GETTING AROUND THE CYBER CURVE. HYPER-CONNECTIVITY IN THE AUTOMOTIVE INDUSTRY.

INTRODUCTION

We and our devices are becoming ever more connected to the Internet, and that's not going to stop. This connectivity will only increase in the future. The smartphone is everywhere, used by everybody, and 'quantifying' yourself with smartbands, smartwatches and other self-monitoring devices is a growing trend. Our fridges know more about what we eat than we do, and they can tweet it. In this Internet of Things (IoT), it is hard to find any sectors where machines and appliances are not becoming smarter and more connected. The industrial sector is now expanding the SCADA (supervisory control and data acquisition) universe, and connected cars are leading the charge.

THE CONNECTED CAR – ALWAYS SMARTER

Is there anyone who has not heard of the Google car? This vehicle of the future can now relegate the human driver to the status of accessory. The only reason a driver is still needed is to comply with the law!

These robotic cars are still prototypes, though at a very advanced stage. There are still technical and legal issues to be resolved before we see fleets of them on our streets. But manufacturers are already competing in ingenious ways to give us safer and smarter cars, by using embedded Information technology and internet connectivity.

PROGRESS HAS A PRICE

These breakthroughs have a price, and the new cars come with a series of limitations. Break-downs occur more frequently, from a wider variety of causes. Maintenance is more complex and expensive. However, the biggest challenge is their exposure to the world of cybercrime and cybervandalism.

Since the cars are now able to communicate with the outside world, they are vulnerable to a wide range of cyber-attacks. The first attempt to take control, remotely, of a car's critical systems dates back to 2011, and was carried out by a team of researchers. The

first successful hacking on a large scale was performed in 2013 [source] on several models from two different makers.

More recently, the hacking of one particular model was performed with the help of a journalist. In a video of the experiment, we can clearly see the driver lose control of the vehicle, which ends up in a ditch. The hackers successfully hijacked control of almost every system in the car – from a distance of more than 12km.

VIRTUAL IMPACT ON THE PHYSICAL WORLD

This case shocked both the public and the manufacturers. Imagine someone disabling the brakes in your car with a simple click, with no physical contact involved. This was a wake-up call for the industry and quickly prompted two levels of reaction: To minimise the threat or to include it as another risk which must be taken into account during the design phase.

While it has an impressive track record in physical safety, cybersecurity is a brand new world for the automotive industry. Spike Reply is an IT security and IoT specialist, which has brought its knowledge and expertise to bear on the automotive industry. It acts as a strategic partner in the development of automotive cybersecurity, focusing on diagnostic protocols and infotainment systems, while maintaining maximum security and reliability.

HOW SPIKE REPLY CAN HELP YOU

Spike Reply assists the development process by:

- Helping auto manufacturers to correctly identify any potential security problems in modern on-board systems and suites protocols (CAN bus);
- Analyzing risk scenarios, quantifying potential impacts and their probability of occurrence;
- Identifying the best countermeasures, while improving the overall systems security level;

and, even more importantly:

- Helping the customer to develop a defensive-oriented mindset, both digital (security) and physical (safety).

Spike Reply recently enjoyed a successful partnership with a world-class car manufacturer, testing and improving system security. The project included a number of different security tests on the infotainment car systems and on-board electronic devices. Attack simulations were carried out, sending non authorized commands to CAN bus (a vehicle bus standard designed to allow microcontrollers and devices to communicate with each other in applications without a host computer). These interfered with the

standard behavior of electronic devices and executed malicious code on the infotainment system, with possible repercussions for driver safety.
Spike Reply then designed a support system to manage the security risks identified on each vehicle, increasing the overall quality and value generation for the customer.

REPLY
SPIKE

Spike Reply is the Reply Group Company, specializing in consultancy services and integrated solutions for Cyber Security. The advent of the digital world, and the inherent interconnectivity of people, devices and organizations, are the source of increased vulnerabilities and new risks.
The rapid evolution of business needs and the continuous introduction of new technologies such as Mobility, Consumerization, Cloud, industrial automation, Internet of Things (automotive, smart homes/cities, wearable devices, …) increase the likelihood of exposure to cybercrime and resources misuse.
Spike Reply assists enterprises creating and maintaining a Cyber Security Program to govern, assess, protect, detect and respond to the threat landscape, developing and implementing the appropriate safeguards.

Reply
www.reply.com