Hackers could make smart homes stupid—or worse

7 January 2015, by Jennifer Donovan

A smart home can be controlled remotely, inviting hacking.

Imagine the smart home of the future. Thanks to a central controller and wi-fi, not only does the thermostat power up and warm or cool the house as you are heading home. Smart light bulbs come on low at dusk and brighten up as the sky gets darker; your washing machine starts a load of clothes when the electricity is cheapest; your smart refrigerator thaws the roast in one section, while another keeps your cheese ready to slice and yet another chills your beer. The doors lock automatically behind you and unlock as you—but no one else—approach. A 2-way nannycam lets you keep an eye on the kids while a sprinkler waters your lawn when water demand is lowest.

But what if a hacker gained access to your central controller? Your roast is frozen, your milk is sour, and the heat has been on full blast all day when you finally break into your house through a window because your front door won't unlock. The washing machine and dishwasher have been running at peak prices for electricity, and the kids have torn their room apart while it looked like they were peacefully napping.

In fact, if the hacker got to every smart home in the neighborhood, utility bills would shoot up and brownouts, if not blackouts would be imminent.

It's a cybersecurity nightmare. And it's exactly what Shiyan Hu is working to prevent.

Hu is an associate professor of electrical and computer engineering at Michigan Technological University. He founded the Michigan Tech Cyber-Physical System Research Group and won a coveted National Science Foundation (NSF) CAREER Award in 2014.

His research now focuses on hardware and system security for smart devices, ones with chips embedded that respond to a central controller powered by wi-fi. "It's a very exciting and challenging field," says Hu.

He and his research group are using machine learning and data mining techniques to develop short-term and long-term algorithms or formulas that can determine if a central controller is getting accurate data and making good decisions. These algorithms can be built right into the controller and the smart devices.

The researchers are working on both the local devices and the systems they control. "We need to analyze the security issues in each device and design ways to cross-check the devices and the systems," Hu says.

Smart appliances learn from repeated behavior, he explains. A smart water heater would know that you shower between 7 and 8 a.m. and don't use hot water again until you get home at 5:30 p.m. But a hacker could confuse that water heater into thinking that you don't need any hot water until 10 a.m.—providing teeth-chattering morning showers—and that you need it to heat up hundreds of gallons between 10 a.m. and 5 p.m., when no one is there to use it.

How big a problem is smart-home cybersecurity? An example is what Hu calls "the pricing curve attack." If the price of electricity is lower at 2 p.m. than it is at 8 p.m., for example, a hacker could fool a central controller into thinking that the rates are lower at the peak time, so everything that was supposed to run at 2 p.m. would come on at 8 p.m instead. And if multiple homes are hacked to see 8 p.m. as the best time to run appliances, an entire neighborhood or town would not only be paying higher rates, but could be brought to its knees by an unsustainable power demand.

Or a hacker could just be playing a prank—turning on all your lights in the middle of the night or turning your refrigerator off so you return from a weekend trip to find everything spoiling inside.

It's not a looming issue now, because smart appliances are still too expensive to be common. A smart refrigerator costs $3,000 to $7,000. A smart washing machine starts at $1,700. Even a package of two smart light bulbs costs $100.

But just like calculators, computers, cell phones and microwaves, the price is coming down, and it will continue to plummet, until smart homes become the standard instead of a novelty.

"We need to think about the security issues now, before we have to deal with them," says Hu.

Provided by Michigan Technological University