COMPUTERWORLD

SECURITY IS SEXY
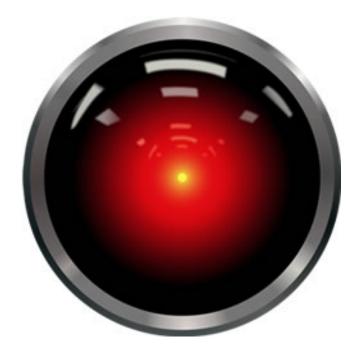By Darlene Storm

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.
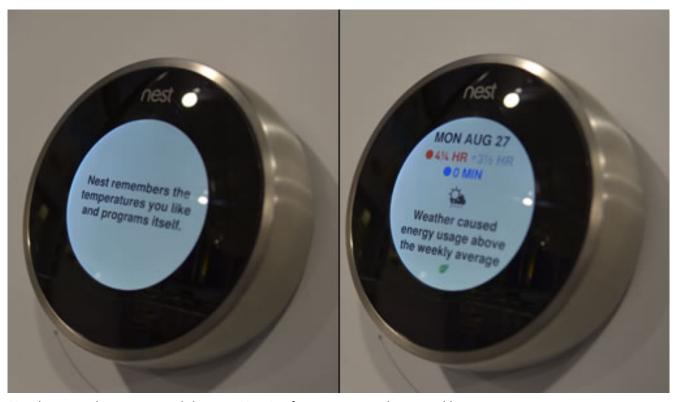
OPINION

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

· Promoted Links by Taboola

Why Google wants to replace Gmail

If you don't have 1 of these 4 cash-back cards you are making a mistake
NextAdvisor

Microsoft tells Windows 10 users to uninstall Office

21 Smartest People In The World…#4 Will Shock You!
PressRoomVIP

A terabyte on a postage stamp: RRAM heads into commercialization

The $1.58 Billion Secret Apple Hid in Your iPhone

The Motley Fool

CIO 100: The Joys and Challenges of Data Analytics

Learn About Microsoft's Point of View on IoT

Microsoft Azure Internet of Things

The Next Big Thing in Wearable Tech

VentureCapital News

Learn How One Man Used 5 Stocks To Retire At 42

Newsmax

+