Benefits and risks of the 'Internet of Things'

October 23 2015, by Lisa Stiffler

Credit: AI-generated image (disclaimer)

Technology publications call 2015 "the year of the car hack."

This summer at DEF CON—one of the world's largest computer-hacker conferences—attendees tested the vulnerability of car computer systems at the first "Car Hacking Village." Members of Congress recently introduced the SPY Car Act, aimed at strengthening security in modern cars.

In other words, the rest of the world is catching up to the University of Washington's (UW) Security and Privacy Research Lab.

Four years ago, with support from the National Science Foundation (NSF), the lab in the UW's Department of Computer Science & Engineering co-led an effort that first exposed weaknesses in car computer systems and demonstrated that hackers could remotely control a vehicle's brakes, door locks and other functions.

"We like to look in the places that no one else is looking yet," said computer science and engineering associate professor Yoshi Kohno, who founded the security lab. "You open that area up, and once people start to show up, you move on to the next thing."

That trailblazing strategy has put the lab, which Kohno runs jointly with assistant professor Franziska Roesner, at the forefront of computer security and privacy. The UW engineers are international leaders in addressing problems others haven't considered and helping guide the direction of the entire field. Their findings have driven security improvements in cars, medical devices, electronic voting machines and online browsing.

The lab's work is increasingly influential as computers are installed in countless everyday devices, making users' lives better and easier, but also putting them at risk for identity theft and even physical harm. This year alone, more than 530 security breaches have compromised more than 140 million records kept by credit card and insurance companies, hospitals, government agencies and others.

To combat these and other cyber threats, Kohno and Roesner investigate ways that people can co-opt a computerized product or use online information, warping it into something never intended.

Take the car example: The UW researchers, in partnership with alumni Alexei Czeskis and Karl Koscher and computer scientists from the University of California at San Diego, were curious about the security of modern vehicles and their computerized systems. So the teams at each university bought cars and plugged their computers into the vehicles' computers to see if they could decode, and ultimately hijack, the cars' software. They did it by listening as the computer systems talked to each other.

"If I go to a foreign country and try to learn the language, one of the best ways to do this is to eavesdrop," Kohno said. Then, he said, you "try to repeat things, and see if you get the same reaction."

Once the engineers figured out how to talk to the cars' computers and manipulate their functions while plugged in, they moved to the next phase: controlling the cars remotely.

The researchers identified a number of digital entry points including Bluetooth cell-phone devices, satellite radio signals and a cellular network that allows users such as dealerships to communicate with cars Through the cell network, they demonstrated that they could remotely take control of the car and drive them

"We were surprised by how easy some things were" when it came to commandeering the vehicles, Roesner said. But up to that point, the carmakers hadn't thought to install systems that would make it difficult.

That's no longer the case. The car hacking experiments caught the attention of the National Highway Traffic Safety Administration, and the Society of Automotive Engineers created a cybersecurity taskforce. The federal car safety legislation can likewise be traced to the work by the UW lab.

Protecting the Internet of Things

While the car hacking work garnered the most public attention, the lab has identified other important security weaknesses.

Kohno was an author on the first publications demonstrating the security risks of wirelessly reprogrammable pacemakers and defibrillators. Former Vice President Dick Cheney even had doctors disable the wireless mechanism in his defibrillator due to hacking concerns. Kohno stresses that the benefits of these devices outweigh the security risks and that patients should have no qualms using them. However, he believes that device manufacturers must improve the security of current and future devices.

Roesner has led groundbreaking work in the area of online data collection, trying to identify who is gathering information and what's being done with it. With further support from NSF, she led the development of a tool called ShareMeNot. Roesner partnered with the Electronic Frontier Foundation to incorporate ShareMeNot functionality in Privacy Badger, a tool that detects and blocks online advertising and other embedded content that tracks people without their permission.

The UW lab, which presently has over a dozen affiliated faculty and nine doctoral students, aims to stay one step ahead of the next cybersecurity challenge. Their current interests include the field of "augmented reality," which includes technologies like Google Glass or Microsoft's HoloLens that take computer-generated information including graphics, sound or videos and projects it into a real-world setting.

With Kohno's and Roesner's help, many of the UW Computer Science & Engineering students will graduate with a better understanding of risks posed by hackers. Professors there teach an undergraduate course in security and privacy that fills up almost instantly and has a waiting list of

a dozen or more.

The course essentially turns traditional software development on its head by taking a finished product that works one way and asking how it could be twisted, potentially for nefarious purposes. "It's kind of a surprising mind switch," Roesner said.

But, she added, it's important for students to grasp if the industry is going to get a handle on security threats.

"In order to build secure systems," she said, "you have to understand how to break them."

More information: Experimental Security Analysis of a Modern Automobile. www.autosec.org/pubs/cars-oakland2010.pdf

Provided by National Science Foundation