Do auto manufacturers realise dangers of networked motors?

July 24 2015, by Madeline Cheah

Credit: Giorgio de Angelis from Pexels

While computers bring great benefits they come with drawbacks too – not least, as news stories reveal every day, the insecurity of often very private data connected to the public internet. Only now that computers are appearing in practically everything, the same insecurity also applies – as demonstrated by the drive-by hack of a speeding Jeep SUV, hijacked and shut down by security researchers as it sped past at 70mph.

Vehicles are growing ever more sophisticated, with technological additions to newer models designed to increase safety, comfort and convenience while providing entertainment features and improving the car's environmental impact. These innovations are more than just marketing ploys for manufacturers to sell their vehicles as cutting edge, they also help save money on materials and to comply with increasingly stringent safety and environmental laws.

Consider the benefits of a fully-connected vehicle: computers are never distracted, never get tired. They may be able to learn from driver behaviour and, using technologies such as active lane assist, can even correct human errors of judgement to a certain degree. Human productivity can be boosted, allowing for example a hands-free phone call while behind the wheel. Concepts such as platooning – where cars follow each other closely in a train – could help reduce congestion while allowing speedier commutes and greater fuel economy.

However this drive-by vehicle hack (on which there will be a presentation at Black Hat conference later this year) and others, such as the method of compromising brake systems using DAB radio signals, demonstrates the dangers of considerably networked, computerised vehicles designed without adequate protections.

More software, more problems

Precise details about how the Jeep was hacked, other than that the public IP address must be known, and that the attack relies on the uConnect mobile phone network, are yet to be revealed. While this gives the manufacturer time to provide a patch to fix the problem in this case, the vulnerabilities of mobile phone and internet network connections have been researched for years and are well-known and well-understood. If anything, this vehicle hack shouldn't come as any great surprise; more surprising is the lack of care paid to securing these well-known angles of attack in the first place.

Exploiting software flaws remotely through an internet connection – the most likely culprit – is made possible because we prize internet and phone connectivity sufficiently that manufacturers will fit it to our vehicles. This allows access to any piece of exposed hardware that is not "air-gapped", in other words physically separate and unconnected from the rest of the system. An attacker can pivot through the system, using one compromised component in order to compromise another, until the keys to the kingdom are acquired – in this case the critical control units capable of shutting down the engine.

Introducing these wireless network interfaces to vehicles presents the greatest danger: the ability to control cars, or even many cars *en masse*, from any distance. This possibility has caused such alarm there are plans in the US (where this attack was demonstrated) to introduce new legislation to tackle the issue.

Complexity creates vulnerability

That's not to say that network connectivity is the only issue. The presence of considerably more software in modern cars alone is a significant contributing factor to security problems. It has been estimated there is a software engineering industry average of 15-50 errors per 1,000 lines of code. The same can be said for integrating so many different systems, features and technologies – added complexity makes security testing much more difficult. These challenges, when vehicles migrate from being connected to being fully autonomous, could potentially have even broader security ramifications.

With any feature that makes something more safe, convenient or entertaining, there is potentially an equal amount of convenience for an attacker if sufficient defences haven't been put in place. The documented incidents of vehicles stolen by hacking keyless entry systems were down to technology designed to make unlocking a car more convenient for customers. Alas, the convenience works both ways.

Achieving safety and security has always been – and will continue to be – a balancing act. The National Highway Traffic Safety Administration (NHTSA) in the US states that in 94% of cases the last failure leading to a crash can be attributed to the driver. In the face of such evidence, despite the security vulnerabilities that may emerge as they are deployed and used, it would be counter-intuitive to ignore technology that could potentially save lives.

What is required to prevent these emerging problems from becoming overwhelming is an engineering process that embeds security in automotive design from the outset, implemented using secure coding practices as is found in other safety-critical areas such as nuclear reactor management or air traffic control, and reinforced with robust security testing procedures.

Only then will we see the world's car manufacturers move from the back foot to the front foot in the face of an internet-full of would-be cyber-carjackers.

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

Source: The Conversation

Citation: Do auto manufacturers realise dangers of networked motors? (2015, July 24) retrieved

24 April 2024 from https://phys.org/news/2015-07-auto-realise-dangers-networked-motors.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.