RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

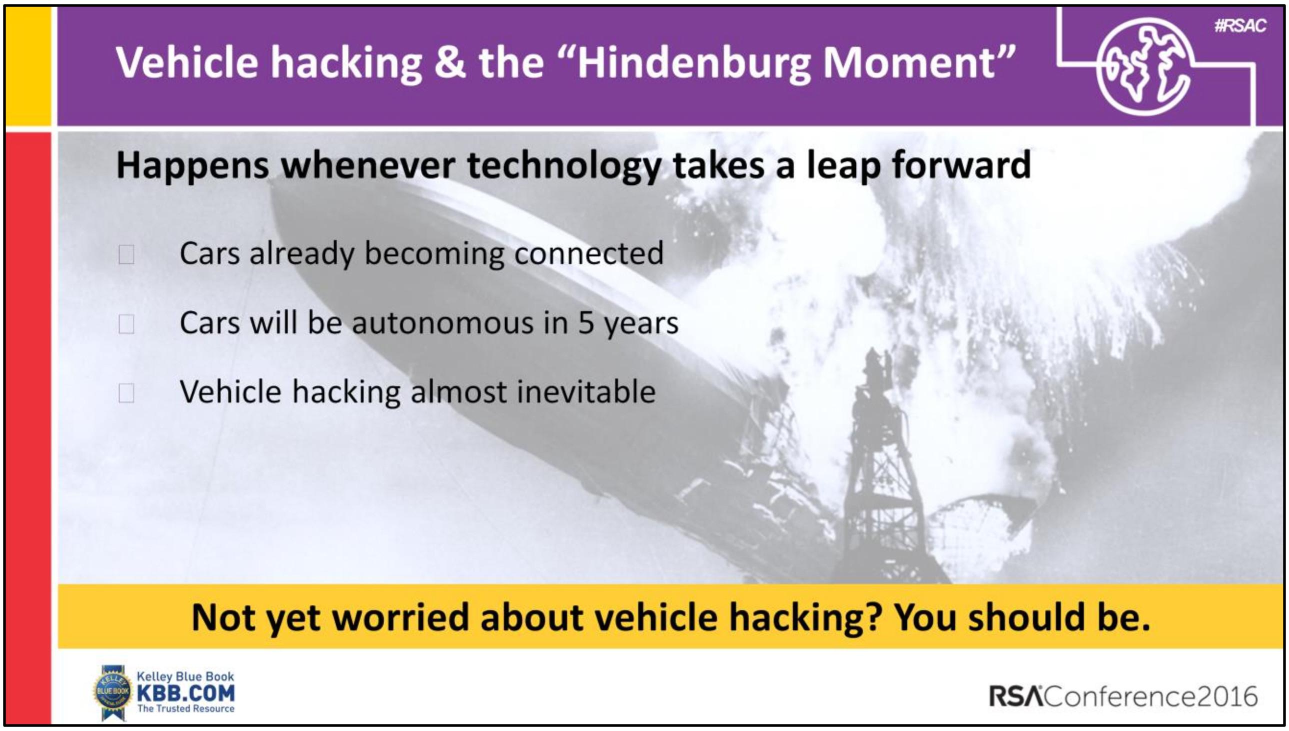
SESSION ID: HT-T11

Braking the Connected Car: The Future of Vehicle Vulnerabilities

Karl Brauer
Senior Director
Automotive Industry Insights
Kelley Blue Book

Akshay Anand
Manager
Commercial Insights
Kelley Blue Book

#RSAC



#RSAC

Vehicle hacking & the “Hindenburg Moment”

Happens whenever technology takes a leap forward

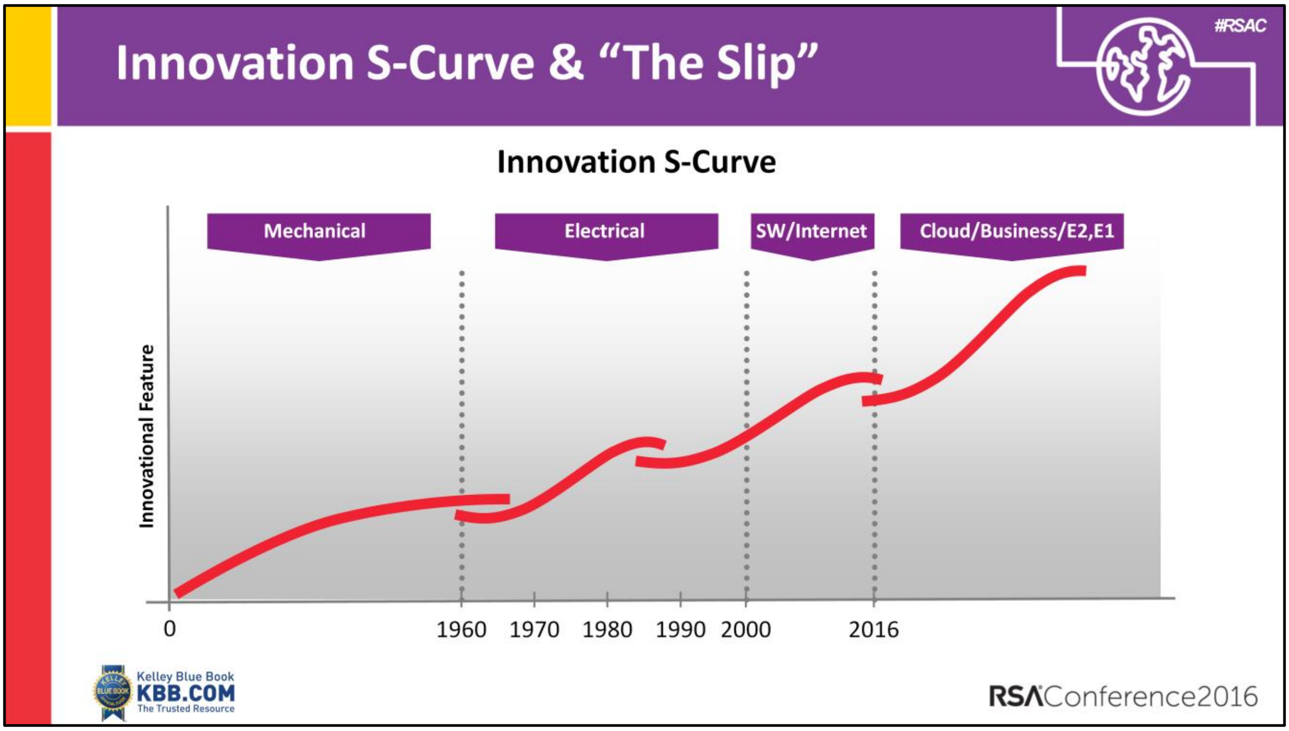
- Cars already becoming connected
- Cars will be autonomous in 5 years
- Vehicle hacking almost inevitable

Not yet worried about vehicle hacking? You should be.

Kelley Blue Book KBB.COM The Trusted Resource

RSAConference2016

- Whenever we shift to a new technology, there is a moment of “growing pains.”
  - Examples of this are the ABS, air bags, etc.
  - Connected cars will likely not be exempt from this.



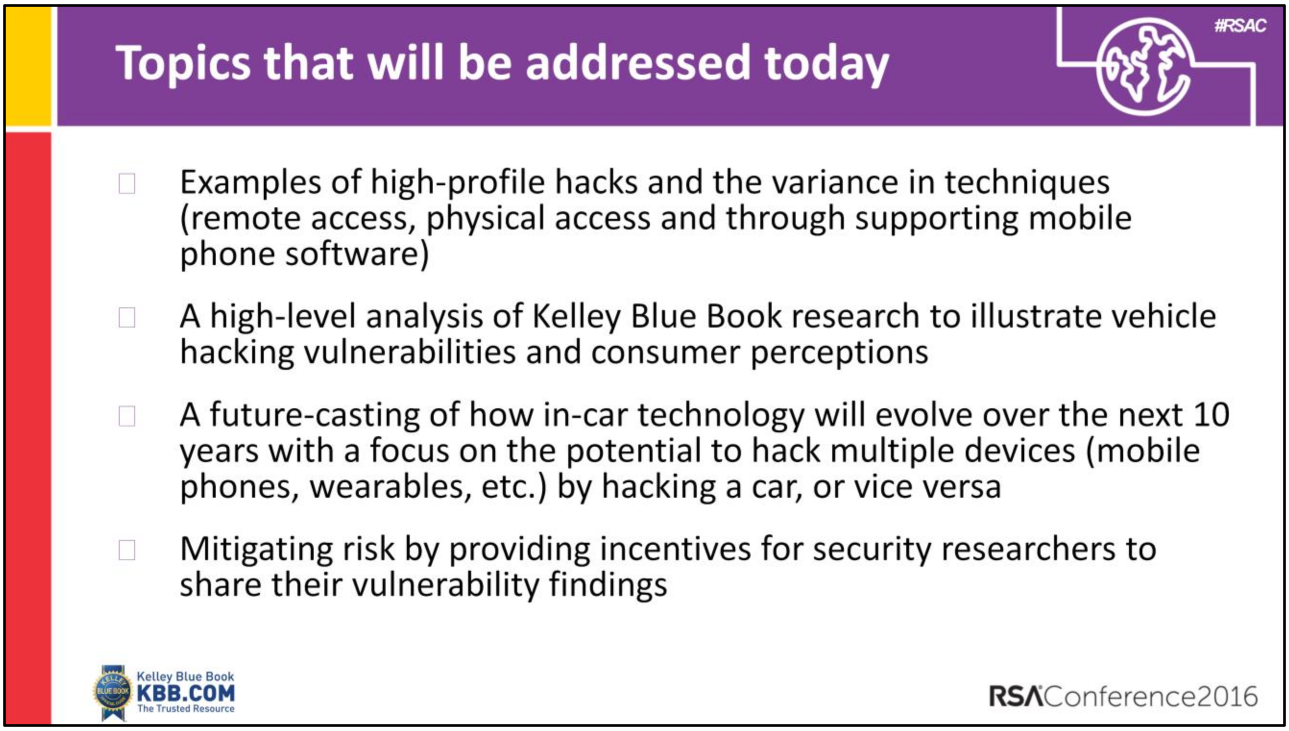
#RSAC

Innovation S-Curve & “The Slip”

Kelley Blue Book
KBB.COM
The Trusted Resource

RSAConference2016

- In a recent conversation with a major automaker engineer working on the company’s team for autonomous vehicles, we discussed the innovation s-curve and “the slip.”
  - When you move to the next level of innovation, you’ll start out at a slightly lower point than where you ended, due to new knowledge of what doesn’t work and potential previous failures/”Hindenberg moments”



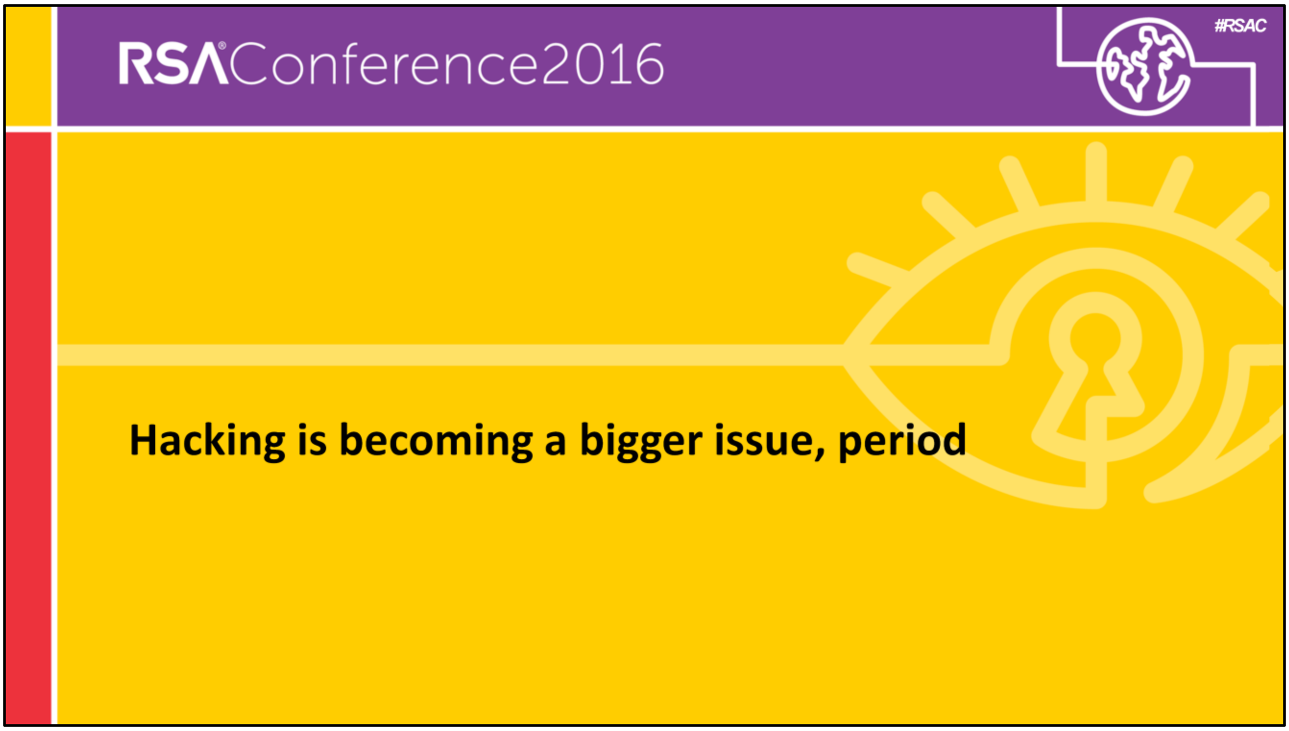
#RSAC

Topics that will be addressed today

- □ Examples of high-profile hacks and the variance in techniques (remote access, physical access and through supporting mobile phone software)
- □ A high-level analysis of Kelley Blue Book research to illustrate vehicle hacking vulnerabilities and consumer perceptions
- □ A future-casting of how in-car technology will evolve over the next 10 years with a focus on the potential to hack multiple devices (mobile phones, wearables, etc.) by hacking a car, or vice versa
- □ Mitigating risk by providing incentives for security researchers to share their vulnerability findings

Kelley Blue Book KBB.COM The Trusted Resource

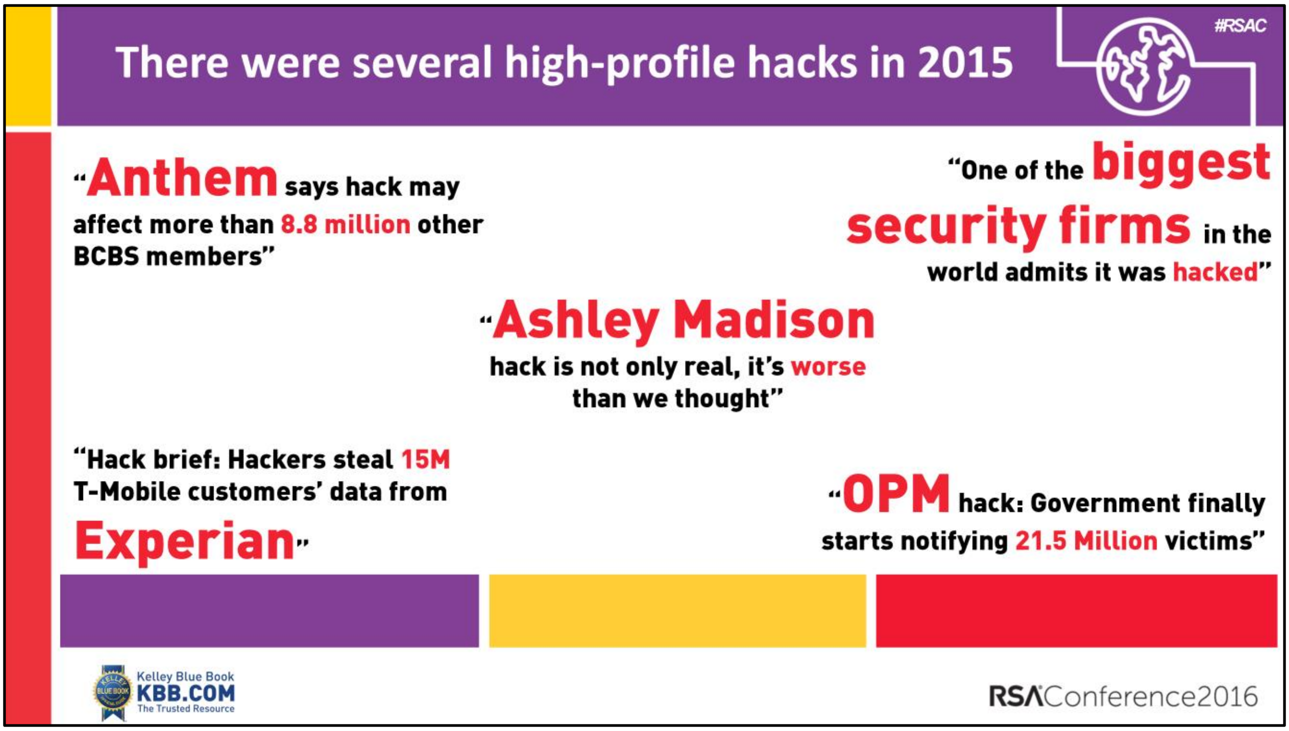
RSAConference2016



RSAConference2016

#RSAC

Hacking is becoming a bigger issue, period



#RSAC

There were several high-profile hacks in 2015

"**Anthem** says hack may affect more than **8.8 million** other BCBS members"

"One of the **biggest security firms** in the world admits it was **hacked**"

"**Ashley Madison** hack is not only real, it's **worse** than we thought"

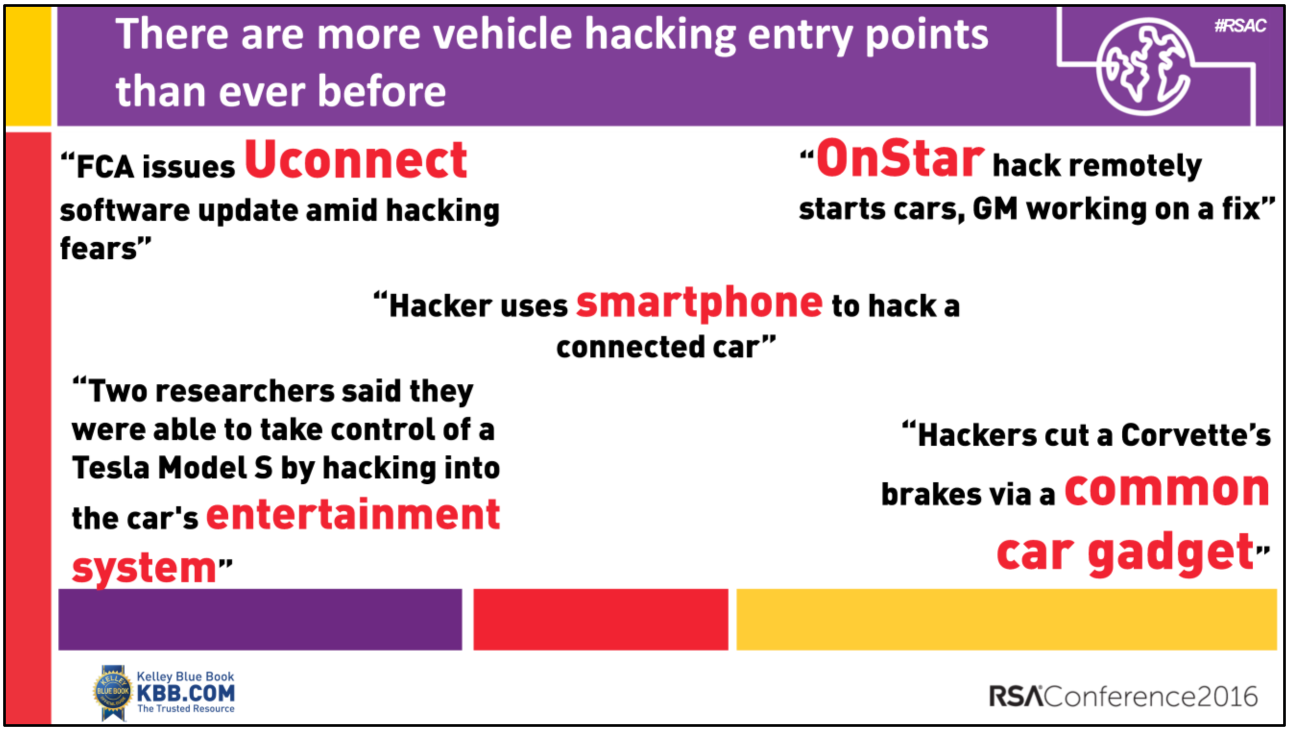
"Hack brief: Hackers steal **15M** T-Mobile customers' data from **Experian**"

"**OPM** hack: Government finally starts notifying **21.5 Million** victims"

Kelley Blue Book
KBB.COM
The Trusted Resource

RSAConference2016

- **Anthem -** Revealed a breach in February that exposed an astonishing 80 million patient and employee records.
- **Hacking Team -** The breach of Hacking Team on July 5 led to a cascade of other security threat revelations and had governments around the globe in hot water. The Hacking Team develops spy tools for government agencies, including those that can go around traditional anti-virus solutions. The breach published more than 1 million emails from the Italian surveillance company, revealing its involvement with oppressive governments as well as multiple Flash zero-day vulnerabilities.
- **Ashley Madison** – An online dating portal for extramarital affairs. Hackers allegedly gained access to millions of its customers information database and posted 10GB of personal data for its tens of Millions of customers, including their names and email addresses.
- **Sony Pictures -** The hack wasn't limited to unreleased movies — the unknown hackers leaked about 200 gigabytes of confidential data belonging to Sony Pictures from movie scripts to sensitive employees data, celebrity's' phone numbers and their travel aliases, making it the most severe hack in the History.
- **Flight Hacker -** During FBI interviews in February and March, Chris Roberts allegedly (cybersecurity consultant) told investigators he hacked into in-flight entertainment systems aboard aircraft. He claimed to have done so 15 to 20 times from 2011 to 2014.



There are more vehicle hacking entry points than ever before

#RSAC

"FCA issues **Uconnect** software update amid hacking fears"

"**OnStar** hack remotely starts cars, GM working on a fix"

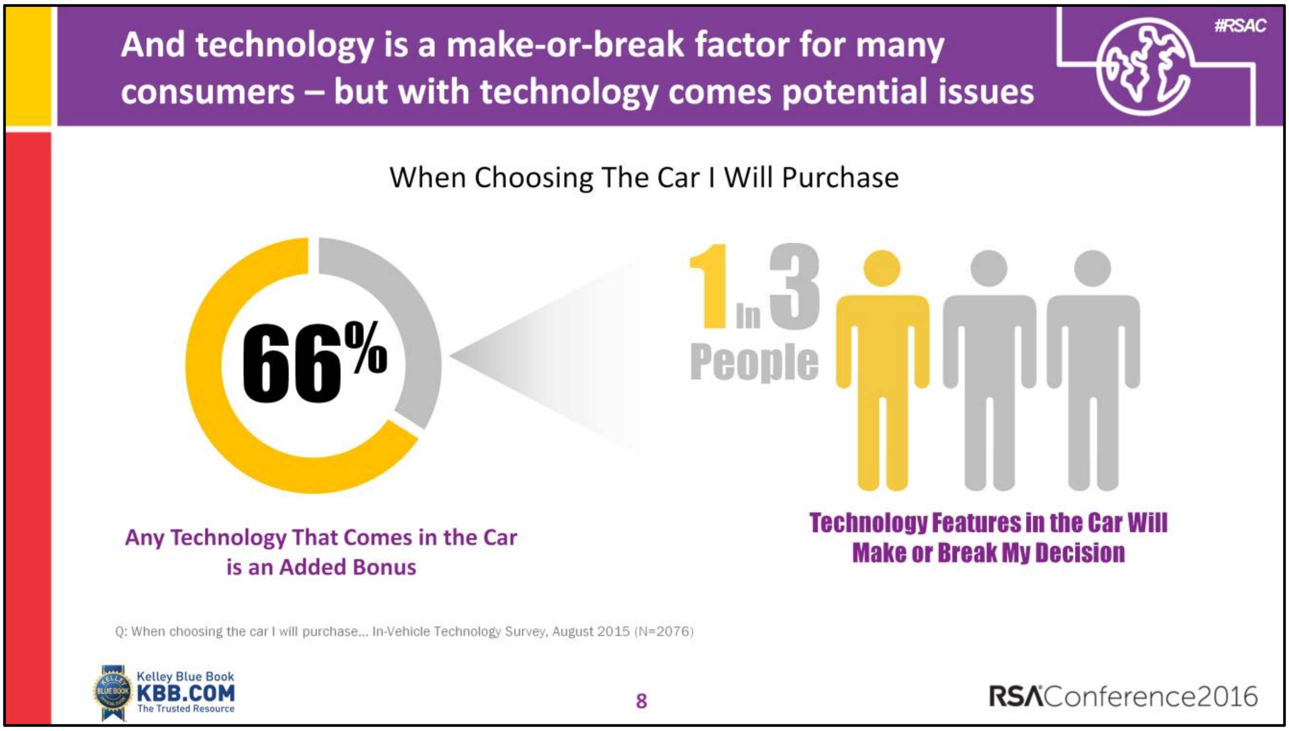
"Hacker uses **smartphone** to hack a connected car"

"Two researchers said they were able to take control of a Tesla Model S by hacking into the car's **entertainment system**"

"Hackers cut a Corvette's brakes via a **common car gadget**"

Kelley Blue Book
KBB.COM
The Trusted Resource

RSAConference2016



#RSAC

And technology is a make-or-break factor for many consumers – but with technology comes potential issues

When Choosing The Car I Will Purchase

66%

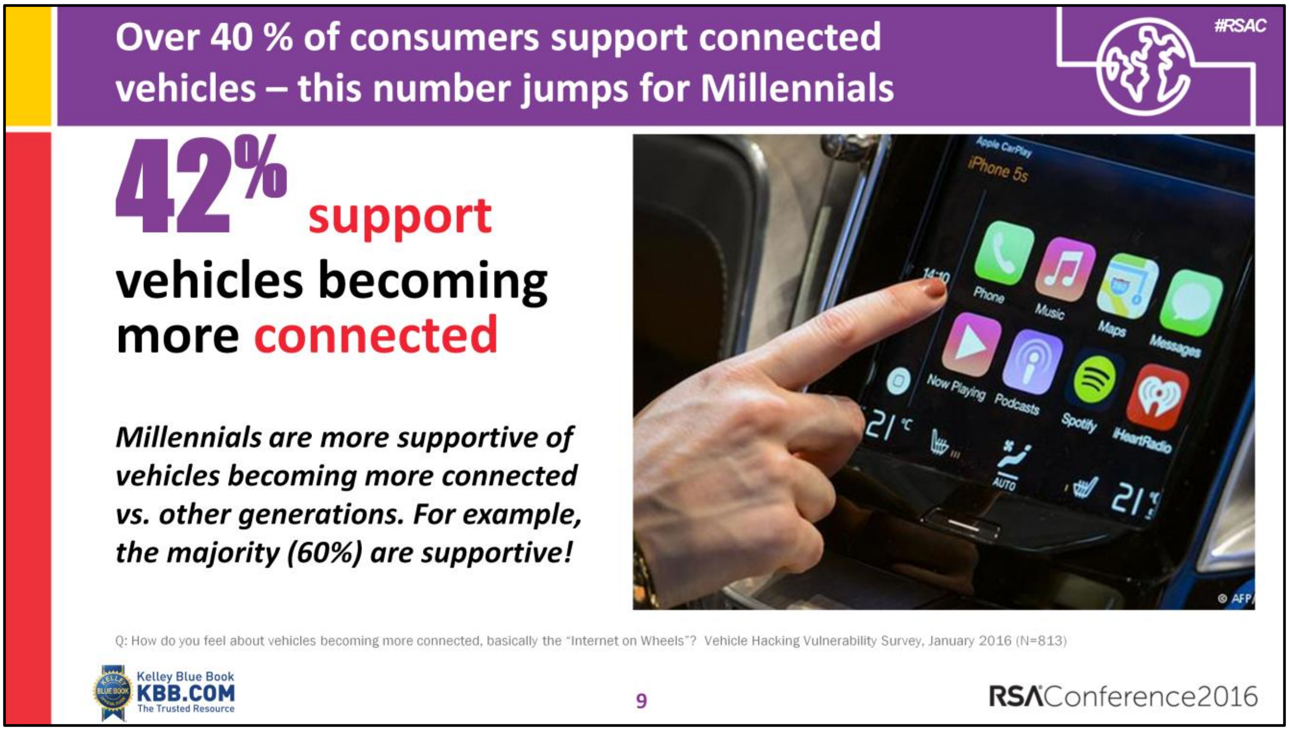
Any Technology That Comes in the Car is an Added Bonus

1 In 3 People

Technology Features in the Car Will Make or Break My Decision

Q: When choosing the car I will purchase... In-Vehicle Technology Survey, August 2015 (N=2076)

Kelley Blue Book KBB.COM The Trusted Resource



#RSAC

Over 40 % of consumers support connected vehicles – this number jumps for Millennials

42% **support** **vehicles becoming more connected**

Millennials are more supportive of vehicles becoming more connected vs. other generations. For example, the majority (60%) are supportive!

Apple CarPlay
iPhone 5s
14:10
Phone
Music
Maps
Messages
Now Playing
Podcasts
Spotify
iHeartRadio
21 °C
AUTO
21
© AFP

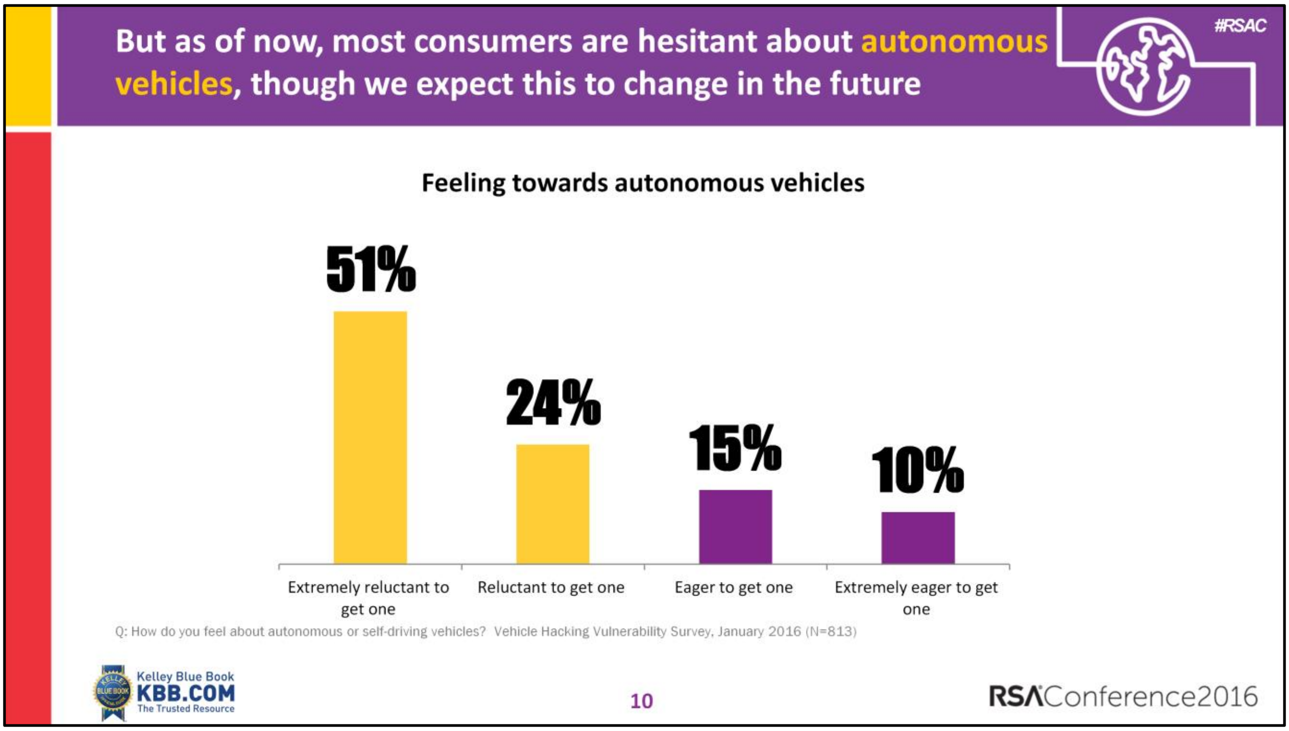
Q: How do you feel about vehicles becoming more connected, basically the "Internet on Wheels"? Vehicle Hacking Vulnerability Survey, January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

9

RSAConference2016

- SUPPORTIVE – Millennials (60%), Generation X (41%), Baby Boomers (42%), and Silent Generation (32%).



#RSAC

But as of now, most consumers are hesitant about autonomous vehicles, though we expect this to change in the future

Feeling towards autonomous vehicles

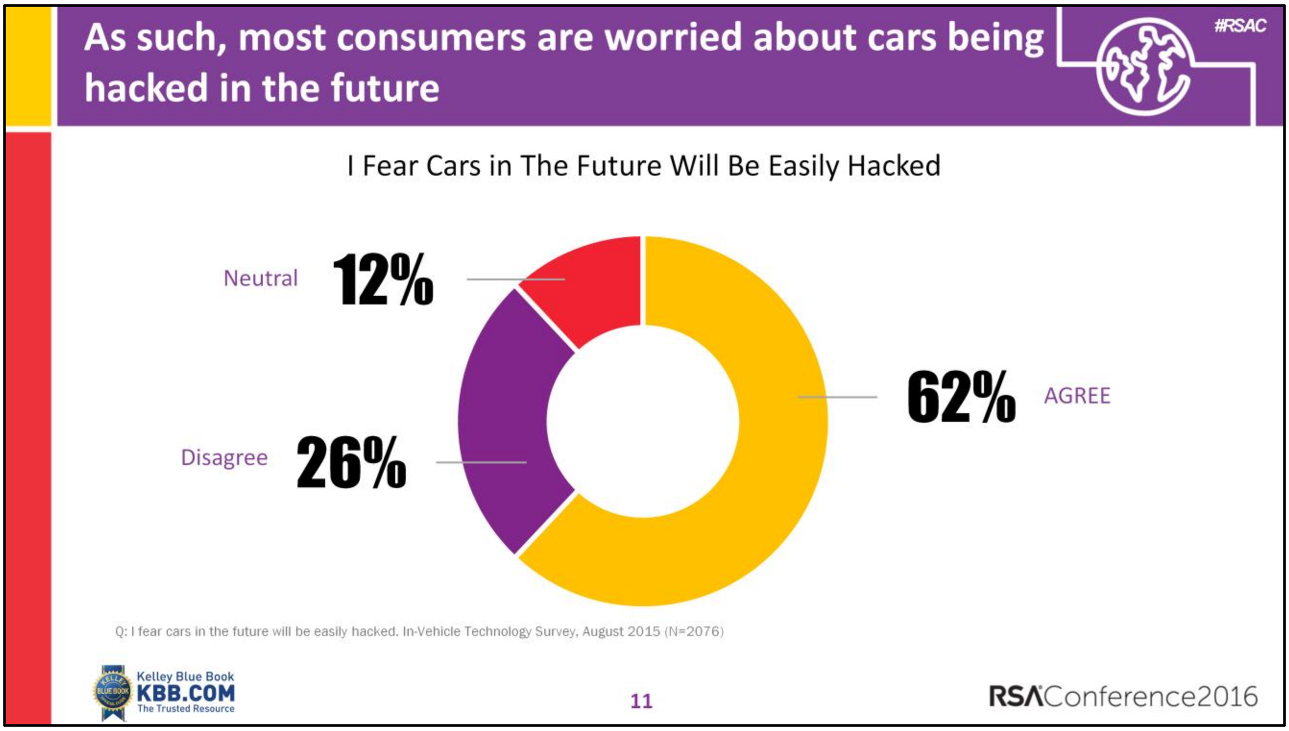
Q: How do you feel about autonomous or self-driving vehicles? Vehicle Hacking Vulnerability Survey, January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

10

RSAConference2016

- Millennials are more eager to get one (42% said “eager to get one” or “extremely eager to get one”)



As such, most consumers are worried about cars being hacked in the future

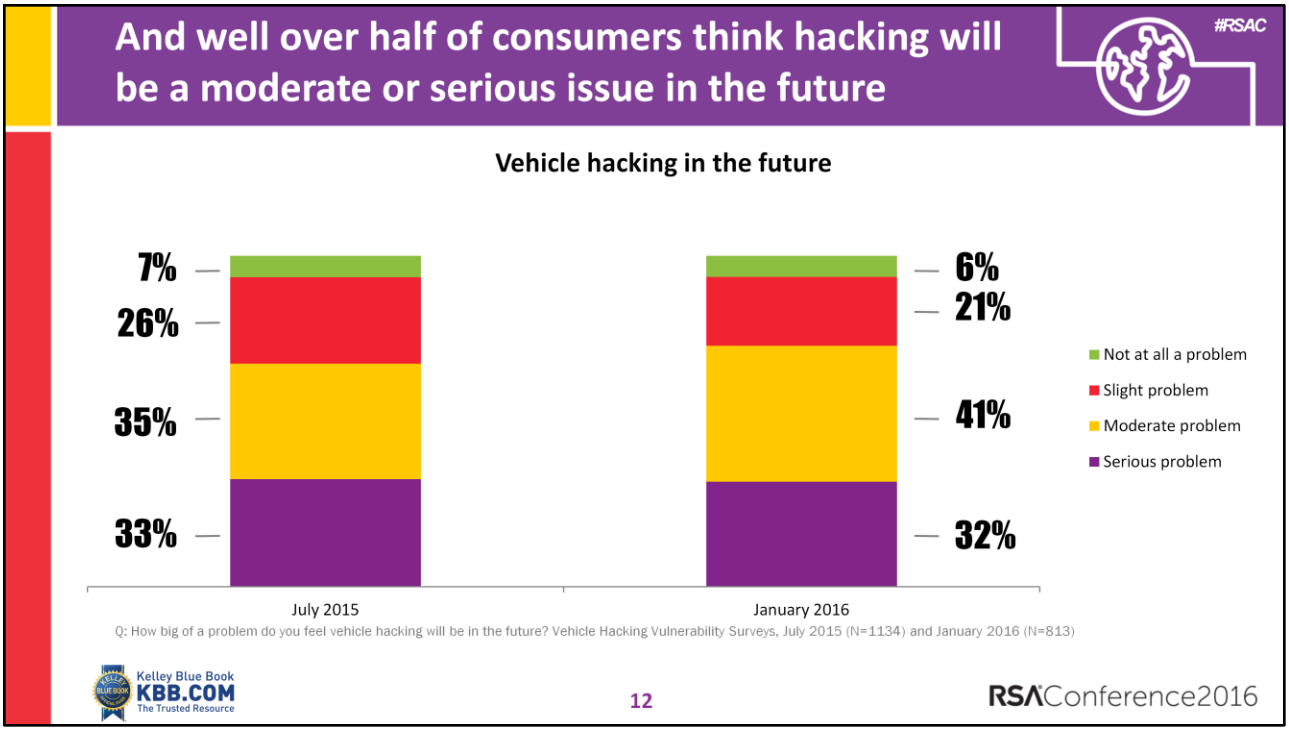
#RSAC

I Fear Cars in The Future Will Be Easily Hacked

Q: I fear cars in the future will be easily hacked. In-Vehicle Technology Survey, August 2015 (N=2076)

Kelley Blue Book
KBB.COM
The Trusted Resource

RSAConference2016



#RSAC

And well over half of consumers think hacking will be a moderate or serious issue in the future

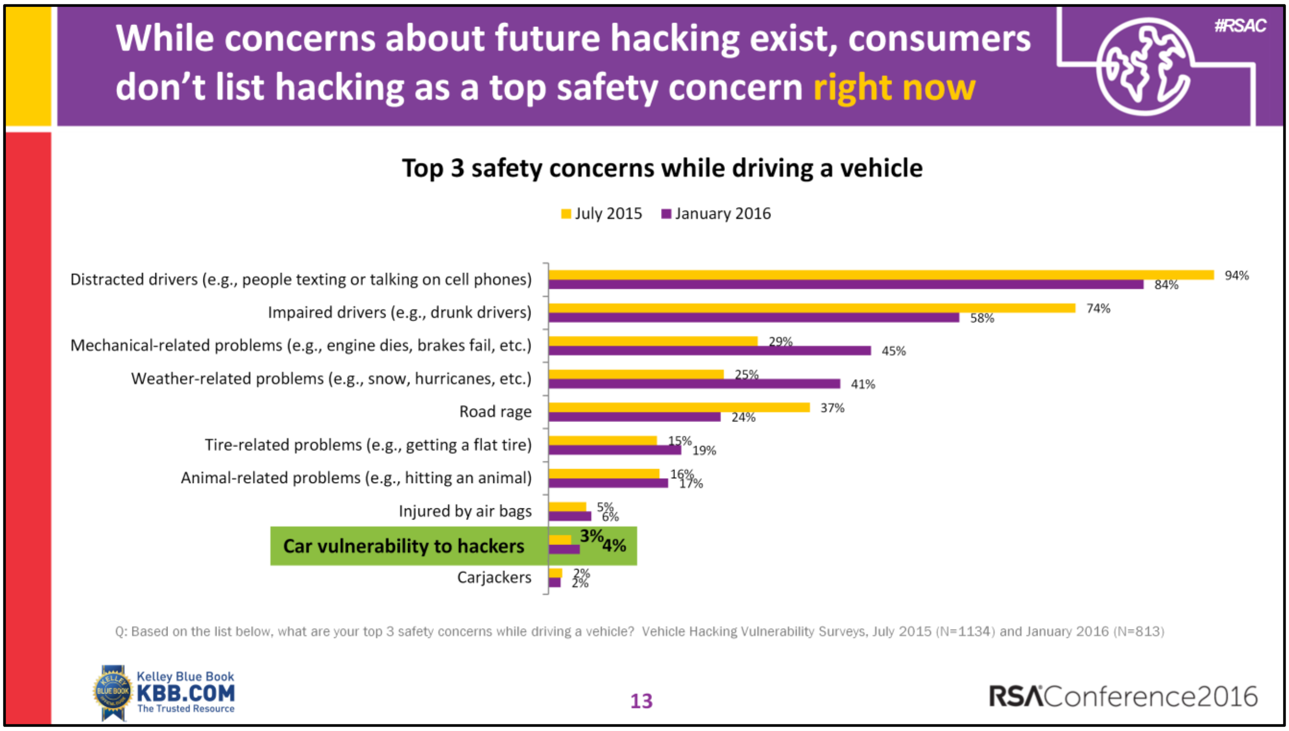
Vehicle hacking in the future

Q: How big of a problem do you feel vehicle hacking will be in the future? Vehicle Hacking Vulnerability Surveys, July 2015 (N=1134) and January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

RSAConference2016

- 73% report "moderate" or "serious" problem – a 5% increase from July
- Segments, regardless of age generation, feel hacking will be a "moderate" or "serious" problem in the future – 70% or more for each age segment.
- Nearly 70% of consumers think vehicle hacking will be a frequent problem within the next 3 years
- About half of consumers see "theft" as the main motive behind hacking a vehicle, followed by a "hacker's ego/showing it can be done" at 31%.
- About a third of consumers say they will consider whether a vehicle can be hacked when shopping for their next vehicle.
- NOTE: In July, we asked "What type of effect did the news story have on you?" and 41% reported they will "somewhat" or "seriously" consider hacking when buying/leasing their next car. In January's survey, 31% said hacking will have a "moderate" or "huge" impact.



#RSAC

While concerns about future hacking exist, consumers don't list hacking as a top safety concern right now

Top 3 safety concerns while driving a vehicle

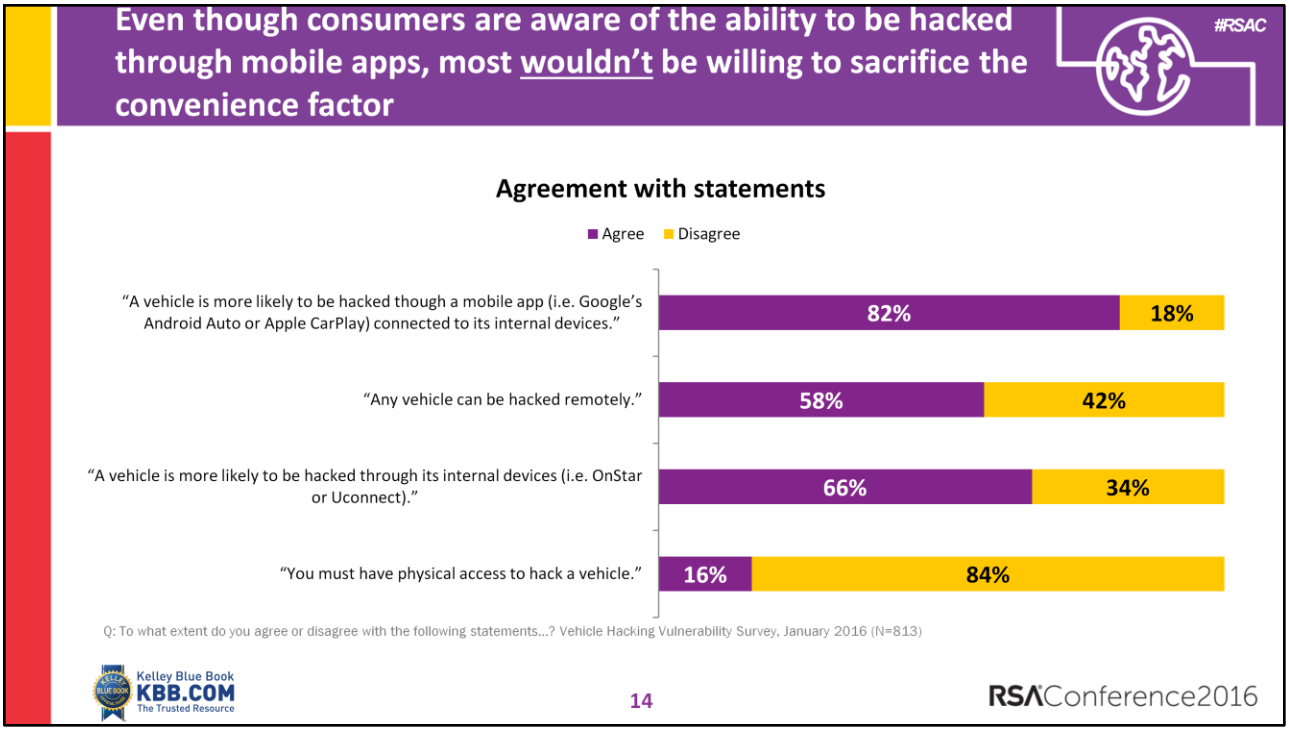
Q: Based on the list below, what are your top 3 safety concerns while driving a vehicle? Vehicle Hacking Vulnerability Surveys, July 2015 (N=1134) and January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

13

RSAConference2016

- Car vulnerability is 2nd lowest choice
- People are more worried about injury from airbag than from car hacking
- Millennials were more inclined to cite "Car vulnerability to hackers" as a top safety concern vs. other generations. For example, 12% for Millennials vs. 3% for Baby Boomers.
- Consumers are currently more concerned with having their privacy invaded vs. vehicle hacking



Even though consumers are aware of the ability to be hacked through mobile apps, most <u>wouldn't</u> be willing to sacrifice the convenience factor

#RSAC

Q: To what extent do you agree or disagree with the following statements...? Vehicle Hacking Vulnerability Survey, January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

RSAConference2016

- About half of consumers (48%) are somewhat or very interested in connected mobile apps (i.e. Android Auto and Apple CarPlay)
- Millennials are way more interested in mobile apps than their counterparts. For example, 68% for Millennials vs. 48% for Baby Boomers. (very and somewhat interested)
- Only 13% of people would never use an app if it increased the potential for their vehicle to be hacked

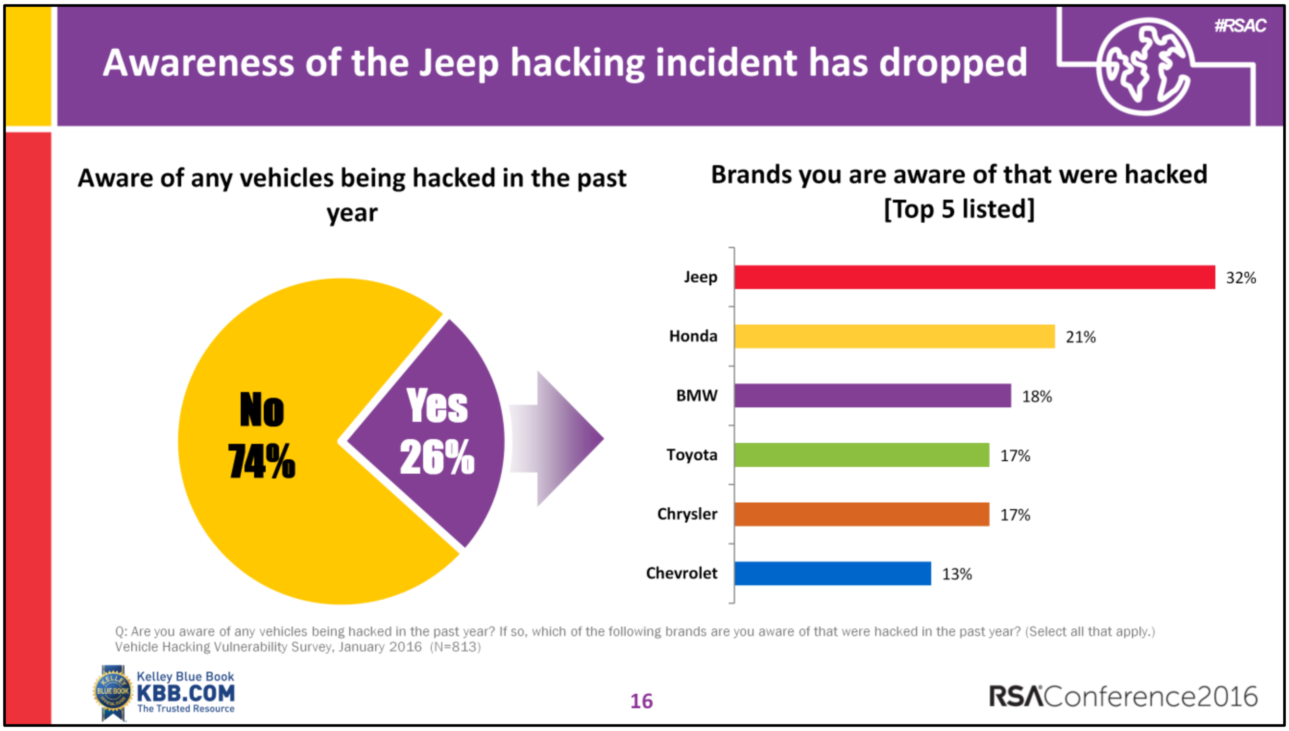
RSAConference2016

#RSAC

Despite the potential threats, consumers still throw responsibility elsewhere

Research Conducted Illustrating Vehicle Hacking Vulnerabilities and Consumer Perceptions

1. Vehicle Hacking Vulnerability Survey #1
   - Fielded in July 2015 to Blue Ribbon Panel members; 1134 survey responses were gathered.
2. In-Vehicle Technology Survey
   - Fielded in August 2015 to individuals on KBB.com; 2076 survey responses were gathered.
3. Vehicle Hacking Vulnerability Survey #2
   - Fielded in January 2016 to individuals on KBB.com; 813 survey responses were gathered.
4. KEY TAKEAWAY: People want access to technology and will ultimately end up choosing convenience over risk.



#RSAC

Awareness of the Jeep hacking incident has dropped

Aware of any vehicles being hacked in the past year

Brands you are aware of that were hacked [Top 5 listed]

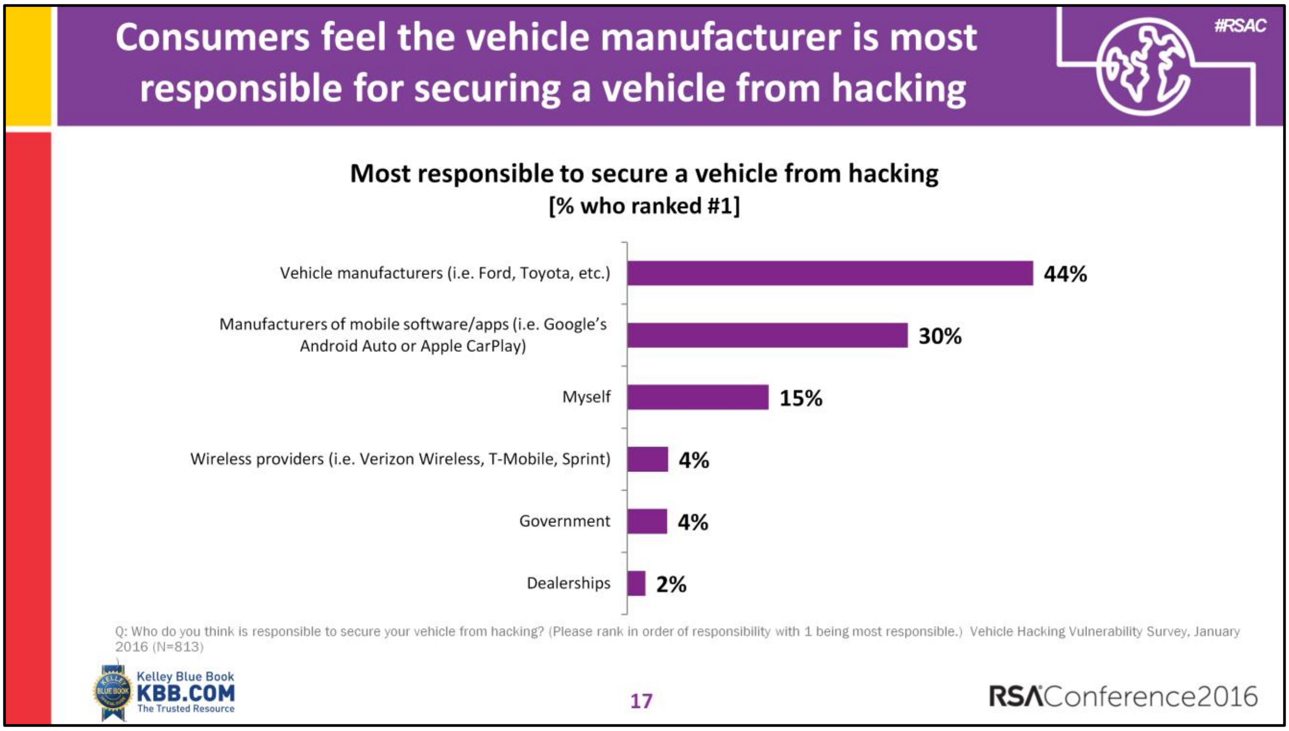
Q: Are you aware of any vehicles being hacked in the past year? If so, which of the following brands are you aware of that were hacked in the past year? (Select all that apply.)
Vehicle Hacking Vulnerability Survey, January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

16

RSAConference2016

- In July, the majority (72%) were aware of the Jeep Cherokee hacking incident. However, the news was topical and we asked the question differently: “Are you aware of the news regarding the hacking of a Jeep Cherokee?” in the previous survey conducted.
- Millennials were less likely to be aware of any vehicles being hacked in the past year vs. other generations.
- Key takeaway: In general, consumers are fairly quick to forget unless it’s being reported in the media at present. Additionally, most don’t own a connected car.



#RSAC

Consumers feel the vehicle manufacturer is most responsible for securing a vehicle from hacking

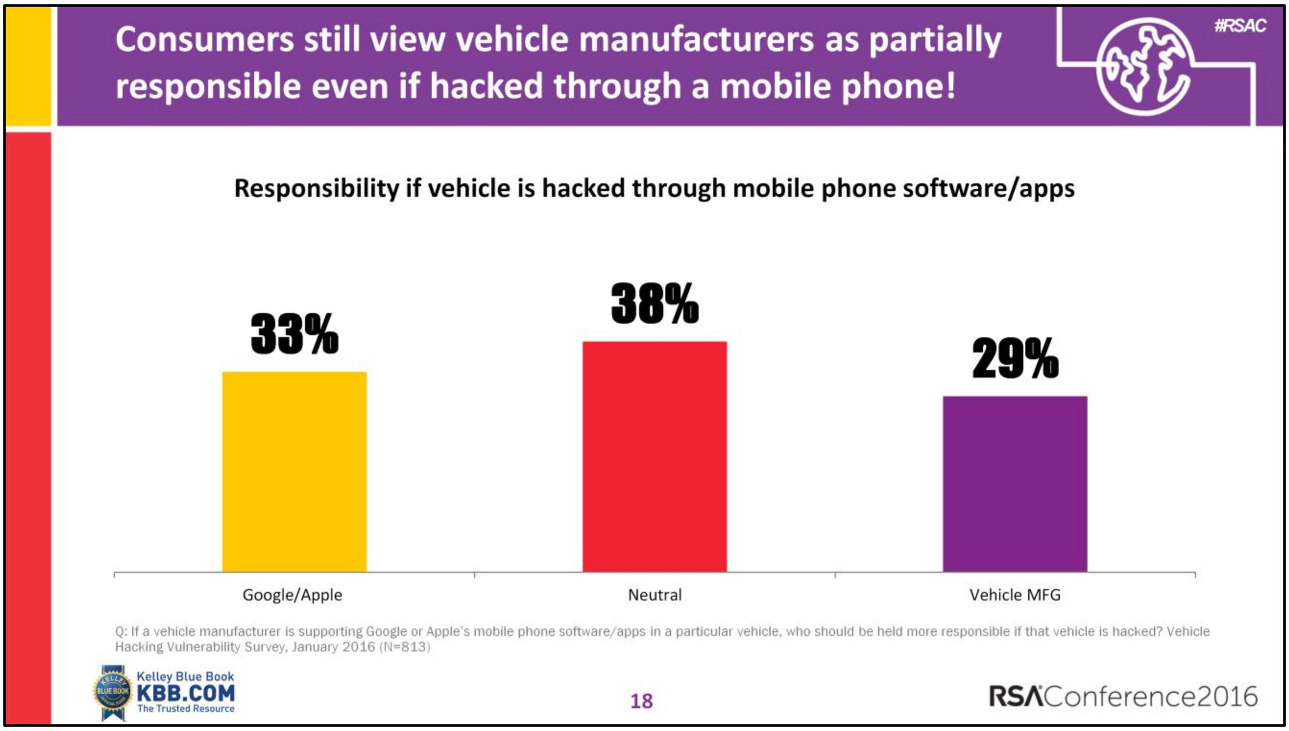
Most responsible to secure a vehicle from hacking
[% who ranked #1]

Q: Who do you think is responsible to secure your vehicle from hacking? (Please rank in order of responsibility with 1 being most responsible.) Vehicle Hacking Vulnerability Survey, January 2016 (N=813)

Kelley Blue Book
KBB.COM
The Trusted Resource

17

RSAConference2016



#RSAC

Consumers still view vehicle manufacturers as partially responsible even if hacked through a mobile phone!

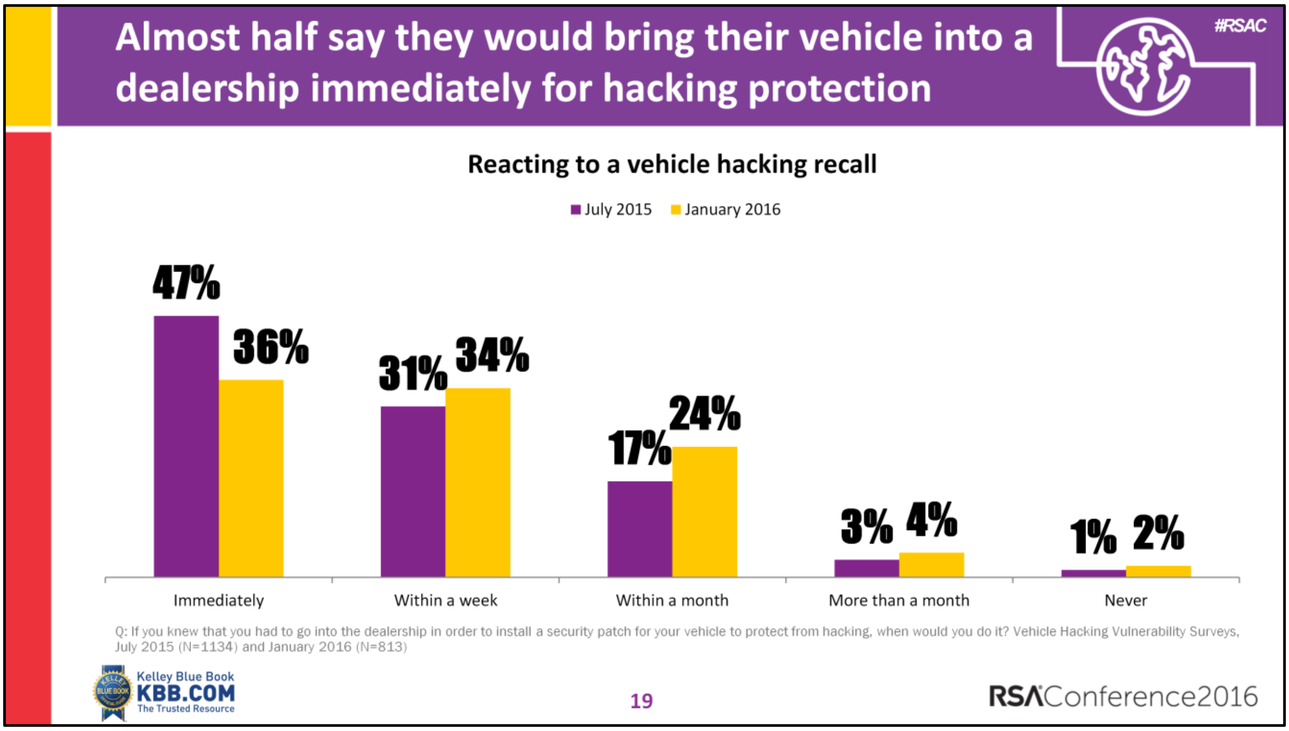
Responsibility if vehicle is hacked through mobile phone software/apps

Q: If a vehicle manufacturer is supporting Google or Apple's mobile phone software/apps in a particular vehicle, who should be held more responsible if that vehicle is hacked? Vehicle Hacking Vulnerability Survey, January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

RSAConference2016

- Key takeaway: Consumers always view the vehicle manufacturer as partially responsible, no matter what method was used to hack into the car



Almost half say they would bring their vehicle into a dealership immediately for hacking protection

#RSAC

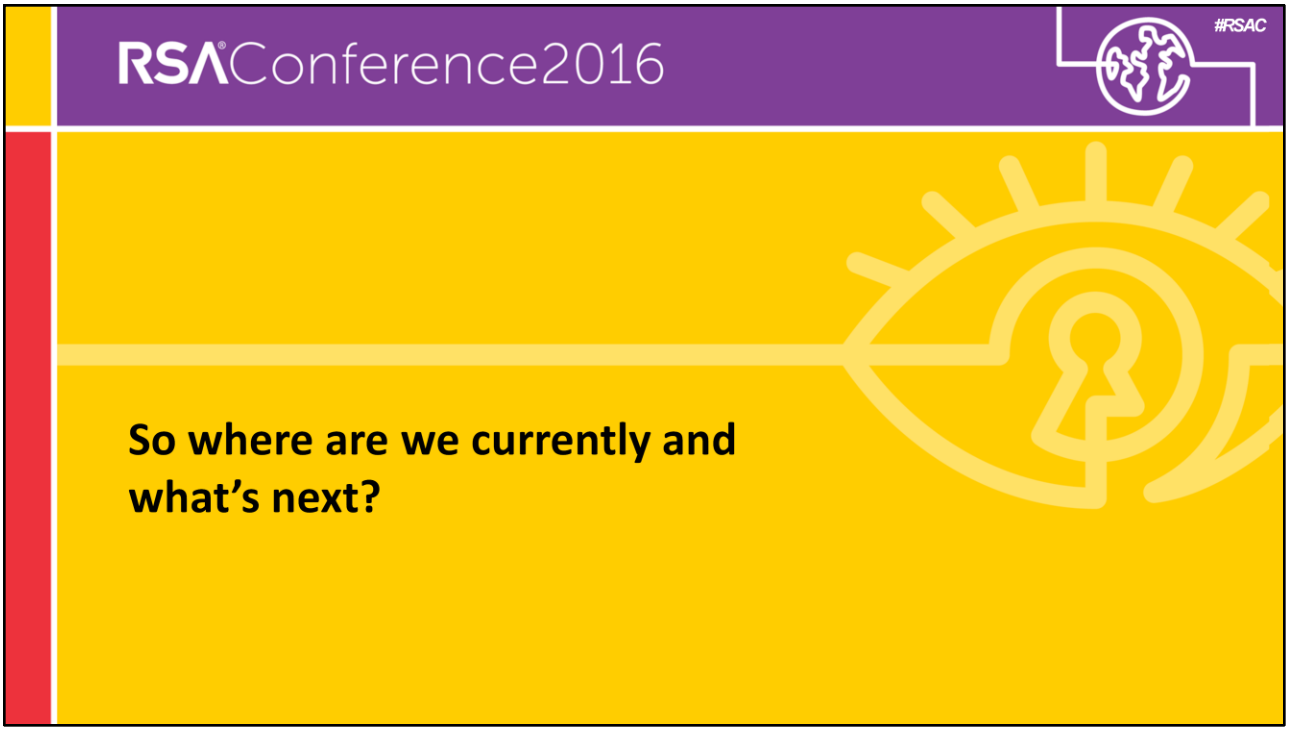
Reacting to a vehicle hacking recall

Q: If you knew that you had to go into the dealership in order to install a security patch for your vehicle to protect from hacking, when would you do it? Vehicle Hacking Vulnerability Surveys, July 2015 (N=1134) and January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

RSAConference2016

- About 70% of consumers take their vehicle in to the dealership 80% or more of the time when there is a recall.
- The group pushing the most for connected vehicles, Millennials, are less likely to take their vehicle in when they receive a recall notice. For example, 65% for Millennials vs. 83% for Baby Boomers and 85% for Silent Generation.
- Key takeaway: Unless updates are over-the-air, it’s unlikely that all vehicles will be protected from hacking at all times. E.g. Similar to computer software updates

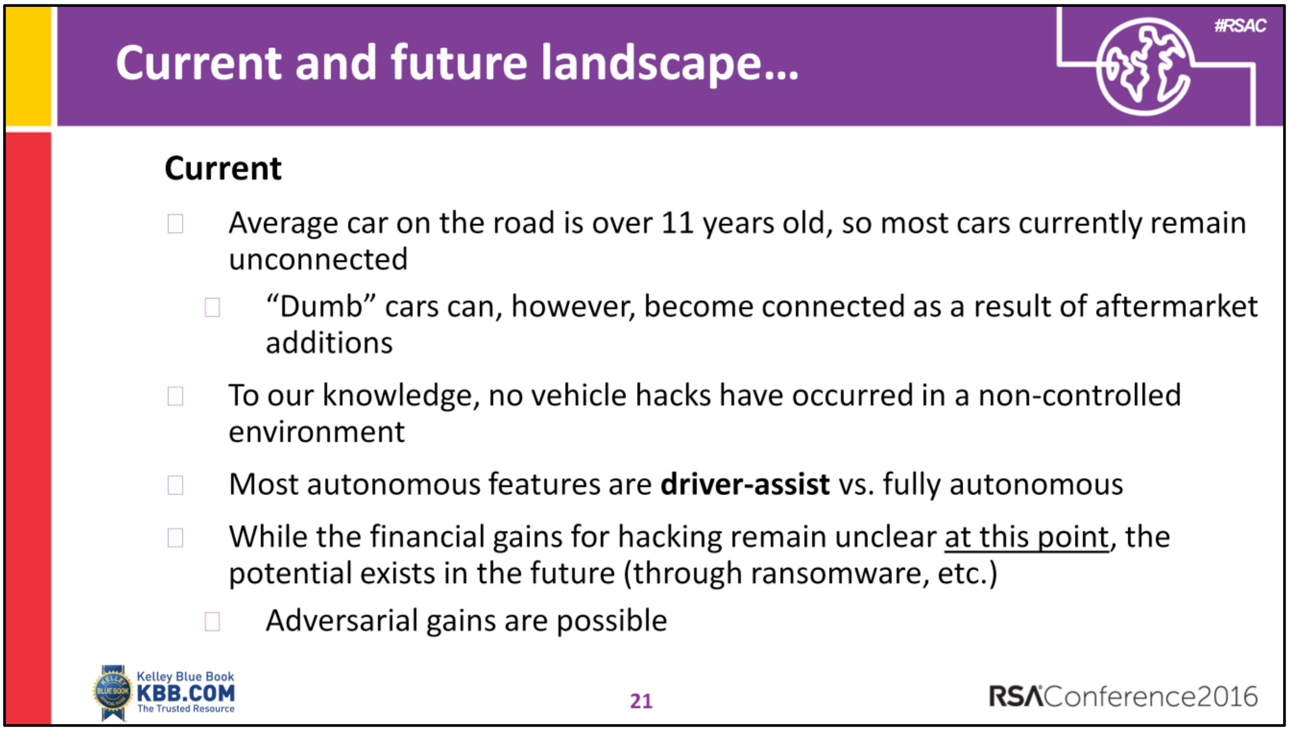


RSAConference2016

#RSAC

So where are we currently and what's next?

KEY TAKEAWAY: Bottom line – consumers, government, manufacturers and software companies, etc. need to do more, as connected technology is only increasing in availability.



#RSAC

Current and future landscape…

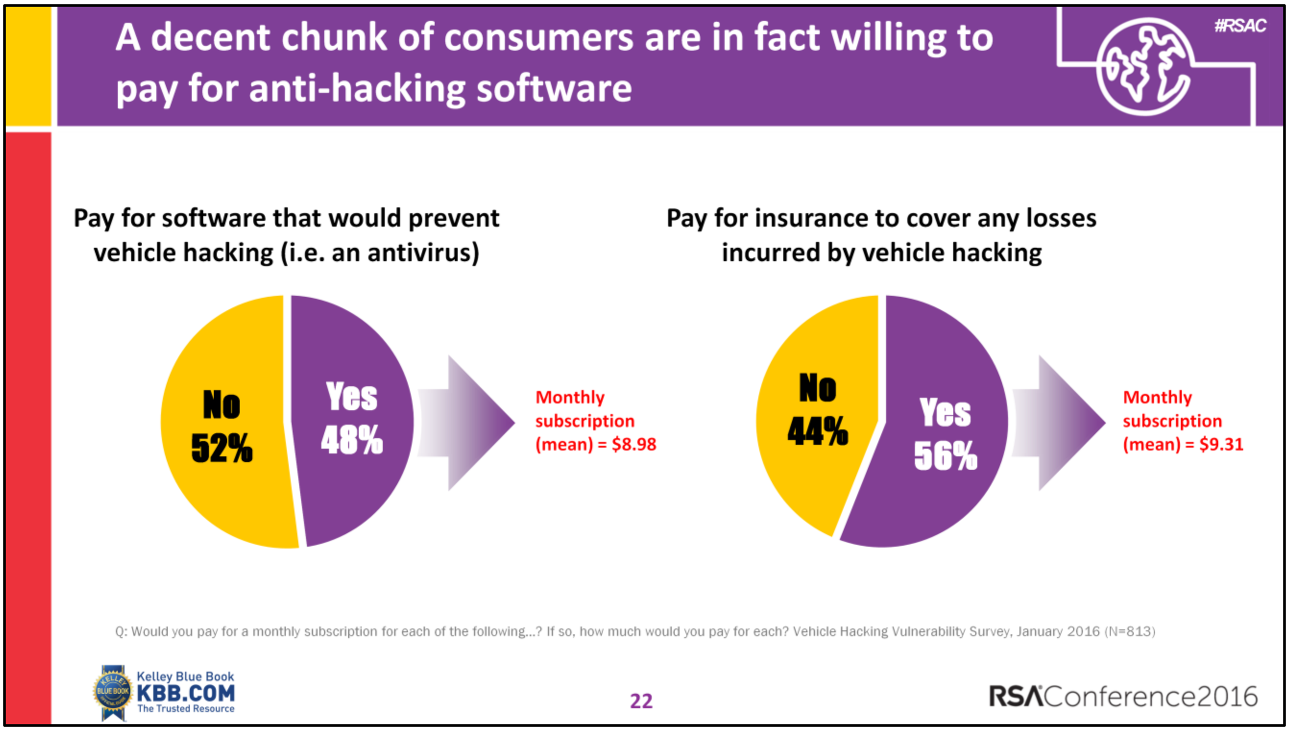
Current

- Average car on the road is over 11 years old, so most cars currently remain unconnected
  - “Dumb” cars can, however, become connected as a result of aftermarket additions
- To our knowledge, no vehicle hacks have occurred in a non-controlled environment
- Most autonomous features are **driver-assist** vs. fully autonomous
- While the financial gains for hacking remain unclear at this point, the potential exists in the future (through ransomware, etc.)
  - Adversarial gains are possible

Kelley Blue Book KBB.COM The Trusted Resource

21

RSAConference2016



#RSAC

A decent chunk of consumers are in fact willing to pay for anti-hacking software

Pay for software that would prevent vehicle hacking (i.e. an antivirus)

Monthly subscription (mean) = $8.98

Pay for insurance to cover any losses incurred by vehicle hacking

Monthly subscription (mean) = $9.31

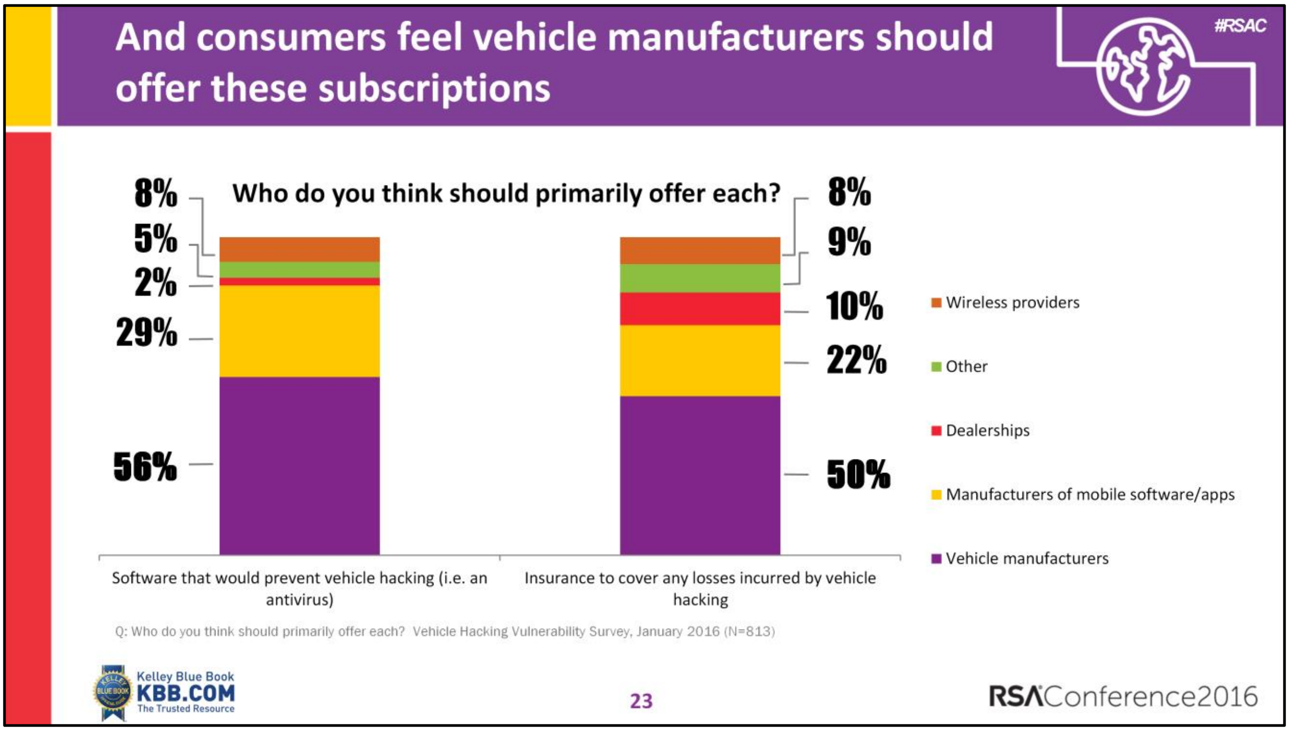
Q: Would you pay for a monthly subscription for each of the following...? If so, how much would you pay for each? Vehicle Hacking Vulnerability Survey, January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

22

RSAConference2016

- Millennials and the Silent Generation are more inclined to pay a monthly subscription for software that would prevent vehicle hacking (i.e. an antivirus) than the other 2 age generations.
- Millennials will pay more money for monthly subscriptions for both Software and Insurance to cover vehicle hacking than other generations. For example for software ($10.67) and insurance ($15.20).



And consumers feel vehicle manufacturers should offer these subscriptions

#RSAC

Who do you think should primarily offer each?

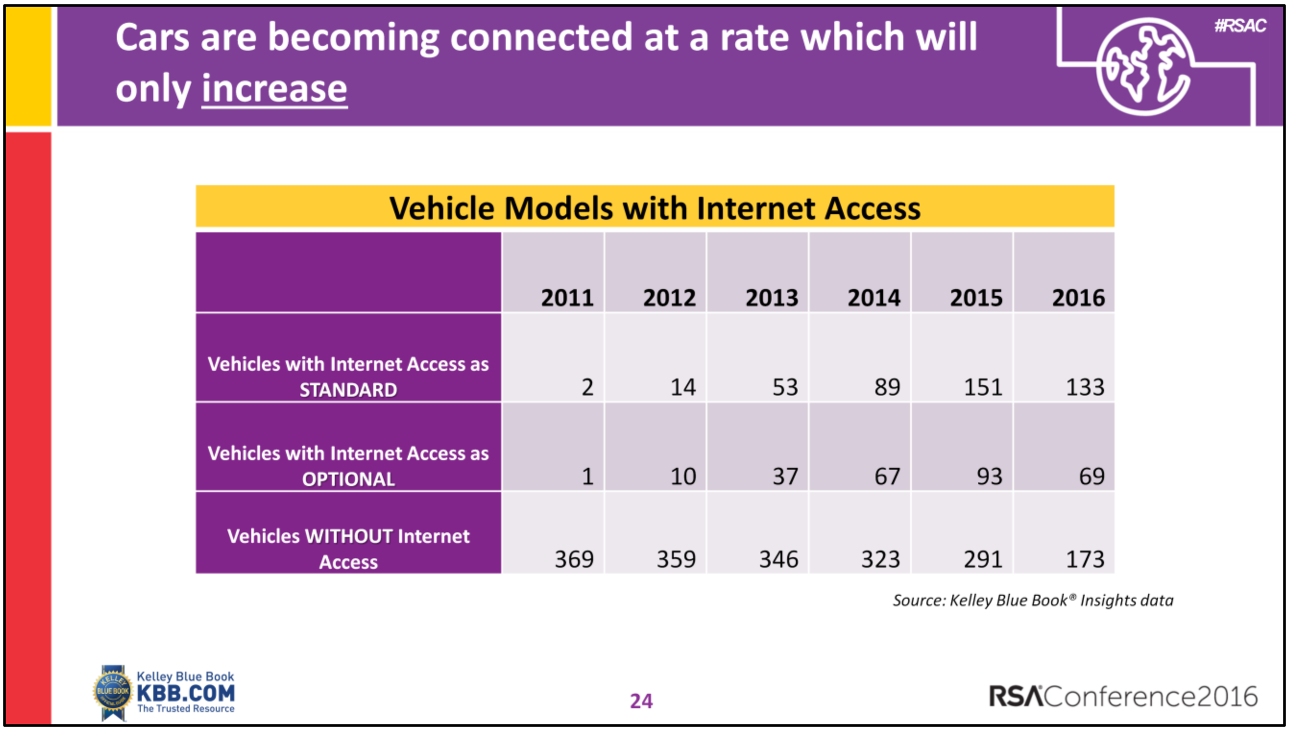
Q: Who do you think should primarily offer each? Vehicle Hacking Vulnerability Survey, January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

23

RSAConference2016

- Segments, regardless of age generation, feel vehicle manufacturers should primarily offer both software and insurance vs. other entities (i.e. manufacturers of mobile software/apps)



#RSAC

Cars are becoming connected at a rate which will only increase

Vehicle Models with Internet Access

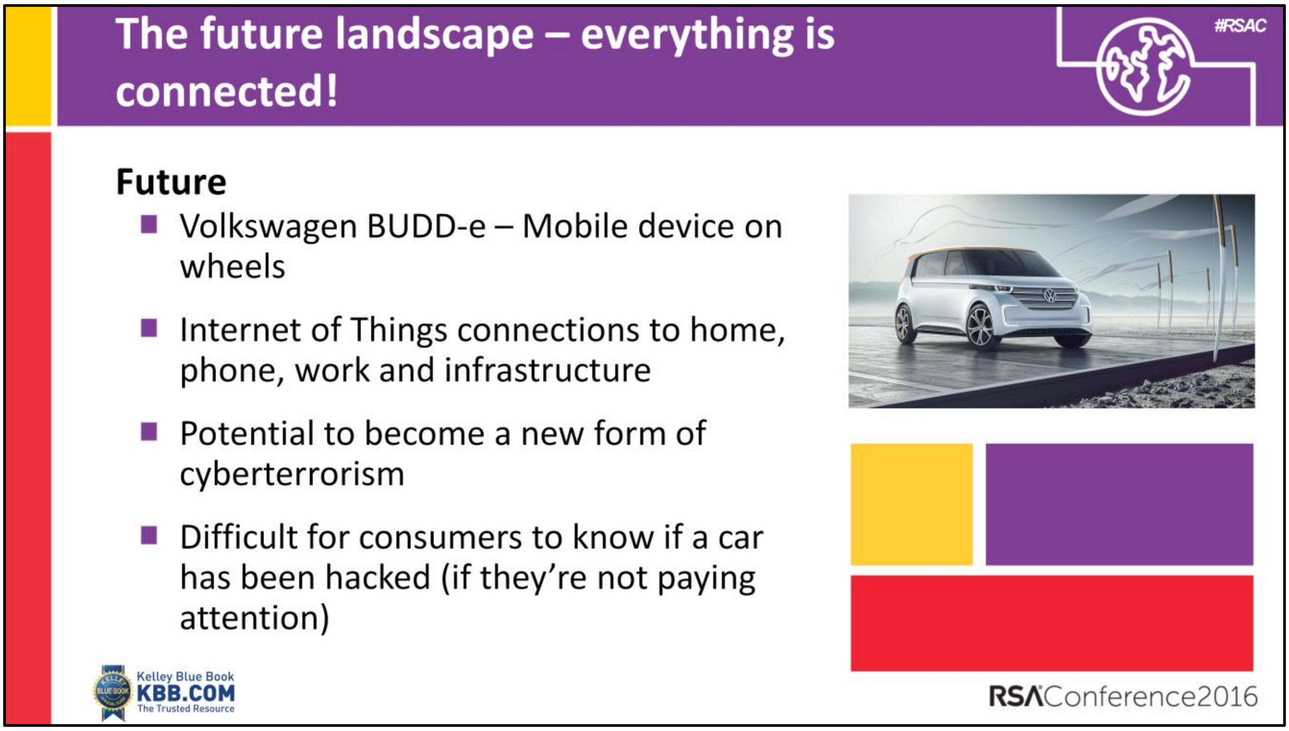
	2011	2012	2013	2014	2015	2016
Vehicles with Internet Access as STANDARD	2	14	53	89	151	133
Vehicles with Internet Access as OPTIONAL	1	10	37	67	93	69
Vehicles WITHOUT Internet Access	369	359	346	323	291	173

Source: Kelley Blue Book® Insights data

Kelley Blue Book KBB.COM The Trusted Resource

RSAConference2016

- Far fewer vehicles exist that are “connected” than those that aren’t.



#RSAC

The future landscape – everything is connected!

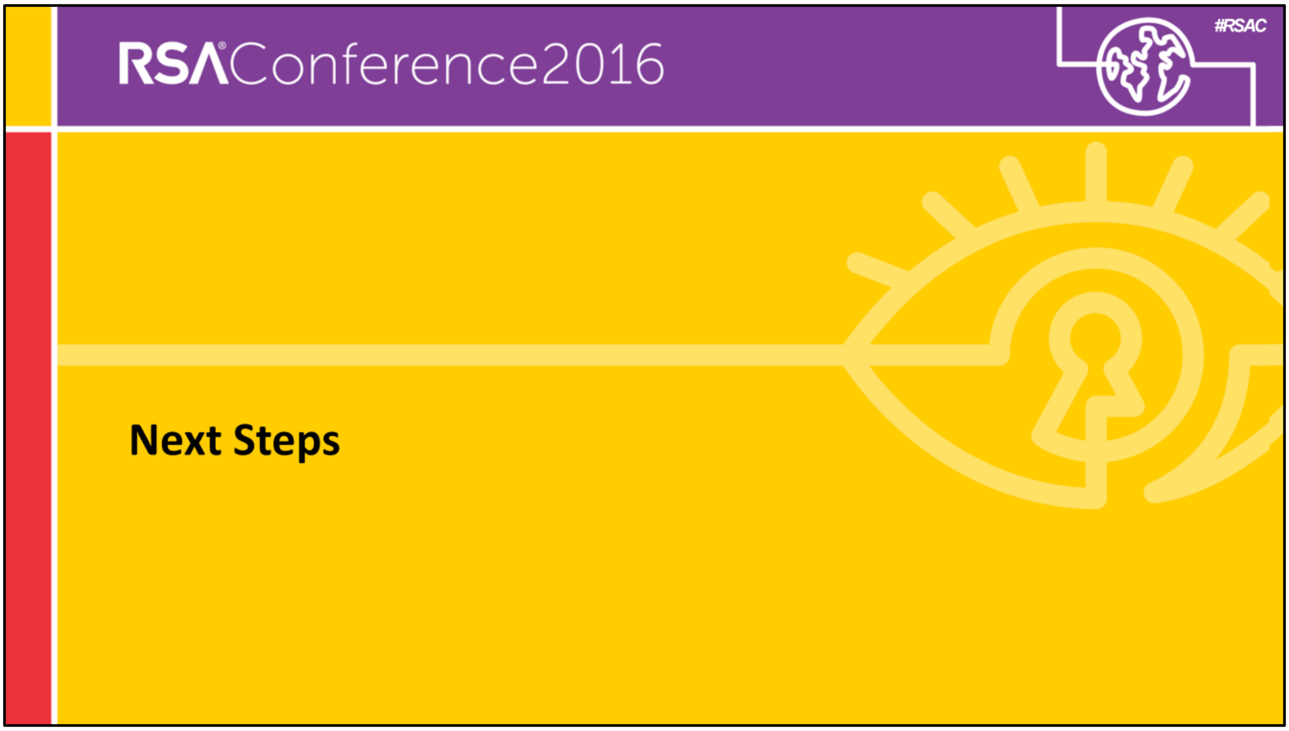
Future

- Volkswagen BUDD-e – Mobile device on wheels
- Internet of Things connections to home, phone, work and infrastructure
- Potential to become a new form of cyberterrorism
- Difficult for consumers to know if a car has been hacked (if they're not paying attention)

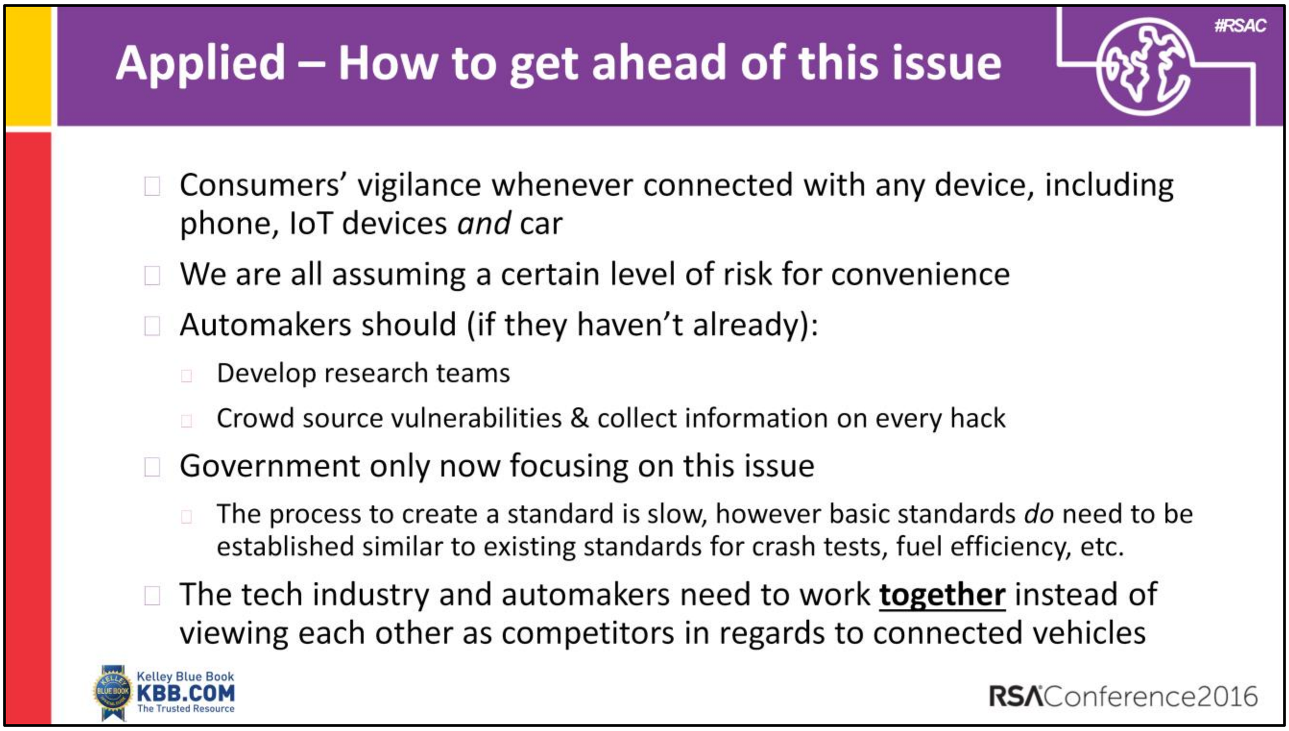
Kelley Blue Book KBB.COM The Trusted Resource

RSAConference2016

- Future
  - Vehicles are becoming a moving mobile device
  - If your car has access to credit card, it could pose financial risk
  - Exploit is posted once it's discovered
  - Potential to become a new form of cyberterrorism
    - How easy would it be to take over one car, then take over a whole freeway of cars?
  - A lot harder to know when car is hacked when fully autonomous (because you're not driving, so you're likely not paying attention)
  - Responsibility at different entry points
    - Hacking your phone, hack your house
  - Anti-virus software for car
  - Emergency service vehicles



Next Steps



Applied – How to get ahead of this issue

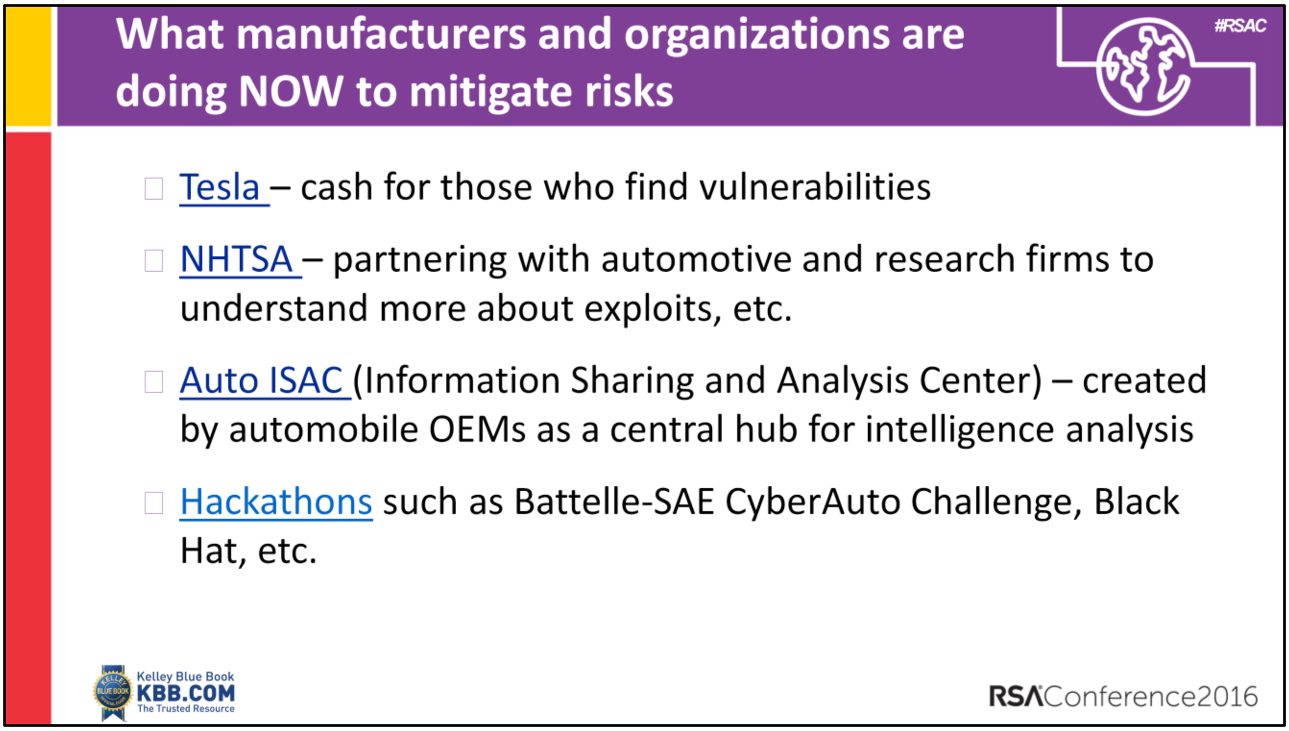
#RSAC

- Consumers' vigilance whenever connected with any device, including phone, IoT devices *and* car
- We are all assuming a certain level of risk for convenience
- Automakers should (if they haven't already):
  - Develop research teams
  - Crowd source vulnerabilities & collect information on every hack
- Government only now focusing on this issue
  - The process to create a standard is slow, however basic standards *do* need to be established similar to existing standards for crash tests, fuel efficiency, etc.
- The tech industry and automakers need to work **together** instead of viewing each other as competitors in regards to connected vehicles

Kelley Blue Book KBB.COM The Trusted Resource

RSAConference2016

- Responsibility
  - Consumers
    - What's cyber-security for computers?
    - Taking control of online footprint
    - Consumers need to be vigilant whenever connected, not just with vehicle
    - Assuming risk for certain level of convenience
  - OEM responsibility
    - Research teams
    - Crowdsourcing
    - Collect information on how they're being used, when hacks happen, systems to automatically push out
    - Partnering with ISPs to help protect consumers
  - Consumers trust automakers to make cars, tech companies to do tech best – OEMs should leverage tech's knowledge
  - NHTSA chief, Rosekind said they will focus on cybersecurity this year



What manufacturers and organizations are doing NOW to mitigate risks

#RSAC

- □ Tesla – cash for those who find vulnerabilities
- □ NHTSA – partnering with automotive and research firms to understand more about exploits, etc.
- □ Auto ISAC (Information Sharing and Analysis Center) – created by automobile OEMs as a central hub for intelligence analysis
- □ Hackathons such as Battelle-SAE CyberAuto Challenge, Black Hat, etc.

Kelley Blue Book KBB.COM The Trusted Resource

RSAConference2016

- Tesla rewards those who find vulnerabilities in their systems
- NHTSA – Automotive Cybersecurity Research Program
    - Partnering with OEMs and security conferences
- Alliance of Automobile Manufacturers creates Auto ISAC to serve as a central hub for intelligence and analysis, providing timely sharing of cyber threat information and potential vulnerabilities in motor vehicle electronics or associated in-vehicle networks.

RSAConference2016

#RSAC

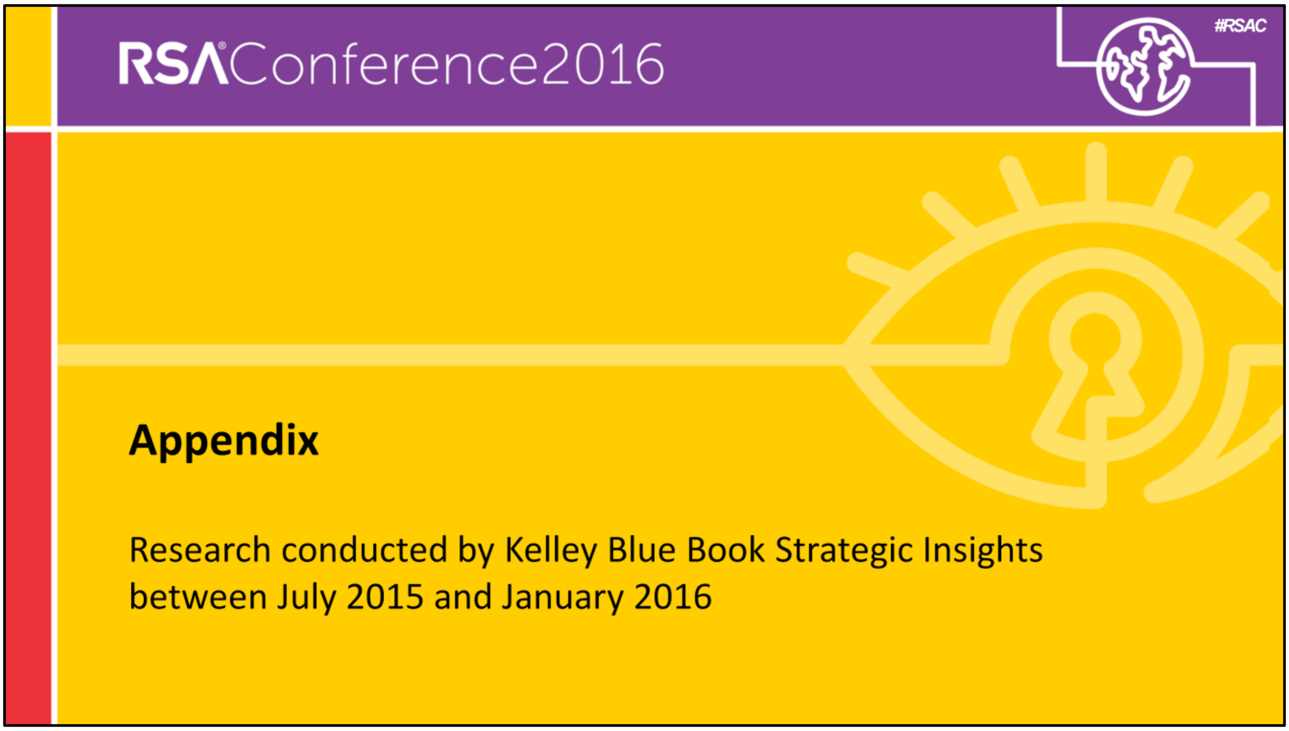
Thank You!

Karl Brauer

Senior Director
Automotive Industry Insights
Kelley Blue Book

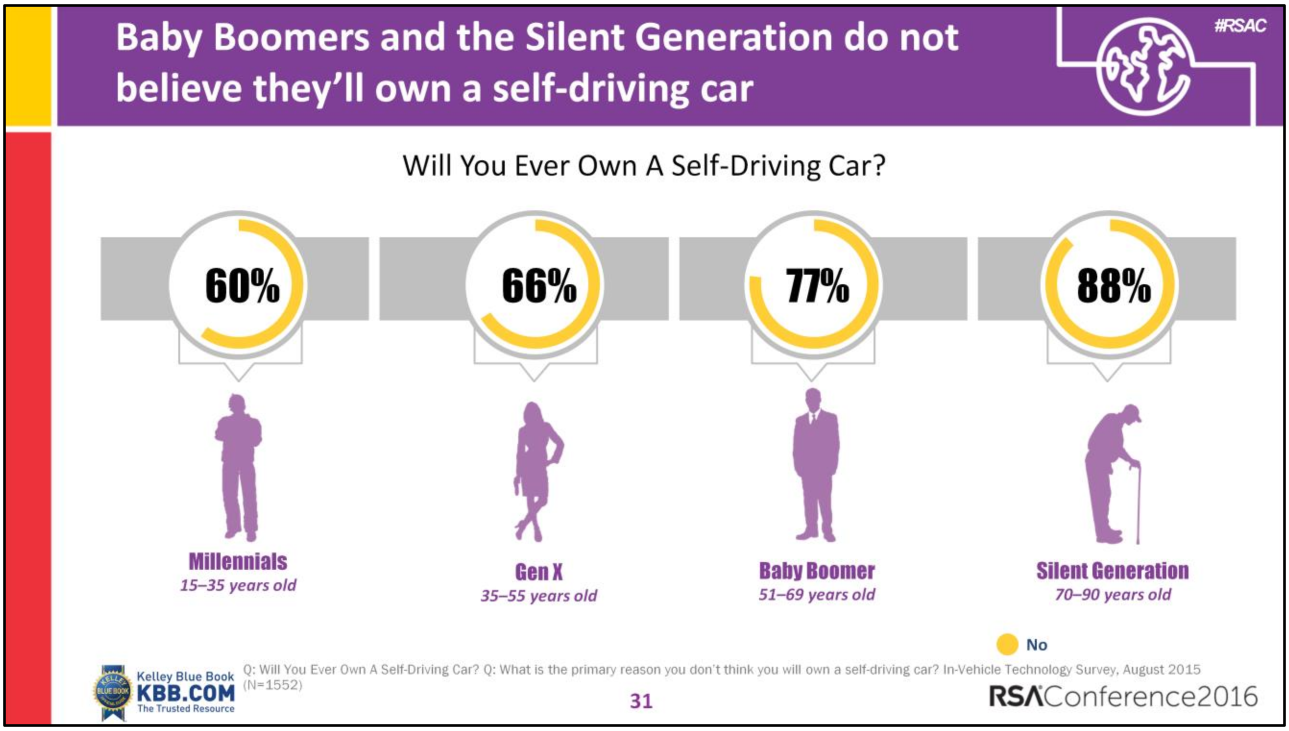
Akshay Anand

Manager
Commercial Insights
Kelley Blue Book



Appendix

Research conducted by Kelley Blue Book Strategic Insights between July 2015 and January 2016



Baby Boomers and the Silent Generation do not believe they'll own a self-driving car

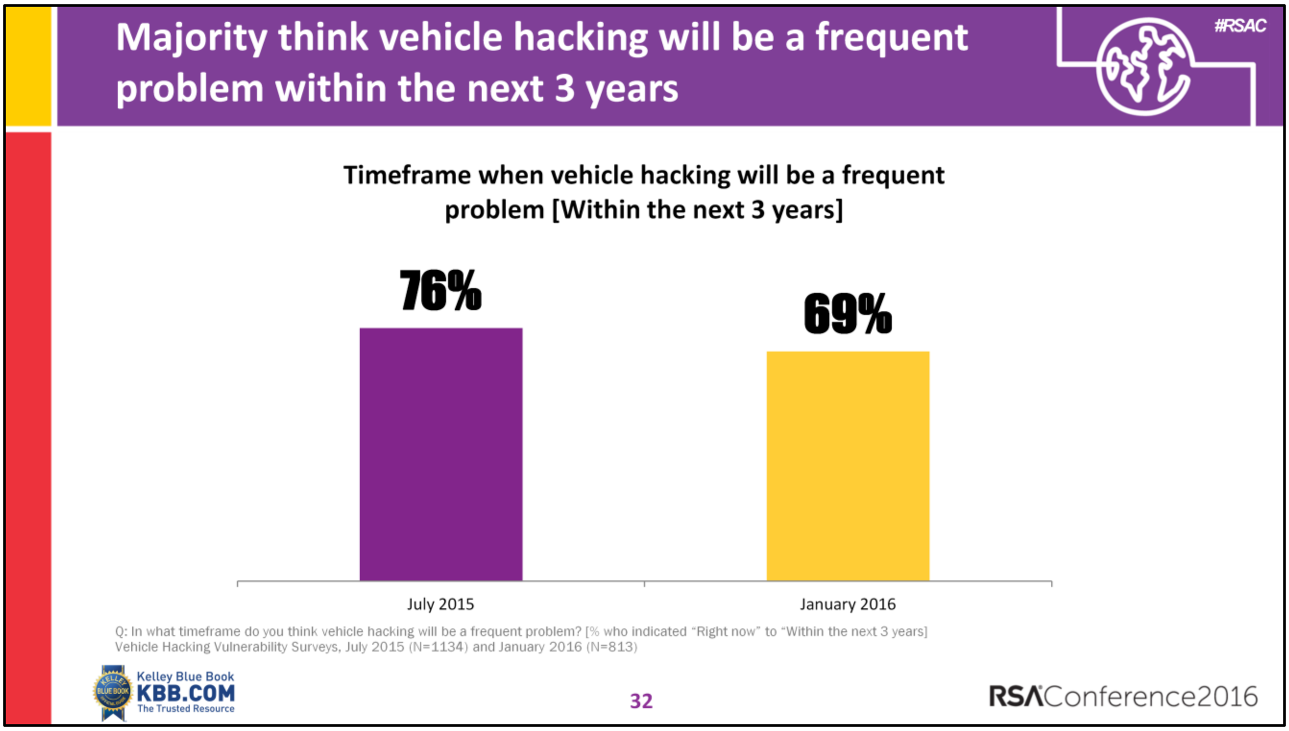
#RSAC

Will You Ever Own A Self-Driving Car?

Kelley Blue Book KBB.COM The Trusted Resource

Q: Will You Ever Own A Self-Driving Car? Q: What is the primary reason you don't think you will own a self-driving car? In-Vehicle Technology Survey, August 2015 (N=1552)

RSAConference2016



#RSAC

Majority think vehicle hacking will be a frequent problem within the next 3 years

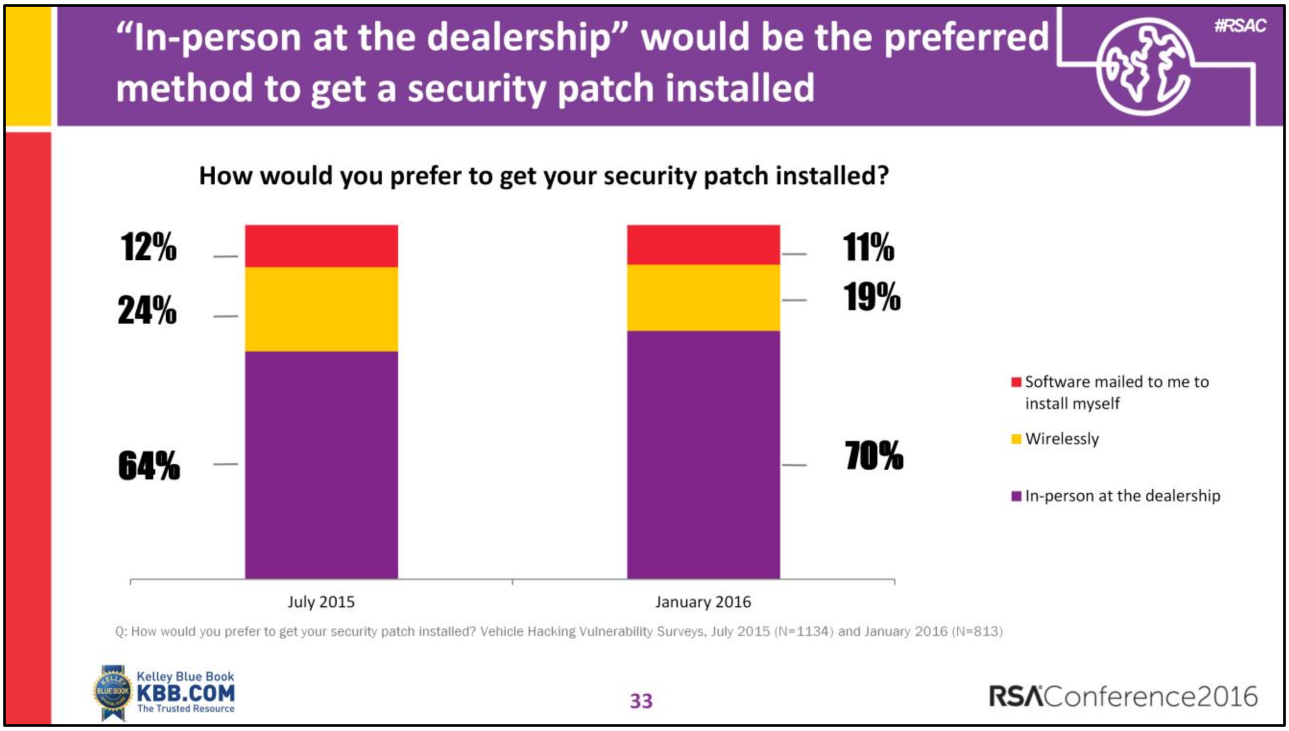
Timeframe when vehicle hacking will be a frequent problem [Within the next 3 years]

Q: In what timeframe do you think vehicle hacking will be a frequent problem? [% who indicated "Right now" to "Within the next 3 years]
Vehicle Hacking Vulnerability Surveys, July 2015 (N=1134) and January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

RSAConference2016

Millennials were less likely to think vehicle hacking will be a frequent problem within the next 3 years vs. other generations. For example, 50% for Millennials vs. 70% for Baby Boomers and 77% for Silent Generation.



"In-person at the dealership" would be the preferred method to get a security patch installed

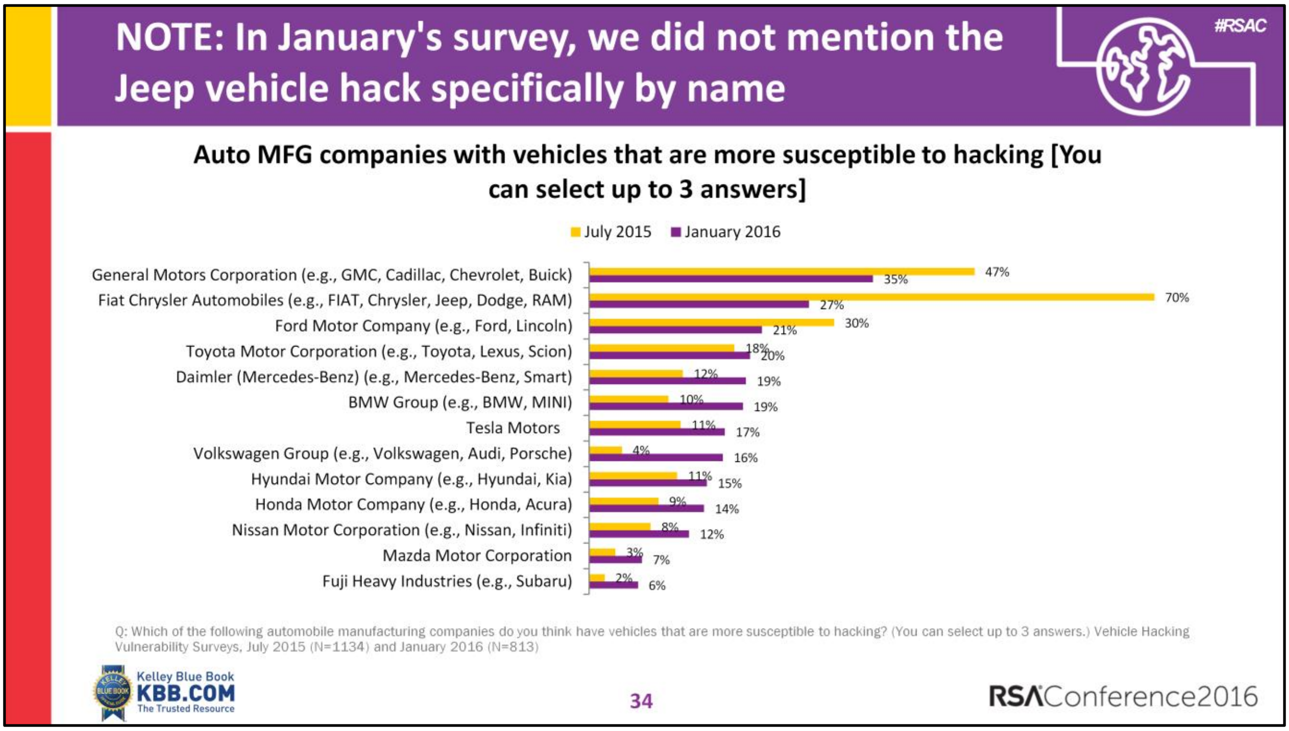
#RSAC

How would you prefer to get your security patch installed?

Q: How would you prefer to get your security patch installed? Vehicle Hacking Vulnerability Surveys, July 2015 (N=1134) and January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

RSAConference2016



#RSAC

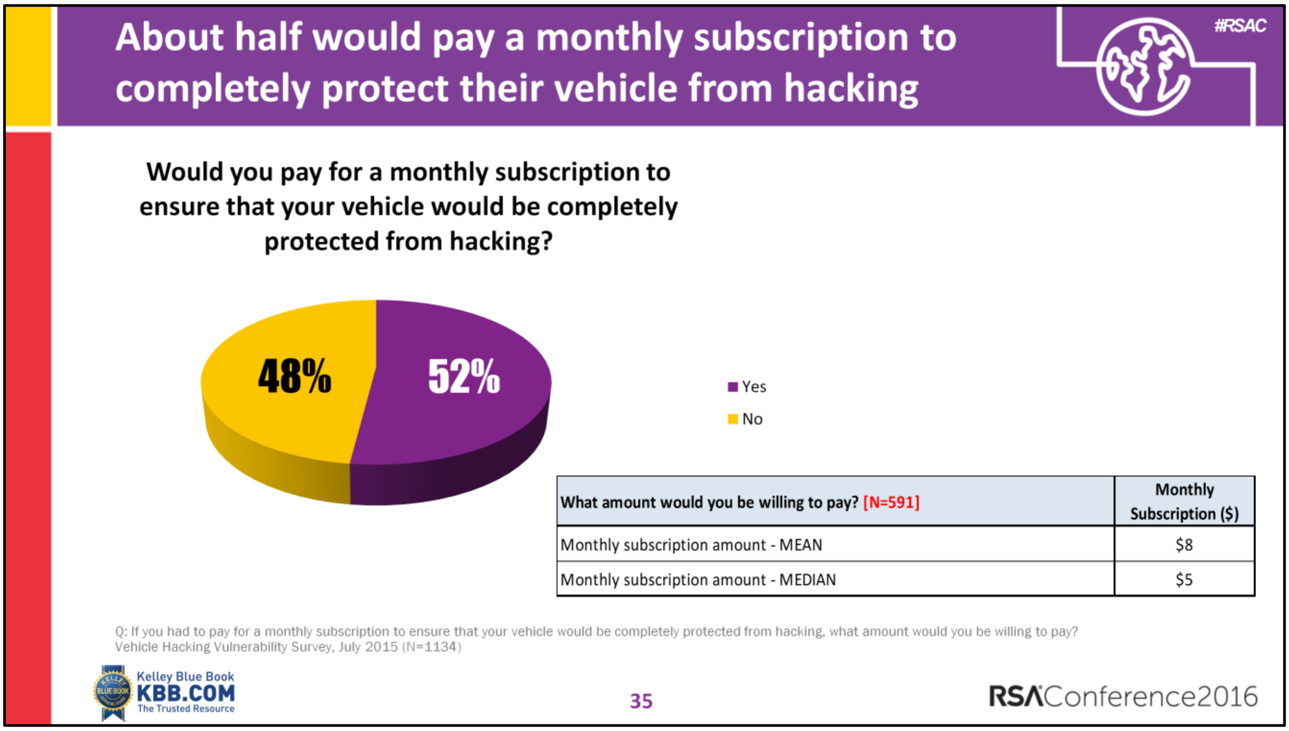
NOTE: In January's survey, we did not mention the Jeep vehicle hack specifically by name

Auto MFG companies with vehicles that are more susceptible to hacking [You can select up to 3 answers]

Q: Which of the following automobile manufacturing companies do you think have vehicles that are more susceptible to hacking? (You can select up to 3 answers.) Vehicle Hacking Vulnerability Surveys, July 2015 (N=1134) and January 2016 (N=813)

Kelley Blue Book KBB.COM The Trusted Resource

RSAConference2016



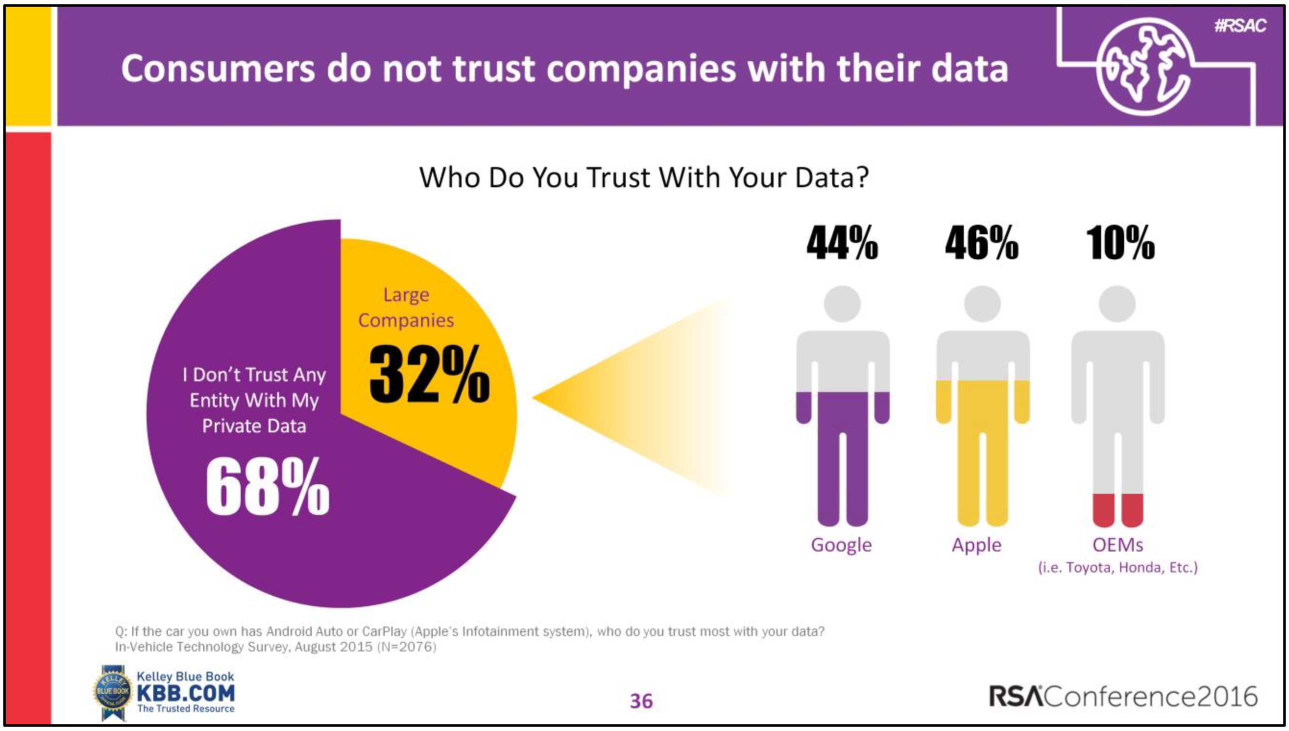
About half would pay a monthly subscription to completely protect their vehicle from hacking

Would you pay for a monthly subscription to ensure that your vehicle would be completely protected from hacking?

What amount would you be willing to pay? [N=591]	Monthly Subscription ($)
Monthly subscription amount - MEAN	$8
Monthly subscription amount - MEDIAN	$5

Q: If you had to pay for a monthly subscription to ensure that your vehicle would be completely protected from hacking, what amount would you be willing to pay?
Vehicle Hacking Vulnerability Survey, July 2015 (N=1134)

- Note: July’s data - $8 was the average monthly subscription amount among consumers



#RSAC

Consumers do not trust companies with their data

Who Do You Trust With Your Data?

Q: If the car you own has Android Auto or CarPlay (Apple's Infotainment system), who do you trust most with your data?
In-Vehicle Technology Survey, August 2015 (N=2076)

Kelley Blue Book
KBB.COM
The Trusted Resource

RSAConference2016

- Consumers do not trust OEMs, but for those that do, they trust Google/Apple vs. OEMs.)
- It’s important to note that while consumers do not want OEMs to have access to their data, they still want to have manufacturers offer a third-party technology to protect their vehicle – likely for ease during the transaction process (instead of having to search for a third-party subscription themselves)
- Could still be tech company’s interface