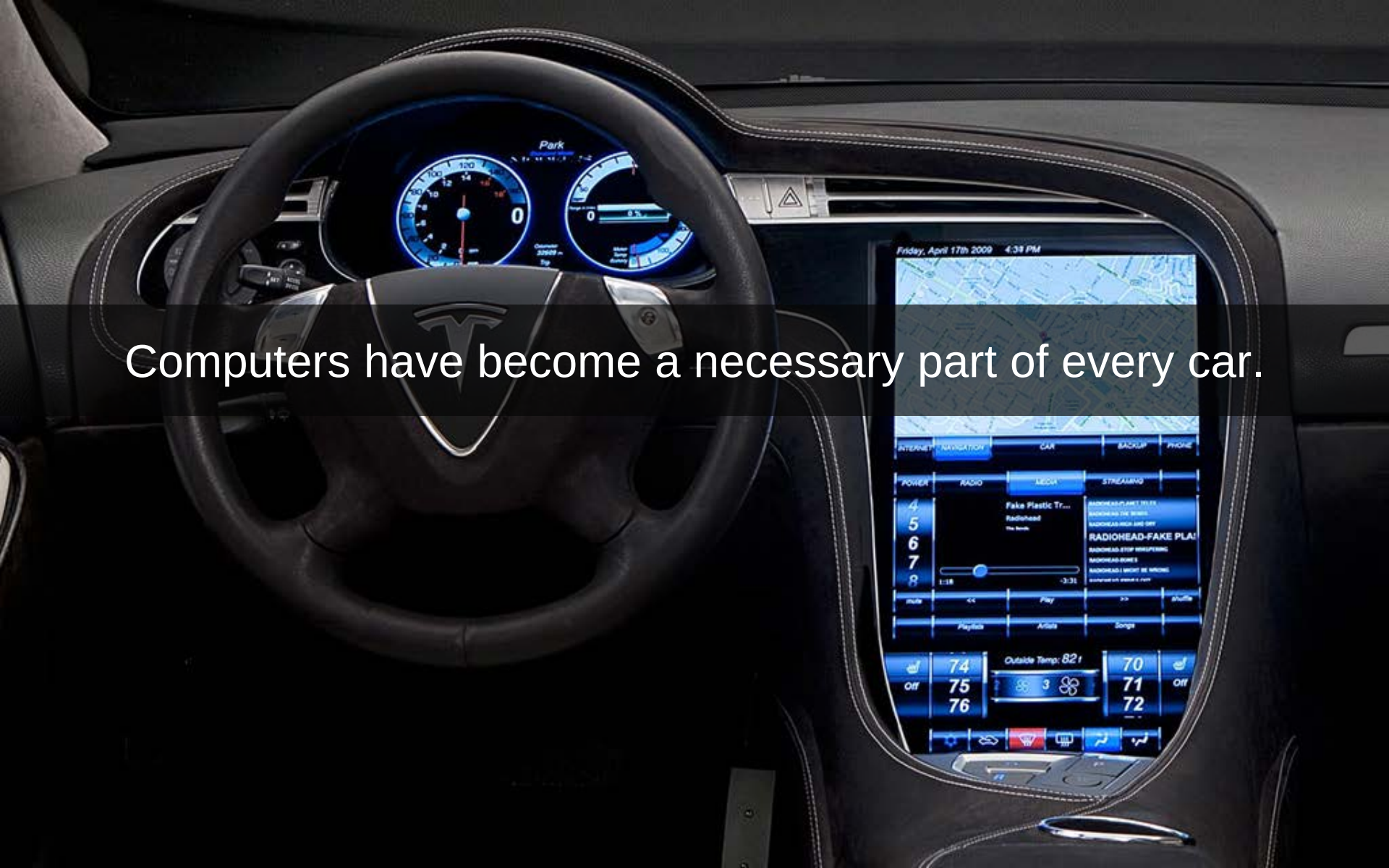
Car Hacking

EECS 3482 Intro to Computer Security

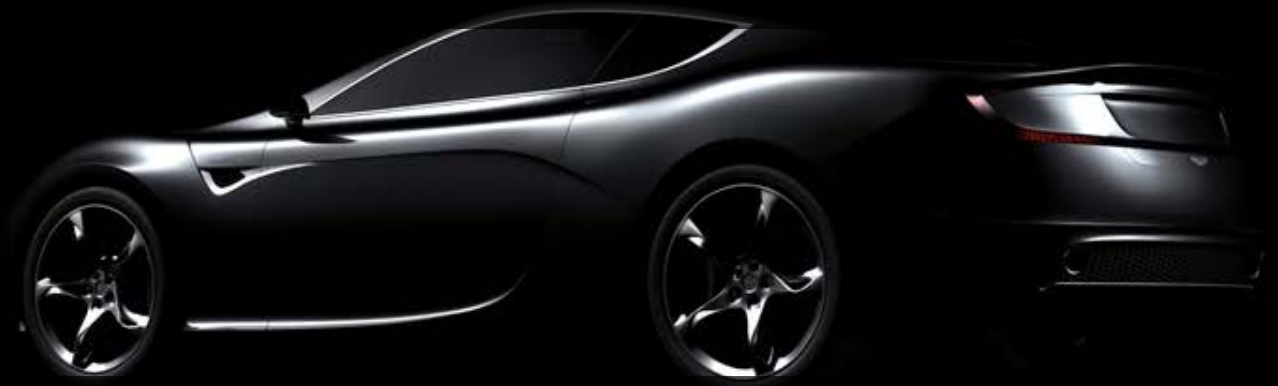
Team 11:
Najiba, Mike, Edward



Computers have become a necessary part of every car.

A vehicle can have upwards of 35 computer controllers

- engine, steering, doors, braking system, sensors, navigation…



Today these controllers are increasingly interconnected to a central control unit.

Drawback

- Like computers, cars are vulnerable to software attacks and unauthorized access
- The more wireless connections a car offers, the greater the opportunity for intrusions

Updating/patching software currently involves:

- Tracking down owners and notifying them
- Transmitting security patch at car dealerships, via USB key
- Infrequent OTA firmware updates

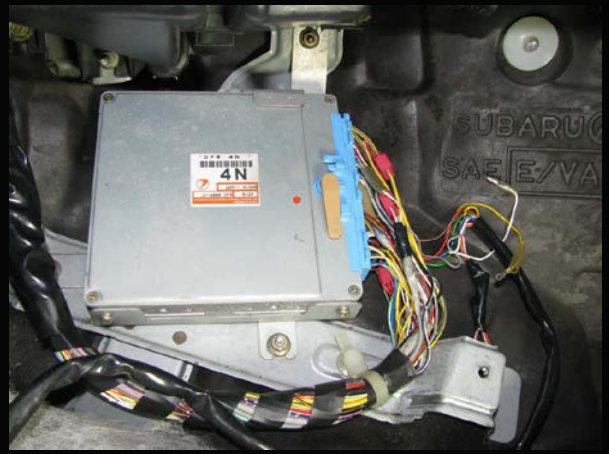
Components you can control with central ECU (electronic control unit):

- Doors, lights, windows, dashboard, horn, engine, steering, braking systems…

- Once access is gained, incorrect data may be fed to central CU: false temperatures, tire pressures, speed, collision distance

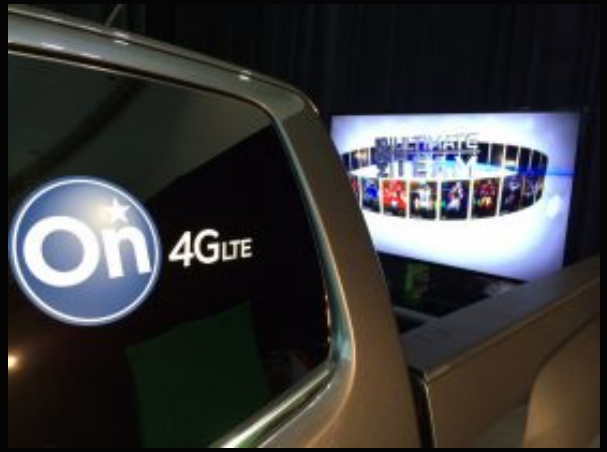
Wired Access:

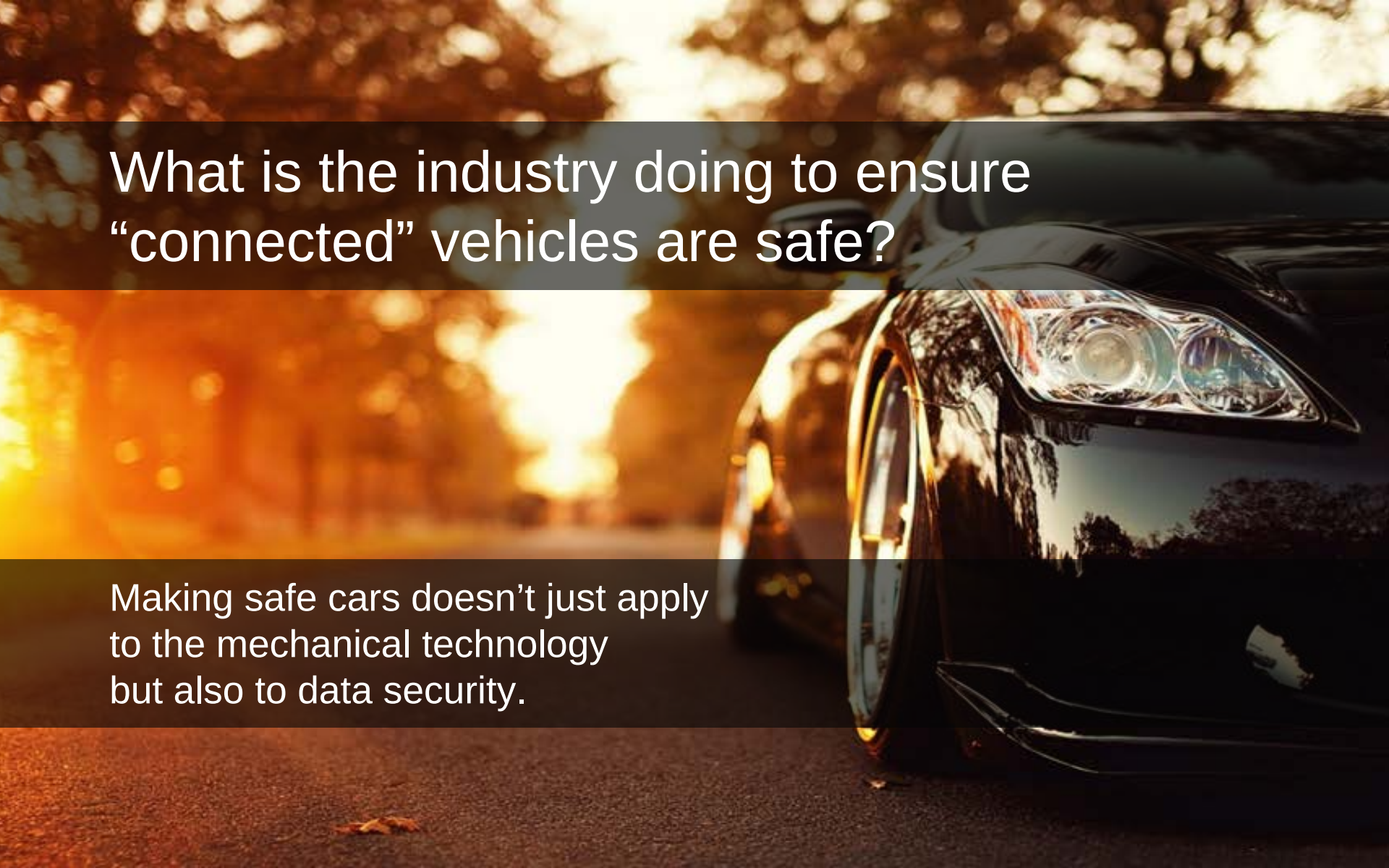
- connect a computer to the ECU



Wireless Access:

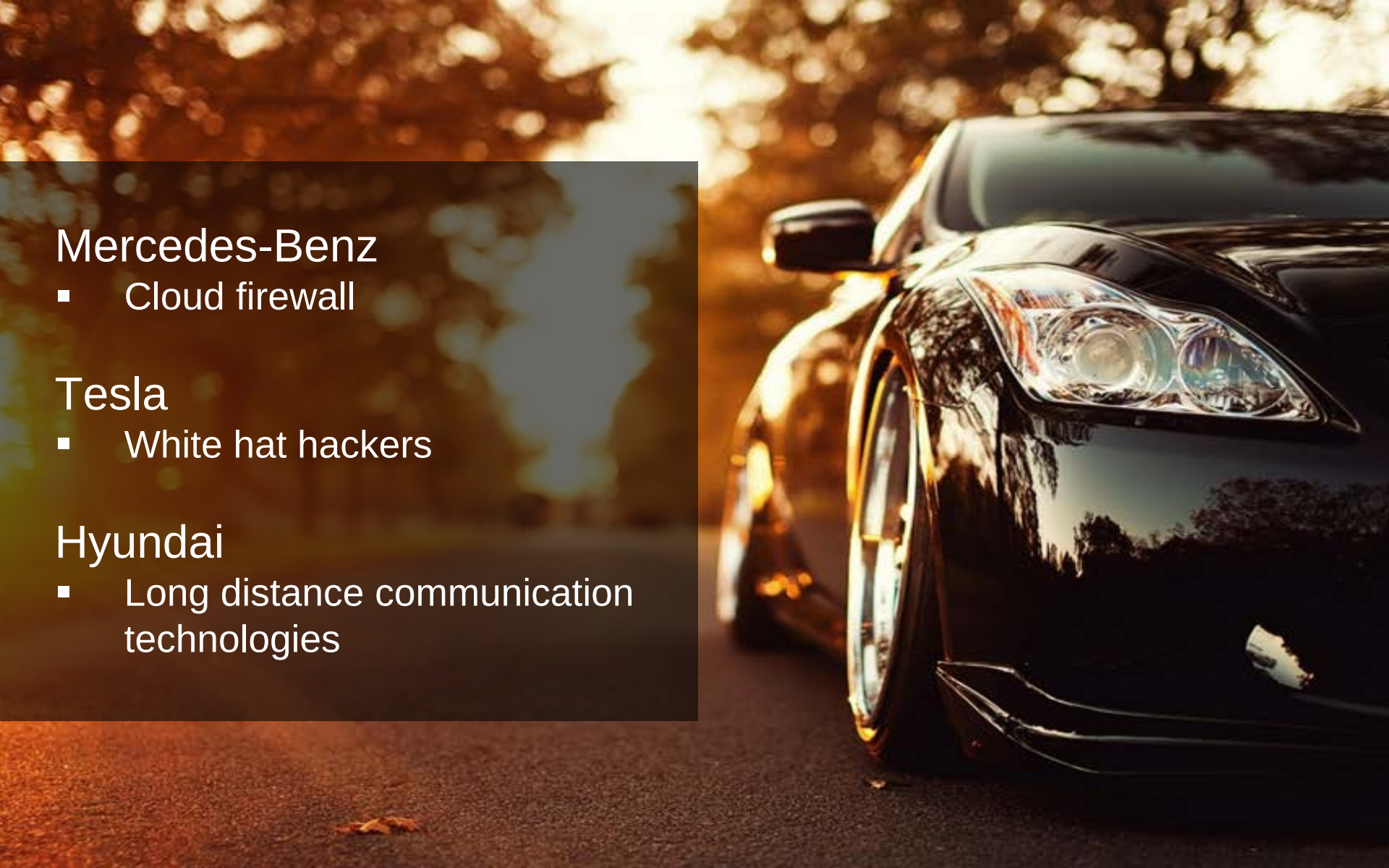
- access central ECU through wireless entry point like OnStar





What is the industry doing to ensure “connected” vehicles are safe?

Making safe cars doesn’t just apply to the mechanical technology but also to data security.



Mercedes-Benz

- Cloud firewall

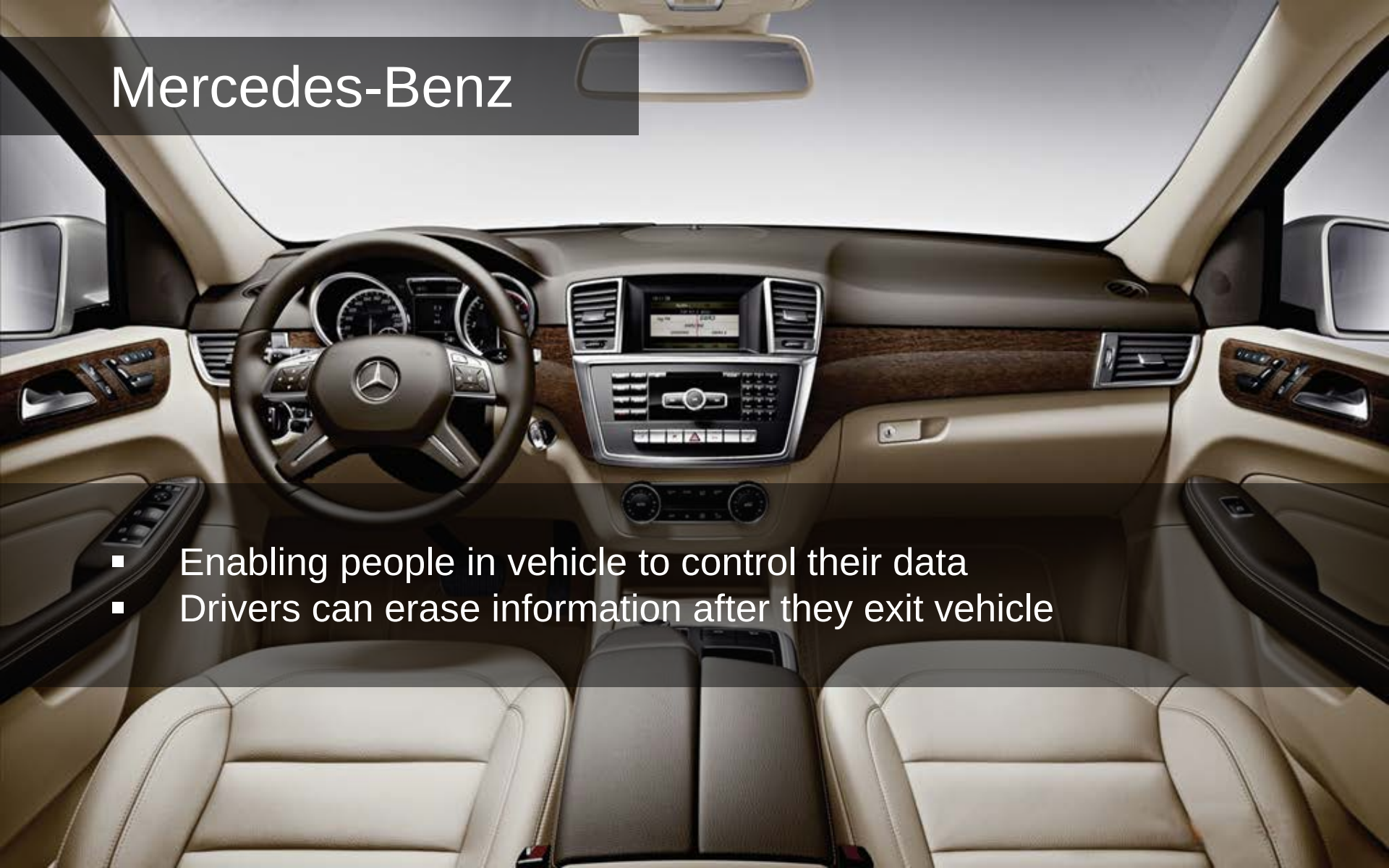
Tesla

- White hat hackers

Hyundai

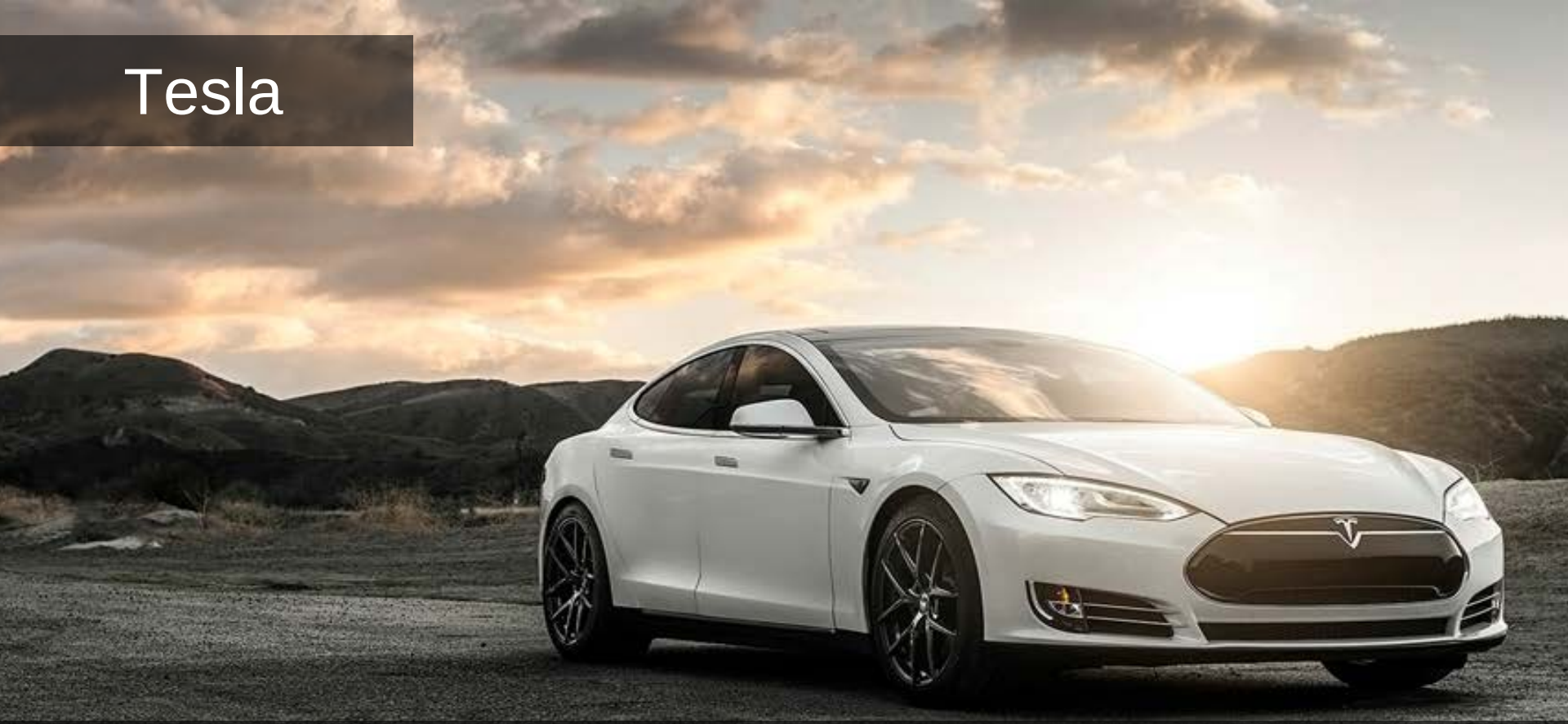
- Long distance communication technologies

Mercedes-Benz



- Enabling people in vehicle to control their data
- Drivers can erase information after they exit vehicle

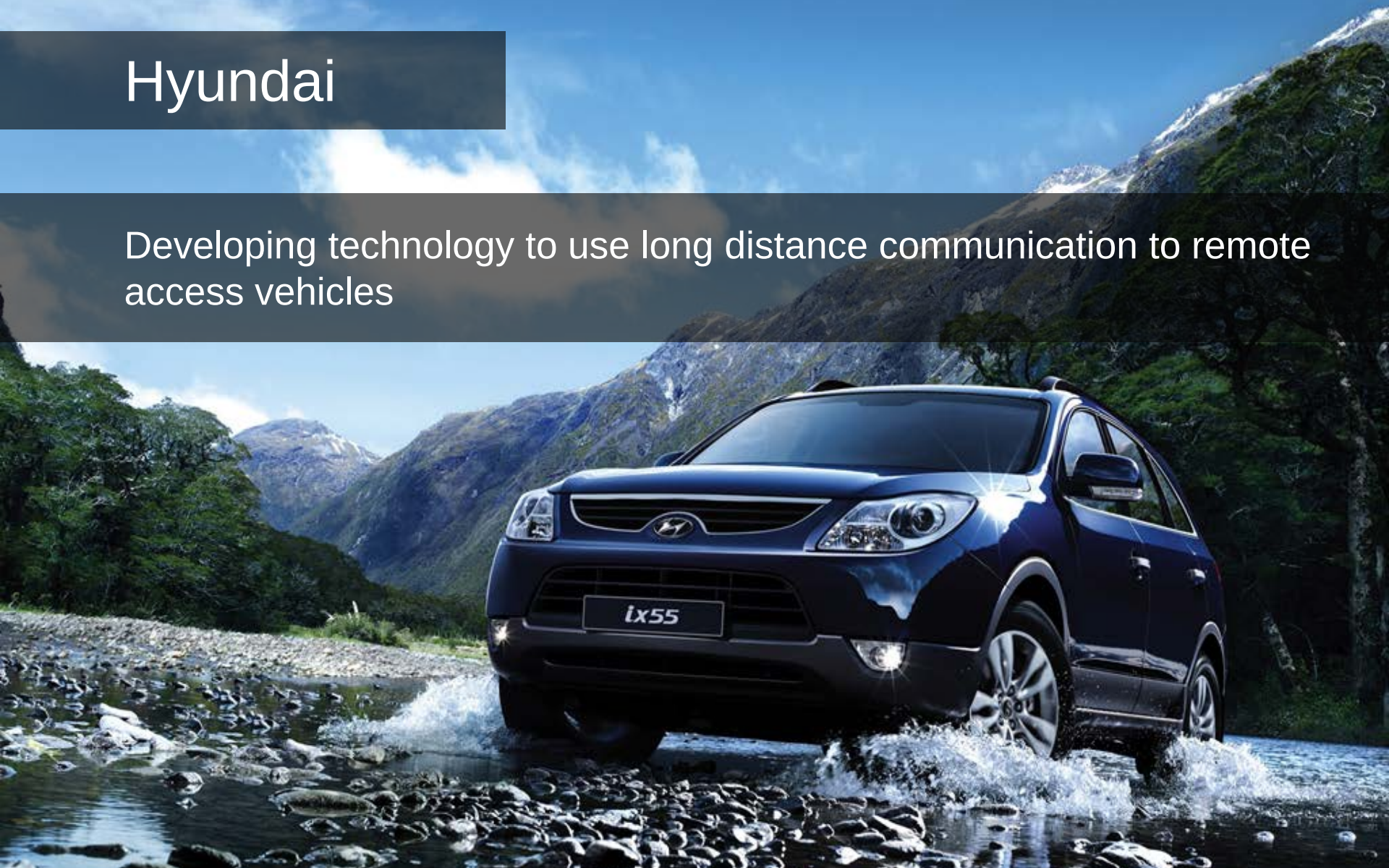
Tesla



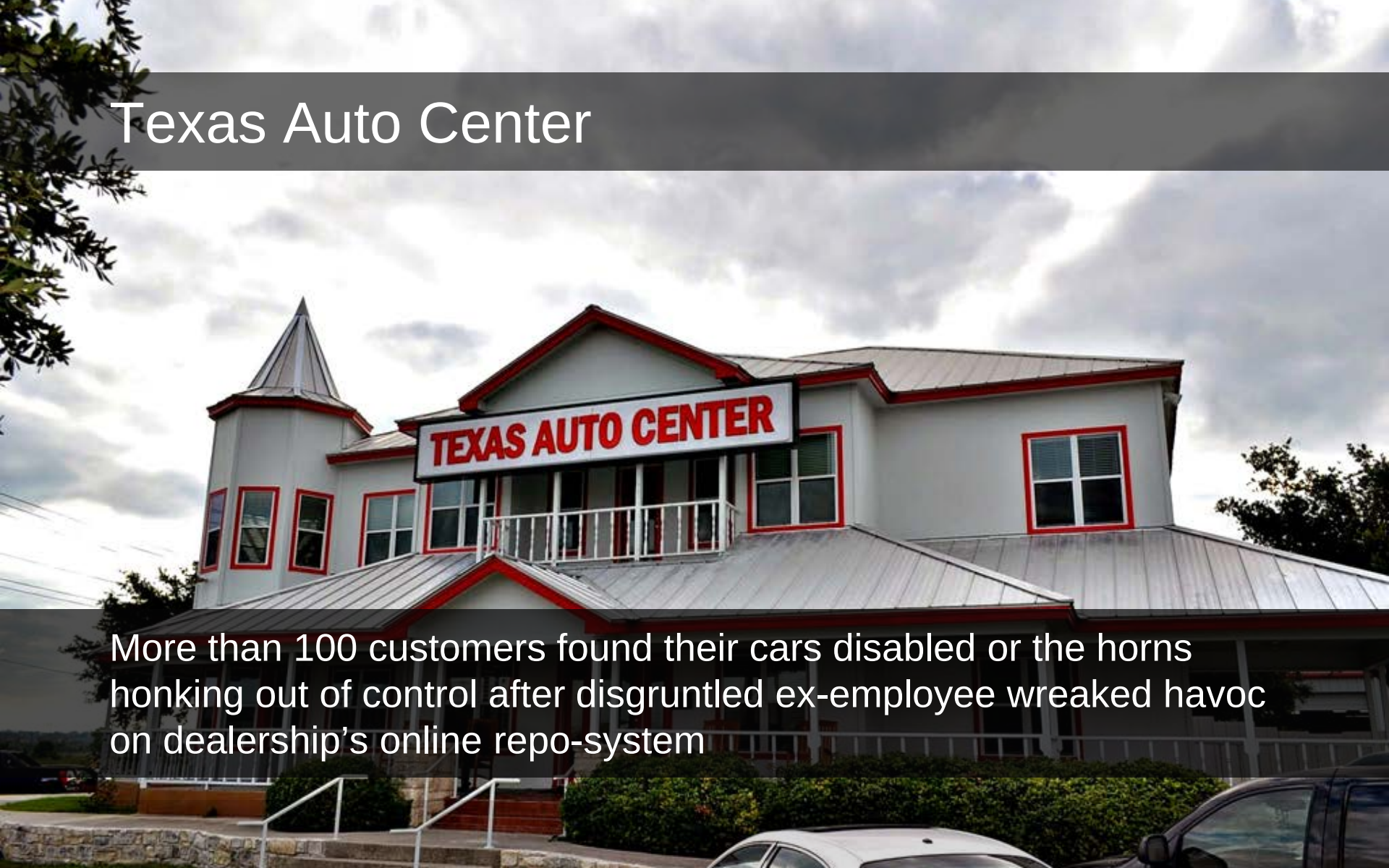
- Hires hackers from all over the world to test information security
- Hires specialists to hack on-board systems in three month projects

Hyundai

Developing technology to use long distance communication to remote access vehicles



Texas Auto Center

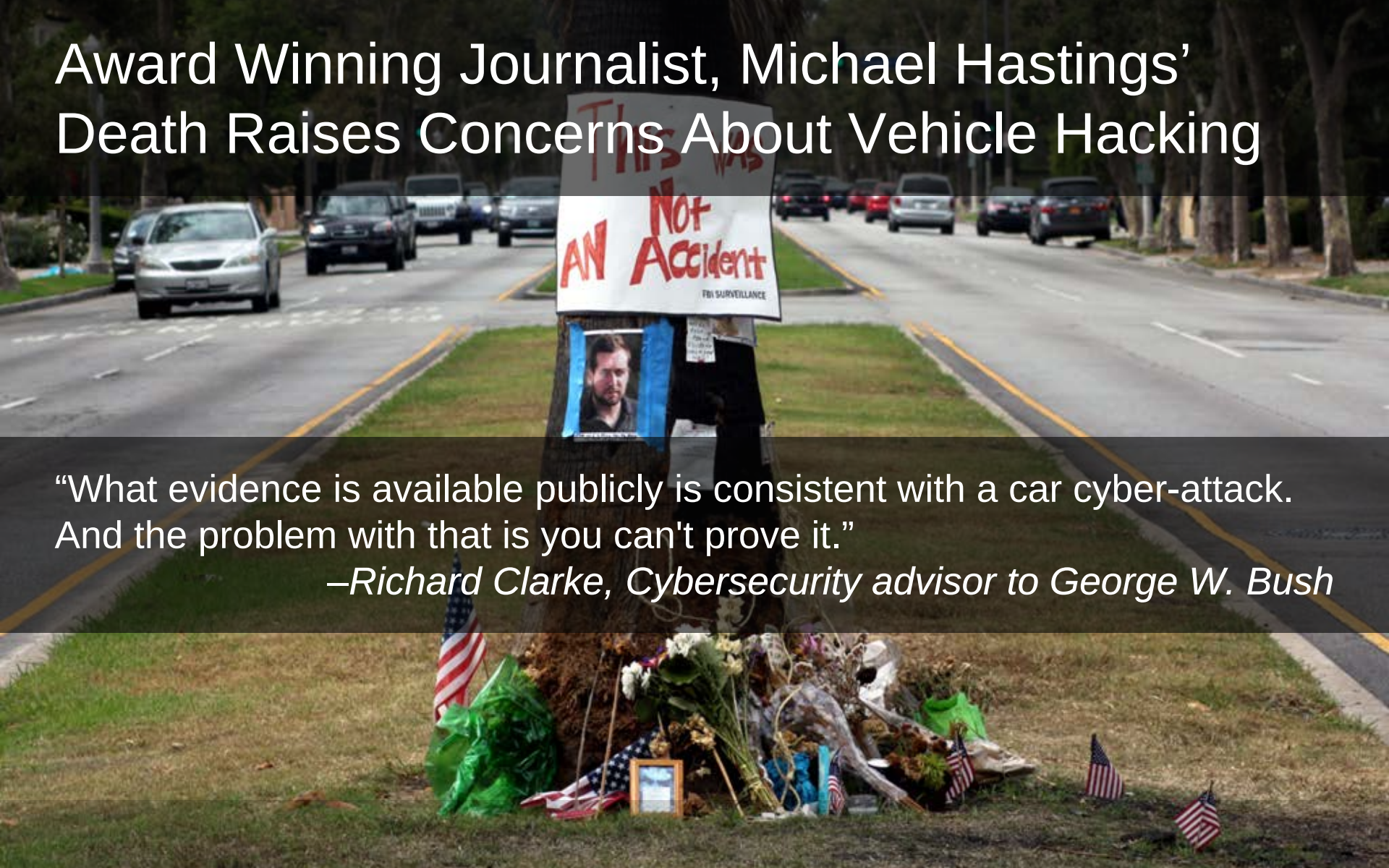


More than 100 customers found their cars disabled or the horns honking out of control after disgruntled ex-employee wreaked havoc on dealership’s online repo-system

DARPA – Defense Advanced Research Projects Agency

DARPA security experts remote hack a vehicle by sending complex radio message to OnStar system then inserting code to ECU

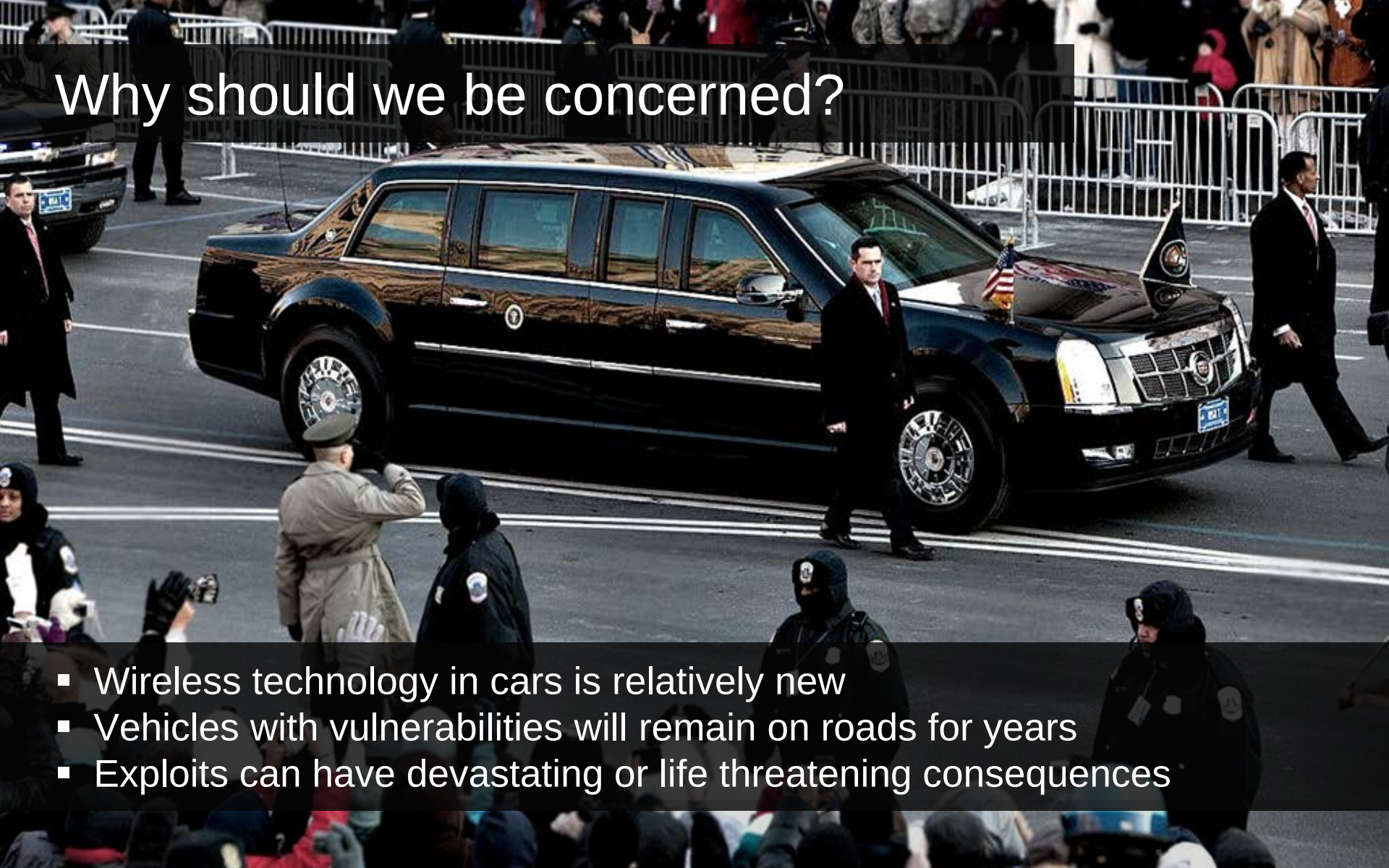
Award Winning Journalist, Michael Hastings' Death Raises Concerns About Vehicle Hacking



"What evidence is available publicly is consistent with a car cyber-attack. And the problem with that is you can't prove it."

–Richard Clarke, Cybersecurity advisor to George W. Bush

Why should we be concerned?

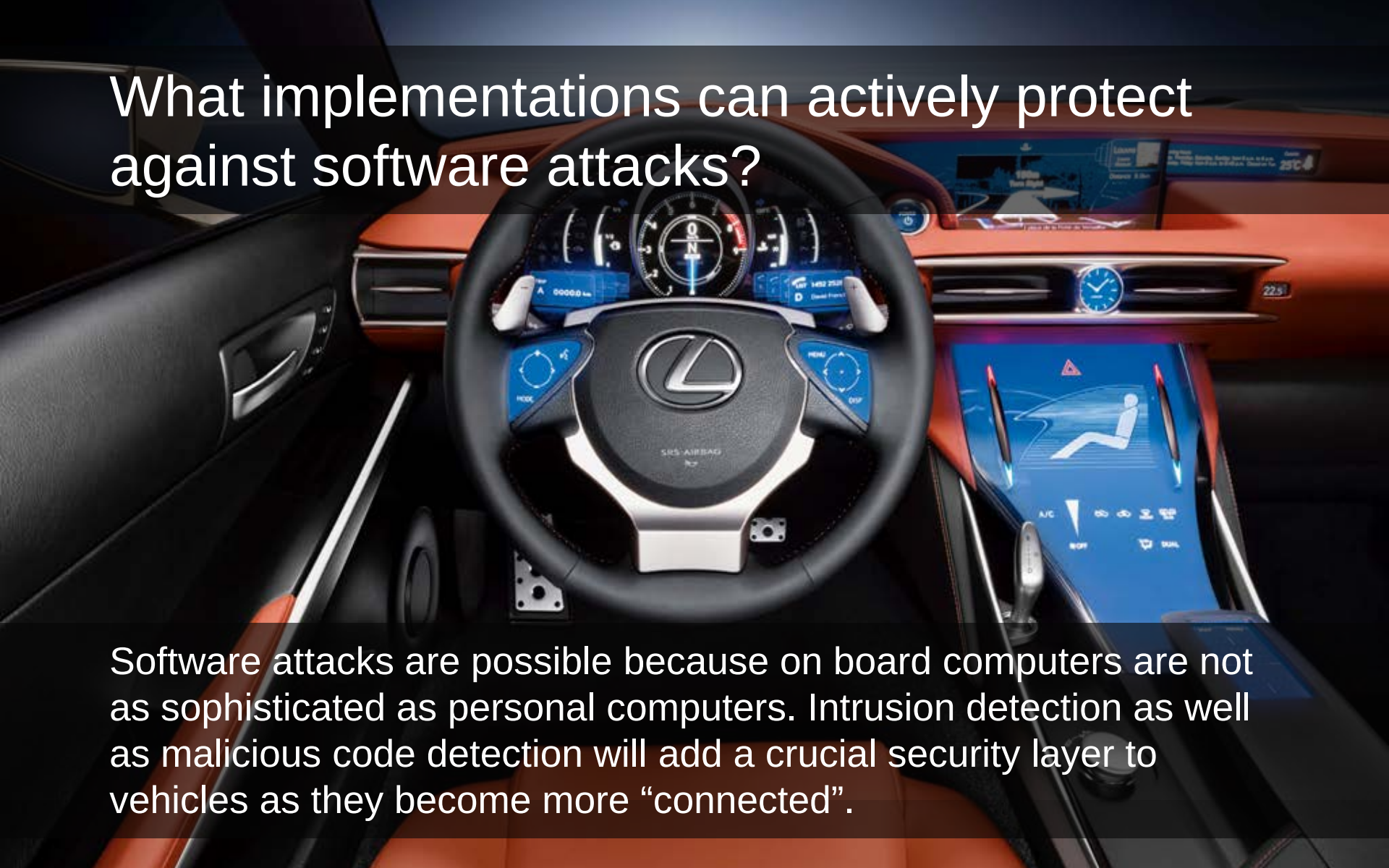


- Wireless technology in cars is relatively new
- Vehicles with vulnerabilities will remain on roads for years
- Exploits can have devastating or life threatening consequences

How can consumers safeguard against hacking?

- Prevent others using physical connections with your car
- Prevent others using on-board diagnostics interface
- Do not use remote controller apps
- Understand your vehicle’s wireless functions
- Uninstall wireless functions

What implementations can actively protect against software attacks?



Software attacks are possible because on board computers are not as sophisticated as personal computers. Intrusion detection as well as malicious code detection will add a crucial security layer to vehicles as they become more “connected”.

Sources

http://www.cbsnews.com/news/car-hacked-on-60-minutes/
http://www.forbes.com/sites/centurylink/2015/01/02/3-hurdles-standing-in-the-way-of-the-internet-of-things-2/
http://ca.norton.com/yoursecurityresource/detail.jsp?aid=car_computer
http://money.cnn.com/2015/02/09/technology/security/car-hack/
http://www.techtimes.com/articles/14637/20140902/tesla-motors-hiring-hackers-to-improve-security-systems.htm
http://www.extremetech.com/extreme/91306-hackers-can-unlock-cars-and-meddle-with-traffic-control-systems-via-sms
http://www.scribd.com/doc/236073361/Survey-of-Remote-Attack-Surfaces