



Connected cars, 5G, and the road to cyber safety

By **Wendy Frank**, principal and Cyber & Strategic Risk 5G Leader, Deloitte Risk & Financial Advisory, Deloitte & Touche LLP



I live near Los Angeles, that sprawling city of dreams and angels, crisscrossed by highways that pulse with the stop-and-go movement of cars and trucks. And like many Angelenos, I hate it: the traffic, the accidents, the smog, the stress, the inefficiency.

For decades, there's been no real remedy for LA's notoriously maddening traffic, but with the mainstreaming of connected vehicles, improvement may soon be on LA's hot horizon. You see, organizations across the automotive-, technology-, telecommunications-, and government sectors have been developing wireless communication protocols that allows cars and trucks to transmit information between each other and to other parts of the traffic ecosystem, such as stop lights, parking spaces, pedestrians, and possibly even bicyclists. This communication system, known as vehicle to everything (V2X), is designed to improve safety, ease traffic jams, and decrease carbon emissions.

The effectiveness of V2X in preventing accidents, improving traffic flows and decreasing fuel consumption hinges on several factors, including the availability, reliability, and low-latency of 5G networks; [the security and privacy of those networks](#), and the security and privacy of the technology ecosystems in which connected vehicles operate. As progress on V2X continues and the manufacture of connected vehicles picks up, National Cybersecurity Awareness Month presents an opportune time to discuss the implications of the increasingly connected world and ways to enable its security, privacy, trustworthiness and resilience.

A closer look at V2X and efforts to secure connected cars

V2X is designed to make roads safer by enabling cars and other connected devices to communicate information about their speed, proximity, location, and other attributes. The technology aims to improve drivers' awareness of potential road hazards, thereby helping them avoid accidents. V2X can improve traffic flows and reduce emissions by warning drivers of congested areas, suggesting more fuel-efficient alternate routes, and even identifying available parking spaces in busy lots to curtail idling and circling.

To foster trust in V2X among consumers and regulators as standards evolve and the regulatory landscape around connected cars takes shape, Deloitte is working with automakers and their suppliers to help them weave security and privacy into product design, development and postproduction by applying the following leading practices:

- Integrating security and privacy requirements into product design
- Conducting assessments to identify security and privacy risks in their products
- Implementing privacy controls
- Deploying software and hardware security controls in their supply chains
- Adopting Secure-by-Design and DevSecOps practices as part of the software development lifecycle
- Documenting vehicle cybersecurity and privacy attributes
- Proactively monitoring their products postproduction for threats and vulnerabilities
- Establishing consistent processes for –
 - Handling product security and privacy events and incidents
 - Disclosing and patching security and privacy vulnerabilities

With respect to 5G, the communications infrastructure that much of the connected world will depend on, Deloitte is collaborating with Virginia Tech to conduct advanced research into 5G security. Through this collaboration, Virginia Tech and Deloitte are working to:

- Discover vulnerabilities in 5G protocols that attackers could exploit
- Investigate the extent to which 5G networks are vulnerable to different types of jamming attacks
- Develop a machine learning solution to autonomously detect jamming attacks
- Create attack graphs that show the potentially cascading impact of a compromise across a 5G network
- Build a zero trust network architecture for 5G based on blockchain principles and technology

Taking the stress out of driving

It's exciting to see the convergence of IoT and 5G come into focus through the [future of mobility](#), given the impact the automotive sector has on our lives as consumers and drivers. I'm encouraged by Deloitte's work with the auto industry, academia and other sectors to build security, privacy and resiliency into this new, connected world of transit. Deloitte has long championed these kinds of cross-sector alliances, which bring together diverse perspectives on complex issues and which are so critical to advancing technology innovation responsibly. They give me hope for a future where it doesn't take two hours of white-knuckle, nerve-fraying driving to get from my home to the office in downtown LA.

Wendy Frank is the Cyber 5G Leader and the Cyber IoT Leader for the Cyber & Strategic Risk practice of Deloitte Risk & Financial Advisory and a principal with Deloitte & Touche LLP.