Modern Automotive Vulnerabilities: Causes, Disclosure & Outcomes

Stefan Savage
UC San Diego

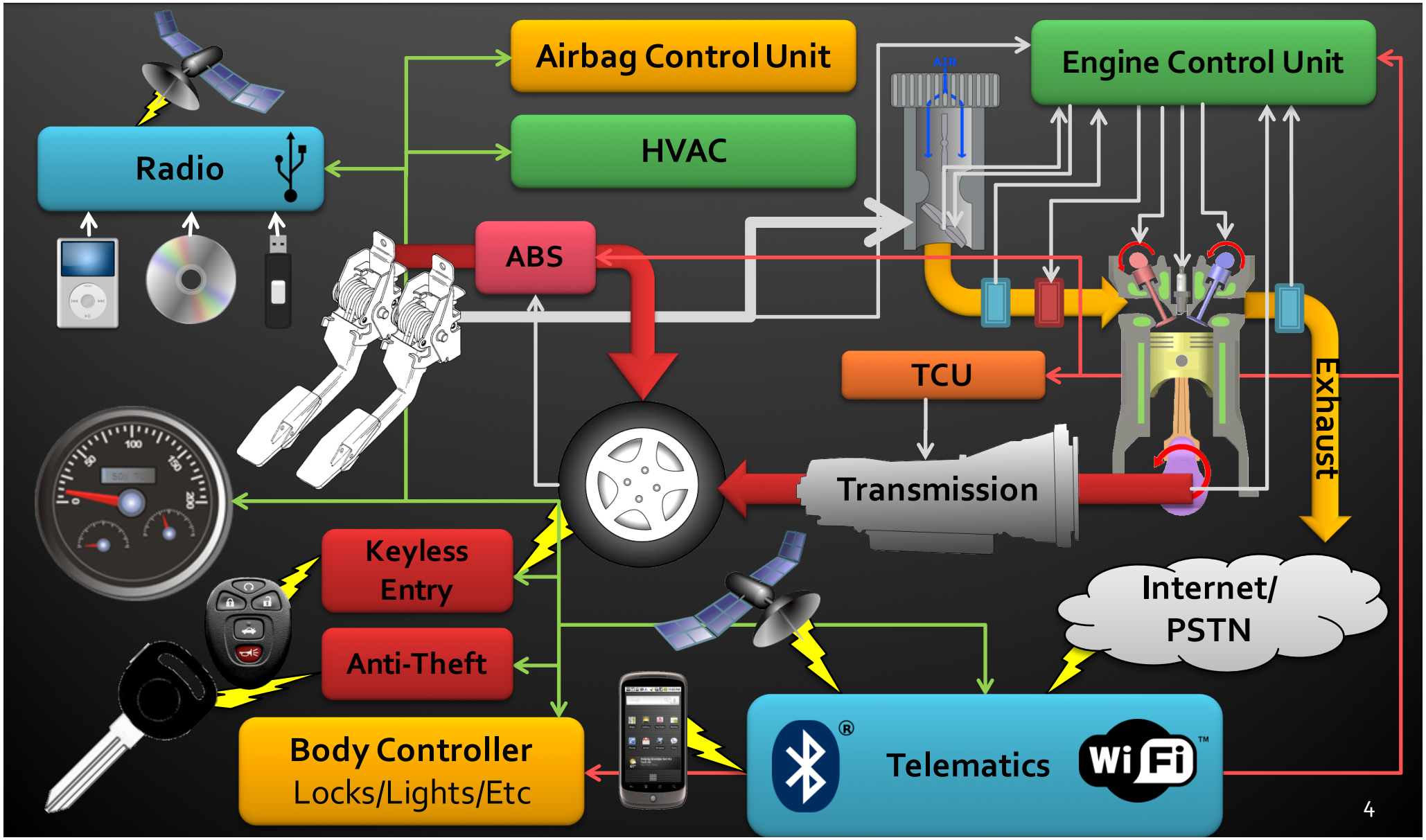
Steve Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage (UCSD)
Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno (UW)

Recap: normal unmodified cars can be remotely compromised

What we'll try to understand today

- Why do we have automotive vulnerabilities?
- What are the challenges in addressing these issues?
- How do security researchers play a role?

The modern automobile: networked and computer controlled

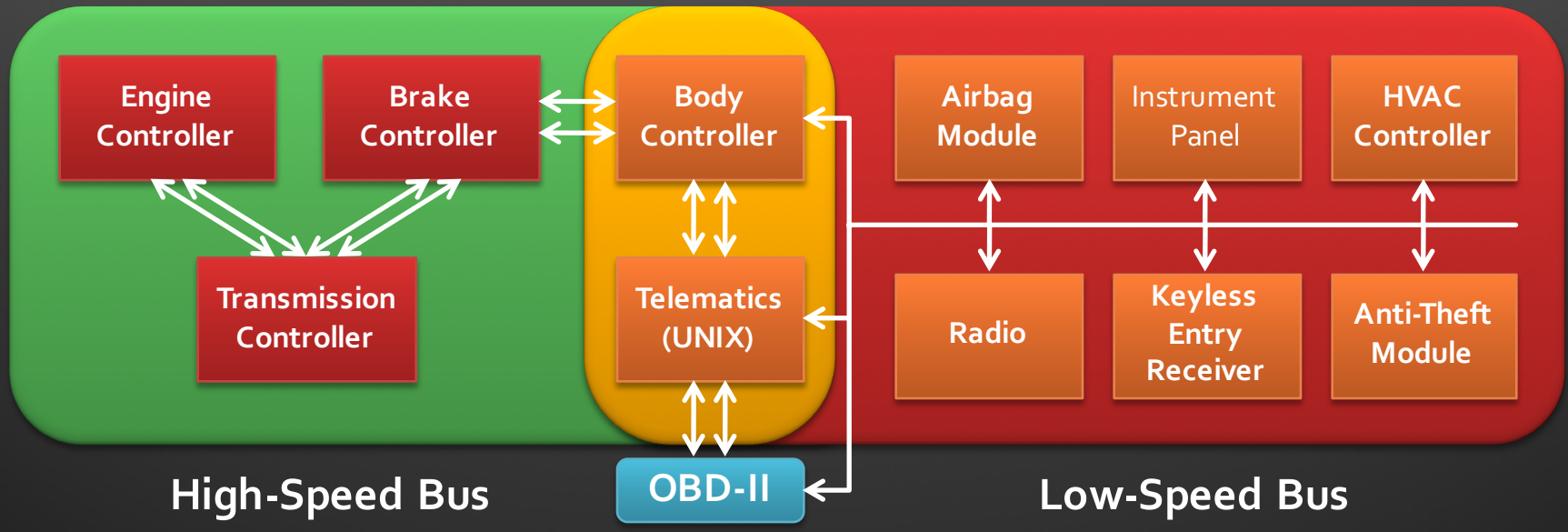


The modern automobile…

… is a super complex distributed system

- **20-40 Electronic Control Units (ECUs)**
  - From 8051s and Atmels to Power & ARM SoCs
  - Dozens of operating/runtime systems
  - Software parts may change completely each year
- **Internally networked** (CAN, Flexray, …)
- **Externally connected** (wired, wireless, media)

A typical automobile network



Car insides are not hardened…

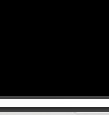
SECTIONS HOME SEARCH The New York Times

Forbes / Security

The Little Black Book of Billion

JUL 24, 2013 @ 09:00 AM 547,828 VIEWS

Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video)



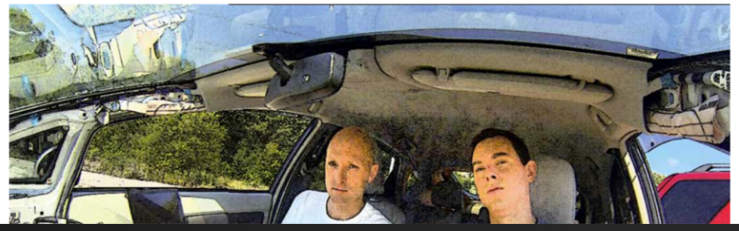
Andy Greenberg, FORBES STAFF

Covering the worlds of data security, privacy and hacker culture.

FOLLOW ON FORBES (1413)

FULL BIO

This story appears in the August 12, 2013 issue of Forbes. ***Subscribe***



- In 2010, we show that network access (via **OBD-II**) is sufficient to completely control a 2009 Chevy Impala
- In 2014, Miller & Valasek show the same thing for the 2010 Toyota Prius and Ford Escape

Why so exposed?

- Open network
  - Pure software bus-style architecture
  - **Innate** coupling between ECUs
  - So "RPCs" between ECUs can be **replayed**
- Same network is used for maintenance
  - Must allow car to be put in **unsafe states**
- Same network is used for ECU update
  - Can **update all software** via network

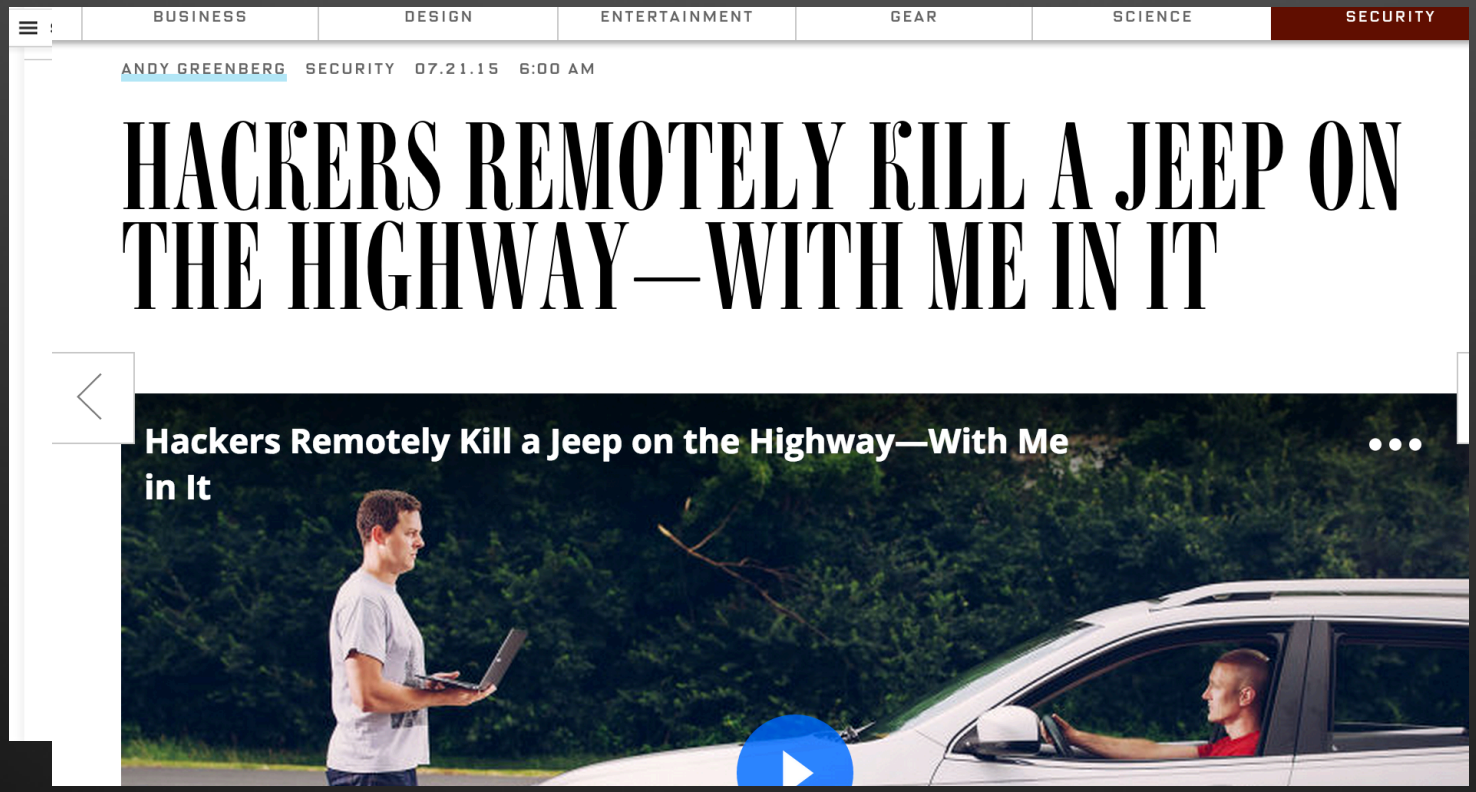
The obvious criticism of these findings…

The Register®
Biting the hand that feeds IT

"I was utterly shocked to discover that apparently if you prise open an embedded system, reflash its program code, you can pretty much do anything to the I/O connected to the system," he said. "Well knock me down with a feather."

with some confidence that this 'discovery' is sheer foolishness. The only risk they encountered was a theoretical one (viz. that a telematics system connected to the in-vehicle networking could hack the car). It's highly theoretical because the challenges of hacking a car are vastly more than hacking a banking system. I just can't see anyone bothering," he concluded.

Car outsides are exposed too



- In 2011, we demoed remote takeover ***without*** physical access and at arbitrary distance (GM Onstar Gen8)
- In 2015, Miller & Valasek developed similar attack against Jeep Cherokee (Fiat Uconnect)

Remote compromise vectors

- **External** attack surface
  - Indirect physical
    - **Shop tools, CD player**, 3rd-party media players, **after-market components**, charging stations, etc
  - Short-range wireless
    - **tooth**, WiFi, keyless entry, TPMS, DSRC
    - ange wireless
    - la

Involuntary braking demo

Why so exposed?

- **Environmental pressures**
  - **No adversaries**, so limited budget for security process
  - Regulatory and market pressure on feature creation
  - Time to market pressures; OEM is integrator
- **Supply chain issues**
  - Cost driven; promotes broad reuse (code does **more**)
  - **Many** vendors; imperfect interface coupling
  - Extreme heterogeneity (hardware, software)
  - Source code; frequently not available… *to anyone*
- **Limited experience with product security**

What to do (as researchers)?

- Provide **information/knowledge** about problems and how to fix
- Create **incentives** to act on that knowledge
- Do so in a way that minimizes **real harm**

- Tricky to balance these…

- **Question: how do you manage disclosure?**

The story of our disclosure

- **Early 2010**: had found full series of vulns for 2009 Chevy Impala (including Onstar compromise)
- **Active choices**
  - Work with OEM (GM) and disclosed to regulator (NHTSA)
  - No name/shame
  - No code/details release
- Why?
  - Goal to *improve* automotive security
  - We thought it was an **industry-wide** problem
  - We realized there was **very little capacity** to deal with the problem

What happened?

- **Short-term**
  - Bugs fixed in next model year & Gen9 Onstar
  - Mitigations rolled out on cell carrier
- **Medium term**
  - GM gets security religion
    - Product CSO (Jeff Massimilla)
      ~100 people working on product cybersecurity
    - Changes to development practice & contracting practice
    - Security design input to overall electrical design

But… no product recall

- All Gen8 devices likely still had vulnerability
  - But what is cost/benefit on recall?
  - Tricky…

- Five years later… **unprecedented** fix
  - Remote update of **all** connected Gen8 Onstar boxes
  - Gen8 Onstar boxes have **no remote update capability…**

GM TOOK 5 YEARS TO FIX A FULL-TAKEOVER HACK IN MILLIONS OF ONSTAR CARS

Contrast: Miller & Valasek

- **2013**: public disclosure of **OBD-II attacks** on Prius & Escape (details and code)
  - Architectural issues, both still work (no "fixes")
- **2015**: **UConnect attack**
  - Coordinated disclosure of details to Fiat, their affected suppliers and NHTSA
  - Patch released before public release of details/code
  - "Voluntary" recall of 1.4M vehicles (**first ever**)
  - Sprint blocks 6667 traffic (**blocking cell-base compromise**)
- Unprecedented impact on **public perception**

Some musing…

- Was one of us right? How to decide?
- Situational differences
  - Level of industry prep/appreciation
    - E.g. time to fix samy Onstar app bug
  - Existence of effective network-layer mitigation
- Indirect impacts
  - **Cost structure for cyber investments**
- We have since done public disclosure on other car issues (MDI C4E) via CERT

Direct and indirect impacts

- **Remote Update**
  - Almost every OEM has the capability or is close to it
  - BMW, Tesla and GM have used publicly
- **Society of Automotive Engineers** (SAE)
  - Vehicle Electrical System Security Committee
  - Two draft standards (guidebook, hardware)
- **National Highway and Traffic Safety Administration** (NHTSA)
  - Now has cyber testing lab (budget still small)
  - But politics…
- **Legislation**… (2+ bills)

Legislative action

- **Senate**
  - Commerce, Science & Transportation (Thune/Nelson)
  - Markey/Blumenthal Bill (SPY Act)
    - NTHTA (security min stds), FTC (privacy), public labeling
- **House**
  - Energy and Commerce Committee (Upton/Pallone)
    - Cyber council (NHTSA, NIST, DoD, OEMs [50%+]); best practices, OEMs document how they comply; safe harbor;
    - Criminalize car hacking
- *And there are other committees drafting…*

Summary

- **Automobiles are computers with wheels**
  - Complex distributed systems with vulnerabilities
  - History, architecture, supply chain and business incentives make security particularly challenging
  - Auto industry and govt know it & are responding
    - At OEM/Government speed…
- **Security researchers have played a key role**
- **Disclosure is a tool, but a *nuanced* one**
  - Balancing harms requires getting past religion
  - Different benefits from different approaches