Whitepaper

Securing the Internet of Automotive Things

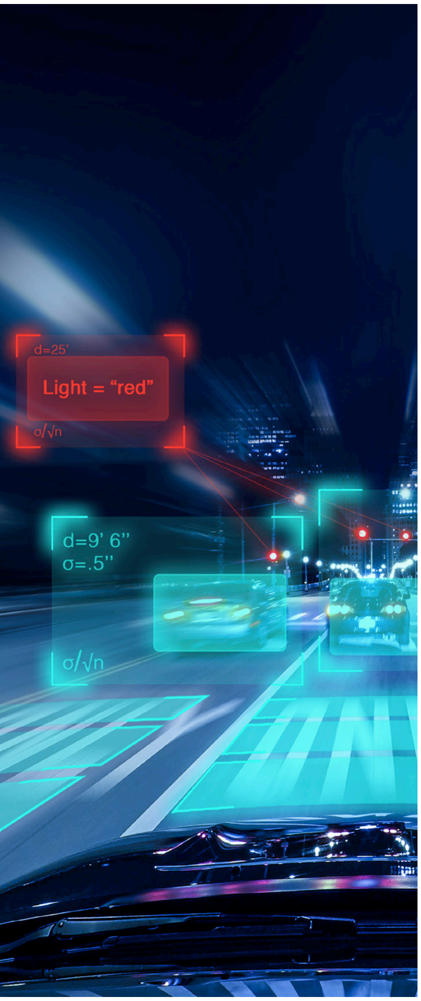
How to Safeguard Drivers and their Data in Connected Cars

BlackBerry Cybersecurity Consulting

The Internet of Things (IoT) is emerging as one of the most significant developments of our era. This growing network of physical devices, vehicles and other items with Internet connectivity can collect and exchange rich data.

The IoT is transforming how companies of all sizes, in almost all industries, operate: in short, the Enterprise of Things (EoT) has arrived. Gartner forecasts that more than 20 billion connected things will be in use worldwide by 2020.[1] KPMG says the projected value of IoT technology will be up to $6.2 trillion by 2025, while the McKinsey Global Institute predicts the IoT's total potential economic impact could reach $11.1 trillion by 2025.[2, 3]

The EoT holds great promise, but it also exponentially accelerates companies' vulnerability to data breaches and cybersecurity threats. Connected devices can be a competitive edge for companies (supporting innovation and new use cases) or a liability (introducing vulnerability to hacks and data breaches). For the automotive industry to realize the full potential of the EoT, they must be able to confidentially and reliably transmit highly sensitive data between connected cars.



The current threat landscape for the IoT

Many organizations are not even aware of all the connected devices in their environment, and bad actors are increasingly targeting this security vulnerability. The growing number of Distributed Denial of Service (DDoS) attacks launched using IoT devices, for example, points to the need to improve device security. In 2016, several massive DDoS attacks delivered by botnets made up of hijacked IoT devices caused major disruptions at various organizations and events (including the Rio Olympics).[4, 5]

Network World magazine predicts that new network security challenges will push security experts to their limits in 2018.[6] But it is not just private organizations reacting to the growing number of IoT cybersecurity incidents; the U.S. government recently introduced legislation to force vendors to ensure basic security within IoT devices sold to the government market.[7]

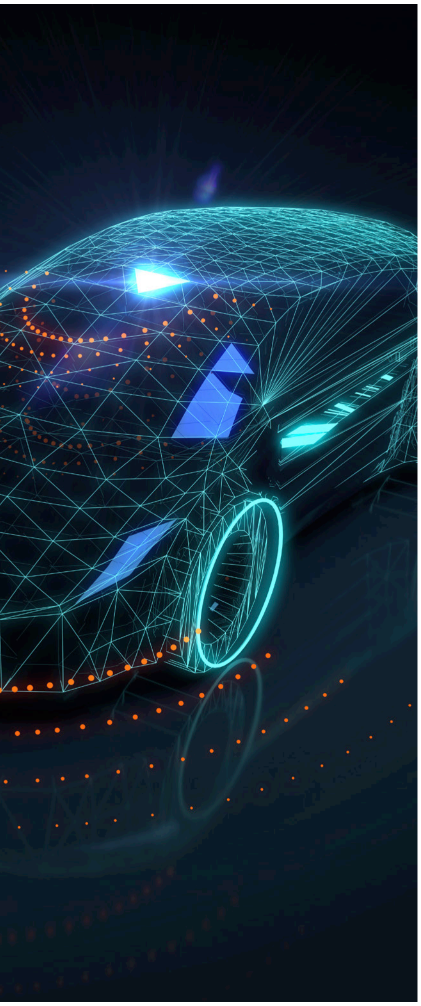
The challenge for companies with IoT devices

The IoT allows billions of smart devices to communicate and share data, and millions of new devices are connected to the Internet every day.[8] This creates a complex challenge for organizations: determining who governs permission to see and use all this data.

The state of IoT cybersecurity remains fragmented. Even where IoT security standards are emerging, they might not always keep pace with the expanding variety of IoT devices and applications.

Organizations may lack clear knowledge of where data from IoT devices resides, where it flows and how to control it. This wide dispersion of data creates a broad attack surface for cybercriminals.

Considering all these factors, robust data security is critical within any environment where IoT devices and applications operate.



Security for the IoT era

There are three main components of information security, which are captured in the CIA Triad.[9]

Confidentiality: limits access to the information in IoT devices
Integrity: ensures that information in IoT devices is trustworthy and accurate
Availability: guarantees reliable access to the information in IoT devices by authorized people

Automotive companies have proven to be eminently capable of ensuring the integrity and availability of information within their connected devices. Yet as cybersecurity threats intensify, ensuring confidentiality has become increasingly difficult. To strengthen this third point in the triad, automotive companies can partner with outside cybersecurity experts.

In the IoT era, there is a need for security solutions that protect the confidentiality of data in IoT devices, no matter where the data originates or where it travels.

The IoT in the automotive industry

Until recently, cars were isolated machines whose sole purpose was transportation. Now, the convergence of the IoT with in-vehicle technologies is transforming the industry. Connected cars are one of the fastest-growing markets in the ecosystem that makes up the IoT. Some factors driving the growth and popularity of connected cars include:

- Increasing concern and awareness about road safety and security
- Automakers' need to differentiate by offering unique selling features in a crowded market
- Rapid technological advances
- Consumers' demand for constant connectivity
- Society's growing dependency on technology

The two industries making the largest IoT investments in 2017 were manufacturing ($183 billion) and transportation ($85 billion), according to the IDC.[10] A Research and Markets report predicts the connected car market will reach $155 billion by 2022, while Business Insider Intelligence forecasts that 75% of the estimated 92 million cars shipped globally in 2020 will have internet connectivity. [11, 12]

Gartner says there will be 250 million connected vehicles on the road by 2020.[13] Even the most basic vehicles today have at least 30 electronic control units, and some luxury cars have as many as 100, according to the International Association of Privacy Professionals (IAPP).[14] While connected car prices are still out of reach for most car buyers, with 70% of global connected service sales coming from premium vehicle brands, by 2022 that number will fall to 50%, according to strategy.[15]

The benefits of IoT devices in the automotive industry

In-vehicle wireless connectivity has the potential to enhance driver comfort, convenience, performance, safety and security. The following are just a few examples of the capabilities of connected cars:

- Remote diagnostics
- On-board GPS
- Collision avoidance systems
- 4G LTE Wi-Fi hotspots
- Infotainment services

As connected cars become more advanced, they are gaining the capacity to consume, create and share data across multiple endpoints: for example, service centers track sensor data to predict maintenance, and insurers capture driving behavior for policy development. Looking forward, the race to create connected cars capable of processing vast quantities of data for fully autonomous driving is well underway.

While connected cars provide an enriched driving experience, their IoT devices can be vulnerable entry points for cybercriminals.

The risks of IoT devices in the automotive industry

Like any IoT device, connected cars come with the risk of data breaches and hacks. According to one prominent cybersecurity expert quoted in Road and Track Magazine, automakers are equipping cars with connected features faster than they can defend them against threats.[16]

Since connected cars are built through the joint effort of Original Equipment Manufacturers (OEMs) and multiple third parties, no single company or party has responsibility for securing the devices. Connected cars' vulnerability also stems from the fact that they are complex machines made up of many different digital systems and multiple connections between the vehicle and external networks. Any system or connection could be a weak link. Once a hacker breaks into one system, they could take over others (including safety-critical systems like braking).

In a survey of automotive industry stakeholders by the U.S. Government Accountability Office, most respondents (23 of 32) said remote attacks are the most concerning for passenger safety, since they could involve multiple vehicles and cause widespread injuries. The same survey found most stakeholders (24 of 32) are concerned about direct access attacks exploiting cybersecurity vulnerabilities in on-board diagnostic systems.[17]

The growing threats and the potential repercussions

While there is no documented incident of a real-life remote hack of a vehicle in motion, researchers working in controlled conditions have shown that it is possible (see box). There has, however, been an instance of a former employee of a car dealership remotely disabling hundreds of vehicles via an online vehicle immobilization system, according to Wired magazine.[18]

There are three main actions that cybercriminals could take when hacking connected cars:

- Remotely taking over critical vehicle functions
- Stealing personal information flowing between connected cars and the cloud
- Accessing the business systems of the connected car's OEM, suppliers or service providers

With more frequent media reports and fictional storylines on hijacked vehicles, consumer awareness of the risk is on the rise – which could eventually lead to mistrust of connected cars. Nearly 80% of consumers believe vehicle hacking will be a frequent problem in the future and the vast majority think auto manufacturers are most responsible for securing connected vehicles, according to research by Kelly Blue Book.[22]

Apart from consumers, the government is also taking notice of the emerging threats. In 2015, 1.5 million vehicles were recalled for cybersecurity vulnerabilities, according to the National Highway Traffic Safety Administration of the U.S. Department of Transportation.[23]

Headline hacks of connected cars

In July 2015, Wired magazine reported that hackers took control and killed the accelerator of a Jeep in motion on the freeway driven by a Wired magazine reporter.[19] The reporter was working with researchers to show the vulnerability of the electronics in today's vehicles. Once into the Jeep's vehicle systems, the researchers took control of the car's engine, transmission, sensors, GPS, radio and climate controls. Chrysler immediately recalled 1.4 million vehicles to fix the bug that enabled the attack.[20]

Wired magazine also reported that a hacker invented a $100 device that attacks GM's OnStar communication system and allows hackers to track, unlock and start the vehicle. The device simply needs to be placed in an inconspicuous place on a target vehicle.[21]

Policies and regulations for IoT cybersecurity in automotive

- After the infamous 2015 Wired magazine story on remote hijacking, Congress introduced an automotive security bill.[24]

- In 2016, the FBI, the Department of Transportation (DOT) and the National Highway Traffic Safety Administration (NHTSA) issued a public service announcement warning consumers and manufacturers to maintain awareness about potential cybersecurity threats to connected cars.[25]

- In 2016, NHTSA issued Cybersecurity Best Practices for Modern Vehicles (non-binding guidance to the automotive industry for improving motor vehicle cybersecurity).[26]

- NHTSA does not anticipate making a final determination on the need for government standards until 2018 when additional cybersecurity research is expected to be complete.[27]

- Automotive industry efforts to address the issue are in the preliminary stages, such as the establishment of an Automotive Information Sharing and Analysis Center to enhance cybersecurity awareness and collaboration.[28]

- The Society of Automotive Engineers (SAE) issued the SAE Cybersecurity Guidebook for Cyber-Physical Vehicle Systems in 2016 to provide guidance to the automotive industry on vehicle cybersecurity.[29]

10 ways the automotive industry can help safeguard connected cars

Safety and security are inseparable, as addressed in the BlackBerry® whitepaper, "Cyber Security for Automobiles: BlackBerry's 7-Pillar Recommendation."[30] The recommendations are designed to harden automobile electronics against attack, but can be extended to other devices and markets. The 7-pillar approach looks at the whole system, aiming to come as close as possible to developing a system where there is an absence of unreasonable risk.

But with dramatic growth predicted for the connected car market in the coming years, auto manufacturers should also take concrete steps now to protect drivers and the confidentiality of their personal data. Manufacturers should either make major investments in building their own cybersecurity capacity, or work with a security partner that can provide consulting services on data protection.

BlackBerry has the experience, expertise and tools to mitigate the risk of cyberattacks and data breaches. The BlackBerry cybersecurity offering leverages extensive research and development in two key domains:

- Security consulting practice (BlackBerry® Cybersecurity Consulting)
- Security software

Together, BlackBerry Cybersecurity Consulting and software provide a complete solution to help defend connected vehicles against data breaches. BlackBerry cybersecurity offerings can help protect the confidentiality and integrity of data, wherever it resides. BlackBerry works with the following automotive industry segments to enhance cybersecurity in connected cars:

- OEMs, which create infotainment systems and Electronic Control Units (ECUs) in connected vehicles
- Supply chain manufacturers, which create components for connected vehicles
- Backend infrastructure providers for connected vehicles

BlackBerry Cybersecurity Consulting partners with organizations to:

1. Adopt a risk and value-based approach to security
2. Help transform the culture of an organization to one that is security-aware and proactive, with security awareness and training programs
3. Understand the possible security weak points in their business through Security Assessment services, which include penetration testing, social engineering attack drills and the evaluation of physical security measures
4. Create a robust incident response strategy
5. Design systems and processes to include the latest security considerations from the outset in order to build the strongest possible secure foundation for new products and services

BlackBerry software enables organizations to:

6. Take inventory of devices and get a single view through unified endpoint management **(BlackBerry® UEM)**
7. Authenticate all network users and allow single sign-on **(BlackBerry® 2FA and BlackBerry® Enterprise Identity)**
8. Develop custom mobile apps and workflows while protecting sensitive information **(BlackBerry® Dynamics)**
9. Enable secure collaboration between all internal and external organizations in your supply chain **(BlackBerry® Workspaces)**
10. Balance security and productivity **(all BlackBerry enterprise software)**

BlackBerry — A global leader in security

Many of the world's most security-conscious organizations, as well as national government agencies, rely on BlackBerry products and services to secure their mission-critical operations. Built on more than two decades of security research and development, **BlackBerry Cybersecurity Consulting** has the in-depth knowledge and investigative experience to help companies identify and mitigate today's increasingly sophisticated threats, including the new and growing threats to connected vehicles.

BlackBerry Secure

Our integrated security solution helps companies manage and secure their desktops, laptops, mobile devices and connected things in a manner that secures communications for all messaging and file types. BlackBerry Secure is a comprehensive approach to security that addresses the entire enterprise from endpoint to endpoint. Being BlackBerry Secure means enterprise-wide solutions that are informed by deep security expertise and experience, continuous technical innovation, industry partnerships and academic collaborations, on-demand cybersecurity expert services and a point of view that recognizes vulnerability wherever it lies.

External recognition for BlackBerry as a security leader

- BlackBerry is the only vendor to have achieved the highest score in 6 of 6 use cases of the Gartner Critical Capabilities for High-Security Mobility Management[31]
- BlackBerry was a leader in the 2017 Gartner Magic Quadrant for EMM[32]
- BlackBerry Workspaces achieved 2 of the 5 highest scores in Workforce Productivity and Centralized Content Protection in the Gartner Critical Capabilities for Content Collaboration Platforms[33]
- BlackBerry ranks in the top 10% of all global cybersecurity organizations in the Cybersecurity 500 ranking published by Cybersecurity Ventures[34]
- BlackBerry has 80+ Security Certificates, more than any other mobile vendor
- BlackBerry has thousands of security-related patents
- BlackBerry is deployed with all 7 of the G7 governments and 15 of the G20 governments

BlackBerry Core IoT Platform

The BlackBerry® IoT Platform is a trusted foundation for the Internet of Things, providing intelligent, end-to-end vertical solutions for complex user problems.[35] It is designed to simplify and solve the complexity of data ownership and control. Built on years of technology investment, it can accelerate the development and deployment of secure, scalable and intelligent connected IoT solutions. The core design principles are:

- **Security**: Delivers authentication, authorization and data security through patented BlackBerry cryptography, certificate and key management technologies
- **Scalability**: Ensures scalability at every layer of the architecture
- **Efficiency**: Enables highly efficient communication between devices and applications, enabling advanced use cases

BlackBerry QNX: Innovative software for the future of connected transportation

The BlackBerry® QNX embedded software platform allows automakers to deliver reliable, secure connected and autonomous cars. Found in more than 240 vehicle models in over 60 million cars, it offers multi-layered end-to-end security technologies to protect connected cars from external hacking threats.[36]

Connected cars need robust security architecture that can adapt over a vehicle's lifetime. The BlackBerry Software Update Management Service is designed to be a scalable, flexible and extensible service for the secure delivery of software update packages. It enables safety- critical updates while also supporting updates that enhance the customer experience.[37]

BlackBerry Cybersecurity: Integrated services and software

1. BlackBerry Cybersecurity Consulting

BlackBerry Cybersecurity Consulting works to analyze and mitigate the increasingly complex cybersecurity risks in individual organizations. We are a trusted security partner, helping organizations identify, respond to and prepare for ongoing cybersecurity threats. While most security consultants test to find holes in a security system and then leave when the real work of repairing those holes begins, BlackBerry® Cybersecurity Consulting supports organizations every step of the way. Our tailored approach gives clients a detailed understanding of their unique security posture, then advises on the appropriate level of risk reduction within their budget.

Services available:

Security/Vulnerability Assessments
Highly accredited consultants assess vulnerabilities in connected devices, including penetration testing services, then provide recommendations for remediation.

Governance, Risk and Compliance
Consultants with in-depth knowledge of the regulated healthcare industry guide and support compliance and/or accreditation for numerous certifications, including HIPAA, PHIPA, GDPR and IEC 62304.

Threat intelligence
An extended assessment that considers the real-life threats to any organization, based on industry and strategy.

Event Handling/Response
Supports development of enhanced incident monitoring and response capabilities, and digital forensic services in the event of an attempted breach.

Wireless Penetration Testing
Tests the reliability of an organization’s wireless network to reduce the risk of an attack.

Social Engineering & Physical Security
Identifies any vulnerabilities in an organization’s staff and physical access to the organization’s building.

Training & Certification
Provides internal and on-premises security courses covering general staff security awareness and social engineering.

Security Engineering
Includes gap analysis, threat modeling and secure implementation review.

2. BlackBerry security software

BlackBerry software provides the embedded intelligence to secure the EoT, so that the IoT can thrive. These are just a few of the capabilities of BlackBerry software:

- **BlackBerry® UEM** manages your diverse and growing set of devices from a single console.
- **BlackBerry® Workspaces** enables secure collaboration on any device.
- **BlackBerry® SecuSUITE** for Enterprise empowers employees with secure and reliable voice and text.
- **BlackBerry® Dynamics** provides the foundation for secure enterprise mobility by offering an advanced, mature and tested container for mobile apps.
- **BlackBerry® AtHoc** is a complementary offering that unifies crisis communications within and between organizations (including triggering organization-wide alerts in the event of cybersecurity attacks or breaches).

From enhanced safety and performance to an enriched driver experience, there is much to be gained from IoT devices in cars. In the current threat landscape, however, robust cybersecurity will be crucial to the future success of connected and autonomous vehicles – not just to protect drivers and their data, but to build trust in consumers. Moving forward, the automotive industry’s primary focus on the physical safety of drivers will expand to include a strong emphasis on defending against cybersecurity threats.

BlackBerry has the experience, expertise and software to reduce the risk of cyberattacks and data breaches in connected vehicles. BlackBerry solutions help protect the world's most sensitive data across all endpoints – including the growing number and variety of IoT devices in cars.

Sources

[1] https://www.gartner.com/newsroom/id/3165317
[2] https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/10/internet-of-things-factsheet-au-2016.pdf
[3] https://www.mckinsey.com/mgi/overview/in-the-news/by-2025-internet-of-things-applications-could-have-11-trillion-impact
[4] https://www.networkworld.com/article/3123672/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html
[5] http://www.securityweek.com/iot-botnet-targets-olympics-540gbps-ddos-attacks
[6] https://www.networkworld.com/article/3217750/internet-of-things/5-iot-trends-that-will-define-2018.html
[7] http://www.securityweek.com/new-legislation-could-force-security-iot
[8] https://www.gartner.com/newsroom/id/3165317
[9] http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
[10] https://www.idc.com/getdoc.jsp?containerId=prUS42799917
[11] https://www.researchandmarkets.com/research/kdts2r/global_connected
[12] http://www.businessinsider.com/connected-car-forecasts-top-manufacturers-2015-2
[13] https://www.gartner.com/newsroom/id/2970017
[14] https://iapp.org/news/a/connected-cars-security-and-privacy-risks-on-wheels/
[15] https://www.strategyand.pwc.com/reports/connected-car-2016-study
[16] http://www.roadandtrack.com/car-culture/a31007/connected-car-defense-against-hackers/
[17] https://www.gao.gov/assets/680/676064.pdf
[18] https://www.wired.com/2010/03/hacker-bricks-cars/
[19] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[20] https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/
[21] https://www.wired.com/2015/07/gadget-hacks-gm-cars-locate-unlock-start/
[22] https://mediaroom.kbb.com/nearly-80-percent-consumers-think-vehicle-hacking-important-frequent-problem-future
[23] https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity
[24] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[25] https://www.ic3.gov/media/2016/160317.aspx
[26] https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf
[27] https://www.gao.gov/assets/680/676064.pdf
[28] https://www.gao.gov/assets/680/676064.pdf
[29] http://standards.sae.org/wip/j3061/
[30] https://blackberry.qnx.com/en/7-pillars-automotive-cybersecurity
[31] https://www.gartner.com/doc/3791263/critical-capabilities-highsecurity-mobility-management
[32] https://www.gartner.com/doc/reprints?id=1-42A6Q84&ct=170607&st=sb
[33] https://www.gartner.com/doc/3799963/critical-capabilities-content-collaboration-platforms
[34] https://cybersecurityventures.com/cybersecurity-500-list/
[35] https://ca.blackberry.com/qnx-radar/core-iot-platform
[36] http://blackberry.qnx.com/content/dam/qnx/markets/auto/auto-software-infographic.pdf
[37] https://us.blackberry.com/qnx-radar/software-update-management