SUPPORT

Aviel D. Rubin
Professor, Computer Science
Technical Director of the Information Security Institute
Johns Hopkins University

Testimony in Support of

SB 443 Consumer Protection - Security Features for Connected Devices
Primary Sponsor: Senator Susan Lee

Senate Finance Committee, 19 February 2020

Chairwoman Kelly, Vice Chairman Feldman, and members of the Committee, thank you for the opportunity to speak before you today on behalf of SB 443 pertaining to security features of connected devices.

My name is Avi Rubin, and I am a full professor of Computer Science at Johns Hopkins University and Technical Director of our Information Security Institute. I am also the Founder and Chief Scientist of Harbor Labs, a Maryland CyberSecurity company that has developed an IoT Security Analysis product. I have been an active researcher in the area of Computer and Network Security since 1992. The primary focus of my research is Security for the Internet of Things (IoT Security). These are the types of connected devices that are addressed in SB 443.

We have entered the era of Smart Things where everyday objects are imbued with computational capabilities and the ability to communicate with each other and with services across the Internet. In fact, the Internet of Things involves the deployment of Smart Things in everyday living environments -- homes, offices, cars, shops, schools, clinics, and more -- resulting in Smart Environments.

According to Gartner, there will be 20.4 Billion IoT Devices online by 2020, and companies will invest $15 Trillion in IoT between 2017 and 2025 (See https://www.vxchnge.com/blog/iot-statistics).

These connected devices offer many potential benefits to the owners of the Smart Environments (more efficient use of energy, for example) or to the occupants of the Smart Environments (personalized services, ready access to information, improved fitness, health and wellness).

However, if these connected devices are not designed, deployed, configured, or managed properly, they can create unsafe conditions and increase risk of harm to persons and property.

In preparation for this testimony, I visited the popular web site Tech Republic for some examples that illustrate a few recent examples of attacks against IoT connected devices. Here are 5 highlights of IoT security failures from Tech Republic in 2018 that give an idea of the magnitude of the risks: (I should point out that even a quick Google search would yield dozens more of these):

1. SirenJack, https://www.sirenjack.com/

   Attacks against public warning systems causing false alarms and distrust of public warning sirens, as well as disruption of daily life. E.g. 150 false tornado warnings in Dallas in 2017.

2. LoJack, https://www.techrepublic.com/article/beware-of-russian-attackers-impersonating-lojack-security-software-to-hack-computers/

Allowed the Russian state sponsored hackers known as “Fancy Bear” to take control of remote machines, ironically exploiting an anti-theft software feature.

3. State Actors hiding malware in routers (VPNFilter): https://www.techrepublic.com/article/vpnfilter-malware-infected-500k-devices-smb-and-home-office-routers-are-at-risk/

   Cisco reported finding 500,000 compromised devices across 54 countries. Compromised devices manufactured by ASUS, D-Link, Linksys, Netgear, and all of the other major manufacturers. The malware included data exfiltration, command execution, file collection, and command and control botnet code.

4. Data Firm LocationSmart leaked cell phone data. https://www.techrepublic.com/article/phone-tracking-service-locationsmart-exposed-api-allowing-free-tracking/

   Vulnerability in a product demo allowed attacker to locate any mobile phone based on its phone number without requiring a password.

5. Amazon Echo recorded and sent conversation. https://www.techrepublic.com/article/no-alexa-isnt-spying-on-you-but-be-careful-with-sensitive-conversations/

   An Amazon Echo accidentally randomly recorded conversations and sent the recordings to someone in the owner’s contact list.

In another well-known example, the Mirai botnet used insecure default passwords on IoT devices, in particular, CCTV cameras, to bring down much of the Internet on the East Coast in 2016 by attacking a DNS service on the Internet with a denial of service attack.

These are just examples of some of the many vulnerabilities that exist today due to the widespread and rapid adoption of IoT. It is imperative to take steps wherever possible to curtail the risks, and this bill, while it may not go far enough, is a great first step in the right direction.

Based on my experience working in the security of connected devices, I strongly support SB 443 because it addresses the concerns that I have raised earlier in this testimony and is consistent with my belief that devices are most vulnerable when they are first connected to a network. By requiring authentication, we can eliminate some of the most persistent threats.

To the members of this committee, thank you once again for the opportunity to give testimony here today.

I encourage a favorable report of SB 443. Thank you for your consideration.