Cyber threats to connected cars

14 June 2018, by David Bradley

Connected cars could be as vulnerable to so-called "cyber attack" as the smartphone in your hand or the personal computer on your desktop, according to a new study from the UK. "Connected cars are no different from other nodes on the internet of things and face many of the same generic cybersecurity threats," the team reports. They point out that the sheer number of putatively connected vehicles represents the biggest problem to be addressed and yet there have been few contributions to the debate. There are threats that are peculiar to connected cars rather than any other Internet of Things (IoT) device, PC, or mobile.

The team – David Morris, Garikayi Madzudzo, and Alexeis Garcia-Perez of the Centre for Business in Society, at Coventry University, UK – highlights several features of connected cars:

- Improved safety through better road infrastructure, onboard safety systems, automatic 'Smart SOS' emergency services' calling (for example, e-Call)
- Enhanced vehicle security through more sophisticated access systems
- Better use of road infrastructure to reduce congestion, enable smart parking, and spread journeys through time
- Safer and more accessible driving for those whose driving abilities are compromised enhancing employment and leisure opportunities
- Greener driving through reduced emissions
- User and usage-based, including driving style and habits, insurance premiums providing an incentive for safer driving
- Improved vehicle maintenance and reliability
- The improvement of air quality
- Opportunities for passengers to use the time spent on car journeys in more interesting and/or productive ways
- Improved payment services for fuel (including e-car battery charging), pay-as-you-drive insurance, parking charges and other car-related mobility services.

The team adds, however, that each additional feature and function in a connected car brings with it digital security risks and vulnerabilities that could expose critical vehicle systems to those who might exploit them for illegal activity. "The potential costs of vehicle cybersecurity attacks and their prevention measures need to be weighed up against the undoubted benefits which technological innovations in connected cars may bring," the team says.

There are four prominent features that must be investigated to which the researchers allude. First, the largely commercial nature of "cyberspace" makes regulation and usage very difficult to control. Secondly, there is such a vast array of components across the globe with countless sources and intermediaries handling them during manufacture and in use. Thirdly, there is huge potential for new vulnerabilities and risks to emerge suddenly, so-called zero-day attacks, for instance. Finally, the very nature of cyber threats is highly covert and so the public, business, and government assessment of potential risk underestimates the reality by a long way.

The team concludes that in order to mitigate the threat of cybersecurity, "Coordinated research and development strategies must be developed. Cross-disciplinary research in implementing security into control systems will be needed to provide the solutions necessary to combat cybersecurity incidents."

More information: David Morris et al. Cybersecurity and the auto industry: the growing challenges presented by connected cars, *International Journal of Automotive Technology and Management* (2018). DOI: 10.1504/IJATM.2018.092187

Provided by Inderscience