White Paper

Cybersecurity for Automobiles: BlackBerry's 7-Pillar Recommendation

Sandeep Chennakeshu

ABSTRACT

Auto cybersecurity is on national agendas because automobiles are increasingly connected to the Internet and other systems and bad actors can commandeer a vehicle and render it dangerous, amongst other undesirable outcomes. The problem is complex and the point-solutions that exist today are fragmented leaving a very porous and "hackable" system. BlackBerry provides a 7-Pillar recommendation to harden automobile electronics from attack. The solution is intended to make it significantly harder for an attacker to create mischief. This paper describes the 7-pillars and how BlackBerry can help.

Cybersecurity for Automobiles: BlackBerry's 7-Pillar Recommendation

Acknowledgement:

This white paper contains thoughts and ideas from several contributors from different parts of BlackBerry. Among those are Adam Boulton, Chris Hobbs, Chris Travers, Christine Gadsby, Grant Courville, Jim Alfred, John Wall, Justin Moon, Scott Linke and members of their teams. As such, this is as much their contribution.

1. The Problem

Cybersecurity for automobiles is on the national agenda of several countries. Why? There are four industry trends that make modern cars vulnerable to cyberattacks and potential failures:

1. Automobiles are increasingly accessible by wireless and physical means to the outside world and bad actors.

2. Software will control all critical driving functions and if bad actors can access and modify or corrupt the software, it can lead to accidents and potential fatalities. The larger the amount of software in an automobile, the larger is the attack surface.

3. Autonomous automobiles will be driverless. By design, these automobiles will talk to each other and the infrastructure by wireless means. This further exacerbates the vulnerability problem in so far as the number of access points through which an automobile may be breached. When this happens, the concomitant effects could be viral as one car can infect another and so on.

4. Autonomous automobiles will deploy artificial intelligence, deep neural networks, and learning algorithms. These automobiles will learn from context. This means that software that was installed as being safety and security certified at production will morph with time, and there need to be new ways to ensure that the automobile is still safe and secure over its lifetime.

This threat is amplified by the following characteristics of the automobile:

- The electronics in a car (hardware + software) is built from components supplied by tens of vendors in multiple tiers who have no common cybersecurity standards to adhere to as they build their components. This makes the supply chain for the car complex and porous in respect to cybersecurity. Every vendor and every component is a point of vulnerability.

- The electronics in a car are a complex network of distributed computers called electronic control units (ECUs). An ECU is a piece of hardware and software that controls an important function in the automobile such as braking, steering, power train, digital instrument cluster, infotainment and more banal functions such as window control and air-conditioning. These

ECUs are networked by buses (physical wires or optical fibre), which carry messages using some defined protocol. This interconnected network allows ECUs to talk to each other. Safety critical and non-safety critical ECUs interact through this network. Some of these ECUs can be accessed by wireless means or physical access (e.g. USB drive). Access means potential infection. Hence, it is paramount to isolate safety-critical and non-safety critical ECUs.

- A car lives for 7 to 15 years. Over this period of time, its software must be updated. This time period brings risk, as hackers become more sophisticated over time and users of cars may download software that may contain malware.

Current practices and standards are inadequate. For example, functional safety standards like ISO 26262 (ASIL-A to ASIL-D), information sharing like Auto-ISAC, software coding guidelines like MISRA and the NHTSA 5-Star overall safety scores (which is more to do with collision), add value but do not solve the cybersecurity and safety problem described. These are point solutions not holistic solutions. There is need for a much more holistic cybersecurity solution for automobiles.

2. Experience Drives Innovation

BlackBerry has a long history of cybersecurity with deep involvement in multiple facets of a holistic cybersecurity solution. As such, BlackBerry understands the issues that need to be solved and has innovated to solve the same. It is therefore no surprise that BlackBerry:

- Is regarded as the gold standard in government, regulated industry and enterprise mobile security.

- Has been a leading supplier of reliable and safe software to the automobile industry for decades.

- Supplies managed PKI (certificates) services, crypto tool kits and asset management (key injection) to major companies.

- Operates a global over-the-air (OTA) secure software update service that has updated over 100 million devices in over 100 countries, with updates every week for over a decade.

- Has built a safety aware culture amongst our automobile software developers through training, work methods and practices to secure safety certification, and extends this training to its customers.

- Developed and deployed world-class vulnerability assessment and penetration testing methods and tools.

- Maintains an active and alert security incidence response team that monitors common vulnerabilities and exposures and reacts to address the same in products with industry leading response times.

- Have built a FedRAMP certified emergency notification service that can be used to provide alerts when issues occur with bulletins on precautions to be taken by those impacted before a solution is delivered.

- We are building a Rapid Incident Response Network to share information between enterprises to learn and act more quickly.

BlackBerry's experience and the products that it brings to bear on cybersecurity are extensive and valuable to the auto industry. BlackBerry's DNA is security. We use our deep experience, vast repertoire of tools, practices and knowledge to innovate and stay ahead. It is via this accumulated knowledge and insight that we have developed the 7-pillar recommendation that is described below.

3. The 7-Pillar Recommendation

Safety and security are inseparable. Our approach to the problem is to look at the whole system and try and get as close as possible to creating a system where there is an *absence of unreasonable risk*.

The 7-pillars recommended by BlackBerry are outlined briefly below. These pillars are described for automobiles but can be extended to other devices and markets.

1. **Secure the supply chain:**
   a. *Root of trust:* Ensure that every chip and electronic control unit (ECU) in the automobile can be properly authenticated (via certificates) and are loaded with trusted software, irrespective of vendor tier or country of manufacture. This involves injecting every silicon chip with a private key during its manufacturing stage to serve as the root of trust in establishing a "chain of trust" method to verify every subsequent load of software. This mechanism verifies all software loaded.

   b. *Code Scanning:* Use sophisticated binary static code scanning tools during software development to provide an assessment which includes: open source code content, the exposure of this open source code to common vulnerabilities and indicators of secure agile software craftsmanship. This data can be used to improve the software to reduce its security risk prior to production builds.

c. *Approved for Delivery:* Ensure that all vendors and vendor sites are certified via a vulnerability assessment and are required to maintain a certificate of "approved for delivery". This evaluation needs to be performed on a continuous basis.

2. Use Trusted Components:

a. *Proven Components with Defense in Depth:* Use a recommended set of components (hardware and software) that have proper security and safety features and have been verified to be hardened against security attacks. Create a security architecture that is layered and deployed with defense in depth (vault within vault). For example: Hardware (System on Chips - SOCs) must be secure in architecture and have access ports protected (e.g. debug ports, secure memory etc.). SOCs should store a secret key, as described above, and act as the root of trust for secure boot verifying software that is loaded. The operating system must have multi level security features such as access control policies, encrypted file systems, rootless execution, path space control, thread level anomaly detection etc. Applications should also be protected as described below.

b. *Application Management:* All applications that are downloaded should be certified and signed by proper authorities. A signed manifest file will set permissions of those resources in the system that this application will and will not be allowed to get access to. The applications must always run in a sandbox and are managed over their lifecycle.

***3.* Isolation:**

a. *ECU isolation:* Use an electronic architecture for the automobile that isolates safety critical and non-safety critical ECUs and can also "run-safe" when anomalies are detected.

b. *Trusted Messaging:* Ensure that all communication between the automobile and the external world and messaging between modules (ECUs) in the car is authentic and trusted.

4. In Field Health Check:

a. *Analytics and Diagnostics*: Ensure that all ECUs software has integrated analytics and diagnostics software that can capture events and logs and report the same to a cloud-based tool for further analysis and preventative actions.

b. *Security Posture:* Ensure that a defined set of metrics can be scanned regularly when the vehicle is in the field, either on an event driven (e.g. when an application is downloaded) or periodic basis to assess the security posture of the software and take actions to address issues via over-the-air software updates or via vehicle service centers.

5. **Rapid Incident Response Network:**
    a. *Crisis Connect Network:* Create an enterprise network to share common vulnerabilities and exposures (CVE) among subscribing enterprises such that expert teams can learn from each other and provide bulletins and fixes against such threats.

    b. *Early Alerts*: Typically, when a CVE is discovered there is a time lag between discovery of the issue and the fix. This time lag is a "risk period" and it is necessary to alert stakeholders on what to do with advisories until a fix can be deployed.

6. **Life Cycle Management System:** When an issue is detected, using Pillar 4, proactively re-flash a vehicle with secure over-the-air (OTA) software updates to mitigate the issue. Manage security credentials via active certificate management. Deploy unified end point policy management to manage, among other things, applications downloaded over the lifetime of the car.

7. **Safety/Security Culture:** Ensure that every organization involved in supplying auto electronics is trained in safety/security with best practices to inculcate this culture within the organization. This training includes a design and development culture as well as IT system security.

4. How does BlackBerry adhere to the 7-Pillar Recommendation

This section shares what BlackBerry provides by way of solutions and services to the 7-pillar recommendation.

1. **Secure the supply chain:**
    a. *Root of trust:* BlackBerry's Certicom unit provides Asset Management equipment that can be used to inject keys into chips at silicon foundries or test houses. This system has been proven in over 450 million smart phone chips deployed. Furthermore, BlackBerry Certicom's managed-PKI service issues certificates that can be included as part of each ECU while they are being manufactured. These certificates have been deployed in over 100 million Zigbee devices and 10 million cars.

    b. *Code Scanning:* BlackBerry is developing a novel binary code scanning and static analysis tool that can provide a list of open source software files included in a build, as well as the files that are impacted by vulnerabilities and can list a wide variety of metrics/cautions that tell a developer what to improve to reduce the security debt of the code (secure agile software craftsmanship). This is a cloud-based tool and hence BlackBerry can continuously upgrade the tool with new "execution engines" (engines that add new capabilities to do deeper scans) to enhance its capability and even add custom features for the auto industry.

c. *Approved for Delivery:* BlackBerry Cyber Security services can conduct "bug bashes" and "penetration testing" on products and IT infrastructure to assess if the enterprise can be certified as secure and approved for delivery.

2. Use Trusted Components:

a. *Proven Components and Defense in Depth:* BlackBerry QNX runs in 60 million cars and offers safety certified secure software from an operating system and hypervisor to a host of platforms and components that are designed with defense in depth security. Further, BlackBerry can lend its expertise to hardware providers to assess security risks with their chip and module designs. BlackBerry Certicom also offers hardened security crypto toolkits and means to inject hardware with secret keys.

b. *Applications:* All applications that are downloaded should be certified and signed by proper authorities. The signature of the applications and a signed manifest file will set permissions of what resources in the system this application will get access to. BlackBerry has fundamental patents in this area and can ensure that applications are signed properly. Further, when built on the QNX operating system, applications will be managed with the right access permissions, path space restrictions and sandboxing to ensure the system is safer.

3. **Isolation:**

a. *ECU isolation:* BlackBerry recommends that all ECUs that are safety critical be run on a network that is physically isolated from ECUs that have external physical access or are not safety critical. Any non-safety critical ECUs access to a safety critical ECU should only be accessed by a security gateway, which enforces strict policies. This gateway could have a firewall with a single outbound port, similar to BlackBerry enterprise servers. All traffic will be authenticated and encrypted with rolling keys. Domain controllers that manage multiple virtual functions (e.g. braking, steering, powertrain) can be isolated by a safety certified hypervisor such as the one provided by QNX. Any one system can fail without "crashing" the other virtual systems or functions. This hypervisor-based isolation can also be used for safety certified and non-safety certified functions that share a single domain controller.

b. *Trusted Messaging:* Messaging between ECUs and the outside world needs to be trusted. All external communication can be managed by the security gateway as described above for safety and non-safety critical ECUs. Messaging between ECUs should be authenticated and encrypted. As described in Pillar 1 each ECU has a unique private key and birth certificate, which can be authenticated by the security gateway and subsequently the Gateway can issue keys to the ECU, which can be used to

sign messages it sends to other ECUs, such that receiving ECUs know the message is from an authentic source as well as being signed. Chips can be designed to render such protocols very fast. BlackBerry Certicom has developed such a protocol.

4. **In Field Health Checks:**
   a. *Analytics and Diagnostics*: BlackBerry is developing analytics and diagnostic clients that can be embedded in ECUs, which can monitor events and log crashes and anomalies. This data is sent to the cloud that can be analyzed for valuable information and acted upon.

   b. *Security Posture:* BlackBerry is developing a cloud-based tool that can access ECUs in the automobile and scan key metrics either on a periodic basis or on an event driven (e.g. when an application is downloaded) basis. This allows the automaker to determine in pseudo real time to scan their automobile and take actions when there is a security or safety risk.

5. **Rapid Incident Response Network:**
   a. *Crisis Connect:* BlackBerry is creating an enterprise network to share common vulnerabilities and exposures (CVE) among subscribing enterprises. This allows a network of skilled resources to share and act faster than if they were fragmented.

   b. *Early Alerts*: Typically, when a CVE is discovered there is a time lag to the fix. This time lag is a "risk period". The Company is developing a scheme to use its BlackBerry AtHoc secure crisis communications platform to alert customers on precautions that can be taken during a risk period until a fix is deployed.

6. **Life Cycle Management System:** BlackBerry has deployed a global, secure over-the-air (OTA) software update service. This service is unique in regard to its scalability, deployment options and security. The service was derived from its smartphone software update service, which served over 100 million devices in over 100 countries with outstanding reliability. This service is now being deployed for automobiles, with the management console for administering complex deployments. BlackBerry is developing a Security Credential Management System (SCMS) to provision and manage certificates for automobiles, which will be used for authentication of messages between automobiles and between automobile and infrastructure. BlackBerry has also developed a unified end point management (UEM) client to be integrated in infotainment units to actively manage customer profiles and content.

7. **Safety/Security Culture:** BlackBerry has developed training to inculcate a safety and security awareness culture in its organizations working on safety and security software. This training includes education, processes, methods,

tools and behaviours that are best practices and can be shared with a wider audience.

While not every aspect of this 7-Pillar defense is deployed commercially, the overall framework is sufficient to build a set of standard requirements and criteria to achieve enhanced safety and security in automobiles.

5. Policy and Recommendations

Policy for automobiles is set by government bodies such NHTSA (National Highway and Traffic Safety Administration) and DOT (Department of Transportation). Typically, automakers do not support a common set of policies and their argument is that it stifles innovation and can raise costs.

However, there have been some policies that have been successful. Mandating seat belts (passive restraint systems) and airbags (supplemental restraint systems), the NHTSA 5-Star scoring system for cars set in 1998 (mainly for front impact collision), which was later upgraded to the entire car in 2011.

Likewise, we feel that NHTSA and DOT can mandate a minimum set of requirements, such as the 7-pillars, with certain criteria to be met to achieve a certain score. A 5-Star scoring system can be used to initially educate consumers and later to make their score a differentiator for their automobiles. However, implementations should not be mandated. This should be left to the automakers to differentiate their offerings. The scoring would be set based on how many of the recommended requirements are followed and how many objective criteria are met with tests. These requirements can also secure involvement with insurance companies to create the basis for insurance rates.

Another area for policy and standardization is vehicle-to-vehicle and vehicle-to-infrastructure communication, collectively called V2X. This communication protocol, frequency bands, message structures, latency, security and misbehaviour management must be standardized. Here, again, we recommend that the standard focus on what is required rather than implementation, which should be up to the automakers and their eco system. A key task in setting the standard will be to ensure interoperability of implementations that adhere to the standard.

Privacy and security of data is another important topic for policy makers and regulators. For starters, automakers have expressed concerns regarding their ability to trust the data from another automobile (especially from a different automaker) or from the infrastructure (e.g. Traffic light) the automobile is communicating with. In this regard, standardization, as suggested above, will help. An equally important concern is how does one protect the rich data that an autonomous car collects regarding a consumer's preferences and behaviours such as drive routes, favourite places to visit, travel times, applications downloaded and even transactions handled via the automobile.

Autonomous cars pose several challenges to regulators, automakers and insurance companies. Regulators need to ensure that there is a national framework and individual states do not set up fragmented rules. Will automakers make their own policies for actions that their driverless cars will take when confronted with a particular situation where machine learning and judgement can cause different outcomes for two different car models or brands? Will such policies and rules be regulated?

Insurance companies and underwriters will need to work with lawmakers and automakers to make the liability borne by an autonomous car proportional to the revenue of each component, and hence their contributing vendors, and not let the purchasing departments of automakers make this decision. These choices, and resulting policy or regulations, are unclear at this time.

Intellectual property presents another challenge. There is a lot of innovation in autonomous cars. Will innovation ever come to fruition or will it be mired in *inter partes reviews*, as today and IP wars. Will the auto industry be like the cellphone industry? Will regulators set rules on the maximum stack of royalties that can be charged per car with appropriate allotments to patent holders, using certain rules, or will it be market driven?

There are many unknowns. However, we need to make a start. To start with we recommend that we begin to define key requirements and criteria that makes the automobile safer and more secure. Towards this end we suggest starting with the 7-Pillars Recommendation by BlackBerry.