeared to be consensus around the argument that IETF MUD wasn't effective as an isolation tool for compromised devices that could lie, but might be effective in assisting the network in defending devices.

The concept of cata-nets (concatenated networks?) was proposed as a networking model relevant to C), and the wider idea that, though our public Internet model is familiar, it is not the only model. (A reference here would help.) In his description, cata-net gateways connect to each other and broker services between end-hosts, but are not transparent packet-forwarders. (N.B. VOIP Session Border Controllers are another example of "real" gateways -- there are lots of others.)