THE ROAD AHEAD

Bernard Montel *examines the driving factors evolving automotive cybersecurity*

The first known vehicle theft occurred in 1896 when Baron de Zuylen, founder of the Automobile Club of France, had his Peugeot stolen by a mechanic in Paris. This catalysed the development of car security systems, advancing from a lock and key device, defending against petty criminals in the early 20th century, to complex cybersecurity infrastructure which now deters attempted breaches from malicious actors globally.

Protecting electronic systems from malicious attacks, damage, unauthorised access or manipulation is at the core of automotive cybersecurity today. Yet as this technology becomes increasingly sophisticated, so do the methods of attack. From ransomware attacks on back-end infrastructure to remote break-ins, the stakes of automotive cybersecurity have never been higher, as manufacturers call for assurances of safety from developers, and consumers take cybersecurity into consideration when purchasing. With cyber-attacks on cars rising 225 per cent in the last three years, now more than ever, the automotive industry faces an important question: how do we become truly cyber-secure?

Global sales of connected cars are expected to surge to 115-million in 2025

According to ABI Research, global sales of connected cars are expected to surge to 115-million in 2025, from the 30-million that were sold in 2020. Today's cars also contain around 100-million lines of code, over 10 times that of an F-35 fighter jet. The growing number of connected vehicles and the expanding industry infrastructure signals an increase in opportunity for hackers to profit from vehicle theft and ransomware alike.

The risks to the development and deployment phases have to be mitigated and decreased in order for the automotive industry to keep pace with other sectors. Attacks against hospitals and educational institutions were an unthinkable concept a decade or two ago yet they're now two of the most targeted sectors. Any industry substantial enough to monetise could be taken advantage of.

Earlier this year, a teenager from Germany found flaws in a third-party software which enabled him to hijack the functions on a Tesla car model through opening and closing doors, adjusting the volume of music and, crucially, disabling security features. Honda also reported that researchers were able to hack the remote keyless entry system of particular models that could unlock doors, and even start the engine.

The main target of attacking infrastructure is to retrieve data. Although many lines of code are needed for vehicles currently on the production line, new types of cars (such as driverless and electric) are widely expected to have anywhere from 300-million to over 1-billion lines of code integrated into their systems. This provides prospective attackers with increasing entry points to capitalise on.

However, cyber-threat is not confined to the theft of physical cars. Cyber-criminals are now targeting Personally Identifiable Information (PII) such as customers' email addresses, bank information and GPS routing. This information can be used to dupe victims into phishing scams or hold organisations to ransom with the threat of data leaks, causing reputational damage and revenue loss from the diminished trust of customers.

Although typical combustion engine vehicles are susceptible to cyber-attacks, Electric Vehicles (EVs) and the infrastructure that underpins them, have an even bigger attack surface. EVs rely on charging points much like regular cars rely on petrol stations, and can be targeted with Point of Sale (POS) attacks while connected to the electrical infrastructure required to charge the battery. Research by the Carlos Alvarez College of Business' Department of Information Systems and Cyber Security found 13 significant areas of security threats and vulnerabilities, such as missing authentication and cross-site scripting, in EV charging points. Monitoring and managing these stations by patching vulnerabilities as they are found is crucial, as no system is infallible.

The cybersecurity attack paths that charging points possess are diverse and numerous. In November 2021, a bug in the app of a charging point provider in the UK gave access to email addresses, names and charging histories of vast numbers of customers. The breach put 140,000 users at risk of identification and exposed the volatility of EV cybersecurity infrastructure. Near-Field Communication (NFC) cards can also be used to steal customer data while EVs take hours to charge, lowering the barrier to entry for prospective hackers. Another risk to EV infrastructure is denial of service attacks (DDOS), incapacitating the infrastructure until compensation is paid out to the hackers.

The increase in 5G infrastructure and edge computing in connected vehicles will add another element in securing infrastructure, with 5G cars expected to comprise of a quarter of connected cars by 2025. Benefits like ultra-low-latency communications and increased Internet of Things will enable millions of connections per square kilometre and eliminate the need for trade-offs between high speed and reliability. However, the expanded network of real-time and non-real-time data will need to be managed effectively across vehicles and the cloud infrastructure to ensure seamless data exchanges.

Like global imaging software such as Google Maps, automotive manufacturers must have a holistic, bird's-eye view of their infrastructure, perceiving threats as mercurial and maintaining visibility of any and all vulnerabilities in the assets which they control. The automotive industry's true test of character will be whether manufacturers and their developers can secure infrastructure quicker than fraudsters can penetrate it.

AS CAR TECHNOLOGY BECOMES INCREASINGLY SOPHISTICATED, SO DO THE METHODS OF ATTACK

Automotive cloud infrastructure is a useful tool for developers, supporting the Internet of Things by keeping car and driver connected as they use their smartphones as a digital key to open and start their vehicle. The cloud can also enhance autonomous driving by providing continuous data flow and uninterrupted network service, helping passengers drive safely. The cloud, however, also houses increasing amounts of sensitive user data such as credit card details and home addresses, information that can be vulnerable due to the expanded attack surface the cloud provides.

Automotive cybersecurity is only as effective as its weakest link. Therefore, it is incumbent on all facets of the vehicle supply chain to ensure cyber readiness against the malignancy of cyber threat. Suppliers, auto makers and dealers are all susceptible to attacks, with dealers leveraging cloud-enabled dealer management systems for automated leads and sales, or automakers harvesting insights from an eclecticism of data generated through app stores and new mobility solutions, the attack surface grows.

Identifying and closing attack paths is critical, and organisations have a responsibility to protect and secure the data and systems which they control. Understanding this risk is as important to an organisations' integrity as financial and legal obligations. With effective communication from CISOs to their board, organisations will be cognizant of where they are exposed, and to what extent.

For car owners, knowing and understanding what the risks are, and then ensuring updates provided by device manufacturers are implemented, is key. Through a comprehensive awareness, from factory to parking lot, the automotive industry can successfully counter cyber-attacks.

By 2030, McKinsey & Company predicts 95 percent of new vehicles sold globally will be connected. The exponential growth of the smart automotive market will inevitably accelerate cybersecurity awareness, but if manufacturers do not secure their infrastructure before attacks expose their vulnerabilities, fraudsters could be driving off into the sunset with large amounts of money.

A hacker's aim is to profit from monetised data-theft. With connected cars holding valuable customer analytics, immediately patching systems closes the door to attackers aiming to expose customer data and enables the end user to trust the organisation which they buy from.

TODAY'S CONNECTED CARS CONTAIN AS MUCH AS 100-MILLION LINES OF CODE ON AVERAGE

We can learn from other sectors, such as the banking and finance industry. Over the years, it has evolved and is now an example of a sector purpose-built for collaborative cybersecurity effectiveness. Across several organisations, quarterly meetings during which threat intelligence is shared are a staple of operations in countering cyber-threat.

COOPERATION IS KEY

Cybersecurity in the automotive industry is in its development infancy, lacking a framework for the dissemination of threat intelligence in what is a highly competitive market. Collaboration between automotive entities, while it might seem foreign, is pivotal in emulating the cybersecurity success of other industries. Together they will be stronger to tackle emerging challenges and multiple variables, one of which being cloud security.

As the world marvels at the latest technological innovations of Tesla, Google and GE among others, the automotive market must redouble its focus on cybersecurity throughout the value chain. Like a seed, the developmental stage of automotive cybersecurity must steer in a cyber-resilience direction in order for organisations to stay one step ahead of bad actors.

Through this continual and constant change, developing a proactive rather than reactive cybersecurity infrastructure will be crucial to effectively counteract the growing threat of cyber-attacks. Security teams must change their mind set from purely physical attacks, to embracing cybersecurity as a key component of both the development and deployment phase of cars' AI functionality ●

Bernard Montel is Technical Director of EMEA for Tenable.

It's vital automotive manufacturers have a holistic, bird's-eye view of their infrastructure

Picture credit: Adobestock