News – A security flaw on many or most recent cars can take out safety (and other) systems… Is this really progress?

Published: 17th August 2017

Author: Kim Henson

Online version:
https://www.wheels-alive.co.uk/news-a-security-flaw-on-many-or-most-recent-cars-can-take-out-safety-and-other-systems-is-this-really-progress/

The internet/world-wide web is a wonderful means of communicating, but now that many modern cars are linked to it, the potential for attacking and disabling vehicle computer systems is very real…

Yesterday, researchers discovered a security flaw that could potentially (and probably does) affect all new vehicles. It allows an attacker to turn off safety features, such as airbags, ABS brakes, and power-steering – or any of a vehicle's computerised components connected to its controller area network or CAN bus.

Commenting on this, Art Dahnert, managing consultant at Synopsys, said *"The problem identified by Trend Micro is related to the design and architecture of the CAN bus found in nearly all new cars today. The development of the technology goes back to the 1980's, predating the World Wide Web. No one at that time thought that someone would deliberately try to sabotage a vehicle over the in-car network.*

The attack involves creating a Denial of Service for a specific target by using the error management built into the CAN bus protocol. When an attacker causes the network to send too many error 'messages' (frames) to a device, the design dictates that the target goes into a Bus Off state. This means that it will no longer respond to messages or send new ones, effectively disabling the device. In the case of an automobile it might be the ABS or airbags or even the electrically-assisted power steering.

Generally, these types of attacks will require access to the vehicle and the ability to persist beyond a restart. However, now that newer vehicles can be connected to the internet in a myriad of ways this is no longer true. Taking advantage of connected phones and telematics features, an attack could happen without direct physical access. And this isn't necessarily isolated to a single manufacture or model of vehicle.

Even though the problem has been identified, resolving it will be a long time coming. There are many factors involved, including the large number of vehicle and component manufacturers as well as the technical difficulties in developing a solution for this type of problem. Not to mention the requirements to allow access by the aftermarket and third party repair establishments."

He adds, "You can't bolt on security, it has to be built in from the beginning. A simple update will not fix the cars on the road today."