COMPUTERWORLD

SECURITY IS SEXY
By Darlene Storm

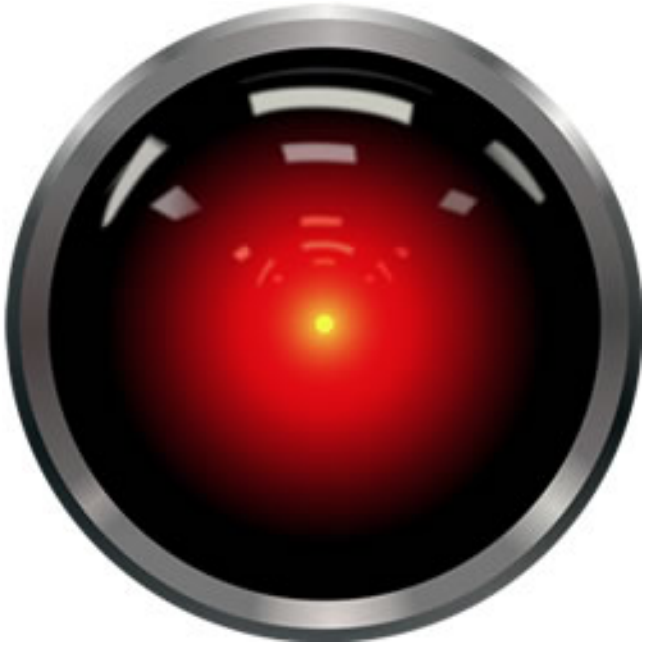
About |
Most security news is about insecurity, hacking and cyber threats, bordering on scary. But when security is done right, it's a beautiful thing...sexy even. Security IS sexy.

OPINION

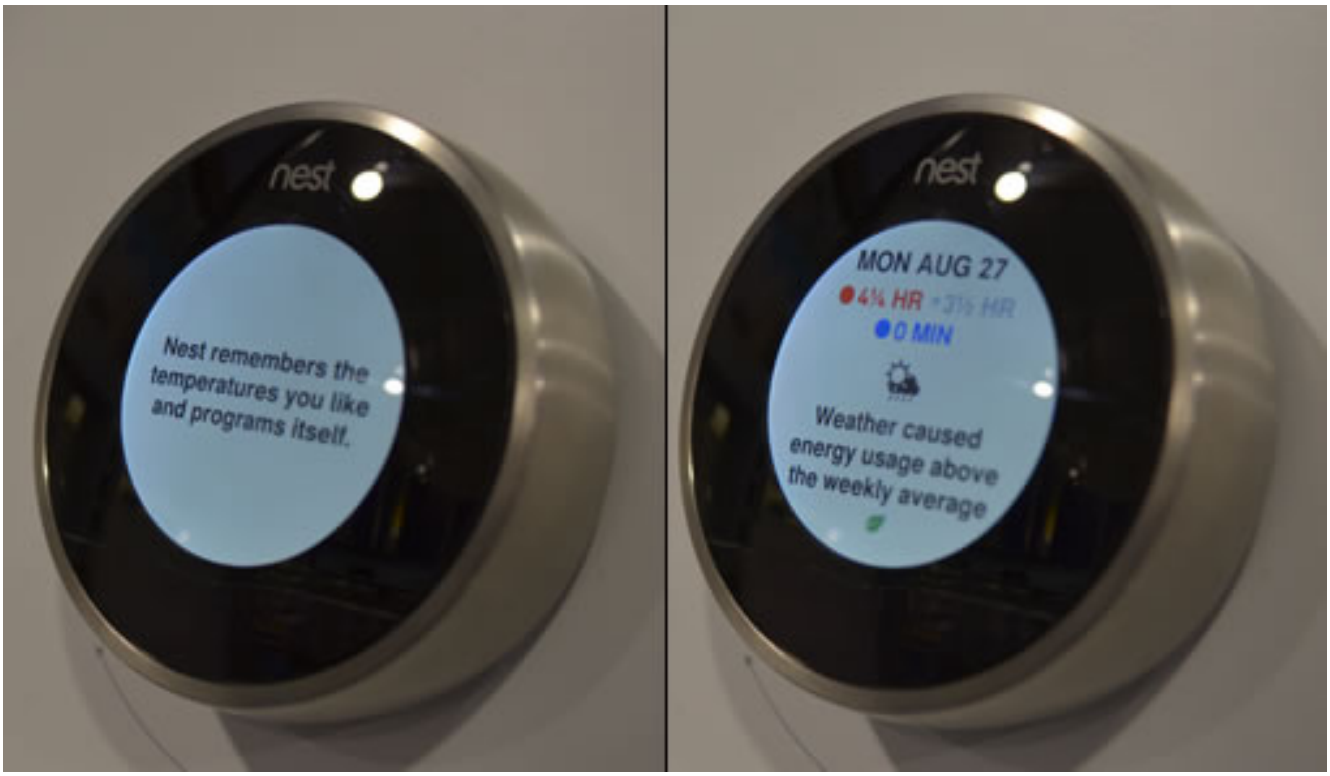
Black Hat: Nest thermostat turned into a smart spy in 15 seconds

Computerworld | Aug 11, 2014 12:25 PM PT

If you had a Nest thermostat, how freaked out would you be if it suddenly displayed "Hello, Dave" along with the HAL 9000 red eye from *2001: A Space Odyssey*? At Black Hat USA, a group of security researchers showed a Nest displaying that as well as the message, "I know that you and Frank were planning to disconnect me, and I am afraid that is something I cannot allow to happen." The group was presenting, "Smart Nest Thermostat: A Smart Spy in Your Home" (pdf).



The Nest thermostat is much more than a regular thermostat because it is a smart device that "learns" your heating and cooling preferences and then builds a personalized temperature schedule to save you money. Since it is part of the Internet of Things, it can also be remotely controlled via the Nest app. Although Nest claims that it will not share collected user data with Google, it knows a lot more about its users than a zip code; it can detect when people are away, network credentials— stored in plain text at that – and can be made to have a persistent backdoor.



Nest learning thermostat and showing Nest Leaf energy usage above weekly average

No one can remotely infect the Nest, as an attacker needs access to the device. Yier Jin, Grant Hernandez and Orlando Arias of the University of Central Florida, and independent researcher Daniel Buentello, found that security was designed into the software, but the hardware can be exploited. Once an attacker has physical access, then all he or she needs is 10 seconds to hold down the power button to trigger a global reset while inserting a USB flash drive to enter developer mode, and then five seconds to load a custom firmware that was not signed by Nest. Yep, 15 seconds and your Nest is pwned to perform as a smart spy.

Oh sure, who is going to break into your house to turn your Nest into a smart spy? But what if you were looking for a "good deal" and bought your Nest off eBay, Craigslist or at a flea market? An attacker could purchase Nest devices in bulk, infect them and then sell them.

There's no "virus" protection or any way to know if the smart appliance is infected. You'd have no idea there was a persistent backdoor into the Nest's root file system; there's no performance impact, so you might never know it was being used for remote exfiltration.

"A Nest Thermostat, as demonstrated, may easily be compromised during transport, deployment, or by an attacker having access to it on a non-secure location," the security team wrote in their research paper (pdf). "It can then become a client on a botnet. Persistent rootkit installation is possible using our ramdisk method and a customized Linux kernel written into the unit. The customized Linux kernel would be used to hide the botnet software, which may remotely control the thermostat, transforming it into a beachhead for a remote attacker."

"The very fact that the compromised Nest Thermostat sits in the network can be used to introduce rogue services," they added. For example, the "Nest could also spoof ARP packets to masquerade as the router, allowing the capture of a targeted computer's network traffic."

Attackers can also "pivot from the Nest Thermostat to other devices on the network. Suddenly, what was once a learning thermostat has been transformed into a spy that can not only report on the routines of the inhabitants of a certain home or office, but also on their cyber activities and provide a backdoor to their local network which could go unnoticed."

The researchers concluded:

> *After a detailed analysis of the hardware infrastructure of the Nest Thermostat, we identified a backdoor associated to the boot process, which, as we demonstrated, can be leveraged by attackers to install malicious firmware. Since the attack happens before the on-board userland is loaded, the firmware verification employed is unable to detect and stop the intrusion. The resulting payload can potentially allow attackers to shape local network traffic from a remote location, further compromising other nodes.*

Oh, the researchers are not done with the Nest and are working on finding a way to remotely exploit the device. They suspect "most of the current IoT and wearable devices suffer from similar issues, lacking proper hardware protection to avoid similar attacks." Daniel Buentello previously has warned us about connected appliances being used against us when he presented, "Weaponizing your coffee pot."

Darlene Storm

Darlene Storm (not her real name) is a freelance writer with a background in information technology and information security.

From CIO: 8 Free Online Courses to Grow Your Tech Skills

View Comments

YOU MIGHT LIKE

+

As demonstrated at the Black Hat conference in 2014, a Google Nest thermostat can be hacked and turned into a "smart spy" â€“ in just 15 seconds. While the device was secure when shipped, and the hack requires physical access, the speed with which the hack can be applied makes these merely minor barriers to success.Â You have two options. The first is the simplest. Reject the smart home and the Internet of Things (we've already established that it can be quite a security nightmare). While they might make things easier on a superficial level, in reality, smart home technology is just saving a bit of time. Is that saving worth risking your privacy over? I doubt you think so. Second, you might want to retain your smart home hardware, but keep better control over it. The Nest Thermostat is a smart home automation device that aims to learn a userâ€™s heating and cooling habits to help optimize scheduling and power usage. With its debut in 2011, Nest has proven to be such a success that Google spent $3.2B to acquire the company.Â The convenience provided by networked smart devices also breeds security and privacy concerns. Nest founder Tony Fadell claimed in an interview, â€œWe have bank-level security, we encrypt updates, and we have an internal hacker team testing the security [the Nest Thermostat] will never take o if people donâ€™t trust it.â€ However, a deep look into the current IoT and wearable device design ow revealed to us that most of the current security considerations, if any, are put on the application and network level. Researchers at Black Hat USA demonstrated how they were able to compromise a popular smart thermostat.Â In less than 15 seconds, an attacker can remove the Nest from its mount, plug in a micro USB cable, and backdoor the device without the owner knowing anything has changed. The compromised Nest can then be used to spy on its owner, attack other devices on the network, steal wireless network credentials, and more. What does this hack mean to the current and future Nest owners? Not much at this point. As we saw with the recent DropCam hack, the attack requires physical access and if a bad guy breaks into your house, it's typically for something much more serious than backdooring your thermostat. As it turns out, Google using Nest products to find out what customers are doing is just one worry. A team of researchers has discovered an easy hack that allows anyone to gain control of Nestâ€™s smart thermostat and turn it into a spying device which can reveal when youâ€™re at home or away, and even divulge your Wi-Fi credentials. Advertisement. Yier Jin and Grant Hernandez from the University of Central Florida, along with independent researcher Daniel Buentello, revealed the hack at last week's BlackHat security conference in Las Vegas, and itâ€™s a pretty simple one. Essentially, all the attacker has to do is hold down the power button and insert a USB flash drive in order to enter developer mode. Nest smart thermostats can be easily hacked to form botnets or spy on owners, researchers showed at the BlackHat security conference.Â LAS VEGAS â€” Google's Nest "smart" thermostats may be the most secure devices in the "Internet of Things," but can still easily be hacked into, three researchers showed today (Aug. 7) at the BlackHat security conference here. Yier Jin and Grant Hernandez of the University of Central Florida, along with independent researcher Daniel Buentello, demonstrated that by holding down the power button on a Nest device for 10 seconds, then plugging in a USB flash drive, one can inject malicious software that can take over the device. MORE: Hacking the Internet of Things.