securityweek.com

New Legislation Could Force Security Into IoT

Tags: NEWS & INDUSTRY SCADA / ICS

6-8 minutes

After years of warnings from security experts and researchers, the Internet of Things (IoT) remains fundamentally insecure. Now a group of senators has introduced bipartisan legislation to force vendors to ensure basic security within their IoT devices if they wish to sell into the government market.

Sens. Mark R. Warner (D-VA) and Cory Gardner (R-CO), co-chairs of the Senate Cybersecurity Caucus, along with Sens. Ron Wyden (D-WA) and Steve Daines (R-MT) today introduced bipartisan legislation: Internet of Things (IoT) Cybersecurity Improvement Act of 2017. Its purpose is to require that all devices bought by the government meet defined minimum security requirements. Its effect will be that without compliance, vendors will lose their largest single market. Compliance, they hope, will then filter down from the public to private sectors, and on to consumers.

"While I'm tremendously excited about the innovation and productivity that Internet-of-Things devices will unleash, I have long been concerned that too many Internet-connected devices are being sold without appropriate safeguards and protections in place," said Sen. Warner. "This legislation would establish thorough, yet flexible, guidelines for Federal Government procurements of connected devices. My hope is that this legislation will remedy the obvious market failure that has occurred and encourage device manufacturers to compete on the security of their products."

The need for legislation is empirically obvious. Vendors simply do not build security into the design of their internet-connected devices. Last year, the IoT delivered the world's largest (Mirai) DDoS attacks. This year there have been numerous examples of vulnerable IoT cameras (including more announced today). Last week, SecurityWeek reported on a fish tank being used to exfiltrate data; and yesterday it was shown that the Amazon Echo can be used by attackers as an always-on listening device.

Martin Zinaich, Information Security Officer with the City of Tampa (FL) told *SecurityWeek* that he found WannaCry attack traffic on his network. He tracked it back to an HP scanner, which was infected with the ransomware. "I now have to worry about large format

scanners. Tomorrow it will be light bulbs, door locks and the candy machine," he said. Adding insult to injury, the scanner's documentation says, closed system "so no antivirus is required."

Under the proposed legislation, vendors selling to the US government will be required to ensure their devices are patchable, they rely on industry standard protocols, they do not use hard-coded passwords, and they do not contain any known vulnerabilities.

Passwords, patching, and vulnerabilities are all likely to be problem areas; but the legislators have tried to cover most angles. For example, with the Amazon Echo vulnerability, the vulnerability is found in the physical design of the device -- and it simply cannot be patched. However, the legislation includes waivers for a number of specific conditions, allowing, for example,'an equivalent level of security' for non-compliant devices.

In this instance, "I don't see any reason why this attack type would prompt a recall of hardware," comments Travis Smith, principal security researcher at Tripwire. "Since the attack requires physical access, the vast majority of users will never have to worry about it. Even if this device were to become compromised, the network traffic of an Echo device is very static. Any attacker sending audio data out would be exposed very quickly to anyone monitoring traffic."

The vulnerability issue is given further consideration in relation to disclosures. Vendors have been known to attempt to limit disclosure through copyright protections, and threats to invoke the Computer Fraud and Misuse Act (CFAA). This new Act exempts security researchers from liability under the CFAA -- an Act that

Krebs describes as "a dated anti-cybercrime law that many critics say has been abused by government prosecutors and companies to intimidate and silence security researchers."

To be covered by this exemption, disclosure by a security researcher will need to conform to a set of standards yet to be defined -- but ones that will probably delay disclosure until the vendor fixes the vulnerability. However, vendors and researchers often disagree on fixes and timescales. Last week IOActive disclosed vulnerabilities in a Diebold ATM and in nuclear radiation monitors that the vendors either ignored or declined to fix. Disclosure has always been a problem, and is likely to remain so within the parameters of the new bill.

Passwords and patching are also always a problem. "When left up to the user," comments Smith, "changing passwords and installing patches is not a priority." Users, he explains, are more interested in getting the device working than in ensuring it is working securely. "The reason Mirai was so successful was not because users could not change their password, but because they chose not to when installing the device. I would add to this bill that devices should force the user to change the default password, but that the default password should be unique to each device as well."

Nevertheless, this new legislation is generally considered to be a useful and valuable start to solving the IoT security problem. Mark Noctor, VP EMEA at Arxan Technologies, calls it a positive step forwards. "By requiring vendors to explain the vulnerabilities in their systems and explain why their device is still considered secure," he comments, "the Internet of Things Cybersecurity Act of 2017 would force developers to take security seriously. Meeting this demand would help guarantee that devices are secure by design, rather

than having security provisions included as an afterthought -- something that is all too common in today's fast-paced market."

The reality, however, is that legislative proposals do not necessarily translate into effective law. Zinaich has such concerns. "The bill is very good, but the likelihood of it staying in place is slim," he told *SecurityWeek*.

Kevin Townsend is a Senior Contributor at SecurityWeek. He has been writing about high tech issues since before the birth of Microsoft. For the last 15 years he has specialized in information security; and has had many thousands of articles published in dozens of different magazines – from The Times and the Financial Times to current and long-gone computer magazines.

Previous Columns by Kevin Townsend: