Which Investigates S2 - EP2

[00:00:00.12] - I'm not sure where you normally listen to this podcast. You might be out walking the dog or on a run. Or you might be cleaning the house. Or you might be on your commute, maybe driving to work.

[00:00:11.01] Wherever you are, right now, I want you to imagine that you're behind the wheel of a car cruising down a motorway at 70 miles an hour. Traffic is good. There are no queues, lovely blue sky. But then the fans turn on. And you didn't do that.

[00:00:27.01] Then loud music starts playing. You didn't do that either. Then the brakes go on, quickly slowing you to a stop. And you definitely didn't do that. The people who did are miles away. They're sat at home. And they've hacked your car.

[00:00:50.81] This is exactly what happened to Andy Greenberg in 2015 as he was driving a Jeep Cherokee down a St. Louis highway. Fortunately, he was expecting the hack. It was part of a demonstration put on by researchers Charlie Miller and Chris Valasek. But the stress and lorry horns were very real.

[00:01:11.12] Later, in the safety of an empty car park, Charlie and Chris also showed how they could remotely control the Jeep's steering, driving Andy into a ditch. A security update soon prevented the same from happening to any other Jeep Cherokee drivers. But as Vaibhav Jha wrote in his 2019 paper titled Towards the Prevention of Car Hacking: A Threat to Automation Industry, the hack ability of cars hasn't reduced. It's increased. As Vaibhav says, quote, "Considering the modern vehicle, it is quite easy to immediately picture a scenario where a car is controlled using a smartphone."

[00:01:48.80] Now in the previous podcast, the first episode of our new tech and security season, I investigated how hackable the smart devices inside your home could be. This is an extension of that, a part two, if you will. With one of the internet of things smartest devices now being a car, often more computer than combustion engine, is a hack like this less or more doable? I'm Greg Foot. And today's Which? Investigates asks could someone take control of your car while you're driving?

[00:02:22.07] [MUSIC PLAYING]

[00:02:42.75] Which? Investigates is a podcast from the UK's Consumer Champion. We work to make life simpler, fairer, and safer for everyone. In this new season I'm exploring concerns around tech and security. Are you being tracked online? How safe is your digital money? And how do you spot a fake review?

[00:03:03.06] Those investigations are on the way very soon. And if you've got something you'd like us to investigate, do get in touch. I'm @gregfoot on social and Which? is @whichuk.

[00:03:19.82] Coming up, I hear how the modern car is indeed now more modem than motor. Hang on, is a modem still a thing?

[00:03:27.08] - When I started working, cars were just like, you know, metal boxes where you have to do an awful lot. You know, you had to ride the windows down. The car didn't give you any help with parking. You had to do all that by yourself. But in actual fact, when you're out trying to see, diagnose what's going wrong with them, then you take them to the garage, the first thing that the mechanic will do is get a laptop out and plug it in and find out what's going on.

[00:03:51.08] - I discover how this development opens more windows for hackers to enter our digital lives.

[00:03:56.85] - Essentially it got to the point where even the most basic cars have got a computer. And once you've got a computer you can plug all sorts of other things into them. Now in some ways that's really cool because there's no buttons to go wrong. And they can change the interface. And they can have new features. But it also means that there's a single point of failure.

[00:04:09.36] - And I ask whether this is something we should be worrying about.

[00:04:13.10] - There's a lot of sort of fear and worry about the connected car. You can imagine all sorts of horrific safety scenarios. And I think it's a legitimate worry if we don't do our job as industry and as security professionals.

[00:04:35.21] - Now, this is where we left last week's episode.

[00:04:38.38] - What a lot of people don't realise is that connected things are not just confined to the home. Many, many different things within this internet of things, within lots and lots of different sectors are becoming connected. And there are lots of new technologies within that make it a particularly interesting target for attackers.

[00:04:56.24] - This is David Rogers, the lead author of the UK's Code of Practise for Consumer IoT security, IoT being the Internet of Things, essentially smart devices connected to the internet. David and I spoke at length about all things IoT and how they could be exploited by hackers. And of all the devices that we talked about, there was one which we felt needed its own episode.

[00:05:19.46] - We start to like build all of these new connected technologies. And that's what makes the sort of car the most connected IoT device there is.

[00:05:28.55] - And the smarter something is, the more connected it is. The more vulnerable it could be to hacking. So how vulnerable is your car? And what can you do to protect yourself? Well that's where we're going today. But let's start the journey by looking back and trying to figure out when cars became smart. It's time for a spot of history.

[00:05:49.27] [MUSIC PLAYING]

[00:05:52.34] To help with this, who better than the author of A Brief History of Motion, journalist Tom Standage.

[00:05:58.58] - People have been building things with wheels on them since about 3500 BC. And what's really surprising is that this idea of a wooden thing with four wheels that's pulled

along by horses stays the same for thousands of years. Then there's this explosion in the 19th century where people figure out how to build steam trains and bicycles. And then the bicycle is actually what evolves into the car.

[00:06:19.43] So when the internal combustion engine is invented, it's much smaller and lighter than a steam engine. You couldn't really put steam engines on road vehicles. It didn't really work. But you could do it with an internal combustion engine. And so the first real car is the Benz Motorwagen 1886.

[00:06:32.75] And essentially if you look at it now, it looks like a tricycle because it is a tricycle. It's got two big spoked wheels. They look exactly like bicycle wheels because they are bicycle wheels. So Benz has bought a lot of the parts for this car from a bike shop.

[00:06:44.42] - You heard right. The bicycle walked so the modern car could run. Or rather the bicycle wobbled so the car could drive. Anyway you get the picture. So when did things start to get a bit more technological?

[00:06:57.50] - I remember in the 1980s, I think it was the Austin Maestro came out. And it had a speech synthesiser in it. And it was very controversial because I think they had to change the voice in Germany from a woman's voice to a man's voice because the German drivers didn't want to be bossed around by a woman. Cars in those days were kind of rubbish, right? I mean they couldn't really do anything.

[00:07:15.50] I remember in the 1980s you started to get cars that had what was called a trip computer. And we now take this for granted. But you get in a car. And it tells you how far you've driven, how long we've been going for, how much fuel you've used, what your MPG is. Now this used to be like a big fancy feature you had to pay lots of extra money for. And it now kind of is absolutely cheap as chips. It's on every kind of car.

[00:07:34.28] - I want to bring in journalist Maria McCarthy here, who has seen for herself this technological rise during her decades of work in the motor industry when I started working cars were just like, you know, metal boxes, where you have to do an awful lot. You know, you had to wind the windows down. The car didn't give you any help with parking. You had to do all that by yourself. And of course you know you really had to get under the bonnet with a [INAUDIBLE] to do a lot of things.

[00:08:01.31] Cars are a lot more like laptops now. When you're like trying to see, diagnose what's going wrong with them, and you take them to the garage, the first thing that the mechanic will do is get a laptop out and plug it in and find out what's going on.

[00:08:13.76] Writing in the US magazine The New Yorker as early as 2013, Gary Marcus, the professor of Psychology and Neuroscience at New York University, gave a bold prediction stating, I quote "It's likely that machines will be smarter than us before the end of the century." It's just eight years since he said that. But as Tom Standage points out, it feels like the smart machines are already very much here.

[00:08:39.68] - Essentially we've got to the point where even the most basic cars have got a computer. And once you've got a computer you can plug all sorts of other things into them. And you can start to make the car do more and more clever things. And if you look at

something like a Tesla, it's just got this big flat screen. It's got no other controls inside it. You know, if you want to adjust the air conditioning, you have to do it using the flat screen.

[00:08:56.81] - As I mentioned in season one, when I looked into how green an electric car really is-- I am a Tesla owner myself. Now don't at me. It's currently got the only reliable charging network in my opinion. And yes, having one big screen inside to control everything about the car does feel like I'm living in the future.

[00:09:14.91] - Now in some ways that's really cool because there's no buttons to go wrong, and they can change the interface, and they can add new features. But it also means that there's a single point of failure.

[00:09:21.23] - Great. Cheers, Tom. That got me worried. So it was time for some reading. And what I read-- well it's not just Tesla drivers who should be concerned. This is from author Steve Tengler in a Forbes article he wrote just last year.

[00:09:34.60] - Here's the nasty truth, nearly every manufacturer has been hacked.

[00:09:39.16] - Yeah. And elsewhere in the article he quoted a report from cybersecurity firm, Upstream, who found that in 2020 there was a 73% growth in what's known as server attacks targeting the software systems in connected vehicles. And what's more, over a third were data and privacy breaches which begs the question how are these cars being hacked? Well let's find out, shall we? Over to David Rogers for a quick guide through a connected cars connected tech and how it can be hacked.

[00:10:09.73] - The key component, something called the Telematics Control Unit, the TCU. Now it sounds a bit complicated. But all it is is how that car would connect to the outside world, how it would connect to the internet.

[00:10:22.57] - And if you're a collector of acronyms, you can take your IoT and your TCU and you can add a CAN. Every connected car has a CAN, a Controller Area Network, a series of cables that thread through the vehicle like your nervous system threads throughout your body. And similarly, the CAN carries messages between the different systems inside your car.

[00:10:44.95] Turns out modern vehicles have multiple CANs. Which? research found that the Ford Focus has seven. The most critical is always the powertrain which handles electronic driving control such as braking, steering, clutch, and acceleration. However, although those were the very things targeted and affected when Charlie and Chris took control of that Jeep, the powertrain isn't the primary attack target for hackers.

[00:11:12.07] They're first and foremost interested in the infotainment system, things like the radio, satnav, and the reversing camera. And no that's not because they get a kick from making your stereo play their favourite tune remotely, David Hasselhoff, say. It's because the infotainment system is an easier way to jump in your car.

[00:11:33.10] [MUSIC - DAVID HASSELHOFF, "JUMP IN MY CAR"]

[00:11:33.52] Come on and jump in my car.

[00:11:36.14] - It's very rare that we perform a test and don't identify some serious vulnerabilities. These are highly complex systems. And there's often a great deal of software in there. And everyone expects that software contains vulnerabilities.

[00:11:50.39] - That's Andy Davis from NCC Group, a cybersecurity firm we frequently work with here at Which? Indeed, it was NCC Group that helped us with our hackable home experiment in the previous episode. The infotainment system is the one most likely to have these vulnerabilities, and therefore the most easy window to break into to gain access to your car's whole connected system. But how do these vulnerabilities develop?

[00:12:16.37] - We are entering a very interesting era. There are a lot of new technologies coming along where the computers are essentially getting more clever and have more knowledge than human beings can ever acquire. So we're relying a lot on those computers to do the right thing. But again, all of that relies on human beings because human beings are engineering all of that software.

[00:12:42.23] - Bugs in software can come from somebody having a bad day. When they're writing the code, they might not be concentrating. They might not completely understand what they're trying to implement or the way that they're trying to do it in the code. It might be through assumptions that they're making that might be incorrect. And humans are humans at the end of the day. They're not perfect.

[00:13:06.80] - Charlie and Chris exploited one of these vulnerabilities to take remote control of that Jeep in 2015. They used the mobile phone connection to the entertainment system to get in. And then they played music, turned on the fans, and applied the brakes. They also took control of the steering, too. But interestingly, that was only when the Jeep was travelling slowly in reverse. And that's because those were the conditions needed for the TCU to enable the self parallel parking feature, which they then took control of.

[00:13:39.62] Chrysler soon issued a software update to close the hacking window that the connected entertainment system provided. But that was 2015. Could a more modern car with even more bells and whistles and connected features be hacked?

[00:13:57.86] In 2019, we put this to the test. Which? purchased two cars, a Ford Focus and a Volkswagen Polo, chosen due to their popularity. And the team tried to hack them. Their first aim was to find a way to compromise the car's braking and steering, something they were unable to do, which is reassuring. But perhaps not surprising, it took Charlie and Chris more than a year to work out how to hack that Jeep.

[00:14:26.09] Do hackers have that much patience? The Which? hacking attempt published in spring 2020 wasn't all good news though. Quote "These cars weren't as easy to hack as other connected products we've looked at, such as dodgy wireless cameras. But our expert team was able to find chinks in each car's security armour that could jeopardise your security and even your safety." End quote. The team discovered that Ford actually revealed its factory's own Wi-Fi password in the car's code. And they managed to successfully hack into the Volkswagen's infotainment unit, proving they'd done so by uploading a logo onto the screen and by modifying some crucial software so the unit shut down every five minutes.

[00:15:14.99] I asked if hackers are patient. But there's a way that they can get into your car without needing to be. In fact, a way that means they don't even need to understand how the hacking works.

[00:15:25.82] - Instead of car thieves going along with lock picks or just a hammer to smash the window and then put two wires together and hotwire the car, they're buying in technology that enables them to do essentially the same thing. They don't need the knowledge. They need to press this button, wave around the antenna at the window near to where the real key fob is, and their accomplice is near in the car. And they're in. And it's really, really simple.

[00:15:51.05] - According to the statistics website Statista, there were almost 90,000 motor vehicle thefts in England and Wales last year, 20,000 more than seven years ago. And the majority of cases were from keyless car theft, which doesn't mean that thieves are nicking the key fobs that these keyless cars are unlocked with. But rather criminals are using mobile gadgets to copy the electronic signals and codes those key fobs produce to gain entry.

[00:16:20.06] - What's happened is that there are these things called relay devices that can pick up the signal from the key fob. Thieves, they will be watching you. It's not a sort of an impulse crime. They will be watching you. And they will be watching your vehicle.

[00:16:34.90] What will happen is they'll come along in the middle of the night. Thief number one will have what's called a relay device. And it will stand near the door. And the device will pick up your key fob signal. Then the signal-- they send that to their colleague, thief number two, who's standing just near the vehicle.

[00:16:52.56] And then, thief number two will point his device at the car. And it will open up because it thinks it's you. It thinks the key has been activated. Then, thieves number one and two get into the car. They drive it off. And you will never see it again.

[00:17:08.07] - There's a video on which.co.uk that shows how alarmingly quickly this can happen. I'll put a link in the show notes in the episode description.

[00:17:16.20] Back to our 2019 hacking attempt then. The Ford Focus in our test used what's called a sleeping key, which goes into sleep mode when it's not in use. As the key is therefore not always emitting a signal, that gives much greater protection against this theft technique. Indeed, our team were not able to successfully retransmit the Ford's key signal during testing.

[00:17:39.16] However, the Volkswagen was vulnerable to a variation of this, called a roll jam attack, which is when someone steals your key's digital signature as you press the fob. Thieves capture the key's code on their device and then use it to unlock your car when they wish.

[00:17:56.22] They can also jam the signal from your key fob to prevent you from locking it. You assume that like normal, a quick press and the doors are locked,

[00:18:03.99] [BEEPING]

[00:18:04.59] But actually, they're not. When we put the results to Volkswagen, they accepted that the key fob is vulnerable to being hacked and advised concerned drivers to quote "Check manually if the car is locked." The Ford wasn't Fort Knox though. It was

possible to breach the fob and then block the owner from being able to start the engine, something that maybe they could use to demand a ransom, say, to unlock it. When we told Ford about this, they said that attack could be replicated on any key free vehicle and added that their cars have a backup location in the centre console, where you can place the fob if it is jammed by an attacker.

[00:18:47.33] There's another angle to all this, though, that we haven't explored yet. A hacker may not be able to gain enough access to steal your car. But could they get enough access to steal something else valuable from it? Tom introduced this one best.

[00:19:02.37] - The other thing I think to watch out for is a lesson from history, which is that the problem with the horse turned out to be the horse poo, right? There was just so much of it. So that made me think kind of well in that case, what's the equivalent for cars? Where's the exhaust that's going to cause the problem in the future? And the answer is obvious. It's personal data.

[00:19:18.89] - Andy agrees.

[00:19:20.09] - I think that's a very serious issue. If you sync your mobile phone with the car's infotainment system and it copies over your address book, maybe text messages, if you're interacting with the phone via the car, then some of that stuff gets stored within the infotainment system in the car. And also, the number of apps that are being used in car and also to communicate with cars-- so for example, if you've got a telematics app like I've got on my car that allows me to have a look at the status of my vehicle to see whether it's locked or unlocked, if the lights have been left on, where it's located, I need to log into that.

[00:20:02.69] And when I sell the car I'd have to specifically make sure that I erased that information from the car before I sold it. Otherwise, when the new owner has that car I could still potentially unlock the car with that app, if my app is still associated with that vehicle. Not only can you unlock the car, you can also start the engine, beat the horn, light the lights, you know, all these kinds of things.

[00:20:27.59] - Comparison website confused.com have just released the results of their own study, looking at the amount of data our cars collect about us and which manufacturers collect more than most. Perhaps unsurprisingly, Tesla comes out on top again, if by on top you mean collects the most data. And while a lot of this data does help the car tailor itself to the way an owner drives, they also log information like which radio stations you've listened to and when. And some manufacturers, like Porsche, even track your mobile phone's location.

[00:21:05.87] Since the start of the pandemic, interest in second hand cars has skyrocketed. According to the Society of Motor Manufacturers and Traders, May and June saw the best months' figures since records began, especially with sales of second hand electric cars, up a whopping 351% year on year. And how many of those owners remembered to wipe their car's memory before selling? And if they didn't, what could that information be used for?

[00:21:34.52] - Whilst it's improved of late, it's dealers not realising they need to reset the satnav or the head unit there to remove your personal data from it. I bet you set your home address in the satnav, right? So that means when you sell your car, whoever's bought it knows where you live.

[00:21:49.28] - This is Ken Munro, who runs Pen Test Partners, a company who regularly test smart products for vulnerabilities. Between December 2019 and February 2020, which surveyed more than 14,000 people who had sold their car in the past two years, over half had synced their phone to their car via Bluetooth or USB. But of those who had synced, nearly a third had made no attempt whatsoever to remove any of their data from their car before selling. But what do the hackers want to do with all this data?

[00:22:22.64] - The easiest way is think about it as a business. You know, we hear a lot about ransomware, for example. Actually, the ransomware operators and the infrastructures behind them, think about it as a business. It makes money. So if we think about hacking as having a few commercially or politically motivated goals, then you start to understand what they're trying to achieve.

[00:22:42.32] - During our chat, he mentioned a recent test that he'd worked on that demonstrates how it isn't just the vehicles themselves that are at risk. Over the last year, we've been looking at lots of different brands of smart car charger. There were problems that allowed a hacker to potentially take over your account and control whether your car charge charged or not. So imagine waking up in the morning, knowing you've got a long journey to go, and your car charger has been switched off by someone nefarious. Now that would really annoy you, right?

[00:23:07.10] But there's a wider implication, too. Because car chargers use a lot of power, the hacker can take control of lots of chargers at once. Turn them off. Turn them on again. Turn them off. And that creates power spikes on our power grid. So if you are to trigger all the charges at a time of peak demand, you could actually start to cause blackouts on the grid.

[00:23:24.74] - We're back to Die Hard IV scenarios again, aren't we? This time the plot is cyber terrorists take down parts of the city using car chargers.

[00:23:38.68] The good news is hacking a car isn't easy, especially in a way that could cause catastrophic consequences. But with our lives becoming increasingly connected, whether that's at home or out on the road, what's important here is what comes next.

[00:23:54.82] - In the past, there may have been some car manufacturers that didn't consider cyber security quite so important as other car manufacturers did. However, the whole landscape has changed because the UNECE, United Nations Economic Commission for Europe, which develops the regulations around cars, there is a new cybersecurity regulation that has just been implemented that actually means that regardless of what the stance of the vehicle manufacturers was previously, they now need to comply with this regulation, which means that they all need to consider cyber security right through the design and development of new vehicles.

[00:24:36.40] - The UN Economic Commission report sounds like good news for our digital safety. But sadly, this won't be made mandatory as part of UK law, meaning we need to continue to put our trust in car manufacturers to take any vulnerabilities with their vehicles seriously. And as you may expect, here at Which? we believe the industry must do better, especially with so many new tech developments and connectivity features rolling out, ones which could give hackers even more of an opportunity to have a rifle through our personal effects or speed off with the whole car.

[00:25:12.43] One obvious tech is driverless cars. They're going to require us to put even more trust into a computer and trust that the system is designed to operate it are robust and secure. In a 2019 survey of over 1,000 people, the American Automobile Association found 71% of respondents were afraid to ride in fully self-driving vehicles. As with all the smart connected technology available to us right now, or a short way down the road, we need to step back and consider the potential cons as well as the clear pros.

[00:25:46.57] As Tom said, just as the horse filled streets with stacks of manure and the petrol car continues to pollute, we need to think of the unexpected side effects this increased connectivity brings.

[00:26:00.19] - I think in the moment, people are-- they won't all these fancy technologies because they solve their own problems as the council or whatever. They're not actually thinking whether this actually has any real social benefit or human benefit and what potential problems might lie in wait for them.

[00:26:15.19] - There's no denying that our interest and desire for a more connected world and our increased reliance on the technology that advances that dream has opened new doors to criminals. And as we've heard in these two episodes, there are some very real concerns.

[00:26:33.58] - So should we build a world that is more connected? Or should we be wary of the risk that that exposes us to? What do you think? I would love to hear your thoughts on this get in touch on social. I'm @gregfoot and which? is @whichuk.

[00:26:49.57] Do the opportunities and solutions that these smart devices offer outweigh the potential pitfalls? Let me know your thoughts. I will leave you with two quick ones. This first one from David.

[00:27:00.55] - I don't think the future is going to be less connected. And I'm a security person. And I'm having to deal with this kind of stuff. But I'm still a big technologist. And I'm a big fan of advancing humanity and advancing technology but in a responsible way.

[00:27:15.10] So just because we can doesn't mean we should. And we shouldn't be afraid to stop. And at the moment, actually, from my observance, there seems to be this big sort of fear of regulators just stopping everything rather than actually-- they seem to be the ones talking sense at the moment. And they're the voice actually of their voters and their populace and their citizens. They're just echoing the concerns of citizens. And it's really down to the industry to address that.

[00:27:42.47] - And the final words on this I'm going to give to author and Emmy winning CBS News correspondent David Pogue, who wrote something five years ago that I think still feels relevant today. He said, quote, "New technology is always a little scary. But let's not exploit that fear." I hope you enjoyed these first two episodes of this new tech and security season of Which? Investigates.

[00:28:11.73] Next time we're opening up our wallets. And we're seeing if the move from cash to contactless brings with it new security concerns, as I ask how safe is mobile banking, cryptocurrency, and the entire future of money itself? As always head on over to which.co.uk for more reviews and advice every day, including, by the way lots of great information on

how to prevent your car from falling victim to thieves, super relevant of course after everything we've been talking about today.

[00:28:41.46] Please do share this episode with anyone you think may find it interesting. And if you would be up for rating and reviewing us on Apple podcasts or wherever you listen to this, we would hugely appreciate it. Today's episode was presented by me, Greg Foot, written and produced by me and Rob Lilly. Editing and original music is by Eric Briar. And our executive producer is Angus Farquhar.

[00:29:03.30] Special thanks go to Richard Headland, Paul Lester, Andy Loughlin, Will Stapely, and Adrian Porter. And I will be back soon with our next investigation.