Securing the Modern Automobile

From Hot Rodding to Hacking

A little about me…

Security professional, software developer, car thief, mechanic

Currently work for Synopsys as a Managing Consultant, but I've worked for Textron (Overwatch), Trustwave (Spiderlabs) and Symantec (Product Security)

I have code running in Norton products (SONAR) and Windows 2000. I was part of Schlumberger's smart card team. Several security based start ups that didn't go anywhere.

ASE certified technician, primarily working for Chrysler, trained on the first electronically shifted transmission (A604) and the early Vipers

As for the Car thief part… stay tuned. ;-)

What we are going to talk about today..

History of Hot Rodding

- *When it started and what it meant*
- *What is Hot Rodding, as it applies to automobiles*

History of Hacking

- *Starting with MIT*
- *How it morphed over the years to the present*
- *What it has to do with cars*

Current Security Issues

- *Examples of Security Failures*
- *What hackers are doing with code today*

Future Security problems

How to fix them

Some history…

- Before Cars…Engines
  - ✓ *1870's Nicolaus Otto, Gottlieb Daimler, Karl Benz, Rudolf Diesel (1890s)*
  - ✓ *Built upon previous work, over 80 years*
  - ✓ *Germany was the "hot bed"*
  - ✓ *Extreme competition for engines -1880s*
- Daimler and Benz
  - ✓ *1886 both work on design for automobile, separately*
  - ✓ *Technically, oldest auto manufacturer*
- Electric automobiles
  - ✓ *Andreas Flocken, Germany, credited with first electric car, the Flocken Electrowagen, in 1888.*

- Why is Detroit the center of US Auto industry?
  - ✓ *In 1909, almost 300 car makers*
  - ✓ *By 1915, 13 of the top 15 auto brands were from Detroit*

- Famous American automotive pioneers
  - ✓ *Ransom Olds, Henry Ford, John & Horace Dodge*
  - ✓ *Walter Chrysler, Henry Leland,*

- Innovations of the "early years"
  - ✓ *Steering wheel, drum brakes, 4 wheel drive, drive shafts.*
  - ✓ *Electric ignition system, transmissions, throttle devices,*

Some *Racing* …

- Man’s competitive nature
  - ✓ *First US City to City race. Between Green Bay and Madison Wisconsin in 1875.*
  - ✓ *200 miles via Appleton, Oshkosh, Waupun, Watertown, Fort Atkinson, Janesville*
  - ✓ *Average speed 6 mph, completed in 33 hours and 27 minutes*
- Others think that it occurred much later
  - ✓ *1887 race from Neuilly Bridge to Bois De Boulogne*
  - ✓ *In the US, Thanksgiving 1895 from Chicago to Evanston and back*

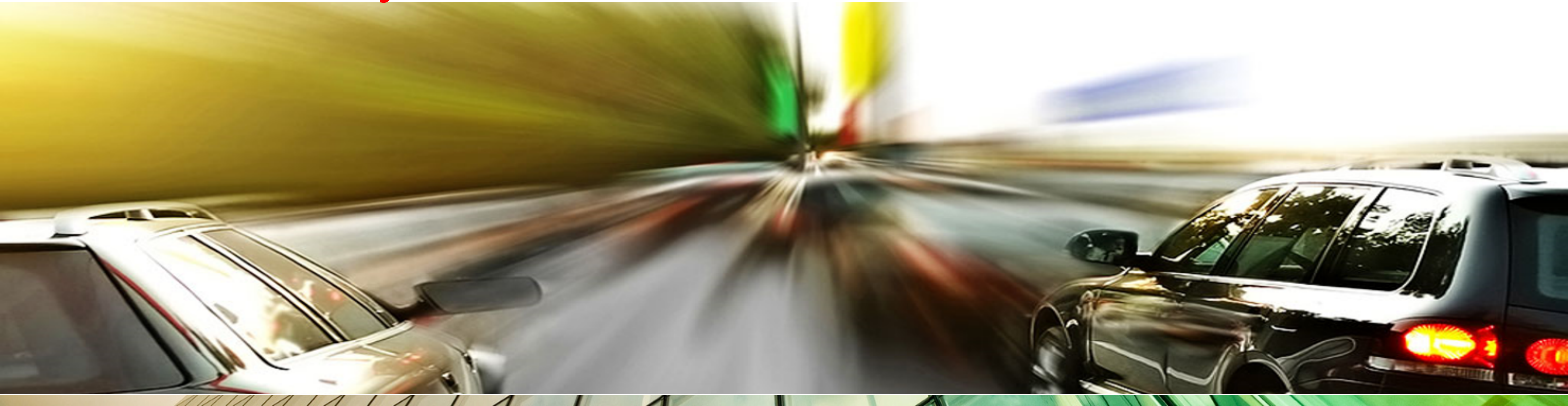
- France was the heart of the racing world
  - ✓ *Dominated by French Automobile Club (ACF), first to launch International races, usually beginning in Paris*
- Indianapolis Motor Speedway opens in 1909
  - ✓ *2.5 miles long*
  - ✓ *Still in use*

So what does this have to do with anything?

Early centers of technology

- *Highly competitive companies and individuals vying for a large share of the “pie.”*
- *Transfer of knowledge between companies. Lots of collaboration.*
- *Extreme rate of technological progress*

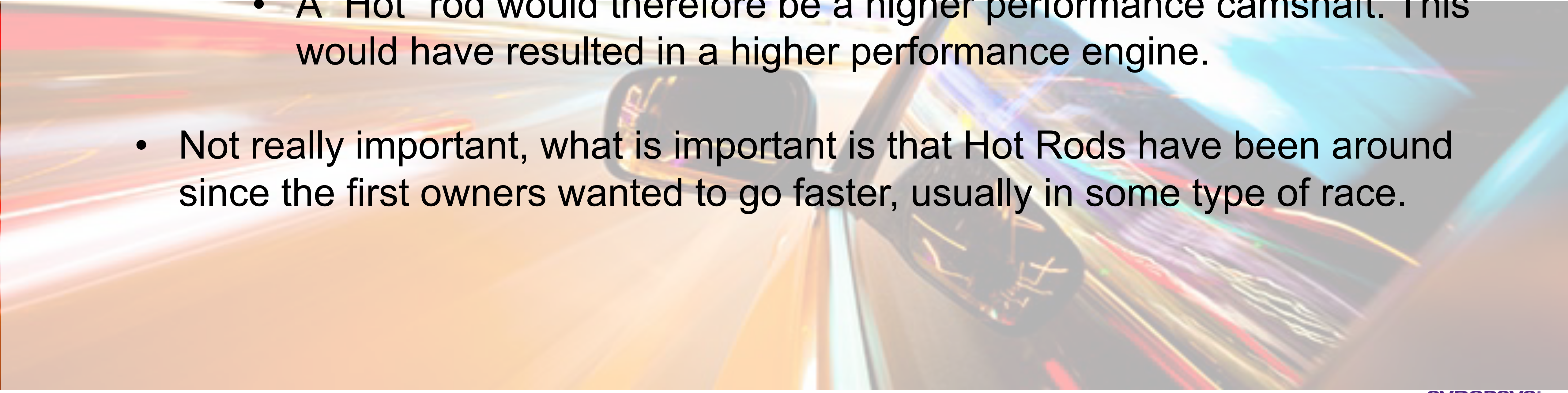
Does any of this seem a little bit familiar?



So, Hot rod

What exactly is a Hot Rod?

- We are all probably familiar with the term, but what does it refer to?
  - Still up for debate regarding the origin of the term,
    - Stolen as in “hot” and
    - Rod as in camshaft or bumpstick, which is the device that opens and closes the engine valves.
      - A “Hot” rod would therefore be a higher performance camshaft. This would have resulted in a higher performance engine.
  - Not really important, what is important is that Hot Rods have been around since the first owners wanted to go faster, usually in some type of race.



From the early days to now (1960's)

Some monumental changes in cars since the early days

- Electric Starters
- Seat belts
- Modern shock absorbers
- Power steering
- Independent Front Suspension (IFS)
- All steel bodies (previously wood)
- Automatic Transmissions
- Radial Tires
- Electronic Fuel Injection
- Cruise Control
- Anti Lock Brakes

Current Technology

The latest and greatest technology

- Electronic Traction/Stability Control
- Supplemental Restraint System (Airbags/Seatbelts)
- Dynamic Shock Absorbers (MR/ER dampeners)
- Electronic Power steering
- Independent Rear Suspension (IRS)
- Aluminum / plastic bodies
- 5 channel ABS with advanced material components (carbon

- 10 speed electronically controlled Automatic transmission
- Advanced self healing Run Flat technology tires (TPMS)
- Direct Injection Fuel delivery systems with VVT
- Adaptive Cruise Control
- Anti Lock Brakes

Some Computers onboard…

- Engine Control Unit (PCM)
- Transmission Control Unit (may be part of PCM)
- Body Control Module (lighting, locks)
- SRS (Airbag and seatbelts)
- Infotainment systems
  - Navigation, Audio, Information/Internet
- ABS/Traction control:

- “Driver Assistance”
  - Cruise Control, Lane Keeping, Blind Spot
- Instrument control panels
  - Display of speedo and driver data/interaction
- HVAC systems (Dual Zone climate control)

A lot of code…

- Chevy Volt has approximately 10 MLOC (million lines of code)
  - ✓ *2 million more than the F-35 Fighter Jet*
- By 2020, Average car is projected to have have 61 millions LOC
  - ✓ *More than the Large Hadron Collider*
  - ✓ *More than Facebook.com (2015)*
- Boeing 787 has approximately 14 million LOC:
- Windows Vista ran with 50 million LOC
  - ✓ *And we know how secure that was ;-)*

“Switching Gears”

Hacking…

- **People** have been hacking things for a long time. **Marconi** was hacked by Nevil Maskelyne during a radio demo.
- **Enigma** machine was cracked prior to WW II .
- MIT and the Tech Model Railroad Club of the 60’s**.**

- “**Core Wars**”, notable Robert Morris, Sr. 1966**.**
- 1969 ARPANet
- John “**Captain Crunch”** Draper, phone phreaking with the **Blue Box**
- **Kevin Mitnick** arrives on the scene in **‘79**

- “**War Games**” with Broderick comes out in 1983
- **Cult of the Dead Cow** from Lubbock in 1985
- Robert Morris Jr and the **Morris Worm** in 1988
- Clifford Stoll, “**Cuckoo's Egg**” published

“Modern years”

Hacking…

- **“I love you”** virus in 2000
- Microsoft’s “**Security Memo**” in 2002.
- **Anonymous** in 2003.
- 2007 **Estonia** suffers Massive Denial of Service (**DoS**) attack**.**

- 2009 – Conficker infects millions**.**
- **2011** BofA Hacked, 85k accounts affected
- **LinkedIn** suffers breach, 6.5 million users affected in **2012**
- **2014** North Korea hacks Sony Pictures, j/K

- 2016 – IoT botnet (**Mirai**) takes down Dyn, affects major web brands
- 2017 - **WannaCry**

So where does that leave us now…

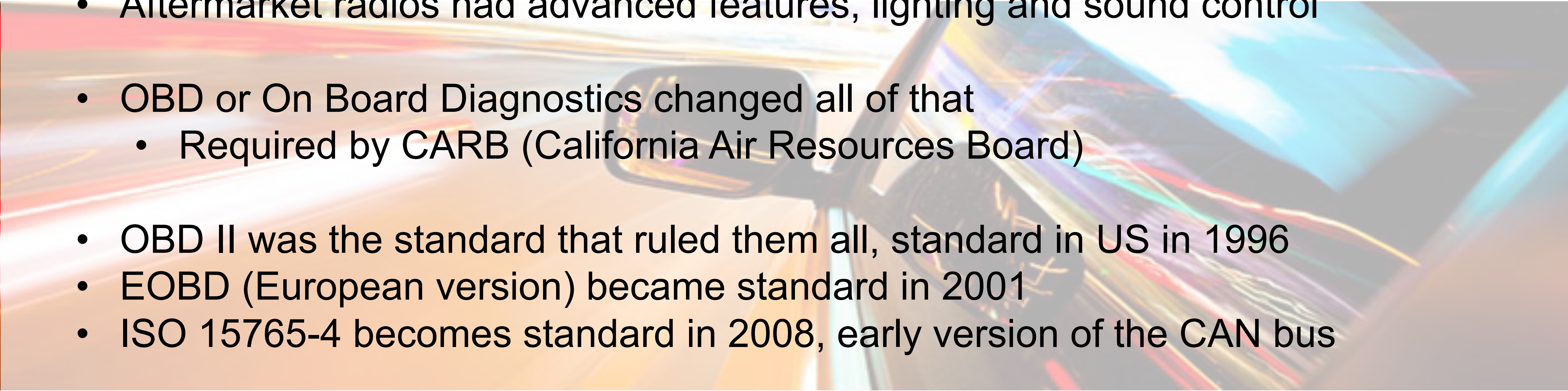
Hackers and Hot rodders

- Cars had minimal electronics until the ‘90s
  - Wanted more performance, replace “the chip”
  - EERPOM, containing spark and fuel tables
  - Matched up with the usual performance add-ons

- Aftermarket radios had advanced features, lighting and sound control

- OBD or On Board Diagnostics changed all of that
  - Required by CARB (California Air Resources Board)

- OBD II was the standard that ruled them all, standard in US in 1996
- EOBD (European version) became standard in 2001
- ISO 15765-4 becomes standard in 2008, early version of the CAN bus

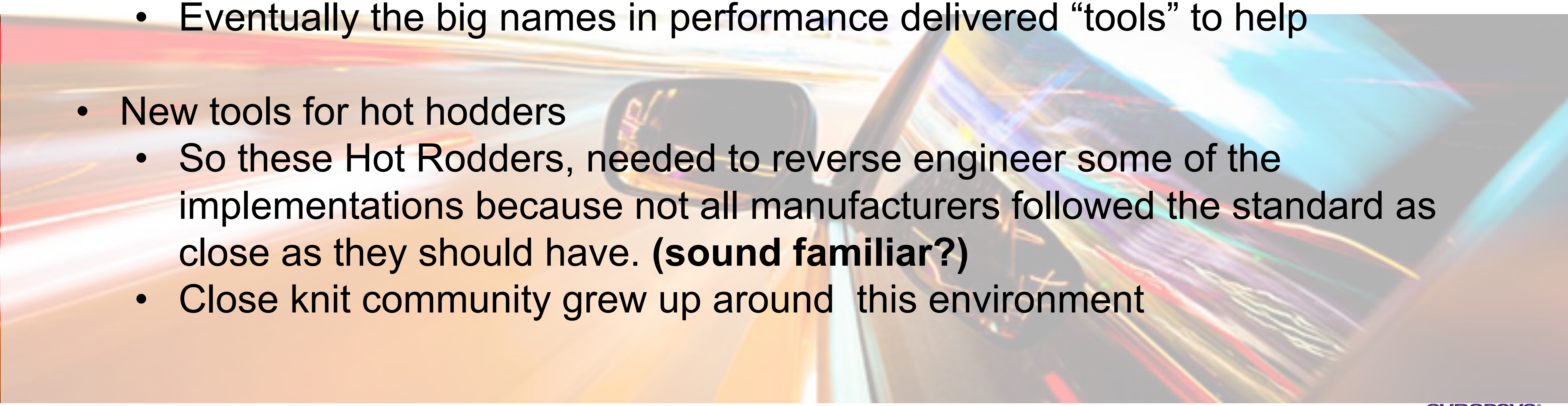


So where does that leave us now…

Hackers and Hot Rodders

- First came the “tuners”
  - These are the pioneers.
  - Maximize the performance of the engine, while still being legal (especially in California)
  - A lot of homegrown solutions at first
  - Eventually the big names in performance delivered “tools” to help

- New tools for hot hodders
  - So these Hot Rodders, needed to reverse engineer some of the implementations because not all manufacturers followed the standard as close as they should have. **(sound familiar?)**
  - Close knit community grew up around this environment



So where does that leave us now…

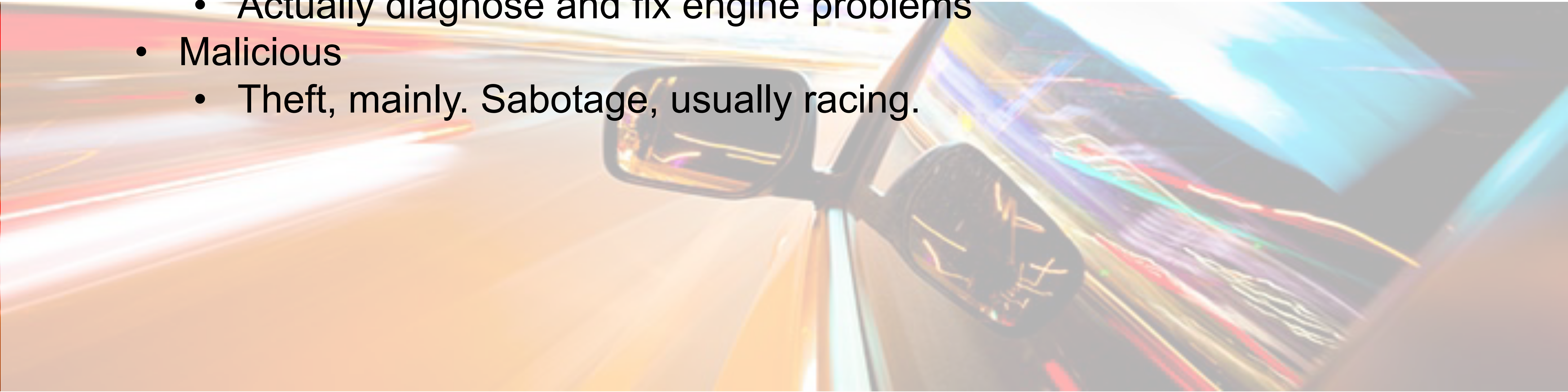
Hackers and Hot Rodders

- Every OEM has it’s own performance community
  - Not a lot of cross over beyond the standard interface aspects
  - Lots of different architectures.

What do hackers do with these tools…

Hackers and Hot Rodders

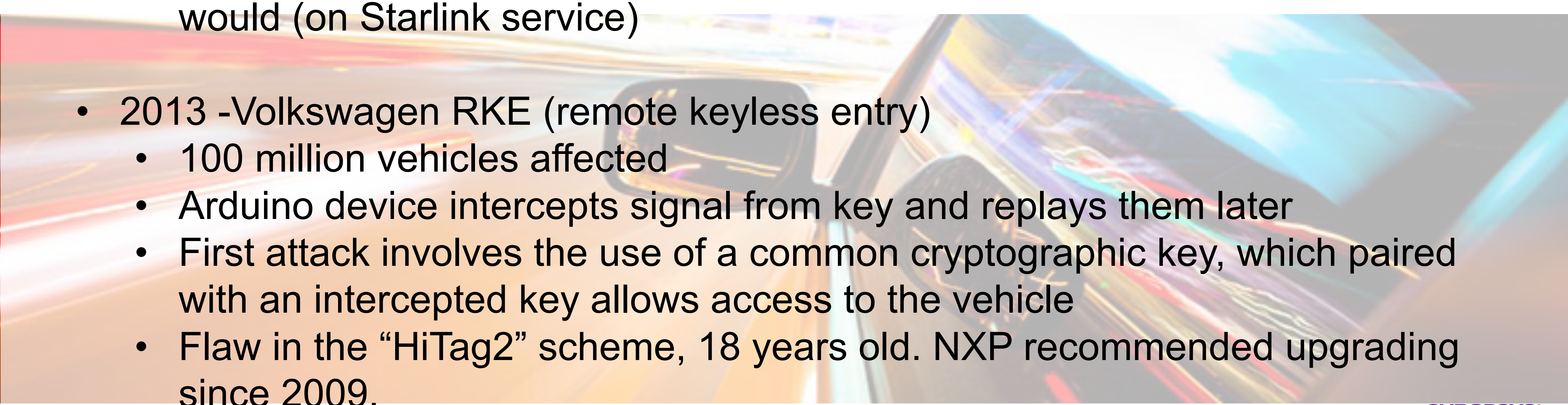
- Customization
  - Lighting and Audio/Video performance
- Performance
  - More horse power, better shifting transmission, disable traction control
- Repair
  - Actually diagnose and fix engine problems
- Malicious
  - Theft, mainly. Sabotage, usually racing.



Famous examples of automotive security breaches

More hacking, less hot rodding

- Subaru – 2017
  - Issues with Starlink. Able to add new users, who could lock/unlock doors, honk horn.
  - No engine or brake function accessible
  - No session time out. Sent in clear text. Have same access to car as owner would (on Starlink service)

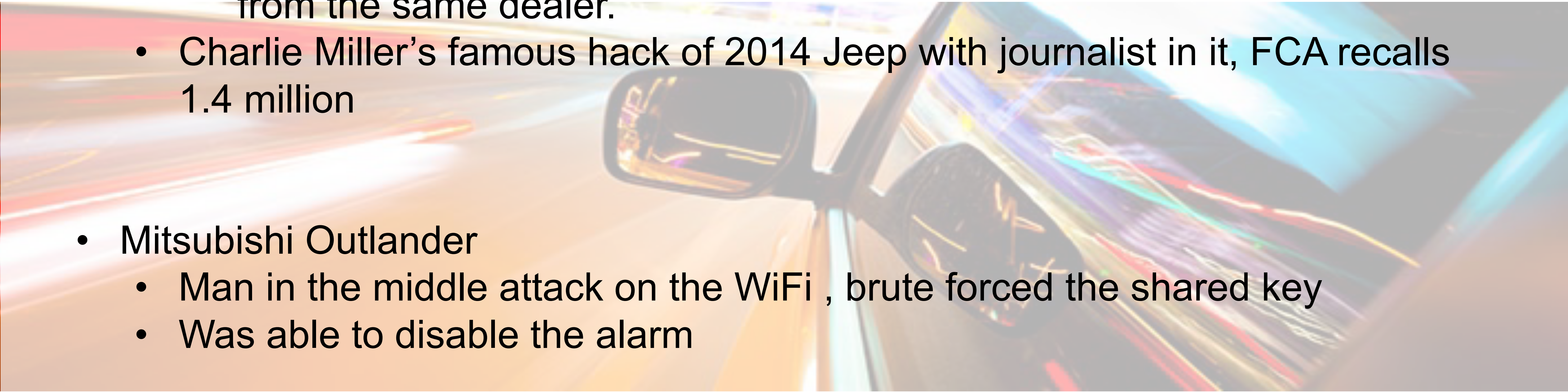


- 2013 -Volkswagen RKE (remote keyless entry)
  - 100 million vehicles affected
  - Arduino device intercepts signal from key and replays them later
  - First attack involves the use of a common cryptographic key, which paired with an intercepted key allows access to the vehicle
  - Flaw in the “HiTag2” scheme, 18 years old. NXP recommended upgrading since 2009.

Famous examples of automotive security breaches

More hacking, less hot rodding

- Jeep
  - Over 30 Jeeps were stolen in Houston
  - In San Diego, a gang was stealing Jeeps and shipping them over the border
    - Database of unique key codes were compromised. All requests came from the same dealer.
  - Charlie Miller’s famous hack of 2014 Jeep with journalist in it, FCA recalls 1.4 million



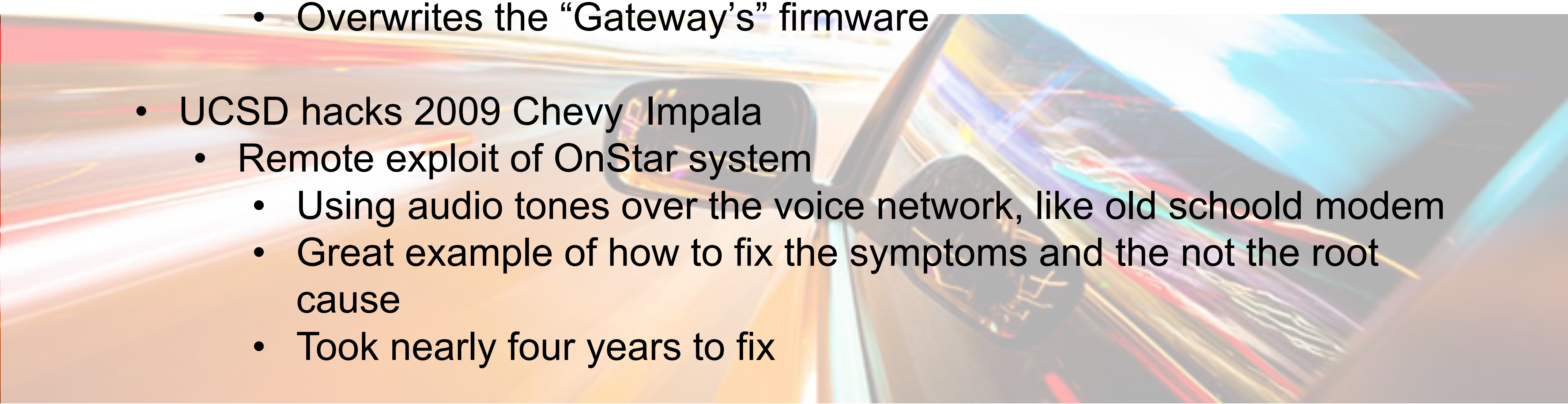
- Mitsubishi Outlander
  - Man in the middle attack on the WiFi , brute forced the shared key
  - Was able to disable the alarm

Famous examples of automotive security breaches

More hacking, less hot rodding

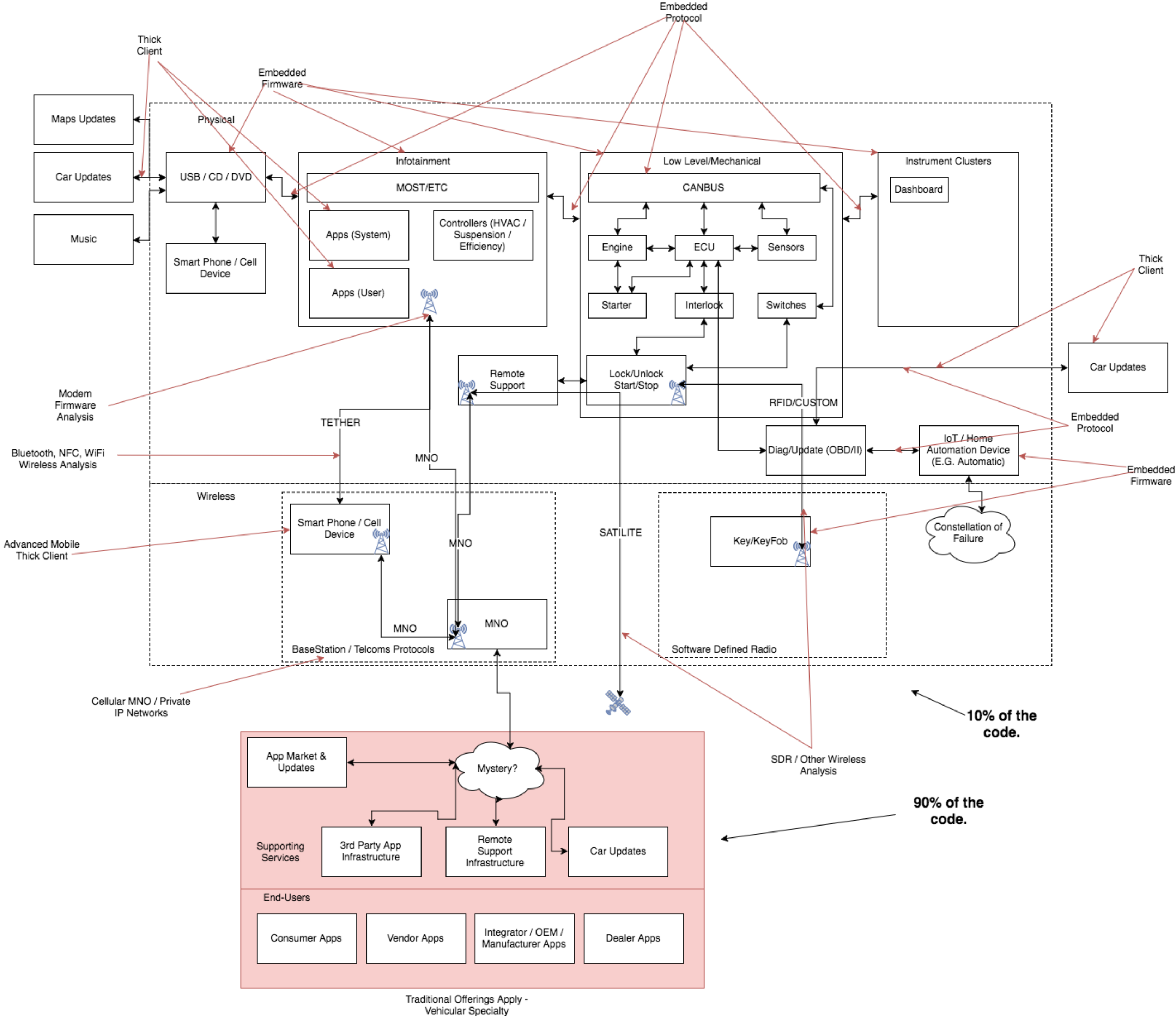
- Tesla hacked in 2016
  - Chinese firm TenCent
    - Malicious hot spot
    - Downloads code into the Tesla browser
    - Exploits a vulnerability with Linux OS
    - Overwrites the “Gateway’s” firmware

- UCSD hacks 2009 Chevy Impala
  - Remote exploit of OnStar system
    - Using audio tones over the voice network, like old schoold modem
    - Great example of how to fix the symptoms and the not the root cause
    - Took nearly four years to fix



Why is this so hard?

More hacking, less hot rodding



It’s the network

More hacking, less hot rodding

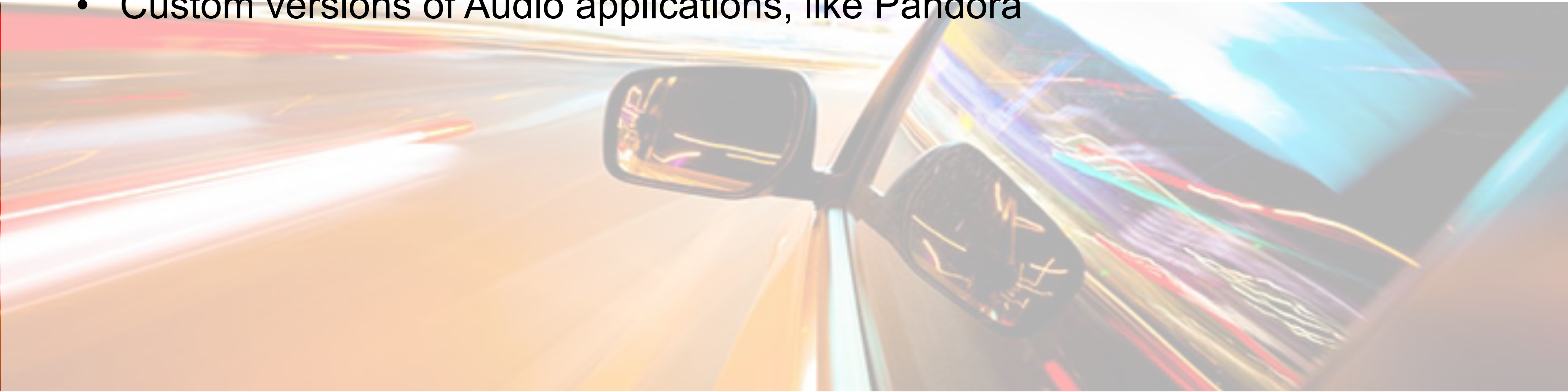
- Hi speed CAN bus
- Lo speed CAN bus
  - Two primary communication networks inside the automobile
- Cellular network
- Wifi Network
- Satelite
  - Early gen OnStar and SiriusXM
- Bluetooth network
- RKE and TPMS

- At least seven different networks, plus USB and audio inputs

More Apps please

More hacking, less hot rodding

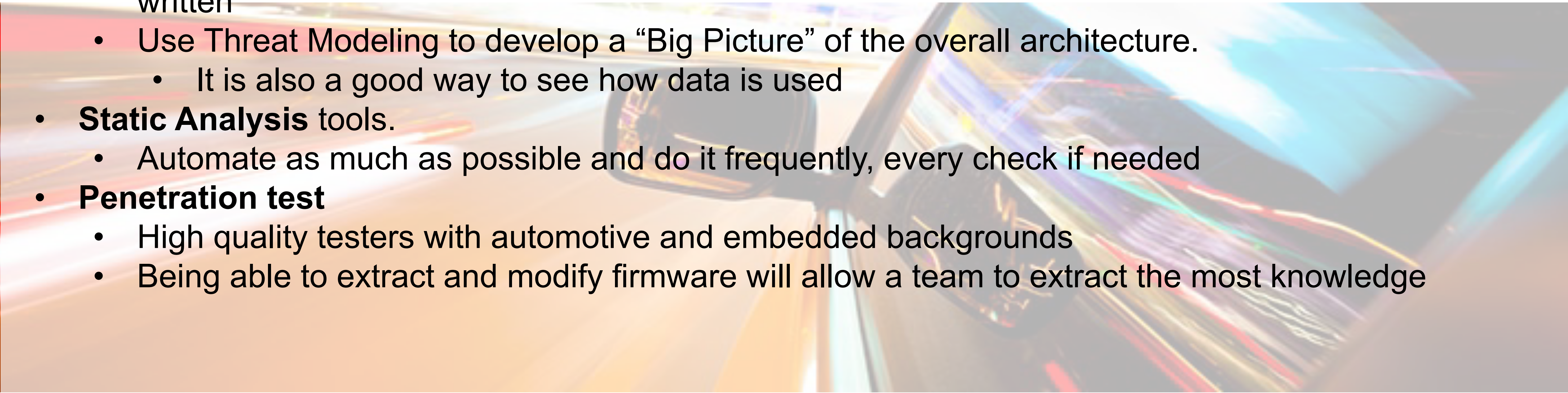
- Android Auto
- Apple Carplay
- Native applications
  - Including web servers and services
  - Custom network stacks running on modified Oses
- Custom versions of Audio applications, like Pandora



So how do we secure this mess?

More hacking, less hot rodding

- This is done the same way we do it now
- **Training** for the development teams
  - Most developers aren’t aware of how their code (assumptions) can be misused. They aren’t taught to think that way.
- **Architecture Review**
  - Review Architecture Designs to ensure that Security requirements are applied before any code is written
  - Use Threat Modeling to develop a “Big Picture” of the overall architecture.
    - It is also a good way to see how data is used
- **Static Analysis** tools.
  - Automate as much as possible and do it frequently, every check if needed
- **Penetration test**
  - High quality testers with automotive and embedded backgrounds
  - Being able to extract and modify firmware will allow a team to extract the most knowledge



Why do we need to do this now?

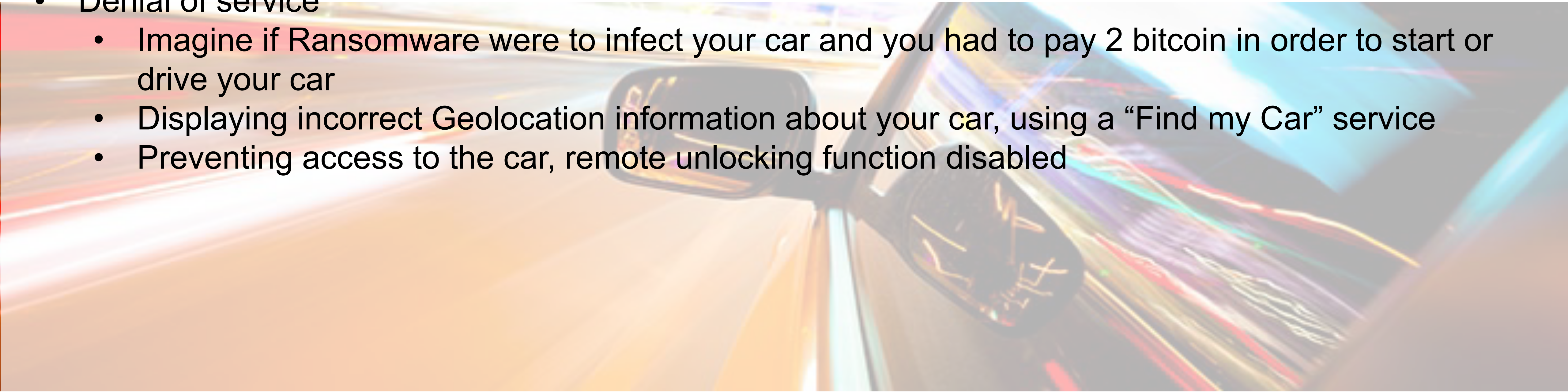
More hacking, less hot rodding

- Self driving cars are on their way.
  - Some say by 2020
  - Definitely by 2030
- V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure)
  - IEE 1609.2
- More functionality and integration
  - Rideshare functionality
  - Hellcat “Red Fob”

What happens if we don’t

More hacking, less hot rodding

- Theft
  - We see this now, however being able to remotely locate all or any particular cars in a geographical location and then have the ability to steal them without notice
  - Definitely ups the game, especially if you can steal a self driving car. ;-)
- Crashes
  - Obvious problem. Injuring the owner or occupants is just bad for business.
- Denial of service
  - Imagine if Ransomware were to infect your car and you had to pay 2 bitcoin in order to start or drive your car
  - Displaying incorrect Geolocation information about your car, using a “Find my Car” service
  - Preventing access to the car, remote unlocking function disabled



SYNOPSYS®

Silicon to Software™