iMedia Connection Blog

- Articles, video, people, jobs a
- Search

- Articles
- Blog
- Videos
- Events
- People Connection
- Resource Connection
- Jobs
- iMedia UK

Home › iMedia Connection Blog › Creative Best Practices Emerging Platforms Opinions Research Social Media Targeting Web Analytics Websites Wireless Word of Mouth

Creative Best Practices Emerging Platforms Opinions Research Social Media Targeting Web Analytics Websites Wireless Word of Mouth

Car and Truck Makers Need to Emphasize Their Vehicles Are Digitally Safe

Tweet Like 0 G+1 0 Share

Posted by Neal Leavitt on September 29th, 2014 at 3:09 pm

Watch any NFL game on Sunday, Monday, Thursday, and you’ll see a bevy of commercials espousing that a given car or truck model is sleek, rough, tough, cool, fuel efficient, family-friendly, sporty, ad nauseum. Adjectives like these are music to a car/truck marketer’s ears.

What you don’t see or hear very often is that hackers continue to pose a threat to all sorts of vehicle models – and even smart charging stations for electronic vehicles (EV) may be vulnerable to hacking. Granted, there haven’t been any major security breakdowns and security professionals say that auto manufacturers are making inroads in improving software security. In fact, Andrew Brown, chief technologist for Delphi Automotive said recently that “quite honestly, the vehicles, systems and components today are quite robust and resistant to cyber-security threats. But that doesn't mean it's 100%."

Added Ed Adams, a security expert:

"There's an awful lot of code throughout the entire supply chain, not just with the auto manufacturers, but with the infotainment systems and applications like Sirius and Harmon. The fact of life is that software is flawed."

Cheryl Dancey Balough and Richard C. Balough, co-founders of Chicago-based Balough Law Offices, LLC, said today's cars have dozens of electrical control units (ECUs) embedded in the body, doors, dash, roof, trunk, seats, wheels, navigation equipment and entertainment centers.

"This architecture provides almost unlimited gateways for external hacking and infection with malware. Some entry points to a car's ECUs require a direct, hard-wired connection, while others can be accessed wirelessly, including using Wi-Fi or radio-frequency identification (RFID). Once entry is gained, a hacker can take over all of a car's computer-controlled systems."

The Baloughs added that in one recent example, a former employee of an Austin, TX-based auto dealer hacked into the computer system and remotely activated the vehicle immobilization system, triggering the ignition system in 100+ vehicles.

"This anti-theft system had been installed by the dealer as a method of addressing non-payment by customers. While the anti-theft device was connected to the car's horn and ignition, the hacker didn't take further control of the car," they noted.

And at last month's Black Hat conference, security researchers Chris Valasek and Charlie Miller investigated the 'hackability' of two dozen different vehicles.

"We examined how a remote attack might work," said Valasek. "It really depends on the architecture – if you hack the radio, can you send messages to the brakes or the steering? And if you can, what can you do with them?"

Both researchers emphasized that their results weren't definitive assertions about actual vehicle security vulnerabilities – they were flagging potential weaknesses.

One model that ranked near the top of the list was the Infiniti Q50 (ironically, which Valasek owns). As reported by *Wired*, the car "was a model of insecure architecture." *Wired* added that the sports sedan has remote keyless entry, Bluetooth, a cellular connection, wireless tire pressure monitoring and an Infiniti Connection system interfacing with a 'personal assistant' app on the driver's smartphone.

"Within the Q50's network, those radio and telematic components were directly connected to engine and braking systems. And the sedan's critical driving systems had computer-controlled features like adaptive cruise control and adaptive steering that a hacker could potentially hijack to physically manipulate the car," said *Wired*.

Love those remote door locks? Also at Black Hat, Australian security researcher Silvo Cesare illustrated how easy it is to hack a key fob. Cesare used a software-defined radio to capture and transmit the wireless signals. All the equipment was off-the-shelf – it took Cesare just a few minutes to unlock his girlfriend's car.

Got a Leaf, Tesla or other EV? Well, your charging station may be vulnerable too. At last year's 'Hack in the Box' conference in Amsterdam, security analyst Ofer Shezaf said hackers could gain access to smart EV chargers and obtain access to logins and payments.

Again, there hasn't been a significant security breach at smart charging stations, but digital news outlet *Quartz* indicated that other technologies for networking/access are being built into smart charging networks. These include RFID, which allow drivers access to power with a touchless card.

"Like using a default or easily guessed password online, these systems could be broken into with little effort," says *Quartz*. "Some charging systems use cellular data connections or even Wi-Fi to connect to other stations or to be accessed for maintenance, also opening doors for hackers."

Shezaf added that charging networking providers need to take a closer look at security issues. The technology's still relatively new, but "this is precisely the time to look at it, before it scales up to whole cities and countries."

As stated earlier, presently, the threat of hackers seizing control of a 'smart' car is still minimal, but Andry Rakotonirainy, a professor at Queensland University in Australia, raised a cautionary red flag.

"A vehicle's communication security over wireless networks cannot be an afterthought and needs to be considered at the early stages of design and deployment from the hardware, software, user and policy point of view," he said.

Hopefully car and truck manufacturers will get the message and market with another critically important selling angle – that their vehicles are digitally safe.

- Add a comment
- Print This Post
- Share

Relevant Posts

- How a consumer electronics social media campaign leveraged a celebrity endorser (4 days ago)
- Why Facebook's latest News Feed update shouldn't matter to you (2 weeks ago)
- E-Commerce Environment Still Facing Supply Chain Challenges (3 weeks ago)
- 2015 in Review: A Social Media Benchmark & Content Summary for the Energy Drink Industry (3 weeks ago)
- 2015 in Review: A Social Media Benchmark & Content Summary for the Luxury Fashion Industry (4 weeks ago)
- Play Post-CES Buzzword Bingo (1 month ago)
- Internet of Things Upending Real Estate Industry (1 month ago)
- Social Media Benchmark & Content Trends for the DMO Industry (2 months ago)
- Social Media Benchmark and Content Trends for Children's Hospitals (2 months ago)
- Social Media Benchmark and Content Trends for the Yogurt Industry (2 months ago)

Leave a comment

Name (required)

Mail (will not be published) (required)

Website

Submit Comment

ABOUT THIS BLOGGER

Neal Leavitt

President
Leavitt Communications

more posts by Neal

- E-Commerce Environment Still Facing Supply Chain Challenges
- Internet of Things Upending Real Estate Industry
- Not Your Neighborhood Community Bank Anymore

All Posts

-

- **Follow iMediaConnection**

  Receive our daily newsletter your email address Subscribe
  iMedia Connection on twitter iMedia Connection RSS feeds iMedia Connection on YouTube iMedia Connection app in Apple iTune store iMedia Connection app in Google Play store
  Like 11K G+1

-
Drive superior performance with your digital ad campaign
Weakness for organic pizza
LEARN MORE
MAXPOINT

- MOST POPULAR
  - Articles
  - Blog Posts
  1. The most meaningless (and hilarious) job titles on LinkedIn
  2. 11 innovative movie marketing campaigns
  3. 10 crucial best practices for native advertising
  4. When brands strike back on social media
  5. 6 killer websites to check out
  6. 4 ways luxury brands are reinventing their appeal
  7. 3 things marketers are doing wrong in programmatic today
  8. The 5 basic types of consumers
  9. The best social media campaigns of 2015 (so far)
  10. 11 mistakes to avoid on your digital marketing resume

  Subscribe to most popular articles »

- ## Categories

  - Ad Networks
  - Ad Serving
  - Creative Best Practices
  - Desktop Apps
  - Email
  - Emerging Platforms
  - Entertainment
  - Humor
  - Jobs
  - Media Planning & Buying
  - Opinions
  - Research
  - Search
  - Social Media
  - Targeting
  - Uncategorized
  - Video
  - Web Analytics
  - Websites
  - Wireless

  - Word of Mouth

- **TOP BLOGGERS**

  - Rick Mathieson (4)
  - Doug Schumacher (4)
  - Agata Smieciuszewski (2)
  - Jeff Hasen (1)
  - Joseph Vito DeLuca (1)
  - Nanette Marcus (1)
  - John Bohan (1)
  - Drew Neisser (1)
  - Benjamin Taylor (1)
  - Winnie Brignac Hart and Lorrie Brignac Lee (1)

- **INDUSTRY JOBS**

    - Sales Managers- Los Angeles
    - Manager, YouTube Strategy & Optimization- Burbank

  see more jobs »

- **LATEST ARTICLES**

  - 4 ways luxury brands are reinventing their appeal
  - 17 creative ways marketers can address the rise of ad blockers
  - What makes a great user experience?
  - 2 answers to the ad-blocking conundrum
  - 3 ways to earn my marketing budget

- # Archives

  Select Month ▼

- Home
- News
- iMedia Blog
- ad:tech Blog
- In Focus
- Podcasts

- Events
- Calendar
- Coverage
- Request Invitation

- People Connection
- Find People
- Become a Member
- Sign In

- Resource Connection
- Find Company

- Job Connection
- Search Jobs
- Post a Job
- Purchase Packs
- Custom Orders
- Customer Service

- Subscribe
- iMedia Daily Newsletter
- iMedia UK Newsletter
- Twitter
- RSS

- Company Info
- About Us
- Advertise with Us
- Privacy Policy
- Terms of Use
- Contact Us

Copyright © 2016 iMedia Communications, Inc. All Rights Reserved.