The Growing Risk of Car Hacking

Did you know that your car(s) can be hacked? We're not saying that it's easy, nor is it inexpensive. But newer model cars, especially those with fancy head units, ADAS systems (adaptive cruise control, lane assist, etc.), and keyless entry features are particularly at-risk. This isn't news to the security community - and is becoming more well-known to consumers by the day. Every year, there are new car hacks presented at top security conferences (DEF CON, BlackHat, CCC, etc.) that security researchers developed in their garages, or in their free time at their workplace. Recently, every month has produced new hacks targeting automotive companies.

Article: 3.1 million customer records possibly stolen in Toyota hack
Article: Security holes found in big brand car alarms
Article: Security Holes Found in Big Brand Car Alarms

Everything is becoming hackable, and cars are no exception. You, the consumer, may not understand these emerging risks, and according to statistics this is not a primary concern (Jeep Grand Cherokee sales went up after the HackTheJeep presentation!. But it isn't just cars - it's every transportation system. Trucks, planes, boats, and trains all are vulnerable. Even infrastructure systems like EV charging stations can produce some pretty scary effects when they get hacked. In fact, this problem exists in most industries that build embedded systems, in both the private and public sectors. This presents serious challenges for the transportation sector, the defense sector, and the global economic marketplace.

Why? If we fail to secure the systems that transport our food, water, and medicine - as Alfred Henry Lewis put it, "There are only nine meals between mankind and anarchy."

What does the growing consistency of hacks affecting automotive companies tell us? The risk is growing. What are the causes of this? How can the automotive industry get a handle on it?

Code Growth and Vulnerabilities

The most dynamically evolving component of a vehicle is **software**. Most vehicle architectures have not changed significantly since the 1980s - save a handful of sensors, wireless radios, and LED screens. What **is** changing all the time is the software stack onboard a vehicle. In 2016, Ford Motor Company made a statement that the new F150 contains **150 million** lines of code- that's more code than an F-22 fighter jet, and Windows XP, Vista, 7, and OSX combined! (also see How Many Millions of Lines of Code Does it Take?). This number will only continue to grow as new features are integrated in future vehicles and Over The Air (OTA) update systems inject new code and features into our vehicles on a weekly (or daily) basis.

Why does this create an issue? It has been statistically proven that there is at least one vulnerability for every 1000 lines of code. But code can be checked for vulnerabilities! Right? Wrong - depending on the industry. What if a manufacturer didn't own the code to their own systems? What if testing this code would drive the price of the system up too high to maintain necessary margins? Do we live in a world where these reasons would prevent our cars from being testing thoroughly for risks?

Challenges with Transparent Testing

Concerning the fore-mentioned questions, the answers are often yes. Like many other problems, code ownership is a **supply chain issue**. There are many tiers of suppliers in the automotive industry that build various components, both software and hardware, and pass them up the supply chain towards the automotive Original Equipment Manufacturer (OEM). The OEM puts everything together, develops whatever wasn't sourced from the suppliers, builds the chassis, and brands the vehicle. But the OEMs themselves don't own the Intellectual Property (IP) rights to software that they buy, and suppliers often obfuscate their software to protect their own IP. Even if OEMs had access to all 150M+ lines of source code, you can imagine how difficult and expensive it would be for an OEM to find and model all of the security vulnerabilities that exist in such a massive code base!

The most common way to test obfuscated software is through a lengthy, expensive process that involves blind testing - called "black-box testing" - to identify a limited number of

vulnerabilities, usually after the product development process is complete. This testing is often rushed and piecemeal, with testers and engineers rushing to meet a launch date for a vehicle or platform. The challenge here is that this form of testing treats the symptoms and not the cause - cybersecurity weaknesses that result from an inherently insecure, partially tested underlying vehicle architecture, and that fixing issues late in the cycle is expensive and time consuming. The automotive industry is in dire need of new assessment methods and processes for managing automotive cybersecurity risk - black-box testing doesn't cut it, and automotive companies don't have the expertise in-house to identify and manage all of their risks - in their software, their hardware, or their infrastructure.

To this point, the automotive industry has done a great job of building attractive, dependable, and efficient vehicles - but now is responsible for building **secure** and **resilient** vehicles, to protect their customers and to protect their brand. This is an entirely new paradigm for an industry that has been focused on physical safety for nearly a century. It's clear that if left to the regulators and insurers to define and enforce cybersecurity requirements, the cost and complexity of compliance will be absolutely crippling for an already hurting automotive industry.

We have to wonder - given the race towards vehicle autonomation and automation - will standards for secure vehicle design come soon enough to protect us all? Will the automotive industry let the security community in to help set the foundations for a future of cybersecure, resilient transportation systems?

Solution: A Future of Managed Risks or the Wild West?

The challenges described herein are significant, but solvable. The largest gaps are in the creation and standardization of frameworks and processes in the automotive industry for secure vehicle design, risk management, and risk assessment. Only through partnerships and open and honest discussions between suppliers, OEMs, and stakeholders will we successfully achieve an affordable and sustainable solution to securing automotive systems, and other cyberphysical systems in the transportation, medical, defense, consumer IoT industries, and others.

We must foster partnerships between OEMs, suppliers, and third-party cybersecurity experts to explore new methods for more transparent testing and find new ways to establish trust around existing and future vehicle technologies. We encourage OEMs and suppliers to embrace the security community and to look for new approaches to collaboration that promote the development of affordable, sustainable and scalable capabilities for securing vehicle systems. By no means a trivial task, but one that can be solved through collaboration, partnerships, and a shared commitment to safe and secure vehicles.

Lastly, we encourage you, the consumer, to stand up and prioritize cybersecurity in the products you purchase and consume. Knowing that your vehicle is secure matters more than any feature you'd pay extra for today - and we must all take it upon ourselves to ask for it. Security is all of our problem - there is no escaping that fact. May we not settle for uncertainty about our own safety. There is a brighter future ahead for all of us if we address these challenges today.

About the Authors

Duncan Woodbury is an automotive cybersecurity researcher and Principal at DTLLC, a cybersecurity risk management firm serving the automotive industry. Duncan has developed some of the first tools for identifying risks and approaches to exploiting automotive systems, and is part of the world's first series of educational Car Hacking events, including the SAE CyberAuto Challenges and CyberTruck Challenges, to spread awareness about automotive cybersecurity and mentor new students and researchers in the area of vehicle security. Duncan has presented tools for automotive cybersecurity research at DEF CON, and volunteers at the DEF CON Car Hacking Village each year.

Don Woodbury is the Director of Innovation and Partnerships for the University of Maryland's Clark School of Engineering. His research interests include the cybersecurity of complex systems, including cars, aircraft, and industrial control systems. He is a former federal executive that led the creation of early cyberphysical system security efforts within the Departments of Defense and Homeland Security.