

CRUNCH NETWORK

# The biggest threat facing connected autonomous vehicles is cybersecurity

Posted Aug 25, 2016 by [Rob Toews \(@\\_RobToews\)](#)



**Rob Toews**  
CRUNCH NETWORK  
CONTRIBUTOR



**Rob Toews** is jointly pursuing degrees at Harvard Business School and Harvard Law School. He is the co-

Connected, autonomous vehicles are around the corner. Many of the most innovative and deep-pocketed companies in the world are racing to bring them to market — and for good reason: the economic and social gains they will generate will be tremendous.

*Techcrunch*

August 2016



# CAR HACKING AT DEF CON 26

by: Mike Szczys

f t 8+

9 Comments

August 11, 2018



# Hackaday

August 2018

# Keen Security Lab

August 2017

Tencent 腾讯



## FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS

Sen Nie, Ling Liu, Yuefeng Du  
Keen Security Lab of Tencent  
{snie, dlingliu, davendu}@tencent.com

### ABSTRACT

In today's world of connected cars, security is of vital importance. The security of these cars is not only a technological issue, but also an issue of human safety. In our research, we focused on perhaps the most famous connected car model: Tesla.

In September 2016, our team (Keen Security Lab of Tencent) successfully implemented a remote attack on the Tesla Model S in both Parking and Driving mode.<sup>[1-3]</sup> This remote attack utilized a complex chain of vulnerabilities. We have proved that we can gain entrance from wireless (Wi-Fi/Cellular), compromise many in-vehicle systems like IC, CID, and Gateway, and then inject malicious CAN messages into the CAN Bus. Just 10 days after we submitted our research to Tesla, Tesla responded with an update using their OTA mechanism and introduced the code signing protection into Tesla cars.