ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Though I hadn't touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system. Next the radio switched to the local hip hop station and began blaring Skee-lo at full volume. I spun the control knob left and hit the power button, to no avail. Then the windshield wipers turned on, and wiper fluid blurred the glass.

As I tried to cope with all this, a picture of the two hackers performing these stunts appeared on the car's digital display: Charlie Miller and Chris Valasek, wearing their

The Jeep's strange behavior wasn't entirely unexpected. I'd come to St. Louis to be Miller and Valasek's digital crash-test dummy, a willing subject on whom they could test the car-hacking research they'd been doing over the past year. The result of their work was a hacking technique—what the security industry calls a zero-day exploit—that can target Jeep Cherokees and give the attacker wireless control, via the Internet, to any of thousands of vehicles. Their code is an automaker's nightmare: software that lets hackers send commands through the Jeep's entertainment system to its dashboard functions, steering, brakes, and transmission, all from a laptop that may be across the country.

To better simulate the experience of driving a vehicle while it's being hijacked by an invisible, virtual force, Miller and Valasek refused to tell me ahead of time what kinds of attacks they planned to launch from Miller's laptop in his house 10 miles west. Instead, they merely assured me that they wouldn't do anything life-threatening. Then they told me to drive the Jeep onto the highway. "Remember, Andy," Miller had said through my iPhone's speaker just before I pulled onto the Interstate 64 on-ramp, "no matter what happens, don't panic."[1]

div,p,Charlie Miller, left, a security researcher at Twitter, and Chris Valasek, director of Vehicle Security Research at IOActive, have exposed the security vulnerabilities in automobiles by hacking into cars remotely, controlling the cars' various controls from the radio volume to the brakes. Photographed on Wednesday, July 1, 2015 in Ladue, Mo. (Photo © Whitney Curtis for WIRED.com) WHITNEY CURTIS FOR WIRED

As the two hackers remotely toyed with the air-conditioning, radio, and windshield wipers, I mentally congratulated myself on my courage under pressure. That's when they cut the transmission.

Immediately my accelerator stopped working. As I frantically pressed the pedal and watched the RPMs climb, the Jeep lost half its speed, then slowed to a crawl. This occurred just as I reached a long overpass, with no shoulder to offer an escape. The experiment had ceased to be fun.

At that point, the interstate began to slope upward, so the Jeep lost more momentum and barely crept forward. Cars lined up behind my bumper before passing me, honking. I could see an 18-wheeler approaching in my rearview mirror. I hoped its driver saw me, too, and could tell I was paralyzed on the highway.

of the radio, now pumping Kanye West. The semi loomed in the mirror, bearing down on my immobilized Jeep.

I followed Miller's advice: I didn't panic. I did, however, drop any semblance of bravery, grab my iPhone with a clammy fist, and beg the hackers to make it stop.

Wireless Carjackers

This wasn't the first time Miller and Valasek had put me behind the wheel of a compromised car. In the summer of 2013, I drove a Ford Escape and a Toyota Prius around a South Bend, Indiana, parking lot while they sat in the backseat with their laptops, cackling as they disabled my brakes, honked the horn, jerked the seat belt, and commandeered the steering wheel. "When you lose faith that a car will do what you tell it to do," Miller observed at the time, "it really changes your whole view of how the thing works." Back then, however, their hacks had a comforting limitation: The attacker's PC had been wired into the vehicles' onboard diagnostic port, a feature that normally gives repair technicians access to information about the car's electronically controlled systems.

A mere two years later, that carjacking has gone wireless. Miller and Valasek plan to publish a portion of their exploit on the Internet, timed to a talk they're giving at the Black Hat security conference in Las Vegas next month. It's the latest in a series of revelations from the two hackers that have spooked the automotive industry and even helped to inspire legislation; WIRED has learned that senators Ed Markey and Richard Blumenthal plan to introduce an automotive security bill today to set new digital security standards for cars and trucks, first sparked when Markey took note of Miller and Valasek's work in 2013.

As an auto-hacking antidote, the bill couldn't be timelier. The attack tools Miller and Valasek developed can remotely trigger more than the dashboard and transmission tricks they used against me on the highway. They demonstrated as much on the same day as my traumatic experience on I-64; After narrowly averting death by semi-trailer, I managed to roll the lame Jeep down an exit ramp, re-engaged the transmission by turning the ignition off and on, and found an empty lot where I could safely continue the experiment.

Miller and Valasek's full arsenal includes functions that at lower speeds fully kill the engine, abruptly engage the brakes, or disable them altogether. The most disturbing

pedal as the 2-ton SUV slid uncontrollably into a ditch. The researchers say they're working on perfecting their steering control—for now they can only hijack the wheel when the Jeep is in reverse. Their hack enables surveillance too: They can track a targeted Jeep's GPS coordinates, measure its speed, and even drop pins on a map to trace its route.

ANDY GREENBERG/WIRED

All of this is possible only because Chrysler, like practically all carmakers, is doing its best to turn the modern automobile into a smartphone. Uconnect, an Internet-connected computer feature in hundreds of thousands of Fiat Chrysler cars, SUVs, and trucks, controls the vehicle's entertainment and navigation, enables phone calls, and even offers a Wi-Fi hot spot. And thanks to one vulnerable element, which Miller and Valasek won't identify until their Black Hat talk, Uconnect's cellular connection also lets anyone who knows the car's IP address gain access from anywhere in the country. "From an attacker's perspective, it's a super nice vulnerability," Miller says.

From that entry point, Miller and Valasek's attack pivots to an adjacent chip in the car's head unit—the hardware for its entertainment system—silently rewriting the chip's firmware to plant their code. That rewritten firmware is capable of sending commands through the car's internal computer network, known as a CAN bus, to its physical components like the engine and wheels. Miller and Valasek say the attack on the entertainment system seems to work on any Chrysler vehicle with Uconnect from late 2013, all of 2014, and early 2015. They've only tested their full set of physical hacks, including ones targeting transmission and braking systems, on a Jeep Cherokee, though they believe that most of their attacks could be tweaked to work on any Chrysler vehicle with the vulnerable Uconnect head unit. They have yet to try remotely hacking into other makes and models of cars.

After the researchers reveal the details of their work in Vegas, only two things will prevent their tool from enabling a wave of attacks on Jeeps around the world. First, they plan to leave out the part of the attack that rewrites the chip's firmware; hackers following in their footsteps will have to reverse-engineer that element, a process that took Miller and Valasek months. But the code they publish will enable many of the dashboard hijinks they demonstrated on me as well as GPS tracking.

nine months, enabling the company to quietly release a patch ahead of the Black Hat conference. On July 16, owners of vehicles with the Uconnect feature were notified of the patch in a post on Chrysler's website that didn't offer any details or acknowledge Miller and Valasek's research. "[Fiat Chrysler Automobiles] has a program in place to continuously test vehicles systems to identify vulnerabilities and develop solutions," reads a statement a Chrysler spokesperson sent to WIRED. "FCA is committed to providing customers with the latest software updates to secure vehicles against any potential vulnerability."

Unfortunately, Chrysler's patch must be manually implemented via a USB stick or by a dealership mechanic. (Download the update here.) That means many—if not most—of the vulnerable Jeeps will likely stay vulnerable.

Chrysler stated in a response to questions from WIRED that it "appreciates" Miller and Valasek's work. But the company also seemed leery of their decision to publish part of their exploit. "Under no circumstances does FCA condone or believe it's appropriate to disclose 'how-to information' that would potentially encourage, or help enable hackers to gain unauthorized and unlawful access to vehicle systems," the company's statement reads. "We appreciate the contributions of cybersecurity advocates to augment the industry's understanding of potential vulnerabilities. However, we caution advocates that in the pursuit of improved public safety they not, in fact, compromise public safety."

The two researchers say that even if their code makes it easier for malicious hackers to attack unpatched Jeeps, the release is nonetheless warranted because it allows their work to be proven through peer review. It also sends a message: Automakers need to be held accountable for their vehicles' digital security. "If consumers don't realize this is an issue, they should, and they should start complaining to carmakers," Miller says. "This might be the kind of software bug most likely to kill someone."

In fact, Miller and Valasek aren't the first to hack a car over the Internet. In 2011 a team of researchers from the University of Washington and the University of California at San Diego showed that they could wirelessly disable the locks and brakes on a sedan. But those academics took a more discreet approach, keeping the identity of the hacked car secret and sharing the details of the exploit only with carmakers.

Carmakers who failed to heed polite warnings in 2011 now face the possibility of a public dump of their vehicles' security flaws. The result could be product recalls or even civil suits, says UCSD computer science professor Stefan Savage, who worked on the 2011 study. "Imagine going up against a class-action lawyer after Anonymous decides it would be fun to brick all the Jeep Cherokees in California," Savage says.[2]

For the auto industry and its watchdogs, in other words, Miller and Valasek's release may be the last warning before they see a full-blown zero-day attack. "The regulators and the industry can no longer count on the idea that exploit code won't be in the wild," Savage says. "They've been thinking it wasn't an imminent danger you needed to deal with. That implicit assumption is now dead."

471,000 Hackable Automobiles

div,p,Charlie Miller, a security researcher at Twitter, and Chris Valasek, director of Vehicle Security Research at IOActive, have exposed the security vulnerabilities in automobiles by hacking into cars remotely, controlling the cars' various cont rols from the radio volume to the brakes. Photographed on Wednesday, July 1, 2015 in Ladue, Mo. (Photo © Whitney Cu rtis for WIRED.com) WHITNEY CURTIS FOR WIRED

Sitting on a leather couch in Miller's living room as a summer storm thunders outside, the two researchers scan the Internet for victims.

Uconnect computers are linked to the Internet by Sprint's cellular network, and only other Sprint devices can talk to them. So Miller has a cheap Kyocera Android phone connected to his battered MacBook. He's using the burner phone as a Wi-Fi hot spot, scouring for targets using its thin 3G bandwidth.

A set of GPS coordinates, along with a vehicle identification number, make, model, and IP address, appears on the laptop screen. It's a Dodge Ram. Miller plugs its GPS coordinates into Google Maps to reveal that it's cruising down a highway in Texarkana, Texas. He keeps scanning, and the next vehicle to appear on his screen is a Jeep Cherokee driving around a highway cloverleaf between San Diego and Anaheim, California. Then he locates a Dodge Durango, moving along a rural road somewhere in the Upper Peninsula of Michigan. When I ask him to keep scanning, he hesitates. Seeing the actual, mapped locations of these unwitting strangers' vehicles—and knowing that each one is vulnerable to their remote attack—unsettles him.

enable attacks over a direct Wi-Fi link, confining its range to a few dozen yards. When they discovered the Uconnect's cellular vulnerability earlier this summer, they still thought it might work only on vehicles on the same cell tower as their scanning phone, restricting the range of the attack to a few dozen miles. But they quickly found even that wasn't the limit. "When I saw we could do it anywhere, over the Internet, I freaked out," Valasek says. "I was frightened. It was like, holy fuck, that's a vehicle on a highway in the middle of the country. Car hacking got real, right then."

That moment was the culmination of almost three years of work. In the fall of 2012, Miller, a security researcher for Twitter and a former NSA hacker, and Valasek, the director of vehicle security research at the consultancy IOActive, were inspired by the UCSD and University of Washington study to apply for a car-hacking research grant from Darpa. With the resulting $80,000, they bought a Toyota Prius and a Ford Escape. They spent the next year tearing the vehicles apart digitally and physically, mapping out their electronic control units, or ECUs—the computers that run practically every component of a modern car—and learning to speak the CAN network protocol that controls them.

When they demonstrated a wired-in attack on those vehicles at the DefCon hacker conference in 2013, though, Toyota, Ford, and others in the automotive industry downplayed the significance of their work, pointing out that the hack had required physical access to the vehicles. Toyota, in particular, argued that its systems were "robust and secure" against wireless attacks. "We didn't have the impact with the manufacturers that we wanted," Miller says. To get their attention, they'd need to find a way to hack a vehicle remotely.

div,p,CHARLIE MILLERCharlie Miller, a security researcher at Twitter, and Chris Valasek, director of Vehicle Security Research at IOActive, have exposed the security vulnerabilities in automobiles by hacking into cars remotely, controlling the cars' various controls from the radio volume to the brakes. Photographed on Wednesday, July 1, 2015 in Ladue, Mo. (Photo © Whitney Curtis for WIRED.com) WHITNEY CURTIS FOR WIRED

So the next year, they signed up for mechanic's accounts on the websites of every major automaker and downloaded dozens of vehicles' technical manuals and wiring diagrams. Using those specs, they rated 24 cars, SUVs, and trucks on three factors they thought might determine their vulnerability to hackers: How many and what types of radios connected the vehicle's systems to the Internet; whether the Internet-connected computers were properly isolated from critical driving systems, and

commands could trigger physical actions like turning the wheel or activating brakes.

Based on that study, they rated Jeep Cherokee the most hackable model. Cadillac's Escalade and Infiniti's Q50 didn't fare much better; Miller and Valasek ranked them second- and third-most vulnerable. When WIRED told Infiniti that at least one of Miller and Valasek's warnings had been borne out, the company responded in a statement that its engineers "look forward to the findings of this [new] study" and will "continue to integrate security features into our vehicles to protect against cyberattacks." Cadillac emphasized in a written statement that the company has released a new Escalade since Miller and Valasek's last study, but that cybersecurity is "an emerging area in which we are devoting more resources and tools," including the recent hire of a chief product cybersecurity officer.

After Miller and Valasek decided to focus on the Jeep Cherokee in 2014, it took them another year of hunting for hackable bugs and reverse-engineering to prove their educated guess. It wasn't until June that Valasek issued a command from his laptop in Pittsburgh and turned on the windshield wipers of the Jeep in Miller's St. Louis driveway.

Since then, Miller has scanned Sprint's network multiple times for vulnerable vehicles and recorded their vehicle identification numbers. Plugging that data into an algorithm sometimes used for tagging and tracking wild animals to estimate their population size, he estimated that there are as many as 471,000 vehicles with vulnerable Uconnect systems on the road.

Pinpointing a vehicle belonging to a specific person isn't easy. Miller and Valasek's scans reveal random VINs, IP addresses, and GPS coordinates. Finding a particular victim's vehicle out of thousands is unlikely through the slow and random probing of one Sprint-enabled phone. But enough phones scanning together, Miller says, could allow an individual to be found and targeted. Worse, he suggests, a skilled hacker could take over a group of Uconnect head units and use them to perform more scans —as with any collection of hijacked computers—worming from one dashboard to the next over Sprint's network. The result would be a wirelessly controlled automotive botnet encompassing hundreds of thousands of vehicles.

"For all the critics in 2013 who said our work didn't count because we were plugged into the dashboard," Valasek says, "well, now what?"

earch at IOActive, have exposed the security vulnerabilities in automobiles by hacking into cars remotely, controlling th e cars' various controls from the radio volume to the brakes. Photographed on Wednesday, July 1, 2015 in Ladue, Mo. (P hoto © Whitney Curtis for WIRED.com) WHITNEY CURTIS FOR WIRED

Congress Takes on Car Hacking

Now the auto industry needs to do the unglamorous, ongoing work of actually protecting cars from hackers. And Washington may be about to force the issue.

Later today, senators Markey and Blumenthal intend to reveal new legislation designed to tighten cars' protections against hackers. The bill (which a Markey spokesperson insists wasn't timed to this story) will call on the National Highway Traffic Safety Administration and the Federal Trade Commission to set new security standards and create a privacy and security rating system for consumers. "Controlled demonstrations show how frightening it would be to have a hacker take over controls of a car," Markey wrote in a statement to WIRED. "Drivers shouldn't have to choose between being connected and being protected...We need clear rules of the road that protect cars from hackers and American families from data trackers."

Markey has keenly followed Miller and Valasek's research for years. Citing their 2013 Darpa-funded research and hacking demo, he sent a letter to 20 automakers, asking them to answer a series of questions about their security practices. The answers, released in February, show what Markey describes as "a clear lack of appropriate security measures to protect drivers against hackers who may be able to take control of a vehicle." Of the 16 automakers who responded, all confirmed that virtually every vehicle they sell has some sort of wireless connection, including Bluetooth, Wi-Fi, cellular service, and radios. (Markey didn't reveal the automakers' individual responses.) Only seven of the companies said they hired independent security firms to test their vehicles' digital security. Only two said their vehicles had monitoring systems that checked their CAN networks for malicious digital commands.

UCSD's Savage says the lesson of Miller and Valasek's research isn't that Jeeps or any other vehicle are particularly vulnerable, but that practically *any* modern vehicle could be vulnerable. "I don't think there are qualitative differences in security between vehicles today," he says. "The Europeans are a little bit ahead. The Japanese are a little bit behind. But broadly writ, this is something everyone's still getting their hands around."

WHITNEY CURTIS FOR WIRED

Aside from wireless hacks used by thieves to open car doors, only one malicious car-hacking attack has been documented: In 2010 a disgruntled employee in Austin, Texas, used a remote shutdown system meant for enforcing timely car payments to brick more than 100 vehicles. But the opportunities for real-world car hacking have only grown, as automakers add wireless connections to vehicles' internal networks. Uconnect is just one of a dozen telematics systems, including GM Onstar, Lexus Enform, Toyota Safety Connect, Hyundai Bluelink, and Infiniti Connection.

In fact, automakers are thinking about their digital security more than ever before, says Josh Corman, the cofounder of I Am the Cavalry, a security industry organization devoted to protecting future Internet-of-things targets like automobiles and medical devices. Thanks to Markey's letter, and another set of questions sent to automakers by the House Energy and Commerce Committee in May, Corman says, Detroit has known for months that car security regulations are coming.

But Corman cautions that the same automakers have been more focused on competing with each other to install new Internet-connected cellular services for entertainment, navigation, and safety. (Payments for those services also provide a nice monthly revenue stream.) The result is that the companies have an incentive to add Internet-enabled features—but not to secure them from digital attacks. "They're getting worse faster than they're getting better," he says. "If it takes a year to introduce a new hackable feature, then it takes them four to five years to protect it."

Corman's group has been visiting auto industry events to push five recommendations: safer design to reduce attack points, third-party testing, internal monitoring systems, segmented architecture to limit the damage from any successful penetration, and the same Internet-enabled security software updates that PCs now receive. The last of those in particular is already catching on; Ford announced a switch to over-the-air updates in March, and BMW used wireless updates to patch a hackable security flaw in door locks in January.

Corman says carmakers need to befriend hackers who expose flaws, rather than fear or antagonize them—just as companies like Microsoft have evolved from threatening hackers with lawsuits to inviting them to security conferences and paying them "bug bounties" for disclosing security vulnerabilities. For tech companies, Corman says, "that enlightenment took 15 to 20 years." The auto industry can't afford to take that

enlightenment happen in three to five years, especially since the consequences for failure are flesh and blood."

As I drove the Jeep back toward Miller's house from downtown St. Louis, however, the notion of car hacking hardly seemed like a threat that will wait three to five years to emerge. In fact, it seemed more like a matter of seconds; I felt the vehicle's vulnerability, the nagging possibility that Miller and Valasek could cut the puppet's strings again at any time.

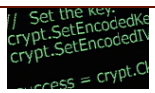
The hackers holding the scissors agree. "We shut down your engine—a big rig was honking up on you because of something we did on our couch," Miller says, as if I needed the reminder. "This is what everyone who thinks about car security has worried about for years. This is a reality."

Update 3:30 7/24/2015: Chrysler has issued a recall for 1.4 million vehicles as a result of Miller and Valasek's research. The company has also blocked their wireless attack on Sprint's network to protect vehicles with the vulnerable software.

[1]*Correction 10:45 7/21/2015*: An earlier version of the story stated that the hacking demonstration took place on Interstate 40, when in fact it was Route 40, which coincides in St. Louis with Interstate 64.

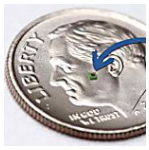
[2]*Correction 1:00pm 7/27/2015*: An earlier version of this story referenced a Range Rover recall due to a hackable software bug that could unlock the vehicles' doors. While the software bug did lead to doors unlocking, it wasn't publicly determined to exploitable by hackers.

#CAR HACKING #CHRYSLER #HACKS #LONGREADS #WIRED CLASSIC



HEAD CRAMP

What Happens When He Fills It With Water Seems Impossible



BANYAN HILL PUBLISHING

Tiny Device to be in 50 Billion Products by 2020 (Read Article)

BUSINESS INSIDER

An Apple Engineer Designed a Sweatshirt That’s Disrupting American Manufacturing

OUTBRAIN

Marketer? Learn how to find your target audience

BABBEL

This App Can Teach You Spanish In Just 3 Weeks

MORE SECURITY

DATABASES

The Scarily Common Screw-Up That Exposed 198 Million Voter Records

LILY HAY NEWMAN

SECURITY

Security News This Week: Microsoft's Patching *Old* Versions of Windows Because Things Are That Bad

LILY HAY NEWMAN

FACEBOOK

Facebook's Counterterrorism Playbook Comes Into Focus

EMILY DREYFUSS

NATIONAL AFFAIRS

The Texting Suicide Case Is About Crime, Not Tech

ISSIE LAPOWSKY

WIKILEAKS

WikiLeaks Reveals How the CIA Could Hack Your Router

ANDY GREENBERG

NORTH KOREA

North Korea's Sloppy, Chaotic Cyberattacks Also Make Perfect Sense

ANDY GREENBERG

FOLLOW US ON TWITTER

Visit WIRED Photo for our unfiltered take on photography, photographers, and photographic journalism
wired.com/category/photo

FOLLOW