NTT Security

Global Overview

Cybersecurity Expertise in the Automotive Industry

The rise of connected vehicles poses difficult questions for automobile manufacturers. As society makes the shift towards a future of fully autonomous cars, cybersecurity is crucial to accelerating mass adoption. In short – the automotive industry must determine how to protect the safety of drivers, passengers, and pedestrians from the threat of car hacking.

Today's connected cars already contain more than one hundred million lines of code[1]. The electrical control units or ECUs in passenger vehicles are part of a tightly-knit network contained within each vehicle. If a hacker were to gain access to the network through a vehicle's wireless communication system, perhaps using a mobile phone or tablet connected to the car's audio system via Bluetooth, vehicle functions could be manipulated.

In addition to taking physical control of the vehicle, the amount of data generated, exchanged, processed and stored in cars is growing – financial, personal and vehicle-specific information that is highly attractive to hackers. From the perspective of physical control and privacy, the number of attack vectors in our increasingly connected vehicles is on the rise.

This isn't the stuff of science fiction. In 2015, researchers proved that they could take control of a Jeep Cherokee remotely and send it off the road. That same year, hackers found vulnerability in BMW's ConnectedDrive technology and exploited the weakness to take control of vehicle functions. In 2016, hackers proved they could break into Volkswagen electronic keys and security systems to unlock vehicles remotely.

Cybersecurity challenges in the automotive sector

Car manufacturers understand that connected cars are as vulnerable to attack as any other machine or device connected to the internet. But while awareness is great, protection is extremely complex.

Product lifecycle is a significant issue. With cars sometimes on the road for 20 years or more and with multiple owners, how can manufacturers and suppliers guarantee they can deliver security updates for the lifetime of a vehicle?

Connected cars are constructed with many different digital systems, any one of which could be vulnerable to attack. And today's cars are still built by original equipment manufacturers (OEMs) and traditional suppliers, alongside a myriad of new software and tech companies in the market.

To overcome consumer mistrust it is imperative that connected cars are designed to be as secure as possible, and that automotive manufacturers overcome any technical and organizational challenges to make it happen. That may be easier said than done in an industry with a complex and fragmented supply chain

Our unique capabilities

At NTT Security we offer the automotive industry a broad range of managed security, risk and compliance services. Our experts have global reach and local resources and understand the specific challenges that you face in the automotive sector both at a global and regional level. Clients we engage with include leading OEMs and supply chain partners. Working with a network of trusted partners and NTT Group companies, we enable your cyber protection using a combination of consulting, managed, cloud, and hybrid security services.

30% of manufacturing organizations believe that revenue would drop by 10-50% following an information security breach.

NTT Security Risk:Value 2018 Report

Continuous consulting and compliance

The consequences of a cyber attack on a connected vehicle could dramatically disrupt operations. The costs in terms of regulatory violations and damaged consumer confidence can't be ignored. Creating, implementing and managing an up-to-date cybersecurity strategy around the manufacture of connected vehicles is a significant challenge. That's where NTT Security comes in.

As consultants to manufacturing organizations around the globe, NTT Security understands the requirements of compliance and risk mitigation for automotive companies. Our proven methodology will significantly improve the security of your systems and products, protecting revenues and operational capability.

NTT Security experts will help shape each security process from a strategic and technical standpoint. This ensures that you are able to create a security infrastructure with the right security policies, processes, architecture, and expertise in place.

External advice can be invaluable to evolve a comprehensive security strategy and, using our proven Global Enterprise Methodology consultancy delivery approach, we will enable you to understand your risk exposure and make informed risk management decisions.

1. Wired Magazine, 2012: https://www.wired.com/2012/12/automotive-os-war/

Managed Security Services

The threat landscape is evolving, threats are becoming more frequent and more sophisticated and given the scale and frequency of attack, automobile manufacturers are struggling to manage all aspects of cybersecurity in house. Partnering with NTT Security as your Managed Security Services provider gives you access to our world-class specialist organization and security experts.

We're here to provide you with end-to-end 24/7 monitoring, management, and support of your security infrastructure. What really sets our Global Managed Security Services apart are our unique threat detection, advanced analytics, and unrivalled threat intelligence capabilities focused on your industry. Wherever the future of connected cars takes your business, you'll have peace of mind and the convenience of being able to engage with one global provider for all your cybersecurity needs.

Manufacturing is one of the top five sectors most targeted by attacks in four out of five regions surveyed.

NTT Security 2018 Global Threat Intelligence Report

Cyber issues affecting the automotive industry

Car hacking is a major concern for security experts who warn that lateral movement within the network of a connected car could allow a hacker to infiltrate the car's weakest point and then move from entertainment systems to the control bus in charge of steering.

The first major car hack: 2015

US white hat hackers Charlie Miller and Chris Valasek remotely hacked a moving SUV from 10 miles away, controlling the brakes, radio, accelerator and windscreen wipers. They exploited several vulnerabilities and weaknesses from the connectivity element to the lack of secure separation between various on-board systems.

Patching complexities

At the time of Miller and Valasek's research, remote patching was not an option. Today it would still be impossible to remotely patch 100 percent of the code in a car. Also in 2015, nearly 51 million vehicle recalls were conducted by OEMs, leading to a spike in lawsuits due to security vulnerabilities exploited by attackers.

Disabling essential systems

in 2017 researchers identified a security issue in the Controlled Area Network (CAN) protocol that car components use to communicate with one another. This vulnerability would allow a hacker to shut off key automated components including safety mechanisms – effectively a denial of service attack rather than a hijack of physical components – but dangerous nonetheless.

"According to a survey by the Fédération Internationale de l'Automobile (FIA) on the acceptance of connected cars in Europe, 56 percent of respondents expect manufacturers to improve security in these vehicles."

NTT DATA, Automotive 4.0: Sensing the road ahead for tier 1 suppliers

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more about NTT Security or visit **www.ntt.co.jp/index_e.html** to learn more about NTT Group.