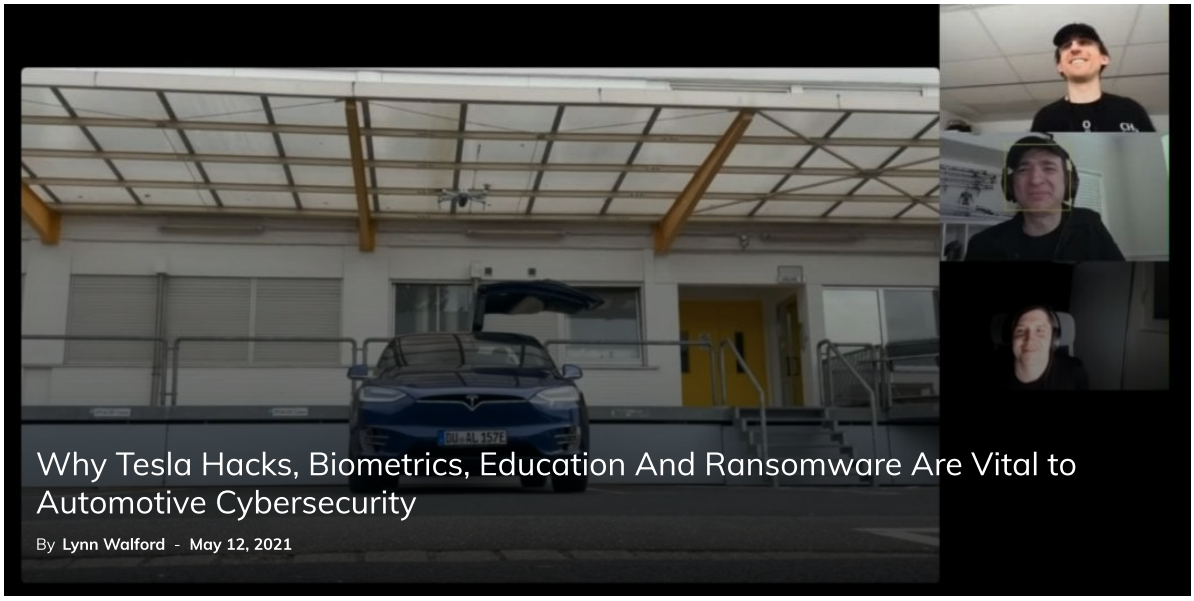

Why Tesla Hacks, Biometrics, Education And Ransomware Are Vital to Automotive Cybersecurity

By Lynn Walford - May 12, 2021

Reading Time: 4 minutes

The GENIVI Alliance Virtual All Member Meeting 2021 cybersecurity track showed shocking threats to automotive. Experts offered solutions. Hot topics included biometrics, threat protection, ransomware and Tesla hacking.

The GENIVI Alliance, is a non-profit alliance focused on delivering open source, in-vehicle infotainment (IVI) and connected vehicle software.

Education and Automotive Cybersecurity

Cybersecurity expert, Dr Ikjot Saini, noted there is no easy direct path to automotive cybersecurity education.

“The global automotive cybersecurity job markets are in a talent crunch and need reskilling, upskilling and cross-disciplinary competencies to manage the risks in this emerging cyberspace,” reports Saini.

She hopes to bridge the gap between education and automotive industry needs by creating communities and certificate programs.

Why Biometric Data is Personal and Protected

Jennifer Dukarski, CIPP/US, attorney at Butzel Long, showed the legal implications of biometric data in vehicles.

"Biometric data is increasingly being used for authentication, driver health monitoring and for monitoring driver attention in the case of autonomous driving," Dukarski tells Auto Futures.

"Privacy efforts must focus on the consent or having a legitimate basis for collection along with the end use of the data and its processing."

She adds, more companies are creating products that collect fingerprints, voiceprints or facial images. It is important to recognize that, depending on how this data is used, many different laws come into play and may require actions addressing both privacy and cybersecurity.

The laws governing biometric data are different in the U.S. and Europe.

"Different states in the U.S. have different privacy and consumer rights. Some states have stiff fines for statutory damages for biometric violations. Security efforts by automakers must be significant and should be the state-of-art within the European Union," says Dukarski.

She adds the first instinct in the U.S. is to think that it is all about HIPAA in the car. Health data collection in the vehicle does not automatically trigger HIPAA. However, it does not mean that health-related data laws are not important to understand.

Ransomware Warnings for IT Departments and Automakers

Claudia Rast, attorney at Butzel Long and Scott A. Bailey CISM, cybersecurity expert and partner at N1 Discovery, gave a presentation "Cybersecurity Roadmap: Navigating the Current Threat Environment". They revealed the best practices to prevent and respond to cybersecurity threats.

They showed how easy it is for hackers to break into networks. Points of entry include email, out of date servers, on-site Microsoft Exchange servers, backdoors, misconfigured firewalls, bring-your-own-device, work-at-home and legacy workstations.

“IT departments want to make it easier for employees and then don’t deploy multi-factor authentication,” warns Bailey.

After hackers find a way to get into a corporate IT infrastructure, they lurk and discover how much a company can pay for a ransom. Hackers used to only ask for ransom money and if they did not get it, give up, says Bailey.

He says hackers now are more sophisticated. They take the data then threaten to upload the sensitive data to the Dark Web. When not paid, they contact employees at home and send images of gruesome violent acts. The hackers threaten they will injure the employees or their families unless the ransom is paid.

Rast noted that one automotive dealership threatened by ransomware was asked for $15 million that they could not pay.

After a breach, laws require notification to law enforcement, authorities and consumers. There are also different ways insurance pays for cybersecurity help, says Rast.

Companies should check with their insurance companies to make sure their third-party IT cybersecurity company is vetted. In some cases after a cyber attack, the insurance company will only pay for an approved cybersecurity provider or pay only a percentage, says Rast.

Bailey mentioned there are ways to hack into systems that IT departments, programmers and automakers do not think about – such as the recent Tesla Model X drone hacking by Ralf-Philipp Weinmann, CEO of Kunnamon, and Benedikt Schmotzle of Comsecuris.

Why You Should Never Trust a ConnMann without ISO/SAE 21434

After the presentation, Rast further explained to Auto Futures why the drone Wi-Fi hacking of the Tesla Model X causes concerns.

There are a couple of concerns raised by the drone hack flying over the Tesla. First, what kind of risk analysis did the Tesla engineers conduct on this software before incorporating the ConnMan open-source software component into its vehicle, says Rast.

The vulnerability in the ConnMan component was accessed by the drone's Wi-Fi module that connected to the Tesla's infotainment system.

One of the issues that the ISO/SAE 21434 draft standard tries to address is security by design. While not fool-proof such a risk-analysis approach at the design stage should have identified the vulnerability. The other concern is the infotainment system that not only serves up in-vehicle entertainment, but also literally opens doors, trunks, seat positions, and other driver-initiated console activities, says Rast.

"The researchers that discovered the vulnerability and piloted the drone reached out to Tesla, and Tesla did patch the vulnerability. The remaining concern is that Tesla is not the only automaker that uses the ConnMan software," says Rast.

> We need to prioritize and make automotive secure at a low cost.

In another GENIVI presentation, Vincent Zhang, automotive cybersecurity technical specialist at Tencent Security Keen Labs in China, demonstrated how the company was able to remotely hack into a Tesla and then revealed some ways to prevent such hacks in the future.

Zhang suggests that companies set up an ad-hoc team to take charge of security. Then make everyone responsible for security. He advises implementing mature security concepts and solutions from the PC and mobile world into automotive scenarios.

Zhang says: "We have to protect at the process level, implement, test and verify security concepts. We need to prioritize and make automotive secure at a low cost."

Lynn Walford

NEXT STORY