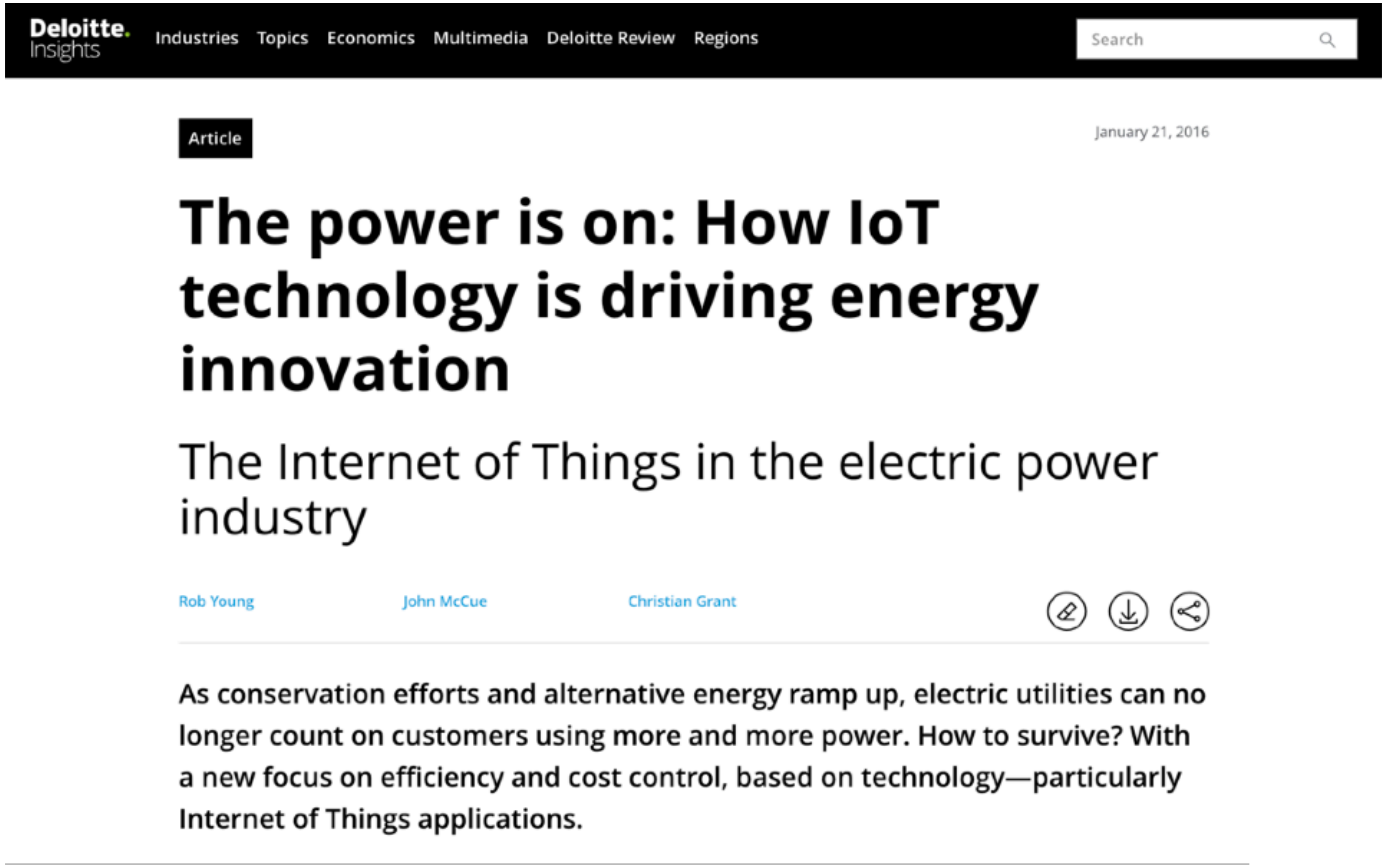


Article

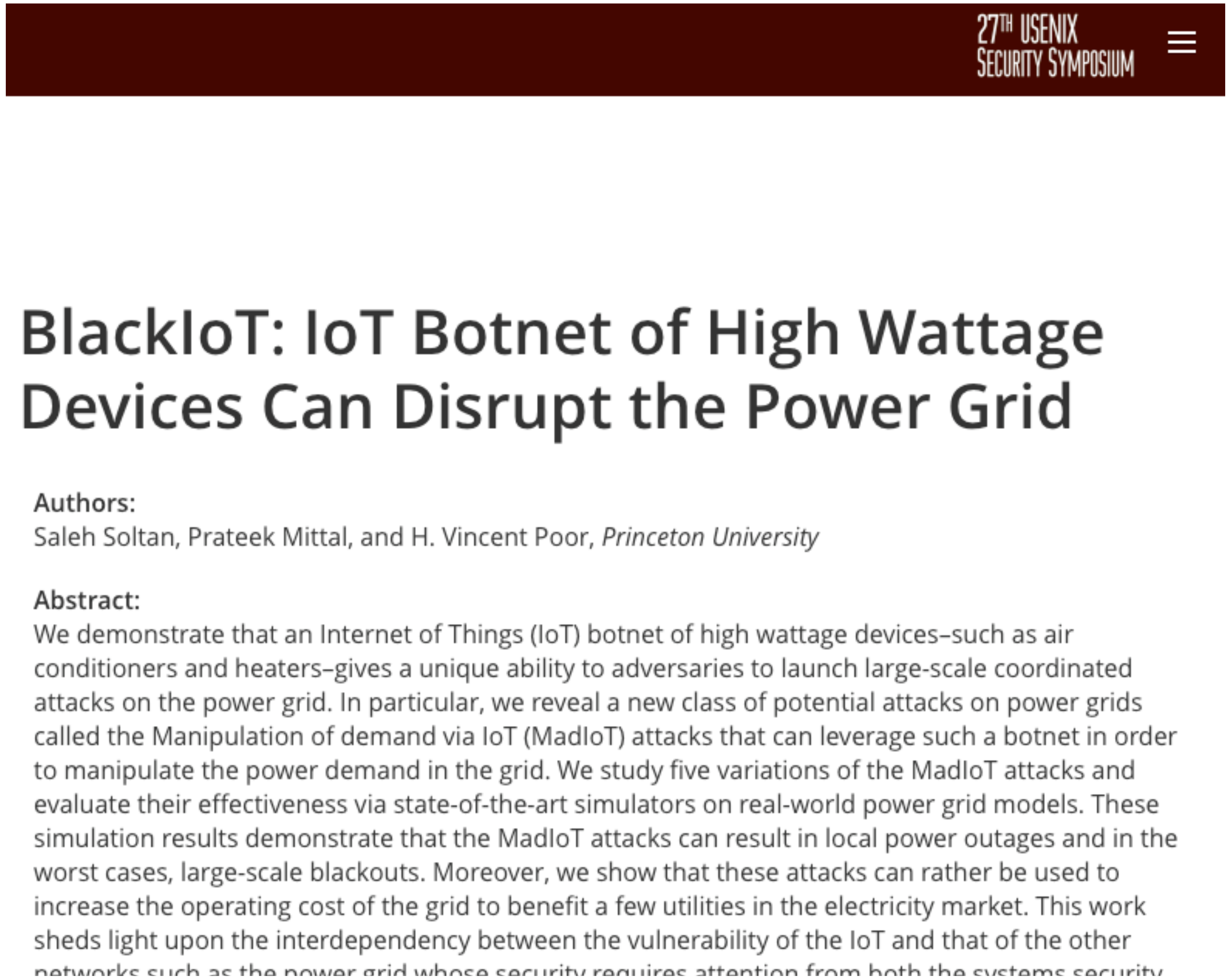
January 21, 2016

The power is on: How IoT technology is driving energy innovation

The Internet of Things in the electric power industry

Rob Young John McCue Christian Grant

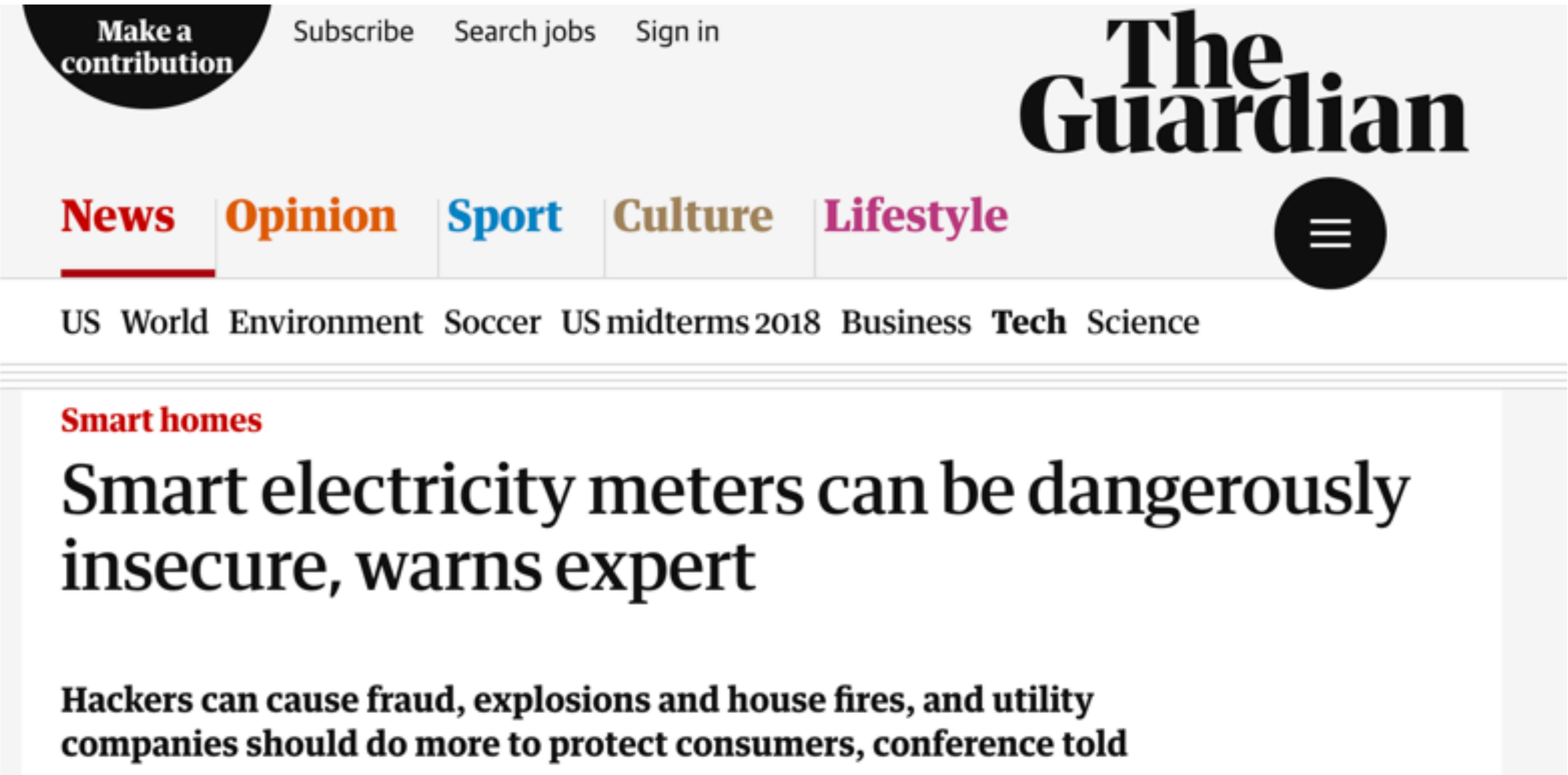
As conservation efforts and alternative energy ramp up, electric utilities can no longer count on customers using more and more power. How to survive? With a new focus on efficiency and cost control, based on technology—particularly Internet of Things applications.



BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid

Authors:
Saleh Soltan, Prateek Mittal, and H. Vincent Poor, *Princeton University*

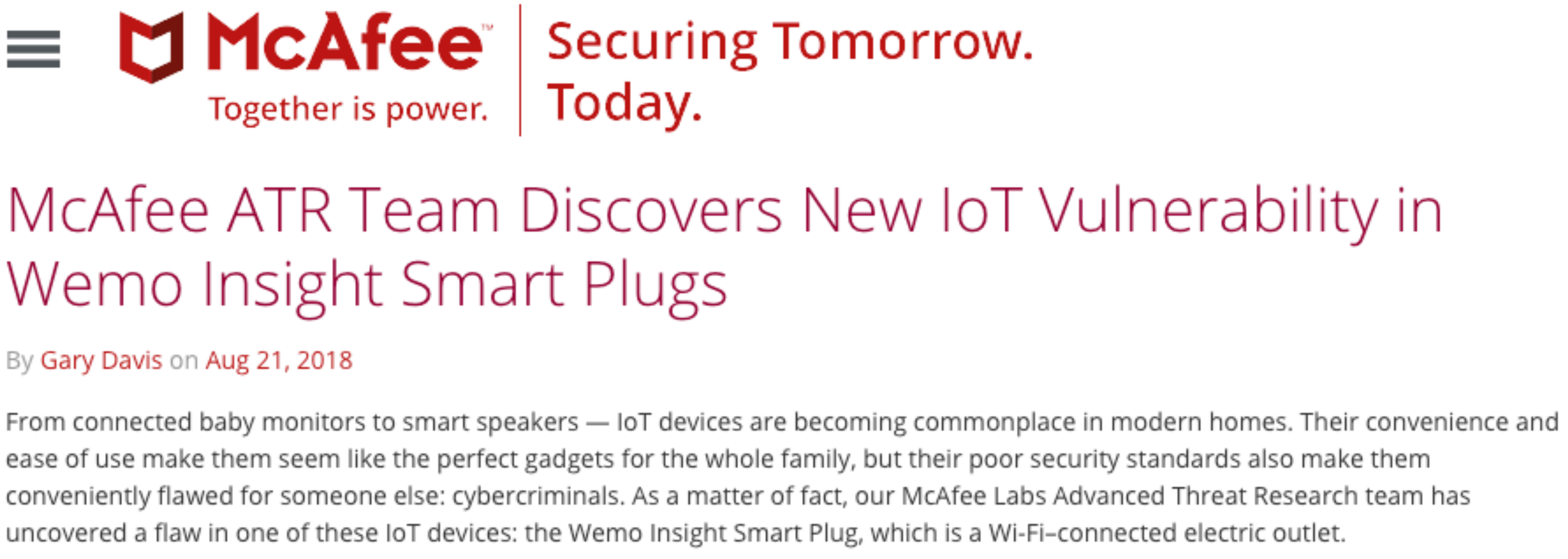
Abstract:
We demonstrate that an Internet of Things (IoT) botnet of high wattage devices–such as air conditioners and heaters–gives a unique ability to adversaries to launch large-scale coordinated attacks on the power grid. In particular, we reveal a new class of potential attacks on power grids called the Manipulation of demand via IoT (MadIoT) attacks that can leverage such a botnet in order to manipulate the power demand in the grid. We study five variations of the MadIoT attacks and evaluate their effectiveness via state-of-the-art simulators on real-world power grid models. These simulation results demonstrate that the MadIoT attacks can result in local power outages and in the worst cases, large-scale blackouts. Moreover, we show that these attacks can rather be used to increase the operating cost of the grid to benefit a few utilities in the electricity market. This work sheds light upon the interdependency between the vulnerability of the IoT and that of the other networks such as the power grid whose security requires attention from both the systems security



Smart homes

Smart electricity meters can be dangerously insecure, warns expert

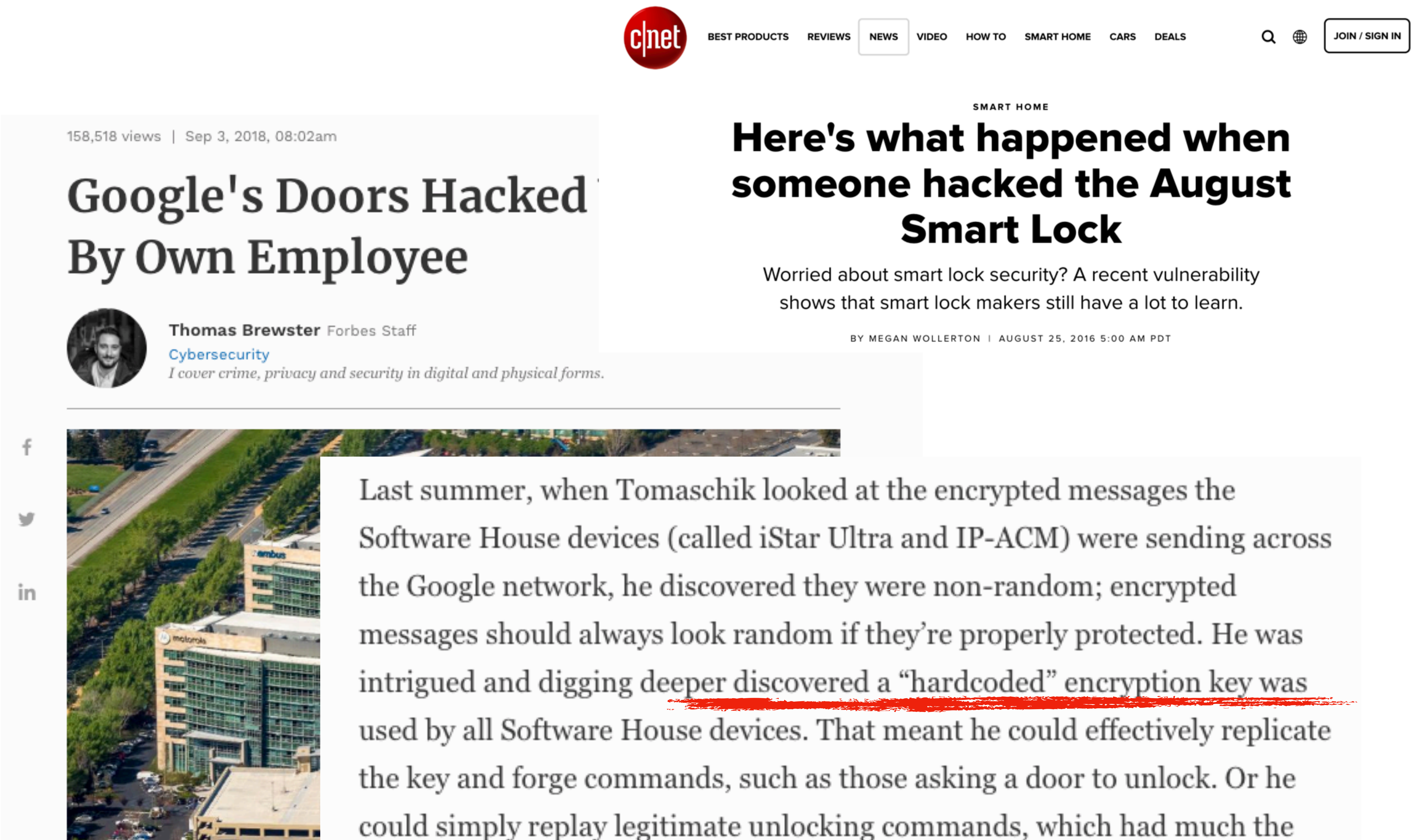
Hackers can cause fraud, explosions and house fires, and utility companies should do more to protect consumers, conference told



McAfee ATR Team Discovers New IoT Vulnerability in Wemo Insight Smart Plugs

By Gary Davis on Aug 21, 2018

From connected baby monitors to smart speakers — IoT devices are becoming commonplace in modern homes. Their convenience and ease of use make them seem like the perfect gadgets for the whole family, but their poor security standards also make them conveniently flawed for someone else: cybercriminals. As a matter of fact, our McAfee Labs Advanced Threat Research team has uncovered a flaw in one of these IoT devices: the Wemo Insight Smart Plug, which is a Wi-Fi–connected electric outlet.



158,518 views | Sep 3, 2018, 08:02am

Google's Doors Hacked By Own Employee

Thomas Brewster Forbes Staff
Cybersecurity
I cover crime, privacy and security in digital and physical forms.

SMART HOME

Here's what happened when someone hacked the August Smart Lock

Worried about smart lock security? A recent vulnerability shows that smart lock makers still have a lot to learn.

BY MEGAN WOLLERTON | AUGUST 25, 2016 5:00 AM PDT

Last summer, when Tomaschik looked at the encrypted messages the Software House devices (called iStar Ultra and IP-ACM) were sending across the Google network, he discovered they were non-random; encrypted messages should always look random if they're properly protected. He was intrigued and digging deeper discovered a "hardcoded" encryption key was used by all Software House devices. That meant he could effectively replicate the key and forge commands, such as those asking a door to unlock. Or he could simply replay legitimate unlocking commands, which had much the