PHYS.ORG

Auto industry must tackle its software problems to stop hacks as cars go online

July 30 2015, by Bill Buchanan

Not what anyone wants to see while driving. Credit: Bill Buchanan, Author provided

Many companies producing software employ people as penetration testers, whose job it is to find security holes before others with less pure motives get a chance. This is especially common in the finance sector, but following the recent demonstration of a drive-by hack on a Jeep, and parent company's Fiat Chrysler's huge recall of 1.4m vehicles for security testing, perhaps it's time the auto industry followed its lead.

The growing number of software vulnerabilities discovered in cars has led to calls for the US Federal Trade Commission and National Highway Traffic Safety Administration to impose security standards on manufacturers for software in their cars. Cars are likely to require a software security rating so consumers can judge how hack-proof they are.

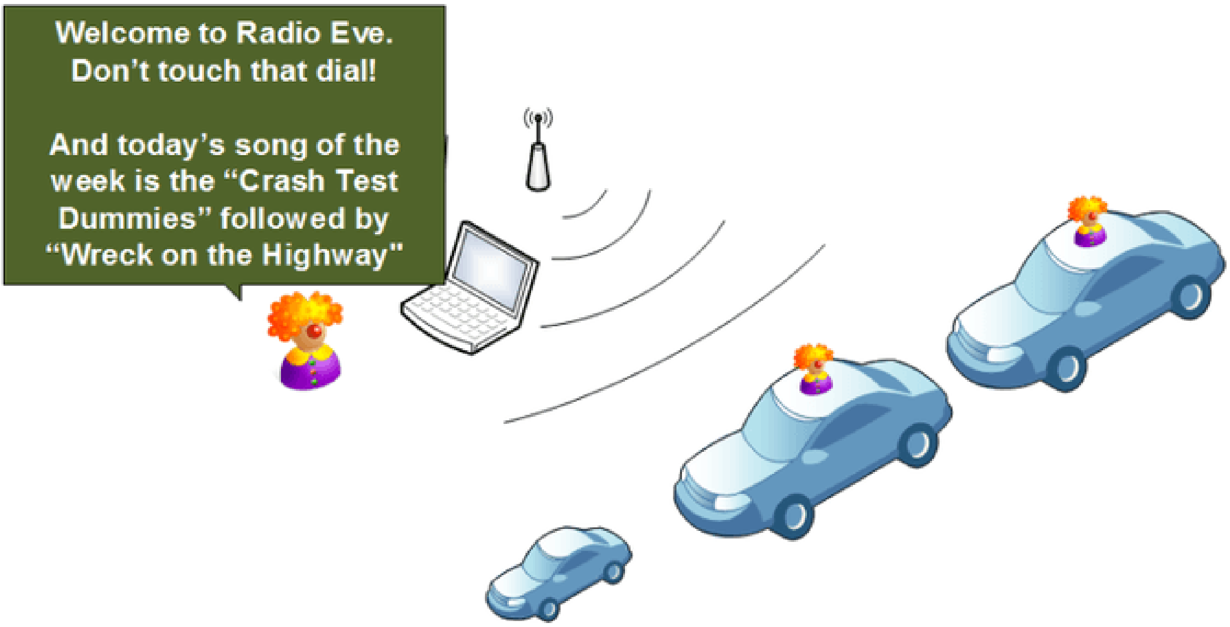
In the past, cars have generally avoided any form of network connectivity, but now consumers want internet access to stream music or use apps such as maps. If a car has a public IP address then, just as with any computer or device attached to the internet, a malicious intruder can be potentially connect to and hijack it – just as the Jeep hack demonstrated.

Andy Davis, a researcher from NCC Group, has shown that it may be possible to create a fake digital radio (DAB) station in order to download malicious data to a car when it tries to connect. While the Jeep hack was performed on a running car, the NCC Group researchers demonstrated that an off-road vehicle could be compromised, including taking control of steering and brakes. As the malicious data was distributed through a broadcast radio signal, it could even result in a nightmare situation where many cars could be compromised and controlled at the same time. More details on how the hack works will be revealed at the Black Hat conference this summer.

More devices, more bugs, more problems

In the last few weeks Ford has recalled 433,000 of this year's Focus, C-MAX and Escape models because of a software bug which leaves drivers unable to switch off their engine, even when the ignition key is removed. Recently, it was shown that BMW cars would respond to commands sent to open their doors and lower their windows – hardly the height of security. The firm had to issue a security patch for more than 2m BMW, Mini and Rolls-Royce vehicles.

As more and more software appears in cars, the problems of patching them will grow. Our desktop and laptop computers can be set to auto-update, but with embedded systems it's not so easy. The next wave of the internet, the internet of things where billions of devices will be network-connected, will evidently bring a whole lot more security problems in terms of finding and fixing bugs – on many more devices than just cars.


Welcome to Radio Eve.
Don't touch that dial!

And today's song of the week is the "Crash Test Dummies" followed by "Wreck on the Highway"

Tuning into the wrong station could give you more than you bargained for. Credit: Bill Buchanan, Author provided

Crowdsourcing debugging

Some companies take this seriously, while others try and distance themselves from flaws in their products. Google runs a Vulnerability

Reward Program with rewards from US$100-$20,000. For example, Google will pay a reward of US$20,000 for any exploit that allows the remote takeover of a Google account.

Google even has a Hall of Fame, for which it awards points for the number of bugs found, their severity, how recent, and whether the bounty recipient gives their reward to charity – Nils Juenemann is currently in top place. Google also awards grants up to US$3,133.7 as part of its Vulnerability Research Grants scheme.

Microsoft and Facebook also operate Bug Bounty schemes to encourage digging out bugs in its own internet software, with a minimum bounty of US$5,000. But while these companies actively seek people to improve software by fixing bugs, companies such as Starbucks and Fiat Chrysler take a negative approach to those who find bugs in their products, unhelpfully describing such efforts as criminal activity.

Change of approach needed

I don't mean to alarm, but software is one of the most unreliable things we have. Imagine if you were in the fast lane of the motorway when a blue-screen appears on your dashboard saying:

Error 1805: This car has encounter a serious error and will now shutdown and reboot

It would be back at the dealer in no time. We have put up with bugs for decades. We can't trust these embedded software systems to be bug-free, yet they're increasingly appearing in safety-critical systems such as speeding one-tonne vehicles. When was the last time your microprocessor suffered a hardware breakdown? Compare this to the last time Microsoft Word crashed and you can see it's not the hardware's fault. This is generally because software suffers from sloppy design, implementation and testing. So while a word processor crash is annoying, a car crash is clearly much worse. **can we say: Potentially in both senses of the word. (?)**

Car owners of the future will need to be a lot more savvy about keeping their vehicles updated. Consider that you are on the motorway one evening and the car informs you:

You have a critical update for your braking system, please select YES or NO to install the update. A reboot of the car is not required, and the update will be installed automatically from your Wi-Fi enabled vehicle

Would you answer YES or NO? If you choose NO, you don't trust the software; if you choose YES you are entrusting it to execute without problems while driving at speed along a motorway. Neither of these are good places to be.

The auto industry has a long way to go to prove that it grasps the risks posed by network-enabled vehicles and to then tackle them with our safety at all costs in mind. An independent safety rating for cars would provide some incentive for manufacturers to get this right. As for penetration testers, the industry may find that bug bounty schemes can help do this difficult work for them for less money than it costs in fines and recalls when undiscovered bugs make it to their products on the market.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Auto industry must tackle its software problems to stop hacks as cars go online (2015,

July 30) retrieved 22 June 2024 from
https://phys.org/news/2015-07-auto-industry-tackle-software-problems.html