nccgroup

Jul 09, 2021 13:43 BST

# Securing the connected cars of the future

As the autonomy of connected vehicles increases and systems become more complex, this leads to more software vulnerabilities. Andy Davis, Global Transport Practice Director at NCC Group, shares his insights into securing the connected cars of the future.

**What are the main security risks facing the future of connected cars?**

Cars can contain hundreds of millions of lines of code, and often, over a hundred embedded computer systems from many different automotive suppliers. This means if devices within the network of a connected vehicle have been poorly designed or are misconfigured, they can be attacked by threat actors, and there are many different wired and wireless entry points

into the ecosystem that attackers can exploit.

The increasing complexity of connected vehicles, as companies incorporate new technologies, means that the attack surface is growing. The main security risks in the case of an attack are driver safety, system failures, or the disclosure of sensitive information.

If hackers access safety-critical components such as steering, braking, acceleration or airbag deployment, or the components that control these, this could potentially result in injury or death. Hackers may also attempt to access personal data in infotainment systems or mount industrial espionage attacks to gain access to intellectual property, stored on other specialist embedded computers. However, the most likely approach taken will be ransomware attacks, which involve displaying messages on the screens of connected cars, convincing the driver that hackers have taken control of the vehicle's safety-critical systems (even if this is false) and demanding money to restore the safety of the vehicle.

**What needs to be done in the future?**

The most effective way to secure connected vehicles is to ensure that cyber security is considered throughout the entire design, development and manufacturing processes. It is much more difficult to address issues and implement new cyber security measures once a car has already been built and sold – therefore, it is crucial that vehicle manufacturers invest in connected car cyber security programmes to address both present and future challenges.

As connectivity increases within modern vehicles, so should cyber security awareness across the global automotive supply chain. New UNECE cyber security regulations require car manufacturers to satisfy the relevant Approvals Authorities that cyber security has been adequately addressed, both technically and from an organisational governance perspective. Failure to comply with these regulations may result in a vehicle manufacturer not being allowed to sell cars. Therefore, they must ensure that cyber security standards are being met.

**How are we helping to protect against the risks?**

Close collaboration between the security industry and vehicle manufacturers is key to improving security standards on an ongoing basis. Our NCC Group Transport practice has been part of an independent review process, validating new automotive cyber security standards and aligning our services (as well as, in some cases, developing new ones) to help support vehicle manufacturers to achieve compliance with the new regulations. The services involve close collaboration between our governance, risk and compliance teams and technical cyber security experts with automotive industry-specific knowledge and expertise.

To create a safer and more secure future for connected vehicles, it's important to help vehicle manufacturers not just in achieving initial compliance with the regulations, but to maintain that compliance by changing cyber security culture.

---

## About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

## Contacts

**NCC Group Press Office**
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

**NCC Group - Financial Media Enquiries**
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

**Regional Press Office - North America**
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750