“Nothing is Unhackable” – Cybersecurity Experts Gather in LA

By

Lynn Walford –

Auto Futures – November 27, 2018

Reading Time: 4 minutes

At the Securing Mobility Summit part of AutoMobility LA, cybersecurity experts have been discussing the challenges and opportunities for the automotive industry. Auto Futures attended the event and talked to the experts about data protection, privacy and how hackers are motivated.

“Cybersecurity is very important to the deployment of advanced automotive features and companies are coming up with many creative ways to stop threats,” says Jeffrey Carr, a cybersecurity consultant and Founder of Spooks and Suits that produces the Securing Mobility Summit.

“At the Securing Mobility Summit we created a relaxed atmosphere where automakers and security experts can discuss important issues for the industry.”

“Security in transportation should be at two levels by design and with added security of services and consulting,” says Mikhail Savushkin, Solution Business Lead at Kaspersky Lab. He revealed, in Russia, on the dark web, hackers are selling identities of rideshare users as a way to not have to pay by the minute to use the vehicles.

Lauren Smith, Policy Counsel at The Future of Privacy Forum is working to develop policies for data protection and security. She noted cars are generating huge amounts of data for automatic emergency braking, eye monitoring, locations, mapping, geo locations, video sensors, vehicle health, and cabin monitoring.

“The car is learning about you. The good news is that the car can save your life,” says Smith. “However it creates privacy and security challenges.”

For shared vehicles, consumer expectations may be lowered as to what is private. There are already cameras in public buses and ridesharing services such as Uber or Lyft, adds Smith.

“There will have to be monitoring of vehicles to make sure nothing illicit happens,” says Smith about autonomous mobility in the future.

In the world of IT security, cybersecurity is usually carried out by finding a vulnerability, patching it or recalling the units. According to Danny Gur, VP of Business Development at Karamba Security, that kind of security is impossible in vehicles because: “It’s about life”. Karamba Security’s solution: “seals the code in modules to make it impossible to change the code.”

Consumers should be aware of not leaving data on their vehicles when they sell them or turn them back to the dealer or at the end of service.

“Cars have become extensions of our lives and our offices,” says John Shegerian, Co-Founder and Executive Chairman ERI. “Most studies show 40% of information that is supposed to be deleted on devices still exists and the same goes for data on cars.”

Shegerian says cars can retain information about the driver’s health, wellness and use of drugs or alcohol says and the companies with the biggest pockets will be liable.

Most carmakers will refer the owner to manually remove data, however, consumers usually will not be able to remove all the data from a vehicle say Shegerian.

Henning Daum, a Senior Technology Consultant with G+D Mobile Security, who was in the audience, suggested, that since smartphones have the ability to be reset and delete all the data in the phone, that cars should have a big red factory reset button to make removing all the data easy.

Cybersecurity is especially important if automakers want to add more services and upgrade them remotely, according to Jillian Goldberg, VP Marketing and Investor Relations for GuardKnox that offers cybersecurity and partners with Palo Alto Networks. She gives these examples: “Say, I want to upgrade my car to all-wheel-drive just for the weekend when I go skiing in Mammoth or I may drive a Porsche but don’t need racing features except for one day at the track.” The added services can be upgraded and paid for when the system is secure.

Blockchain is a solution to track the identity of a car, says Chris Ballinger founder of MOBI. The non-profit organization of automakers, tier 1 providers and blockchain companies seeks to promote standards and accelerate adoption of blockchain, distributed ledger, and related technologies.

In the afternoon participants were given a demonstration on '3PO' – GRIMM's mobile car hacking lab. Matthew Carpenter, a Principal Security Researcher at GRIMM prepared a simple set of instructions to reverse engineer the CAN Bus functions of a 2012 Ford Focus. A notebook computer is connected to three CAN Buses with software designed to bookmark the execution code. After the code is bookmarked the software can find and isolate the code. During the demo, a programmer was able to identify the code used to unlock the doors of the vehicle.

Bryson Bort, the Founder and CEO of GRIMM, created a SaaS arm of the company called Scythe. He says: "Nothing is unhackable, it is more of a question of motive." Scythe enables organizations to fully validate their defenses through simulated threats.

John Gomez CEO, Sensato Cybersecurity Solutions, says that they are not called hackers anymore but attackers. Organized cybercriminals are recruiting college graduates to attack businesses, offering high salaries and gifts to the hackers who can successfully attack the target.

Programmers can also be motivated by prizes and incentives. Down the hall, groups of programmers vied for prizes of $40,000, $30,000 or $15,000 Visa prepaid gift cards for first second and third place at Code AutoMobility LA hackathon. They were tasked with building apps using APIs provided by VISA and General Motors. The teams of programmers, who arrived on Sunday morning brought sleeping bags and napped on bean bag loungers. Although parking and restrooms are available there are no showers.

"We brought baby wipes to clean ourselves up," says one programmer who says she learned the baby wipe life hack while camping.

Auto Futures will have full coverage of AutoMobility LA and the LA Auto Show throughout the week.