Securing the Connected Car: Connectivity Best Practices, Challenges & Implications
By: Shaun Kirby, Director, Automotive & Connected Car, Cisco

Often dubbed a "data center on wheels," the Connected Car is one of the fastest-growing markets in the ecosystem that makes up the Internet of Things (IoT). The convergence of IoT and in-vehicle technologies, like remote diagnostics, on-board GPS, collision avoidance systems and 4G LTE Wi-Fi Hotspots, has paved the road for new and exciting opportunities in this industry. In fact, the Connected Car market is expected to reach $155 billion by 2022, while 75 percent of the estimated 92 million cars shipped globally in 2020 will be built with internet connectivity.

As the market grows, the biggest opportunity for profit comes from the ongoing services that can be offered and the ongoing revenue that subscriptions to these services can create. Although this is where the value lies, many consumers who purchase Connected Cars have been hesitant to "turn on" their connected services. Recent statistics tell the story. A 2016 Spireon survey showed that consumers are interested in Connected Cars (especially those with safety features), but 54 percent said they have not actually used Connected Car features. Similarly, Kelly Blue Book found that 42 percent of consumers support cars becoming more connected, while 62 percent said they fear that cars in the future will be easily hacked.

Concerned Consumers – Are Connected Cars Secure?
While there is evidence that the adoption rate for connected services is growing (willingness to pay for connected services went from 21 percent in 2014 to 32 percent in 2015), many consumers still have lingering concerns over the security of these vehicles. It doesn't help that Connected Cars have received some negative press. In 2015, Chrysler recalled 1.4 million vehicles after hackers demonstrated to *WIRED* that they could remotely hijack (and crash) a Jeep over the Internet. Then, in March 2016, the FBI, the Department of Transportation (DOT) and the National Highway Traffic Safety Administration (NHTSA) issued a public service announcement warning consumers about potential cyber security threats to Connected Cars.

Yet, consumers may not realize that security is not solely a Connected Car issue – it is an inherent concern with IoT, given the copious amount of data collected and shared between devices. When it comes to IoT, people fear not knowing what devices are doing and what they are actually capable of doing. The reality is that today's networks were not built for the tsunami of devices coming online, including the millions of Connected Cars. As networks evolve to better meet the needs of IoT and Connected Cars, automakers must take extra measures to ensure appropriate levels of connectivity at each step of the vehicle's lifecycle.

Securing the Connected Car at Each Step of the Vehicle's Lifecycle

Security must be a top priority – from the design of the vehicle, to the time the driver takes the wheel, and beyond – to improve adoption rates and drive profits. The key to securing the Connected Car's vast, potential "attack surface" is enabling the right levels of connectivity at the right times. In addition to knowing when connectivity should be on or off, it's also critical to know what a vehicle should be allowed to do with that connectivity at different stages throughout its lifecycle.

Automating this knowledge and ensuring proper connectivity to match each vehicle state is crucial to end-to-end security. It also eliminates the need to manually track and monitor connectivity — a complex task when you're shipping millions of vehicles around the world. Let's take a look at the role of connectivity in securing each step of the Connected Car's lifecycle.

- **Vehicle Design:** Auto manufacturers must ensure the right technologies – such as in-vehicle routing, security, IoT connectivity and more – are designed into the vehicle from day one. OEMs must consider the types of services they want to enable throughout the life of the car, choose the right connectivity partner and management platform, and design features into the vehicle accordingly. If these features aren't designed and integrated into the vehicle correctly, there is a greater risk for security issues later on down the road. For example, some manufacturers are designing Connected Cars with in-vehicle video capture capabilities and even the ability to measure biometrics, with the intention of using the collected data to improve and personalize the customer experience (if the user opts in). If a competitor or a malicious user hacks into these data streams, a great deal of information about the manufacturer's fleet and their customers is exposed.

- **Manufacturing:** Connectivity and security need to be engrained in the manufacturing process itself. Auto manufacturers must have converged networking and IoT solutions to automate manufacturing operations, mitigate risk and maximize uptime on the factory floor. Connectivity of mission-critical machines can enable zero downtime (which is vital when every minute of downtime on the factory floor costs $20,000) and therefore, enables more efficient manufacturing of Connected Cars. Further, OEMs can tap into data they collect to improve quality and produce a more reliable vehicle. There is also a safety aspect here, as manufacturers can use smart, real-time sensing and analytics to address safety and security concerns on the plant floor, and even use IoT and wearables to monitor health of employees and their locations. Access to this information must be limited only to authorized personnel.

- **Testing:** With Connected Cars, the ability to test and verify that connected services are working before the vehicle leaves the factory (and then being able to turn those connected services off during shipping) is required to reduce defective vehicles. In this stage, manufacturers must test each individual service before shipment, paying extra attention to services that deliver real-time updates to the driver, such as 3D maps, traffic or weather applications. If any of these are hacked or sabotaged during the car's lifecycle, it can jeopardize the driver's safety and lead to an accident.

- **Shipping:** Once testing is complete and the vehicle is ready for shipment, the ability to automate connectivity is essential. While vehicles are in shipping containers, manufacturers must be able to automatically disable connected services, while maintaining the ability to track vehicles during their journey. This prevents the abuse of connected services while vehicles are en route to the dealership. Remember: if a hacker can sabotage the vehicle during shipment from the OEM to the dealer, they could potentially plant a back door and obtain access to sensitive data during the car's life.

- **Demoing:** Once the vehicle arrives at the dealership, it is time to turn connectivity back on. Again, an automated system allows OEMs to safely resume connection so that salespeople can demonstrate all the services and devices to potential buyers. During this time, security measures are needed to prevent theft, hijacking or illicit remote control of vehicles. For example, information like the VIN is used to register the vehicle to a new owner's mobile app. If security is weak, anyone who could have recorded that VIN while visiting the showroom could later use it to control or possibly even steal the vehicle. Proper certificate-based security architecture can help prevent this situation.

- **Post-purchase – Maintenance & Aftermarket:** Connected Cars allow for proactive, predictive maintenance based on real-time data. Over-the-air (OTA) software updates help secure this information and provide patches and bug fixes to prevent data breaches. Moreover, the Connected Car is opening up new opportunities for aftermarket sales as companies move to leverage the vehicle's connectivity to deliver their own connected services. Undoubtedly, the growth of aftermarket connected services is stirring up additional security concerns, so creating the right security standards and partnering with aftermarket solution providers and third-party security experts will be key in keeping vehicles safe.

Enhancing the Driver's Experiences & Ongoing Monetization

The Connected Car's devices and services can provide value long after the customer has driven off the dealership lot. Once the vehicle is sold, manufacturers must be able to automate the transfer of billing for connectivity to the owner, while maintaining the ability to provide free trials of certain services for defined periods of time (which are billed to either the manufacturer or third-party content/service providers). This requires a platform that can enable split billing, while also allowing the OEM to consistently push new services to Connected Cars throughout the life of the vehicle to enhance the driver's experiences and create new, ongoing revenue streams. These new services, too, must undergo the same security considerations as those that were designed into the vehicle from the start.

As the opportunities for new subscription-based services and connections with external networks continue to grow, security will remain top of mind. In the near future, we will see smart drive-thrus, in which fast food restaurants can connect with customers' vehicles and use GPS coordinates to predict ETAs for even faster, fresher service. We will see gas pumps equipped with sensors that automate payments upon a vehicle's arrival, without the need to swipe a credit card. We already see cars connecting with social gaming platforms with in-app purchases to entertain passengers on long road trips. Everything from entertainment, to automated payments, to micro-transactions that take place between the vehicle and other infrastructures must be secured so that they are widely adopted, and in turn, drive profits for OEMs and aftermarket providers alike.

The Future of the Connected Car

The Connected Car is no longer science fiction – it is here today and can provide consumers with a secure, safe, reliable and enriched driving experience. However, to do so requires close attention to security and connectivity at each step of the vehicle's lifecycle. Ultimately, the ability to secure data that a vehicle generates comes down to constantly identifying and monitoring how that data should be used. To streamline these efforts, automakers should partner with security experts and invest in IoT connectivity management platforms that are capable of automating how and when a vehicle connects, and what the vehicle is allowed to do with that connection. Automated connectivity management platforms enable manufacturers to identify what vehicles are allowed to do with their connectivity. If they do anything else, the platform can detect that anomalous behavior and automatically shut off the connectivity, preventing illicit activity that could compromise the vehicle's security and safety.

The Future of the Connected Car

While IoT platforms and partnerships can help assuage security concerns and position automakers for success, there is an entire ecosystem of responsibility for the Connected Car. With new devices, connections and data points arising every day, no single party is 100-percent responsible for Connected Car security. Everyone – from the OEM, to the dealership, to the bank that enables automated payments, to the developers of aftermarket services – must do their part to keep cars safe, consumers happy and our "data centers on wheels" rolling securely.

About the Author, Shaun Kirby

Shaun Kirby

Director and Chief Technology Officer
Cisco Consulting Services

As Chief Technology Officer of Cisco Consulting Services, Shaun Kirby is responsible for sensing and evangelizing the key trends that will disrupt and transform the business world. Working across industries, he incubates game-changing solutions to propel customers ahead of the curve, while leading the interlock between the field and Cisco Engineering and Research and Development.

Kirby's current role is backed by years of deep industry experience. Prior to his role as CTO, he led Cisco's Innovations Architecture Practice, which developed robust reference architectures for visionary solutions. These were powered by Cisco technology as well as client-specific architectures and roadmaps for implementation.

Before joining Cisco, Kirby served as the Chief Architect for Vitria Technology's Professional Services team. He spearheaded the design and implementation of complex, leading-edge information systems for Vitria's flagship customers and facilitated unique engineering and field team collaboration that yielded industry-shaping products and solutions. In this capacity, he played a key role in the visioning for a new technology space, Business Event Management (BEM). As Director of Client Delivery and Quality Assurance at Vitria, he established the standards, tools, and best practices that enabled world-class solution delivery.

Kirby has served as a trusted advisor to CIOs, CTOs, and other technology executives, beginning with his extensive experience as a management consultant at Deloitte. He has authored articles, presentations, and technology briefs on a wide range of topics, including sensor fusion, augmented reality, and contactless gesture interfaces. As an inventor, Kirby holds several patents pending in these areas.

Kirby holds a B.S. in Electrical Engineering and Engineering Physics from Princeton University, and a M.S. and Ph.D. in Physics from the California Institute of Technology.