ANOTHER REASON GM MAY HAVE COME AROUND TO CISA

Last week, Wired had a story about a hack of GM vehicles that the car company took 5 years to fix. As the story explains, while GM tried to fix the vulnerability right away, their efforts didn't completely fix the problem until GM quietly sent a fix to its vehicles over their Verizon network earlier this year.

> GM did, in fact, make real efforts between 2010 and late 2014 to shield its vehicles from that attack method, and patched the flaws it used in later versions of OnStar. But until the surreptitious over-the-air patch it finished rolling out this year, none of its security measures fully prevented the exploit in vehicles using the vulnerable eighth generation OnStar units.

The article uses this is a lesson in how ill-equipped car companies were in 2010 (notably, right after they had been put through bankruptcy) to fix such things, and how much more attentive they've gotten in the interim.

> GM tells WIRED that it has since developed the ability to push so-called "over-the-air" updates to its vehicles. The company eventually used that technique to patch the software in its OnStar computers via the same cellular Internet connection the UCSD and UW researchers exploited to hack the Impala. Starting in November of 2014, through the first months of 2015, the company says it silently pushed out a software update over its Verizon network to millions of vehicle with the vulnerable Generation 8 OnStar computer.

> Aside from the strangely delayed timing of that patch, even the existence of any cellular update feature comes as a surprise to the UCSD and UW researchers. They had believed that the OnStar computers could be patched only by driving them one-by-one to a dealership, a cumbersome and expensive fix that would have likely required a recall.
>
> GM chief product cybersecurity officer Jeff Massimilla hints to WIRED that performing the cellular update on five-year-old OnStar computers required some sort of clever hack, though he refused to share details. “We provided a software update over the air that allowed us to remediate the vulnerability,” Massimilla writes in an email. “We were able to find a way to deliver over-the-air updates on a system that was not necessarily designed to do so.”

What Wired doesn’t note is that GM was in the thick of recall hell by November 2014 because of its delay, during the same period, in fixing ignition problems. It’s not just the network problem GM wasn’t fixing, it was more traditional problems as well. Whatever hack GM pulled off, starting in November 2014 as a kluge to fix a long-running problem, GM did so while under great pressure for having sat on other (more obviously dangerous) problems with their cars. GM also did so knowing their recognizable Impala would be shown on 60 Minutes exhibiting this problem.

> In late 2014, they demonstrated it yet again for a *60 Minutes* episode that would air in February of 2015. (For both shows they carefully masking-taped the car’s logos to prevent it from being identified, though car blog Jalopnik nonetheless identified the Impala from the *60 Minutes* demo.)

So GM had a lot more urgency to find curious hacks in November 2014 than they did in 2010.

That obvious urgency doesn't stop GM from claiming they've changed their ways, pointing to a quick fix they made in July (though they said nothing about the apparent vulnerability of Escalades to the same hack researchers used on a Jeep Cherokee).

> Massimilla also admits that GM took so long to fully protect its vehicles because it simply wasn't ready in 2010 to deal with the threat of car hackers. He contrasts that response to GM's cybersecurity practices today, such as issuing a fix in just two days when it was alerted to a flaw in its iOS OnStar app in July. "The auto industry as a whole, like many other industries, is focused on applying the appropriate emphasis on cybersecurity," he writes. "Five years ago, the organization was not structured optimally to fully address the concern. Today, that's no longer the case."

While I think the article pays too little attention to the recall bonanza in the industry and how that may have changed GM's attentiveness to cybersecurity flaws, it claims that one thing that has motivated quicker responses is that, unlike the researchers who did the original hack on OnStar, researchers are now releasing their results generally. Significantly, the researchers that found this problem have now switched to full disclosure of their results.

> Savage says that if he were doing the same research today, he'd reconsider the decision to shield GM from public pressure. When he, Koscher, and other researchers revealed another car hacking technique in August, for instance—this time hijacking cars through a common Internet-connected gadget many drivers plug into their dashboards for insurance

> purposes—they publicly named every company whose bugs they'd exploited.

I raise all this not just for what it says about cars and hacking but also — of course — because of what it says about cybersecurity policy.

As I've noted, GM was actually a late supporter of CISA, writing a letter to announce their support just before recess in August, when business groups were making a big push to get it passed. I suggested at the time that GM might have been motivated by their Escalade vulnerability, hoping (possibly knowing) that if they revealed such vulnerabilities to authorities the government — the entire government, according to the plain letter of CISA — would be unable to launch any action against the company. On its face, it would appear that limitation would apply to NHTSA.

I'm not sure how this would work in practice — and neither are any of the lawyers I've been asking about this. But GM now knows that NHSTA is under far more pressure to order expansive recalls. And it also knows that researchers will default to publishing their research on vehicle insecurities, unlike what they did for this hack 5 years ago.

Those two things may well explain GM's sudden interest in sharing information with the government.