The Opinion Pages | Contributing Op-Ed Writer | Zeynep Tufekci

Why 'Smart' Objects May Be a Dumb Idea

AUG. 10, 2015

The early Internet was intended to connect people who already trusted one another, like academic researchers or military networks. It never had the robust security that today's global network needs. As the Internet went from a few thousand users to more than three billion, attempts to strengthen security were stymied because of cost, shortsightedness and competing interests. Connecting everyday objects to this shaky, insecure base will create the Internet of Hacked Things. This is irresponsible and potentially catastrophic.

That smart safe? Hackers can empty it with a single USB stick while erasing all logs of its activity — the evidence of deposits and withdrawals — and of their crime. That high-tech rifle? Researchers managed to remotely manipulate its target selection without the shooter's knowing.

Home builders and car manufacturers have shifted to a new business: the risky world of information technology. Most seem utterly out of their depth.

Although Chrysler quickly recalled 1.4 million Jeeps to patch this particular vulnerability, it took the company more than a year after the issue was first noted, and the recall occurred only after that spectacular publicity stunt on the highway and after it was requested by the National Highway Traffic Safety Administration. In announcing the software fix, the company said that no defect had been found. If two guys sitting on their couch turning off a speeding car's engine from miles away doesn't qualify, I'm not sure what counts as a defect in Chrysler's world. And Chrysler is far from the only company compromised: from BMW to Tesla to General Motors, many automotive brands have been hacked, with surely more to come.

Dramatic hacks attract the most attention, but the software errors that allow them to occur are ubiquitous. While complex breaches can take real effort — the Jeep hacker duo spent two years researching — simple errors in the code can also cause significant failure. Adding software with millions of lines of code to objects greatly increases their potential for harm.

A FRIDGE that puts milk on your shopping list when you run low. A safe that tallies the cash that is placed in it. A sniper rifle equipped with advanced computer technology for improved accuracy. A car that lets you stream music from the Internet.

All of these innovations sound great, until you learn the risks that this type of connectivity carries. Recently, two security researchers, sitting on a couch and armed only with laptops, remotely took over a Chrysler Jeep Cherokee speeding along the highway, shutting down its engine as an 18-wheeler truck rushed toward it. They did this all while a Wired reporter was driving the car. Their expertise would allow them to hack any Jeep as long as they knew the car's I.P. address, its network address on the Internet. They turned the Jeep's entertainment dashboard into a gateway to the car's steering, brakes and transmission.

A hacked car is a high-profile example of what can go wrong with the coming Internet of Things — objects equipped with software and connected to digital networks. The selling point for these well-connected objects is added convenience and better safety. In reality, it is a fast-motion train wreck in privacy and security.

The Internet of Things is also a privacy nightmare. Databases that already have too much information about us will now be bursting with data on the places we've driven, the food we've purchased and more. Last week, at Def Con, the annual information security conference, researchers set up an Internet of Things village to show how they could hack everyday objects like baby monitors, thermostats and security cameras.

Connecting everyday objects introduces new risks if done at mass scale. Take that smart refrigerator. If a single fridge malfunctions, it's a hassle. However, if the fridge's computer is connected to its motor, a software bug or hack could "brick" millions of them all at once — turning them into plastic pantries with heavy doors.

Cars — two-ton metal objects designed to hurtle down highways — are already bracingly dangerous. The modern automobile is run by dozens of computers that most manufacturers connect using a system that is old and known to be insecure. Yet automakers often use that flimsy system to connect all of the car's parts. That means once a hacker is in, she's in everywhere — engine, steering, transmission and brakes, not just the entertainment system.

For years, security researchers have been warning about the dangers of coupling so many systems in cars. Alarmed researchers have published academic papers, hacked cars as demonstrations, and begged the industry to step up. So far, the industry response has been to nod politely and fix exposed flaws without fundamentally changing the way they operate.

In 1965, Ralph Nader published "Unsafe at Any Speed," documenting car manufacturers' resistance to spending money on safety features like seatbelts. After public debate and finally some legislation, manufacturers were forced to incorporate safety technologies.

No company wants to be the first to bear the costs of updating the insecure computer systems that run most cars. We need federal safety regulations to push automakers to move, as a whole industry. Last month, a bill with privacy and cybersecurity standards for cars was introduced in the Senate. That's good, but it's only a start. We need a new understanding of car safety, and of the safety of any object running software or connecting to the Internet.

It may be hard to fix security on the digital Internet, but the Internet of Things should not be built on this faulty foundation. Responding to digital threats by patching only exposed vulnerabilities is giving just aspirin to a very ill patient.

It isn't hopeless. We can make programs more reliable and databases more secure. Critical functions on Internet-connected objects should be isolated and external audits mandated to catch problems early. But this will require an initial investment to forestall future problems — the exact opposite of the current corporate impulse. It also may be that not everything needs to be networked, and that the trade-off in vulnerability isn't worth it. Maybe cars are unsafe at any I.P.

Zeynep Tufekci is an assistant professor at the School of Information and Library Science at the University of North Carolina and a contributing opinion writer.
She invites you to visit her blog, follow her on Twitter and join her on Facebook.