The Security of Driverless Cars

Dr Deeph Chana, Deputy Director, Institute for Security Science and Technology, Imperial College London

The emerging landscape

The opportunities that driverless vehicles present are undoubtedly profound. None more so than the emergence of multi-modal transport services (trains, planes, automobiles … and boats) that will intelligently cooperate to take us from A to B without any human intervention. Replacing the old biological controllers — namely us — the autonomous vehicle will excel in everything from energy efficiency to just being safe. The technology of today already affords us a near-term vision of the car where:

- route planning and optimisation
- refuelling and recharging
- transactions with services (tolls , shops , parking lots)
- authentication and hand-shaking for the purpose of site access control

are all automatically achieved by the vehicle, without the human 'in-the-loop'. Removing the human from all of these *piloting* activities in concert, including that of physically manoeuvring the vehicle, will prove to be the real transformation in experience that autonomy will bring to car users. The main outstanding technical piece needed to achieve this -- the driving bit -- is a problem that is rapidly being cracked by some of the largest and smartest companies in the world. Furthermore, the use of artificial intelligence and deep-learning technology is poised not merely to deliver our replacement, but a significant upgrade. A 'driver' that will be better at learning, anticipation and adaption and one that will work tirelessly, around the clock. Driver 1.0 looks set, almost inevitably, for extinction. But, don't worry if you're feeling somehow obsolete, all of this will leave us with far more time to get on with the more important things in life like texting and motorway Tinder and will eliminate that potent source of stress, road rage — although there are no promises about the more general problem of rage *on* the road. However, let's leave the debate as to whether or not this transport paradigm-shift represents a psychological step forward for the road user for another day and settle for the fact that it certainly will be a technical leap-forward on how we go about the business of moving about.

Considering the comprehensive nature of the transformation we're talking about, it is not unreasonable to ask if a re-think on what it means for a car to be secure and safe is motivated. Ironically, when we do pose

the question, rather than the longer-term prospects of some kind of dystopian robo-world emerging, understanding how to be secure against humans emerges as the more pressing concern. For whatever motivation — and there are plenty to choose from — humans are the most likely to seek the means and methods for compromising the whole operation; either by delivering costly nuisance cyber-hacks or by engineering complex orchestrated attacks that result in large scale economic hits or even the loss of life. Tragic incidents in urban settings around the world such as the most recent in Barcelona, illustrate how the car, even in its current form, may be used to generate terror and fear with global resonance and impact.

Paradoxically, the driverless car simultaneously represents an opportunity for virtually eliminating such incidents and the means by which their impacts could be greatly amplified. Both of these outcomes will be made possible by the unprecedented interconnectivity the car of the future will possess, where participation in a massive and distributed network of things including other cars, buildings, IoT devices, knowledge repositories and databases will provide access to huge computing power and a physical reach far beyond the individual car. Which outcome becomes reality rests on how well considered the design of this entire car-system will be to security problems and whether security will be 'designed in' from the start. The argument that security is not the primary purpose of the car or that security incidents are generally not that likely to occur is a rationale that risks this aspect of the system's design being given far less attention than it deserves. We might consider such arguments as rooted in the simplistic view of what we understand the car to be today rather than the reality of what it is about to become. It would be liberating and perhaps more in keeping with the technical revolution to consider the very concept of a car to be a fading reality, being replaced by a completely new mode of transport that bears only a superficial resemblance to the automobile. It may look like a car, move like a car, but in all other aspects it will not be one.

The Gateway project

Within the Gateway project -- one of the UK's autonomous vehicles urban demonstrators -- we have been considering what security for driverless cars should look like in the near, medium and longer-terms. In the near-term we have examined the more practical aspects of securing vehicles that are being rapidly developed in the market by viewing our trial vehicles as moving cyber-physical systems: the driverless car is far more than just a moving piece of office IT. In the medium-term, problems such as ensuring that vehicles can trust connections to things around them with a digital pulse, including other cars, remains an open but tractable problem. Detecting security issues during the operation of such systems, countering problems in real-time and the legal ramifications of failure are all things that will keep our community and our wider networks working for some time to come.