31 October 2019

By Electronic submission to: home-iot-nccoe@nist.gov

Re: Comments on Draft NISTIR 8267: Security Review of Consumer Home IoT Products

IEEE-USA believes that the recommendations in NISTIR 8267 could be ineffective and devices easily compromised, and that the recommendations do not go far enough to address the actual threat vectors associated with consumer IoT devices.

IEEE-USA believes that NIST should instead develop recommendations that include means within consumer gateways in the home (e.g. router firewalls between the home local networks and the public internet) that enforce access restrictions, as well as monitor traffic to detect and block aberrant traffic. Ideally, such in-home gateways should work synergistically with ISP-based systems that employ both high-level and deep packet inspection of traffic from many homes, to detect aberrant traffic with the ability to download updates to in-home gateway traffic blocking rules.

Considerations:

- Individual IoT devices must be treated as untrustworthy because:
    - Many of these devices may come from OEMs in countries with active cyber-hacking operations and there is no practical way to ensure the absence of malware designed into these devices from bad actor OEMs;
    - Even if the devices are clean as designed and shipped, the need to allow updates provides a pathway to inject malware after installation and commissioning; and
    - Monitoring/reporting of private information from within the residence may be abused in ways consumers do not anticipate. (Consumers may be forced to "authorize" surveillance by shrink-wrap/'accept to continue' contracts that either intentionally permit collection/use of private information, or do so to minimize supplier risk.)
- NIST should consider the following threat categories:
    - malware/bots that harm external network elements from IoT devices;
    - interception of in-residence private data, etc.; and

**IEEE-USA** | 2001 L Street, N.W., Suite 700, Washington, D.C. 20036-4928 USA
Office: +1 202 785 0017 | Fax: +1 202 785 0835 | E-mail: ieeeusa@ieee.org | Web: http://www.ieeeusa.org

- dangerous takeover of devices (e.g. initiating toaster fires, medical device interference, or interfering with safe motor vehicle operations).

The only workable solution is to provide detection, protection, and remediation upstream from the IoT devices in gateways and within the ISP networks providing the services.

IEEE USA's Cybersecurity[i] and Digital Personal Privacy, Awareness and Control[ii] position statements specifically speak to these concerns with IoT, and the importance of NIST leadership in this area. Addressing the broader eco-system, consumer education and controls, as well as traffic information sharing aspects of IoT are critical for consumer and national cybersecurity.

Sincerely,

Thomas M. Coughlin

Thomas M. Coughlin
2019 IEEE-USA President

---

[i] https://ieeeusa.org/wp-content/uploads/2019/06/cybersecurity0619.pdf
[ii] https://ieeeusa.org/wp-content/uploads/2018/08/DigitalPrivacy0618.pdf