Brooks Flanders

Subject: FW: Jefferies Mobility Technology - Weekly Newsletter May 20, 2018

-------- Original Message --------
Subject: Jefferies Mobility Technology - Weekly Newsletter May 20, 2018
From: Jefferies Global Mobility Technology Team
To:
CC:

Jefferies

INVESTMENT BANKING

Mobility Technology

Jefferies Mobility Technology Weekly

May 20, 2018

Guest Features:

Karamba Security

Autonomous Security for Autonomous Vehicles

By Ami Dotan, Karamba Security CEO and Co-Founder

As a groundswell of innovation swirls around autonomous vehicles, investors are jockeying for position to enjoy the gains. Statista projects the market for driver-assistance systems to grow to more than $59 billion USD in 2020. In the same year, Gartner estimates a quarter of a billion connected cars will be on the road.

No doubt, autonomous vehicles will transform how we live. Our cities could soon be filled with cars, trucks and even passenger drones (yes, flying cars) fully driven by artificial intelligence. We can expect a ripple effect through cultures and economies—affecting where we buy homes and how we spend time in transit. And while the opportunities are exciting, we can expect challenges along the way.

Safety, cybersecurity, and government regulation are big hurdles we have to address. And until we solve these problems, the success of the autonomous vehicle is married to uncertainty.

What Is Certain?

There is a high level of certainty there will be real-world cybersecurity attacks on autonomous vehicles. With over 100 million lines of code in today's premium vehicles, countless vulnerabilities exist. We also know that hackers have the expertise to launch attacks today.

Real and Imminent Threats

Analysts predict professional hackers, nation states, and terrorists will target fleets of trucks—most likely for ransom or to hijack goods. As cars become an entertainment center, private data and payment information will be subject to cybercrime. Whether its data theft or blackmail, a single publicized incident will shake the fragile confidence in connected and autonomous vehicles, affecting consumer trust and slowing the adoption rate.

The Good News?

It's preventable. As a team of cybersecurity experts, we feel it's imperative to solve the vehicle security conundrum with technology custom-developed to fit the characteristics of future mobility.

Following years of research and development, we've designed end-to-end cybersecurity that autonomously blocks the critical threats before they can do damage. And we've proven this can be done without placing a performance burden on highly constrained computer systems and networks.

Automakers can start securing autonomous and connected vehicles today by:

1) Hardening the vehicle's mission-critical systems

2) Building security into the fabric of the vehicle's software

Why Hardening?

To initiate an attack on a vehicle, hackers enter via external connection points, like telematics, WiFi, vehicle-to-vehicle communications, or over-the-air (OTA) updates. Once inside, they take control of the vehicle's gateway, gain access to an unprotected CAN bus network, and take command of Electronic Control Units (ECUs) that govern braking, steering and accelerating.

The best strategy is to stop hackers where they begin their attacks, on a vulnerable ECU. There are two primary methods hackers use infiltrate a vehicle's external connection points: 1) by launching an in-memory attack (aka fileless threat); or 2) by dropping malicious code (aka dropper) into an ECU.

Applying traditional security methods to the autonomous car is simply inadequate. It takes too long to discover, patch and remediate a known vulnerability. Plus, heuristic detection and signature-based security solutions too often fail to stop unknown, zero-day threats. It is also well known that heuristics can lead to false positives. If security blocks a legitimate command, like braking, it could be disastrous. These datacenter cybersecurity paradigms are not suited for life-impacting threats.

How Do You Harden Security?

Patented Karamba Carwall technology automatically hardens the ECU environment to detect and block all attacks—before any damage can occur. And unlike competing solutions, Carwall is specifically designed to run in resource-constrained embedded systems without impacting car performance. By hardening the code, we can create a self-defending vehicle. This means cybersecurity remains stable and reliable over the life of the car or truck.

Securing In-Vehicle Networks

In addition to securing ECUs, it is critical to secure network communications. Karamba SafeCAN is the industry's first ultra-light network security software to encrypt and authenticate communications between ECUs—without slowing performance. From the key exchange to message authentication, SafeCAN is designed to maximize protection while minimizing the burden on limited-resource systems.

End-to-End Vehicle Security

When deployed together, Karamba Carwall and SafeCAN deliver end-to-end protection—from the external connection points where hackers first gain entry—to the in-vehicle networks where hackers take control. This solution detects and stops threats, improving both safety and security on the road.

The Self-Defending Vehicle

We've created a new industry model for autonomous cybersecurity. After all, if we are to achieve our common goals, the self-driving car must also be a self-defending car.

With this groundbreaking technology available today, investors can help the automotive industry achieve the dream of self-driving vehicles. We are so close to realizing its full business potential.

Awards

Karamba Security was named a 2018 Gartner Cool Vendor for IoT security. Also this year, Karamba SafeCAN received the Tech CARS Award by Auto Connected CAR News for "Best Automotive Cybersecurity Solution."

In 2017, Karamba Carwall won "Best Automotive Cybersecurity Product" by TU-Automotive and "New Product Innovation Award in the Automotive Industry" by Frost & Sullivan.

karambasecurity.com

Jefferies Mobility Technology Group

A Global, Cross-Functional Coverage Team

MOBILITY TECHNOLOGY

Storm Duncan
Managing Director
Head of Mobility Technology
+1 (415) 229-8700
Storm@Jefferies.com

Shiva Kumar
Senior Vice President
Mobility Technology
+1 (650) 573-4816
shiva@jefferies.com

Chris Hayes
Vice President
Mobility Technology
+1 (415) 229-1419
christopher.hayes@jefferies.com

Aditya Sinha
Associate
Mobility Technology
+1 (650) 573-4863
asinha@jefferies.com

EUROPE

Dominic Lester
European Head of Investment Banking,
European Head of TMT and
Global Joint Head of Technology
+44 (0)20 7029 8330
dlester@jefferies.com

ISRAEL

Natti Ginor
Managing Director
Head of Israel Markets
+1 (212) 284-2112
nginor@jefferies.com

INDIA

Mohit Pande
Managing Director
Investment Banking, India
+91 22 43566032

AUTOMOTIVE

Tom Fennimore
Managing Director
Global Head of Automotive IB
+1 (212) 708-2608
tfennimore@jefferies.com

AUTOMOTIVE AFTERMARKET

Rex Green
Managing Director
Co-Head of Automotive Aftermarket
+1 (617)-342-7886
rhgreen@jefferies.com

Jonathan Carey
Managing Director
Co-Head of Automotive Aftermarket
+1 (617) 342-7865
jcarey@jefferies.com

Treavor Hill
Senior Vice President
Automotive Aftermarket
+1 (617) 342-7929
thill@jefferies.com

SOFTWARE

Steve West
Managing Director
Head of Software
+1 (415) 229-1425
stevewest@Jefferies.com

SECURITY

John Metz
Managing Director
Head of Infrastructure and Security Software
+1 (415) 229-1412
jmetz@Jefferies.com

CHINA

Wei Su
Managing Director
Joint Head of China Investment Banking
and Asia Head of TMT and Cleantech

mpande@Jefferies.com

+852 3743 8745
wsu@Jefferies.com

Clients First–Always℠

Jefferies.com