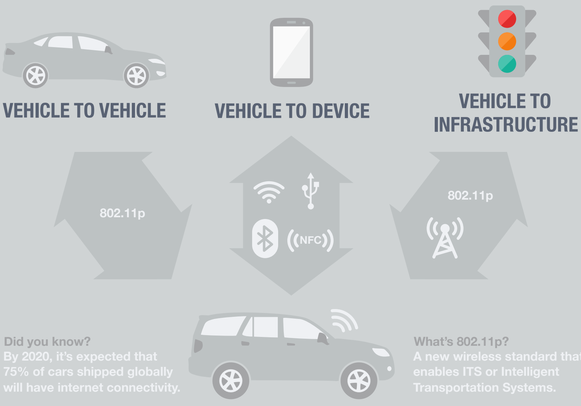
UNDER THE HOOD OF A CONNECTED CAR HACK

Today's modern vehicles can contain over 100 processors, many of which control critical systems within the vehicle. Essentially a computer on wheels, the connected car presents new security vulnerabilites all drivers should be aware of.

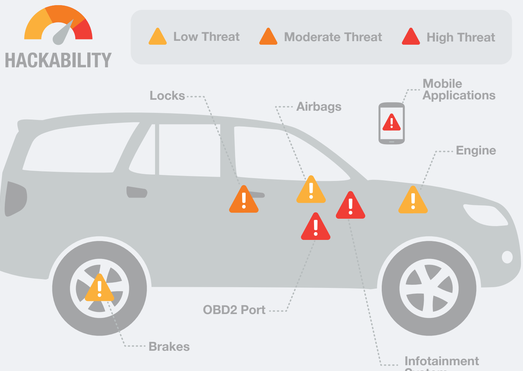
MULTIPLE POINTS OF VULNERABILTY



Did you know?
By 2020, it's expected that 75% of cars shipped globally will have internet connectivity.

What's 802.11p?
A new wireless standard that enables ITS or Intelligent Transportation Systems.

PRIMARY ATTACK POINTS



INFOTAINMENT SYSTEM

Typically the primary communication interface of a connected car, the infotainment system hosts high-value and sensitive applications that are easily hacked if not protected.

OBD2 Port

Located underneath the dashboard, the OBD2 port is a physical connection that is highly vulnerable. This diagnostic port is used to connect third-party devices which monitor speed, braking, and location.

MOBILE APPLICATIONS

Interfacing with vehicle systems are applications running on the driver's personal mobile device. These applications may contain binary libraries that expose vehicle data or functionality.

HOW A CONNECTED CAR GETS HACKED

1 EXTRACT BINARY CODE FROM DEVICE

2 REVERSE-ENGINEER SOFTWARE

Reverse-engineering tools (i.e. IDA pro) are fast, low in cost and easy-to-use.

3 TAMPER WITH BINARY CODE

4 REDEPLOY MALICIOUS SOFTWARE

&

WHAT YOU CAN DO TO PREVENT IT

1 KEEP SOFTWARE UPDATED:

Check with your manufacturer and service provider to make sure you always have the latest version installed.

2 DON'T JAILBREAK YOUR CAR OR DEVICE:

In addition to making your car less secure, it may also void warranties.

3 CHECK OUTLETS PERIODICALLY:

Make sure you know what is plugged into any USB or OBD2 ports on your vehicle. Carefully consider what you choose to plug in.

4 ASK MANUFACTURER IF APPS ARE HARDENED:

Verify that all mobile and pre-installed apps are hardened, in addition to any third-party apps you choose to download.

ARXAN