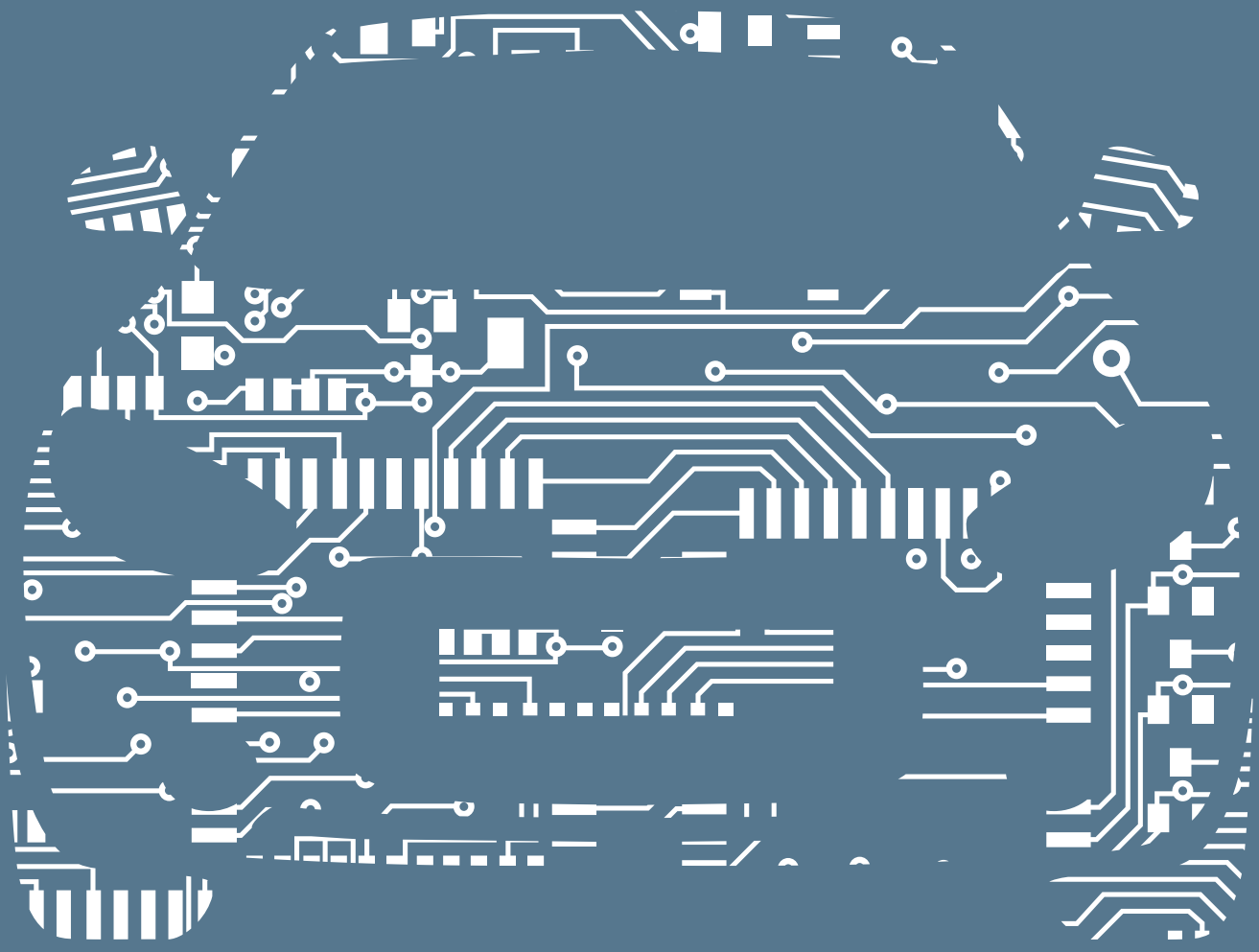
Roke

Part of the
Chemring Group

The future of connected cars: Putting the brakes on cyber attacks



roke.co.uk

Enable • Defend • Defeat

Putting the brakes on cyber attacks

As the connected car gains momentum, Roke's expert in Information Security, Mark West, explores the ways in which we can protect against the increasing threat of cyber attacks.

According to The Society of Motor Manufacturers and Traders (SMMT) more than 1.5 million UK motorists now have cars featuring self-activating safety systems.

The majority of new cars now have connected features as standard, with more than half of new cars registered in 2016 having safety-enhancing collision warning systems. Other technologies such as adaptive cruise control, autonomous emergency braking and blind spot monitoring are also surging in popularity.

So it's no surprise that the UK is set to see the number of connected cars reach nearly 8.6 million by 2020, with worldwide figures rising to 160 million.

There are obvious advantages that connected cars offer us. If our vehicles communicate with road signs, traffic lights, other cars and traffic management centers, they will automatically know the best routes through a town or city, saving time for passengers.

There are also wider benefits in terms of safety. For example, if we know in advance that a pedestrian is crossing the road or that a motorcycle is about to pull out in front of us, our vehicle can brake before we have a chance to react, vehicles behind us can be alerted and reduce their speed automatically, and accidents can be avoided. There are also long-term economic and environmental benefits offered by fewer cars on the road, as car sharing replaces outright ownership.

Yet there also comes a new risk. All of this connectivity relies on computers and, according to automotive research centre Thatcham Research, it's this convergence between automotive and computer technology that could provide a big opportunity for cyber attackers.

THE GROWING THREAT OF CYBER ATTACKS

Worryingly we've already seen vulnerabilities exposed that could leave drivers open to cyber attacks. The potential danger was illustrated dramatically last year when two white-hat hackers (ethical computer hackers specialising in testing devices to ensure that they're secure) remotely took control of a Jeep Cherokee and cut its transmission on a motorway. Part of a research initiative, the well-publicised incident prompted Chrysler to recall 1.4 million vehicles.

As more and more of the car becomes connected it will become possible for hackers to seize control of the vehicle or any one of its component parts. Allowing a hacker to brake, steer or accelerate a vehicle has far-reaching and dangerous consequences.

Research carried out by the International Data Corporation (IDC) in 2016 revealed that almost half of British drivers are still concerned about the security of driver-aid applications such as cruise control and self-parking. Yet what the majority of consumers do not realise is that cyber security considerations need to go far beyond assessing these relatively commonplace features when it comes to buying a car.

To truly understand how automotive cyber security works, you need to break down the various layers of a car and ensure the entire ecosystem of the car is protected. At a foundation level this includes securing individual electrical components, known as electronic control units, or ECUs, such as the car's brakes.

The second layer takes into consideration network security by identifying any vulnerabilities in a car's network communications. One also needs to consider any electronic units that are connected to the outside world, such as infotainment units. In addition to these layers of protection, it's vital for manufacturers to ensure their supply chain risk is managed as part of the overall cybersecurity effort.

Even those drivers who do have an understanding of wider security threats may still not fully appreciate the level of cyber security protection to consider. Furthermore, the IDC research revealed that automotive manufacturers themselves believe there could be a security lag of up to three years before cars with driverless features catch up with cyber threats.

“As more and more of the car becomes connected it will become possible for hackers to seize control of the vehicle or any one of its components parts.”

REDUCING THE CYBER SECURITY THREAT

Although automotive manufacturers recognise the threat of cyber attacks on connected cars, there's no consensus on how to prevent or protect against potential threats. Like all computer software, as the number of lines of code increases, so does the opportunities for exploitation.

At the moment the newest cars on the market operate with around 100 million lines of code, but with the rise of truly autonomous cars this figure will grow exponentially.

In a bid to reduce the threat of cyber attacks, manufacturers have invested heavily in security, conducting extensive testing to ensure their cars are as safe as possible. It's an uphill struggle for manufacturers however, as the plethora of different technologies, from multiple vendors, needs to integrate and operate seamlessly. While one component may be secure on its own, weaknesses can be introduced as soon as it's combined with another.

The only way to mitigate against the risk is to introduce a baseline level of security that works industry wide, on a global basis, ensuring that every car is built with security baked into the very first stages of design. This standard baseline needs to be created and adhered to by every automotive manufacturer, collaborating and taking full advantage of the available skills and expertise in the computer security industry to guarantee the highest levels of protection.

From this established baseline, effective security measures can be developed to enable manufacturers to offer consumers a range of connected options with the right level of cyber security certification for their use. Yet the further these products progress from the industry baseline, the more critical the collaboration approach becomes, ensuring manufacturers, cyber security experts and consumer interest bodies are all working together for the benefit of the car owner.

Organisations such as the IoT Security Foundation (IoTSF), of which Roke is a member, have emerged to drive collaboration in response to the complex challenges posed by security in the IoT. By combining the ideas and expertise of IoT security professionals, manufacturers, government agencies, academics and more, the non-profit organisation aims to raise the quality bar to ensure connected devices are as secure as possible.

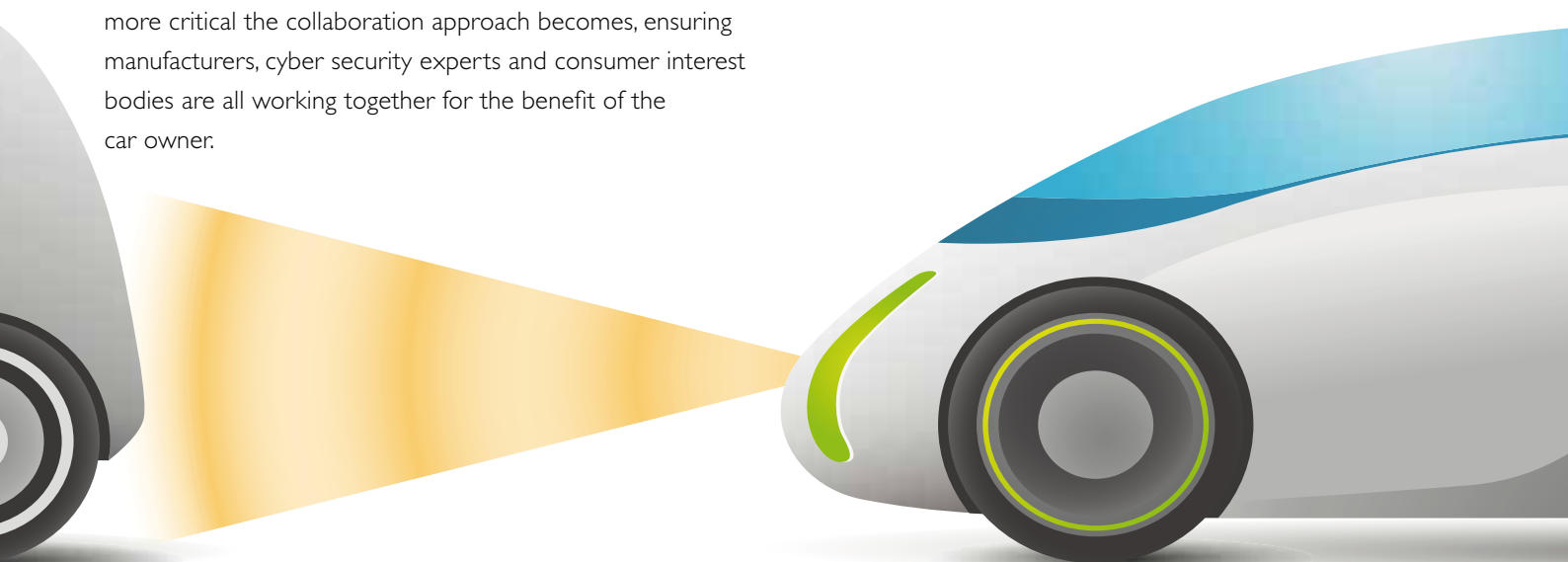
THE CHANGING INSURANCE MODEL

One of the first challenges to address around setting a standard is how the right level of cyber security is determined and how manufacturers can ensure that they meet public demand.

This is where we can expect to see changes to the insurance system, as insurers start to factor risks around poor cyber security into their calculations. Where the cost of inadequate security will be borne by the insurance companies, they have an incentive to factor that into their models, which will potentially affect consumer choices and in turn, drive manufacturer behaviour.

This means that assessing and pricing risk, and ultimately premiums, can be more accurate than ever. These premiums could also be adjusted depending on the cyber security rating of a car, offering incentives for consumers who take steps to protect themselves against cyber attacks.

However, connected cars are also likely to shake up the entire liability model that we've become used to. PwC has highlighted how we are likely to see a move away from outright vehicle ownership towards car sharing, particularly as the increase in autonomous electric vehicles continues. This further complicates who holds responsibility for the



vehicle at any one time and requires a fresh approach to how insurance products are both costed and sold.

COLLABORATING TO REDUCE RISK

As developments in technology bring the fully connected car to reality, risks are emerging that could dampen public enthusiasm and outweigh the convenience and potential benefits. The automotive industry is in a race against time to guarantee public safety and the protection of personal data.

To win this race, the automotive industry must work both together and with relevant professional and academic experts to standardise legislation, adopt universal rules for interoperability, and agree on a standard rating system.

It will only be through independent thinking, testing and third-party certification that the automotive industry can fully guard against cyber security threats to win public confidence and ensure the success of the connected car.

Roke is collaborating with Thatcham Research and others to create an accreditation system for cars, much like the European New Car Assessment Programme (NCAP) rating currently offered to validate a car's safety.