Coalition seeks to protect internet from weaknesses of many 'connected' devices

November 23 2016, by Josephine Wolff

As an increasing number of devices—from cars to light bulbs to kitchen appliances—connect with computer networks, experts are raising concerns about privacy and security. Just this fall, attackers used compromised home devices, including security cameras and DVRs, to bombard an internet infrastructure company with traffic, slowing internet access for much of the U.S. East Coast.

To address these concerns, an organization of academics and industry leaders released a report today that provides guidance on how to build security and privacy protections into the emerging internet of things (IoT). The report emphasizes several recommendations for internet-connected devices, ranging from improved procedures for updating software on those devices to ensuring that those devices can continue to function if internet access is disrupted.

Instead of targeting the device manufacturers, the report's editors hope their suggestions will resonate with policymakers who are contemplating the appropriate role of government in regulating the internet of things.

"The report is aimed at influencing policy bodies—legislative committees, commissions, the Federal Trade Commission, the White House," said Nick Feamster, a computer science professor at Princeton University and the acting director of Princeton's Center for Information Technology Policy, who is one of the report's lead editors. "We hope, of course, that the IoT industry reads it too."

The report was issued by the Broadband Internet Technical Advisory Group, a nonprofit organization that encompasses industry and academic members. It is not the first group to take up the issue of internet of things security and privacy. The Federal Trade Commission, for instance, released a report last year focused on consumer security and privacy risks associated with the internet of things.

But the new report offers a unique viewpoint on some of the threats and challenges posed by the internet of things because its focus is on broadband network management, rather than device security. Also, many of the group's member organizations are internet service providers; the report's second co-editor is Comcast Vice President Jason Livingood. Accordingly, the new report considers the risks of the internet of things from the perspective of network management, and the authors discuss how networking technologies can be leveraged to protect users.

"It's definitely an ISP (internet service provider) problem as well as a consumer and a device manufacturer problem," Feamster said. "When we talk about insecure IoT devices, we can talk about securing the devices, but we can also take a complementary view and say, 'Let's assume the devices may be difficult to secure and it may be difficult to follow these recommendations—maybe there's a role for in-home networking technology to basically firewall or segment to protect these devices from each other or from the rest of the internet.'"

The report emphasizes the importance of segmenting home networks so the devices connected to the network cannot easily be used to compromise each other. "Many home networks do not, by default, isolate different parts of the network from each other, the report points out. Making it harder for devices on a home network to talk to each other may help mitigate the impacts of any individual device's security weaknesses.

"A lot of the discussions that have happened so far have been fairly general, so we tried to come up with some more specific things that people can focus on," Livingood said. "I also think it could serve as a little bit of a call to action to the IoT device manufacturers to try to figure out how they can band together and try to develop some kind of certification programs for security."

Even some of the more familiar recommendations in the advisory group's report—for instance, making it easier to update software that runs on devices—may be less straightforward than they initially seem, Feamster said. "Some of these recommendations sound obvious but it's not so obvious that they should go one way or another," he explained. "Take secure over-the-network software updates _ and the ability to update credentials on a device—those sound like basically good ideas. But there's obviously a cost to doing that: what do you do about that when the cost of the device is 99 cents, so the cost of updating it may exceed the cost of deploying it?"

In other words, deciding whether or not it should be possible to distribute software updates and security patches to devices such as security cameras or thermostats may depend on the cost of the device and the cost of software updates. So the report, while it recommends making it possible to update devices in general, also points out that, "in some cases, replacing a device entirely may be an alternative to software updates. Certain IoT devices may be so inexpensive that updating software may be impractical or not cost-effective."

Another scenario the authors consider is what happens to internet-of-things devices in the event of an internet outage. The report makes recommendations for how these devices should respond to interruptions to network connectivity. Specifically, the report recommends that "an IoT device should be able to perform its primary function or functions (e.g., a light switch or a thermostat should continue to function with

manual controls), even if it is not connected to the internet because internet connectivity may be disrupted due to causes ranging from accidental misconfiguration or intentional attack."

Membership in the Broadband Internet Technical Advisory Group includes industry leaders such as Google, Cisco, AT&T and Disney, as well as community organizations such as the Center for Democracy & Technology, and Public Knowledge. Researchers from Princeton, Carnegie Mellon University, the University of Oregon and the Massachusetts Institute of Technology contributed to the report.

More information: www.bitag.org/

Provided by Princeton University

Citation: Coalition seeks to protect internet from weaknesses of many 'connected' devices (2016, November 23) retrieved 27 April 2024 from https://phys.org/news/2016-11-coalition-internet-weaknesses-devices.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.