Safer journeys

An overview of security and privacy in the connected automotive ecosystem

automotive.vodafone.com

Vodafone
Power to you

About this report

This report explores the security and privacy risks associated with the advent of the connected vehicle, and the extended automotive ecosystem that it's helped to create.

Using our long experience working in the automotive sector, we examine some of the technological, process and human considerations for making connected services safer in the years to come. This report will be relevant for anyone involved in decisions around connected vehicle services, particularly those with responsibility for security.

Further reading:

Vodafone IoT Barometer 2016

Connected, Automated, Shared

Data is at the heart of connected services

Connected vehicles are an unprecedented source of data. This data is an opportunity to create value across industries — but it's also at risk.

New services are driving automotive ecosystems

Our report **"Connected, Automated, Shared"** shows how the connected vehicle has opened up possibilities for a whole new ecosystem of value-added automotive services.

Such services help drivers and vehicle occupants in all kinds of ways, from providing streaming media to locating stolen vehicles, cutting insurance costs to preventing breakdowns.

Connected vehicle services give drivers a superior user experience, and give manufacturers and their partners a powerful way to grow revenue and customer loyalty.

That's why the automotive industry is pushing connected vehicle technology — sensors, processors and connectivity — into new models, both consumer and commercial vehicles, at a rapid pace.

29% of IoT adopters across all sectors say they're using IoT to connect multiple organisations or industries together to form a greater whole[1] — the connected vehicle ecosystem is a perfect example.

Data is at the heart of connected automotive services

Connected vehicle services depend on the rich data gathered by sensors either built into the vehicle at point of manufacture or added later. For example:

- Stolen vehicle recovery applications monitor the vehicle's location via GPS and cell tower triangulation.
- Usage-based insurance (UBI) applications record details of driving style, location and time.
- Servicing alerts may track everything from tyre pressure to oil temperature.
- Fleet management applications, used by leasing, rental and haulage companies, may monitor which individuals are using the vehicle and their mileage.

This data is a valuable asset in its own right, and it may be gathered, stored, used and shared by many different organisations, both to deliver services to individual customers, and in aggregate as a source of insight into everything from vehicle performance to consumer preferences.

The automotive ecosystem is now extensive, including OEMs, dealerships, insurers, component suppliers, public sector bodies, and other service providers, all transacting in information in complex ways.

Automotive sector organisations are ahead in recognising the value of data. In our Barometer 2016 research, 45% "strongly agreed" that "IoT can only deliver real value if you effectively use the data it generates" — compared to 30% across all sectors.

Sensitive data needs protection

Much of the data that the connected vehicle gathers, or has access to, is both valuable and sensitive if misused.

The data may include:

Location and location habits: the vehicle knows where you live and work, and can reveal private trips such as visits to medical clinics.

Driver behaviour: data about driving style is an exceptionally reliable way to identify an individual[2], and could be used to prove that a driver is speeding or distracted in the moments before an accident.

Payment information: card details may be registered with the vehicle in order to enable automated parking and toll payments or in-car purchases of media content.

Intellectual property: the car may hold commercial data owned by third parties, including music and video, application code, or proprietary data sources such as weather and traffic information.

Personally identifiable information: the vehicle may hold data or metadata about the driver and occupants, including names and phone numbers, call records, addresses, email and social media account details, even biometrics for authentication.

Vehicle telematics information: information about routine vehicle performance and usage may be commercially sensitive intellectual property.

Add all this data together, and the connected vehicle can potentially paint a detailed picture of an individual's life[3] that could be used for identity theft, blackmail or other purposes. In the commercial vehicle space, such data could help target hijackings, industrial espionage or disruption. Even when anonymised and aggregated, the data remains sensitive[4]. Of course, even aside from its data, the car itself is a valuable asset that has safety risks if compromised.

It's easy to see that the connected vehicle is an attractive target for hackers, and if the full value of the connected vehicle is to be achieved, all of the parties involved, not least the drivers themselves, must be able to trust that sensitive data is secure and private. The automotive ecosystem must respond to protect the functional integrity of the vehicle and its data.

Securing the vehicle is only the first step

The connected vehicle is only one link in the chain that sensitive data passes through. To be effective, protection must be truly end to end, and that means both securing the vehicle and protecting the data against threats to privacy.

Securing the vehicle

First, manufacturers and their component suppliers must work to make sure that the connected vehicle itself, and any aftermarket devices connected to it[5], are secure against tampering and disruption. This is what the media has mainly been focused on in terms of vehicle security risks, thanks to high-profile hacks of steering systems and remote unlocking.

People are naturally concerned about what would happen if hackers could remotely cause a crash on the highway, or steal cars at will. The reality is that, at least today, hacking into core vehicle systems is a significant effort that takes time, skill and often physical access to the vehicle and one of its electronic control units (ECUs).

White-hat researcher Charlie Miller commented on a nine-hour hack, which required physical access to the vehicle's diagnostic port: "It's hard, so I'm not worried about it. It's not like one day someone is going to make all the cars in the world stop. But we can't ignore it just because I'm not worried about it."[6]

While today's hacks are difficult and complex, they will eventually be productised and automated, available to anyone willing to pay for them.

Protecting the data

Second, and just as importantly, it's about protecting the data. This means securing it against tampering and theft by a malicious attacker (whoever that might be — including the owner of the vehicle, potentially).

It also means addressing the privacy implications around "legitimate" uses of the data: including how much is gathered, who has the legitimate right to access and retain it, how and when it's used, whether it's anonymised, which other parties it's shared with, and how long it's retained for.

> Privacy is on the radar of the automotive sector. In our Barometer 2016 research, we found that automotive respondents were nearly twice as likely to say they were concerned about maintaining data privacy than about security breaches.

Security must be end to end

Security is only as good as the weakest link. If the user's driving experience and data is to be protected, manufacturers and other ecosystem players must address four factors.

77% of automotive organisations say that IoT security should be an end-to-end solution[7].

1 In-car systems

This includes any ECUs, sensors and networking infrastructure installed in the vehicle at time of manufacture or in the aftermarket. With around 100 ECUs in a modern car, there are plenty of points for an attacker to target.

2 Stages of the data lifecycle

Security should follow the data end to end, looking at everything from the data source to the various back-end applications that use it. Hackers won't necessarily just attempt to compromise a vehicle system directly; they could disrupt the vehicle using a legitimate connection from another system. Similarly, they don't have to steal data directly from the car if they can extract it by the terabyte from a central database somewhere.

3 Ecosystem players

It's not just the OEMs and their IT service providers that must take security measures seriously. The responsibility is on any public or private sector organisation that may have cause to interact with car systems or the data as part of the wider ecosystem. The manufacturer may have a thorough security strategy, but once a partner has access to a store of data or a direct connection to vehicle systems, their security measures are what counts.

This may include retailers, vehicle insurers, local authorities, central government bodies such as highways agencies, fleet operators, and technology service providers. It may also include new players created to help the ecosystem function, including IoT service providers, data aggregators and brokers; data analytics providers and regulators. And industry bodies like the GSMA will also play a central role.

But getting many different stakeholders working together — particularly when they represent such different worlds as IT and automotive — can be a huge challenge.

4 Local markets

Security and privacy inevitably have a significant legal aspect to them, including issues such as data protection standards and data breach disclosure rules. Vehicles are mobile and the automotive industry is globalised, so many different jurisdictions may be brought in to play, depending on where the vehicle is designed, manufactured, assembled and driven, where services and their hosting infrastructures are based, and where data is gathered, communicated, processed or stored.

Beyond the purely legal issues, there are market variances to consider in terms of political, economical and social behaviours, and availability of technology standards.

The challenge ahead

Achieving consistent end-to-end data protection is an ambitious goal. How close are we to reaching it?

As the Vodafone IoT Barometer research shows, organisations in every sector are aware of security and privacy as an area of concern. Progress is being made, but the challenge ahead is significant, in three main areas: **technology**, **process**, and **cooperation**.

Technology

The typical vehicle today is, from a security point of view, immature. Legacy technologies that are vulnerable to attack — such as the CAN bus intercar communication system, developed in the 1980s — are still widespread. As the computerisation of the car progresses, and the overall system complexity grows, so does the number and severity of potential vulnerabilities.

Although cars may have millions of lines of code, dozens of processors and complex networks, they lack many of the basic security concepts common to conventional IT systems, such as encrypting traffic, authenticating systems, restricting access, and monitoring for exceptions.

Our research found that the top concerns for automotive-sector organisations is that IoT security is an "unknown quantity" — ahead of any other sector — followed by increasing complexity[8]. Many are looking for help to get a clear view of the risks.

41% of automotive-sector businesses "strongly" agree that the complexity of their IoT infrastructure has increased in the last 12 months[9].

Process

The challenge is not just technology itself, but the process of getting it into vehicles. Automotive development cycles are shortening, but it still takes 3–5 years from first design to launch[10]. Integrating security technologies such as firewalls and intrusion detection systems into the vehicle won't happen overnight. By comparison, the pace of the security threat landscape is fast, with new attacks and countermeasures emerging in weeks or even days.

More fundamentally, manufacturers and their suppliers need to anticipate where the whole connected services ecosystem will be in 3–5 years. That's difficult when the ecosystem is still developing.

Our research found that automotive-sector businesses are more confident than others that they have what it takes to manage IoT security.

- **60%** say their employees have the necessary skills;
- **71%** say their processes are adequate;
- **71%** say their technology is robust enough[11].

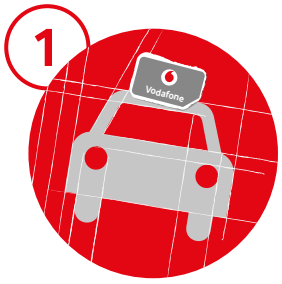
Cooperation

Looking beyond the vehicle infrastructure, the relationships needed for a secure, resilient ecosystem aren't yet in place. There's historically been little interaction between many of the vertical sectors that we expect to have a much closer relationship in the connected services ecosystem. Manufacturers, insurers, technology providers, data aggregators and other types of businesses are still negotiating how these relationships will work, and security and privacy are a key part of those negotiations.

As relationships multiply and solidify into communities, we'll see greater development of and adoption of standards, which are a key part of not just assuring service interoperability, but of achieving security. Standards for the security of connected vehicles are only just being initiated by regulators like the US NHTSA and ISO, and by IT industry bodies[12].

What's the way forward?

Using our knowledge of automotive, IoT and security, we've identified three broad areas that manufacturers and their partners will need to address in order to help secure the connected services ecosystem.



Evolving the vehicle architecture.

Just like any IT system that handles sensitive data, the connected vehicle must: authenticate access requests; encrypt data at rest, in transit and in use; monitor and log activity; and be patched on a regular basis to close newly discovered vulnerabilities.

Read more on page 9.

Planning for security and privacy.

Before forming new relationships within the connected vehicle ecosystem, businesses must evaluate the risk to security and privacy that they are exposing themselves to, particularly in terms of compliance with privacy regulations. Data handling should be governed by formal agreements and privacy policies.

Read more on page 10.

Building security expertise.

Automotive companies need to think and act like technology companies — and that means recruiting and developing expertise in security. To compete for the best talent, businesses will need to try many different approaches, including tapping the resources of the wider security community.

Read more on page 12.

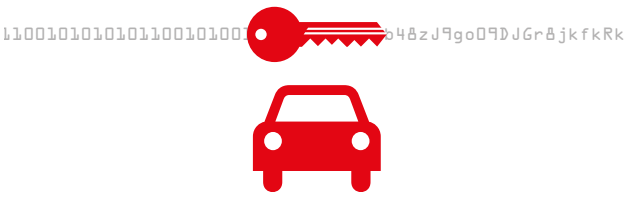
Evolving the vehicle architecture

Vehicle manufacturers and their suppliers must start to apply IT and network security best practices to the sensors, ECUs and network interfaces in the vehicle infrastructure. The goal is to ensure the integrity of device, data, and secure storage and transmission.

Key capabilities should include:

Authentication and access controls

Authentication is a key pillar of security. Without it, it's impossible to prevent unauthorised access to vehicle data and to control systems. Authentication should happen at each point of interaction, including between the user and the vehicle, between discrete car systems, between the vehicle and remote systems (such as smart city infrastructure or application services accessed over the internet), and local connected devices such as the user's smartphone or smart home.



Encryption

Encryption must protect data wherever it's stored, transmitted or processed within the car, to prevent unauthorised capture and ensure the integrity of the data. The challenge here will often be around performance: today's smartphones, desktops and servers are fast enough that real-time encryption and decryption rarely noticeably impact performance. But with small, low-cost embedded chips in the vehicle, and no margin for delay while on the road, the extra processing burden of encryption could be a problem.

Monitoring

Monitoring of activity and traffic around the vehicle, when combined with alerts about exceptions or unusual behaviour, enables rapid response to a live breach, acting as a backup in the event that attackers circumvent other security measures[13]. With comprehensive logging of this monitoring, manufacturers and their partners can also forensically investigate a breach after the fact and patch vulnerabilities.

Patching

Every IT security system only offers effective protection when it's regularly maintained. Just like you'd update a PC, smartphone apps or enterprise software to close newly discovered security vulnerabilities, so vehicles must be able to have their software patched — and for practical reasons, this must be done over the air. BMW patched 2.2 million cars over the air to close a vulnerability; conversely, Fiat Chrysler had to recall 1.4 million vehicles to patch its own[14]. System and component suppliers must consider the practical lifetime of the vehicle on the road and commit to maintaining security for their components for that duration — factoring in the cost implications of doing so. There is a cost benefit to patching, however: estimates suggest that 60% of warranty claims are software-related[15].

Planning for security and privacy

Transparency is a cornerstone of effective security. Before you enter into a contract — whether that's as a consumer buying a vehicle from a manufacturer, or an insurer partnering with a telematics data provider — you should know exactly what you're getting into.

Transparency is vital

If you're giving another organisation access to sensitive data, you should be able to assess the risk they are exposing you to, and verify that they're taking the appropriate measures to protect your privacy and comply with relevant legislation. In the connected services ecosystem, where data is so central and commercial relationships potentially complex across multiple legal jurisdictions, that's especially important.

54% of automotive-sector businesses say they "feel safe" sharing data with others[16].

Document your relationships

Having a traceable and reliable record of what data has been shared with different third parties is good practice when it comes to sharing data. Any organisation that handles sensitive data, or profits from it, should make a formal data processing agreement with its customers, partners and suppliers, which sets out in clear contractual terms the rights and responsibilities relating to the gathering, use and security of data.

This is more than just a token privacy statement on a website. Privacy standards should be referred to often and used not just in procurement, but in internal processes around service development and the training of customer service and IT staff. Violating the company's policies should be a serious issue that is quickly addressed.

47% of automotive-sector organisations say they are already establishing clear security best practice and guidelines for staff in order to improve the security of their IoT projects[17].

Meeting expectations

Privacy is a right increasingly protected by law in most regions. Perhaps most prominent and recent is the 2016 EU General Data Protection Regulation (GDPR).

Companies' policies and behaviours should comply with local legal requirements in order to avoid potential sanctions[18], but it's also vital to meet the expectations of society and the user base about what is acceptable and fair.

What should a privacy policy cover?

Data processing agreements and privacy policies should clearly but comprehensively set out:

What data is gathered. This will vary by application, but should certainly state how frequently data is sampled, how precisely data such as location is measured, what technologies are used, and at what stage it is aggregated or anonymised. Do users have control over this data collection, and any way to monitor it or shut it off, temporarily or permanently?

The purpose for which it's gathered. When and how will it be used? For example, location data may be gathered as an inherent part of delivering a service like stolen vehicle recovery — but is data continually being gathered, or only when triggered by the user? Is that data also used for customer profiling and marketing, or any other business purpose? How can users opt out of those uses, and what are the consequences of doing so (for instance, in-vehicle features becoming unavailable)?

Who will use it. Will the data be shared with any partners or subcontractors? Will it be shared with any government bodies or regulators as a matter of course?

How long it will be retained for. Where will data be stored and processed, particularly with regards to data sovereignty and jurisdiction? The EU GDPR enshrines a "right to be forgotten" — how can users exercise that right, or other legal rights such as data portability?

How it will be protected, and such protection verified. In a general sense, what measures are in place, such as encryption, access controls, physical controls and monitoring? What process will the company follow in the event of a breach to protect its users, and how would it disclose a breach?

How and when these policies are updated. The law changes, as does the technical and commercial environment and user expectations. Policies should be owned and actively managed by a team internally. They must be reviewed periodically and updates published. How are users notified of these changes and do they have any right of refusal?

Making privacy a foundation, organisation-wide

When we give customers advice about privacy, we do so from decades of experience as one of the world's largest network operators. Our infrastructure carries private data for hundreds of millions of consumers and business customers, and our multinational operations mean we're subject to many different legal jurisdictions.

In response, we have a global privacy framework that protects data wherever it's created, used or shared. We set policies at a group level for all our local teams to follow, and we manage data-sharing relationships between us and our partners through Data Processing Agreements.

We monitor the effectiveness of all these privacy efforts through regular policy reviews and impact assessments, under the authority of our independent privacy governance body. So you can see: for us, privacy is a very serious matter and we don't leave anything to chance.

Developing security expertise

Security is something you do, not something you have. It takes intelligence, specialist skills, and sustained effort. Automotive manufacturers and the rest of the connected services ecosystem will need to try new approaches to get the expertise they need.

Look at unconventional ways to get access to talent

Whether you're an automotive company, parts manufacturer, insurer, retailer or city authority, technology is now a core part of what you do. You need access to technology skills in general, and cybersecurity skills in particular.

> On appointing its first cybersecurity chief, GM's EVP of global product development said:
>
> "We went to the Navy, the nuclear part of the Navy, we went to Boeing Co. and Virginia Tech to ask who you hire, how you hired them and what you charged them to do. We have to look at car technology on a critical systems level. We see this a competitive advantage."[19]

Security experts are in short supply[20], and companies are trying many different approaches to recruit the best talent. One option is to "acquihire" experts by taking over specialist cybersecurity firms — as component manufacturers like Harman[21] and Lear[22] have done. Another is to headhunt — if you have the budget. Tesla's security chief is from Google[23], and Uber has not only lured a security chief from Facebook, but also hired the two hackers who took control of a Jeep in 2013[24]. From a more regulatory-focused standpoint, self-driving vehicle lobbying group Self-Driving Coalition for Safer Streets, backed by Google and Ford, has enlisted an administrator from the US National Highway Traffic Safety Administration (NHTSA) as its head[25].

It can also be fruitful to court the wider cybersecurity community as a kind of friendly crowdsourced vulnerability scanner. Most ethical hackers will have a disclosure policy that will lead them to report any vulnerabilities to you before announcing them publicly; you can encourage the community to test your products through a "bug bounty" programme. Tesla offers $10,000 bounties (and attends hacker conference Defcon to build relations with the community); Fiat Chrysler Automobiles has started paying bug bounties too[26], and GM offers recognition and a warm welcome[27] to white hat hackers, although as of yet, no money[28].

Open up

Collaboration on something as sensitive as security does not necessarily come naturally, but the automotive sector and its partners must work together to stay ahead of changing threats, sharing insights and formulating standards that simplify interoperability.

In 2015, the industry created the Auto-ISAC — an Information Sharing and Analysis Center for threat information[29]. This (along with the trade bodies' many other cybersecurity related activities[30]) is a positive start, but collaboration really has to be just as cross-industry as the ecosystem itself, and involve regulators as more than just a target for lobbying.

Whether it be data from inside transmissions or on-board diagnostics, many vehicle-makers are understandably concerned about protecting the privacy of their business and their customers. Indeed, it was just two years ago that former VW CEO, Martin Winterkorn, warned that the car was becoming a data octopus, encouraging automotive leaders to commit themselves to protecting the privacy of their customers[31]. Of course, decisions must be made about the extent to which the aftermarket is given access to connected vehicle data, too[32].

91% of enterprises say that it's important to work with an end-to-end provider for IoT[33].

Call on partners

Technology providers can provide a valuable source of independent advice, expertise, human resources, and facilities for development and testing of secure systems. For example, at Vodafone we offer a full range of professional services to help customers develop IoT designs that are robust, practical and secure, and we also offer testing of applications and hardware on our networks.

Taking security seriously

Vodafone participates extensively in IT and automotive forums that are helping to shape a new generation of standards and best practices around security. We help lead the GSMA Fraud and Security Group, as well as being active members of the EU's ENISA Automotive Group and the SAE International association.

Of course, we also take security seriously in our own infrastructures. All our data centres are compliant with ISO 27001, and where applicable we also exceed national standards, such as the UK government's Cyber Essentials Plus accreditation.

About Vodafone

Our combined experience in the automotive industry, in Internet of Things technologies, and in the IT security community, has given us a unique perspective on how to address today's security and privacy challenges.

We understand automotive

At Vodafone, we've seen the challenges and developments of the connected vehicle ecosystem first hand. Many of the world's top vehicle manufacturers already choose Vodafone as their partner for connected cars. Today we have more than 900 experts working alongside manufacturers including BMW, General Motors, Porsche and Volkswagen Group to shape the future of the automotive sector.

Our Automotive business unit has been producing technology products for the automotive sector, both manufacturers and the aftermarket, for more than 40 years. Our roots in the industry run deep. So we understand the very particular development constraints affecting vehicle components, as well as the way that the automotive industry works, and we've consulted for years with many of the top automotive OEMs about their security strategies.

What's more, our wider IoT division has been working closely with organisations including car insurers, city authorities, retailers, and other businesses that are moving into the connected services ecosystem. In fact, as a connectivity and services provider, we've often served as an impartial mediator in some of the first partnerships between these industries in applications such as insurance brokering, UBI and fleet management.

For more than
40 years
our Automotive business unit has been producing technology products.

We have a complete view of the data lifecycle

When it comes to appreciating the lifecycle of data from collection to processing, we have a privileged view. As well as manufacturing and supplying accredited in-car telematics devices that gather the data in the first place, we provide a full end-to-end solution across the whole value chain: from SIM and network through to management platform, APIs, applications and the underlying cloud and hosting products run from our own managed data centres.

Through Vodafone's specialist Automotive division we are uniquely positioned to provide end-to-end services, such as stolen vehicle recovery and usage-based insurance. Our capabilities include designing and manufacturing in-car hardware, plus delivering global connectivity, applications and round-the-clock monitoring from our service operations centres. We have built security in at every stage, meaning we can offer customers an unrivalled level of protection and privacy.

We are also a leading player in the broader connected transport ecosystem. Our vision is to be the hub that connects a multitude of industries. Already we are helping public transport companies, car insurers, fleet operators, car-sharing schemes, advertisers and public sector organisations work together to create new journey experiences.

We provide a full
end-to-end
solution across the whole value chain.

We are security experts

We're an active participant in the IT security community, too. Of course, as a truly global telecommunications company, we are responsible for critical infrastructure and we're adept at defending that infrastructure against sophisticated and persistent attack, as well as complying with security and privacy standards, in order to protect our hundreds of millions of consumer and business customers and their private data.

We've listened to the security and privacy concerns of our customers and continually evolve our security strategy in line with those expectations and market requirements. We also take seriously our responsibility for serving highly regulated industries and delivering mission-critical services like blue-light emergency services communications.

To that end, we operate a 24x7 cyber defence response and monitoring centre. We help share all of the insights we've gathered by taking an active part in standardisation and security bodies such as ETSI, GSMA, ENISA and 3GPP.

We operate a
24x7
cyber defence response and monitoring centre.

Next steps

The days where vehicles were self-contained machines are long gone. More and more vehicles on our roads are connected, joined by a torrent of data to an expanding ecosystem of public and private sector organisations. This flow of data is what enables a multitude of new services that will make our journeys more enjoyable, our cities safer and our commutes quicker.

Securing these vehicles and this data is a significant challenge. It will take new technology, new processes, and new relationships between organisations in different industries.

To talk to us about what actions you can take to tackle security and privacy in the connected vehicle ecosystem, get in touch: **automotive.vodafone.com**

References

1. Vodafone IoT Barometer 2016
2. https://www.wired.com/2016/05/drive-car-can-id-within-minutes-study-finds/
3. https://www.theguardian.com/technology/2014/mar/13/phone-call-metadata-does-betray-sensitive-details-about-your-life-study
4. http://www.cyberliving.uk/big-data-the-broken-promise-of-anonymisation/
5. https://argus-sec.com/remote-attack-aftermarket-telematics-service/
6. http://www.theregister.co.uk/2016/08/04/jeep_hacking_final/
7. Vodafone IoT Barometer 2016
8. Vodafone IoT Barometer 2016
9. Vodafone IoT Barometer 2016
10. https://www.bcgperspectives.com/content/articles/automotive_innovation_accelerating_innovation_new_challenges_automakers/?chapter=5#chapter5_section3
11. Vodafone IoT Barometer 2016
12. https://techcrunch.com/2016/01/28/security-and-privacy-standards-are-critical-to-the-success-of-connected-cars/
13. http://www.automotive-eetimes.com/content/5-best-practices-securing-connected-car/page/0/3
14. http://www.forbes.com/sites/thomasbrewster/2015/02/02/bmw-door-hacking/#43402d285a34
15. https://www.bcgperspectives.com/content/articles/automotive_innovation_accelerating_innovation_new_challenges_automakers/?chapter=5
16. Vodafone IoT Barometer 2016
17. Vodafone IoT Barometer 2016
18. http://www.bloomberg.com/news/articles/2015-09-02/carmaker-push-to-tap-data-gold-mine-faces-privacy-threat
19. http://www.wsj.com/articles/gm-hires-cybersecurity-chief-to-help-in-vehicle-development-1411499354
20. http://fortune.com/2015/12/07/high-paying-cybersecurity-jobs-go-begging-across-the-world/
21. http://thehill.com/policy/cybersecurity/264845-popular-speaker-manufacturer-buys-auto-cybersecurity-firm
22. http://www.lear.com/Press-Room/4279/lear-acquires-arada-systems-a-leading-automotive-technology-company-that-special.aspx
23. http://www.businessfinancenews.com/23423-tesla-motors-inc-hires-google-inc-cyber-security-expert/
24. http://www.icscybersecurityconference.com/#!Uber-Hires-Car-Hackers-Charlie-Miller-Chris-Valasek/c17dy/55e439f00cf2c1d1fd651347
25. http://www.theverge.com/2016/4/26/11510076/self-driving-coalition-ford-google-uber-lyft-volvo-nhtsa
26. http://disruptiveviews.com/fca-offers-rewards-ethical-hackers-car-breach/
27. http://www.fastcompany.com/3054535/gms-cybersecurity-secrets
28. http://arstechnica.com/security/2016/01/gm-embraces-white-hats-with-public-vulnerability-disclosure-program/
29. http://www.autoalliance.org/index.cfm?objectid=8D04F310-2A45-11E5-9002000C296BA163
30. http://www.autoalliance.org/auto-issues/cybersecurity
31. http://www.spiegel.de/netzwelt/netzpolitik/cebit-vw-chef-martin-winterkorn-warnt-vor-auto-als-datenkrake-a-957753.html
32. http://www.bvrla.co.uk/policy/update/connected-vehicles-driver-and-vehicle-data
33. Vodafone IoT Barometer 2016

automotive.vodafone.com