

Protecting the Connected Car



Martin Borrett

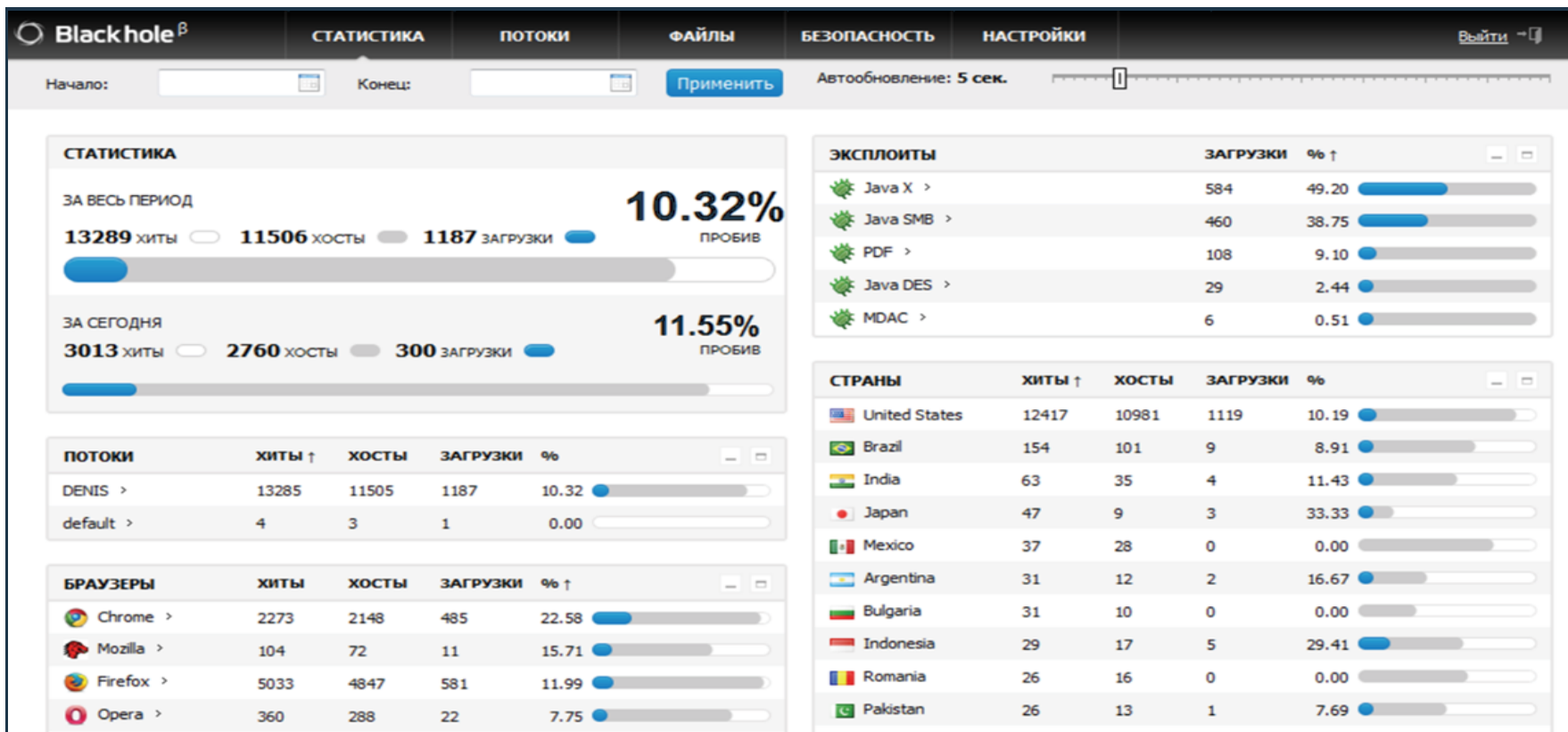
IBM Distinguished Engineer
CTO IBM Security Europe



Paradigm shift in crime

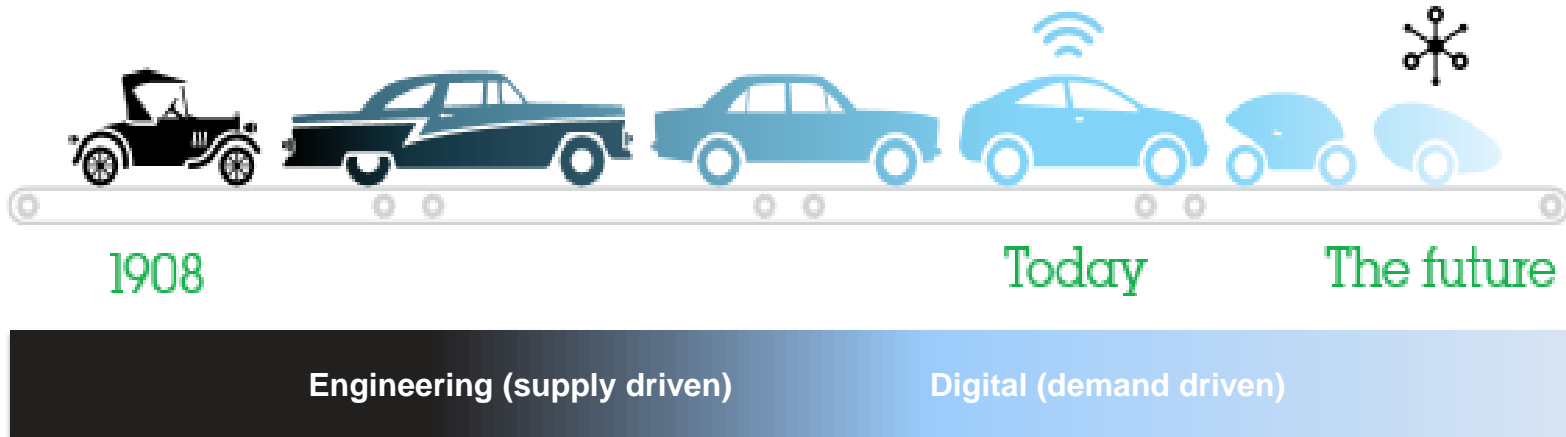


Cyber criminals use BUSINESS INTELLIGENCE

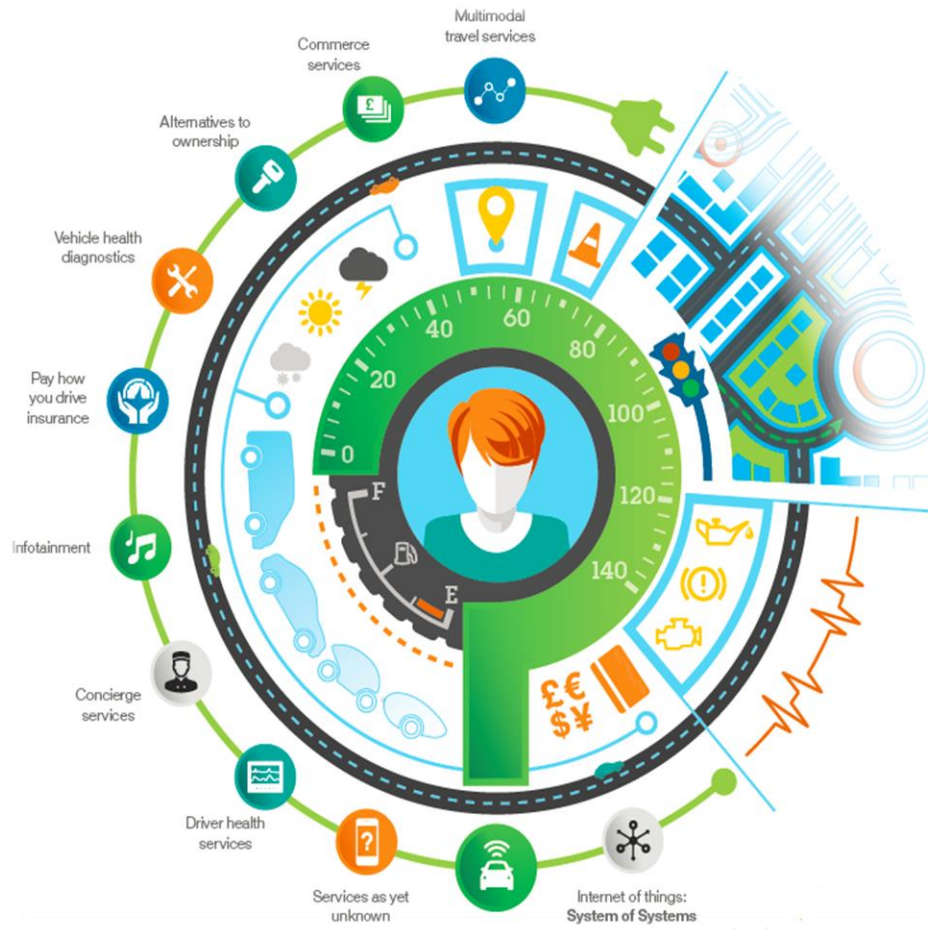


Automobile Evolution

For more than 100 years the automotive industry has created competitive advantage mainly through engineering excellence.



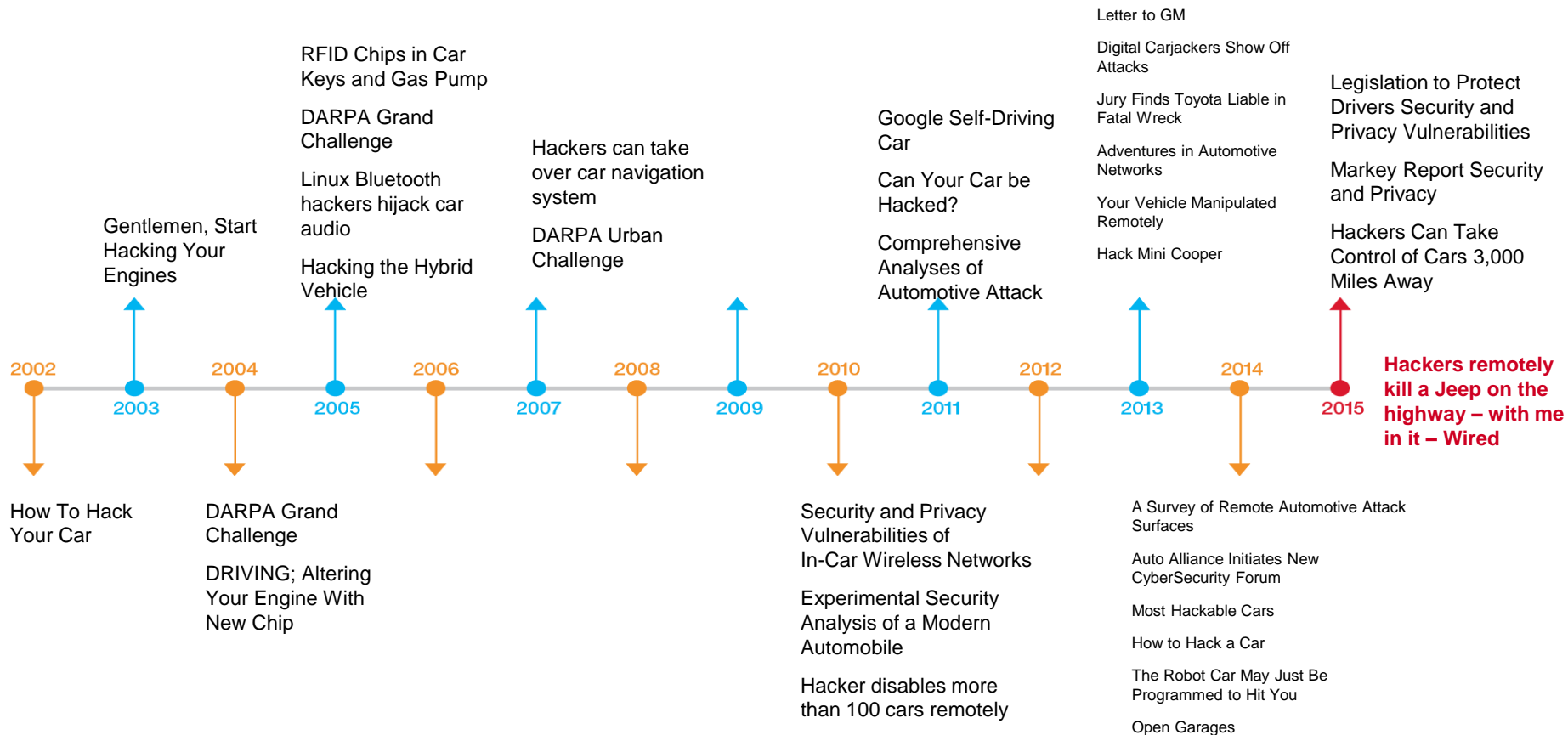
A Complete Digital In-Vehicle Experience



Customers expect the same digital experience they are familiar with from their smartphones.

Vehicles and smartphones are converging and the integration of both worlds increases the complexity and importance of a strong security posture.

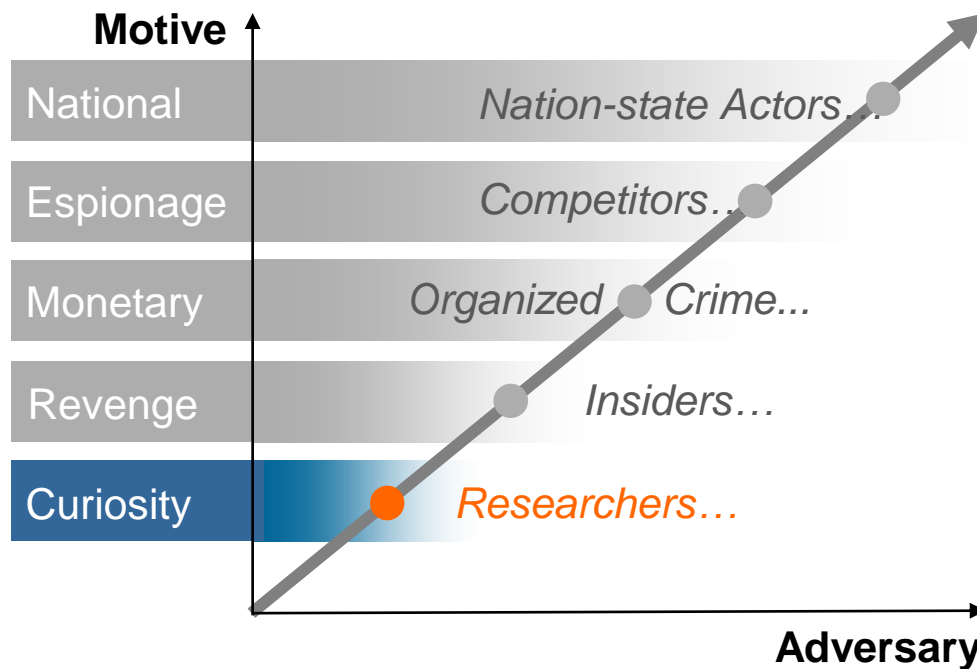
Cyber attacks are impacting the automotive industry



Threat to connected Vehicles

Cyber threat for connected vehicles just started. Number of **attacks** and intensity will dramatically **increase** over the next years, comparable to other IT environment.

- Comparable to business IT connected **vehicles are threatened** by cybercrime
- Other than standard IT only few researchers and hackers are currently interested in vehicles (see chart)
- Adoption rate of higher sophisticated attackers is **predicted short term**



IT Security Issue Root Causes

*Vehicle innovation was driven by engineering for more than 100 years. Today more than 80% of **innovation is driven by IT**. Vehicles became data centers on wheels.*

- More than **100 ECUs** (Electronic Control Units) from different suppliers operating together
- Up to **100 million lines of code** incl. related vulnerabilities
- Multiple **wireless network** interfaces used in parallel for communication
- Standard IT mechanisms for update or patching not available
- Vehicles **lack of security** mechanisms
- Standard IT technology (smartphone, USB-device...) linked or integrated into vehicle



Impact of Vehicle Trends

***Digitization is** the major **driver** for future innovations with significant impact on security requirements.*

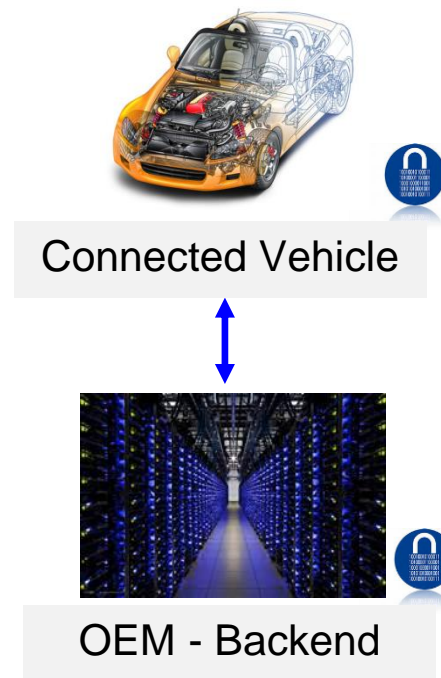
- **Connected Vehicles** become a central part of the digital life
- Car2X communication will lead the path from driving assistance to **autonomous driving**
- **Software updates** will become generic in the lifecycle of the vehicle
- Protection of data privacy needs to be **compliant** with local law
- In vehicle data is valuable for car makers and require special protection against **espionage**
- The automotive industry is in a transition phase to become **digital companies**



Connected Vehicle Security Principles

*The fundamental **security principles** for the information system have to be applied to vehicles.*

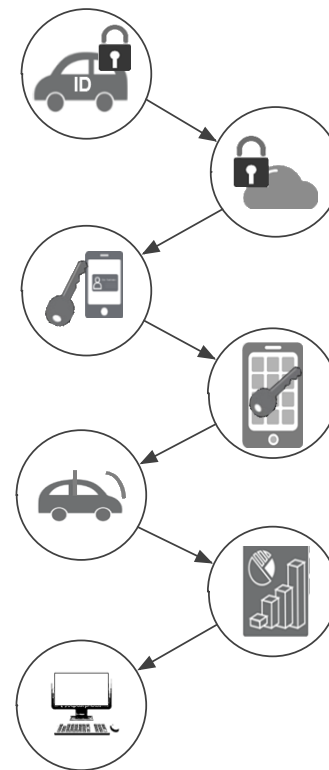
- **Security via obfuscation** is more threat than solution for entire vehicle life-cycle
- **Security by design**, vulnerability management and patching are required
- **Standardized Security elements** need to be added to vehicles and backend system
- Vehicles do require **trusted environment** as basis for security elements added
- **Compliance** becomes more important for future vehicle innovations, providing evidence is mandatory
- Security is never 100%. Intention must be to mitigate risk to become “**affordable**”



Connected Vehicle Security Elements

*IBM / G&D security architecture consists of **security levels** of protection, working in an integrated fashion, to achieve end to end vehicle security.*

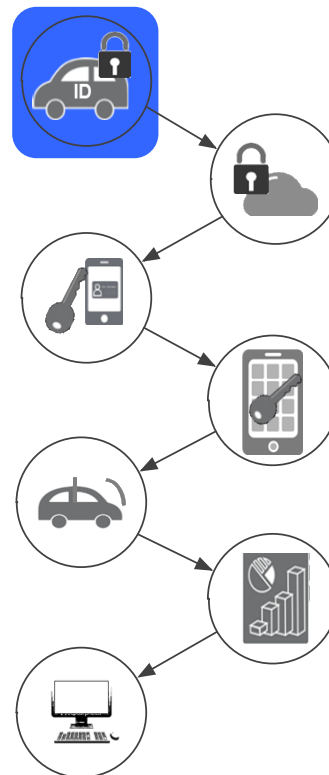
- **Trusted Identity** of all involved entities
- **Secure Data Storage** within vehicle
- **Access Control** and Management
- Communication **Encryption**
- **Intrusion Detection and Prevention System**
- **Security Intelligence**
- **Security Operation Center**



Connected Vehicle Security Elements

*First security level deals with **identity**. Each entity involved in interaction needs to be able to identify itself and prove identity.*

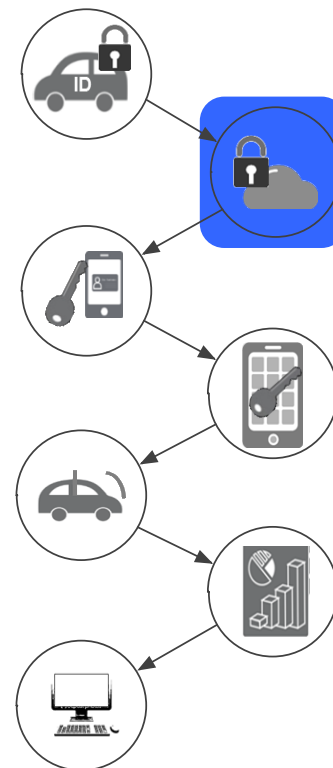
- First security level, in **vehicle and backend system**
- **Identify itself and prove own identity**
- Based on **key management mechanisms**
- Important for **compliance** reasons too
- Entities to **identify itself** up to end to end vehicle security architecture, potentially vehicle, ECU, backend system, driver, diagnostic system, mechanic, 3rd party etc.



Connected Vehicle Security Elements

*Second security level deals with **data**. Defined software, security keys, vehicle or driver data needs to be stored and processed securely.*

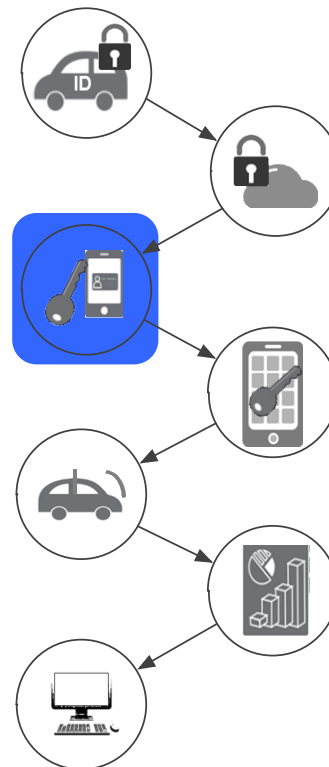
- Second security level, in **vehicle**
- Trusted **anchor** to securely operate from
- Stores security **software and keys**, able to secure **vehicle or driver data** too
- Extension might be future vehicle **operation log**
- Prerequisite is to clearly identify **data** that requires **to be secured**



Connected Vehicle Security Elements

*Third security level deals with **access rights**. Closely linked to the identity, not every entity is allowed to request, operate or change all.*

- Third security level, in **vehicle and backend**
- Links identity to **permissions**
- Not every identity will have similar permissions
- Important for **compliance** reasons too
- Prerequisite is to clearly identify vehicle functions that require dedicated permissions; these vehicle functions will be monitored even more closely by further security levels



Connected Vehicle Security Elements

*Fourth security level deals with **encrypted communication**. According data model defined for vehicle part of communication need to be encrypted.*

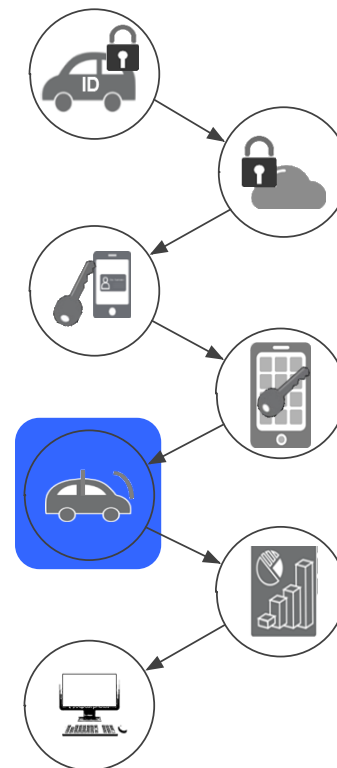
- Fourth security level
- Securely links vehicle to **ecosystem**
- At least part of **communication needs to be encrypted**; encryption mechanism should be applicable to different wired and wireless connections
- Prerequisite is analog secure data storage to classify and identify data to be encrypted



Connected Vehicle Security Elements

*Fifth security level aims to **detect and react on anomalies** within vehicle.
An Intrusion Detection and Prevention System fulfils this task.*

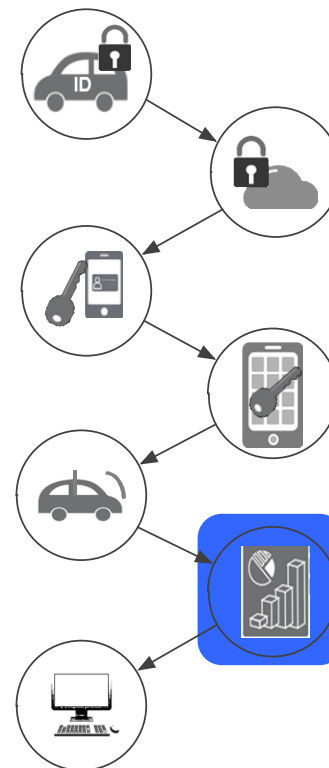
- Fifth security level
- **Rule based Intrusion Detection and Prevention (IDPS) System** watching out for anomalies
- Rules can either only **monitor communication** on dedicated networks and alert in case of violation, or even **prevent** dedicated **activities**
- Prerequisite is to have the IDPS system getting access to required vehicle networks



Connected Vehicle Security Elements

*Sixth security level deals with **security analytics and intelligence**. Vehicle status information received in backend can be correlated.*

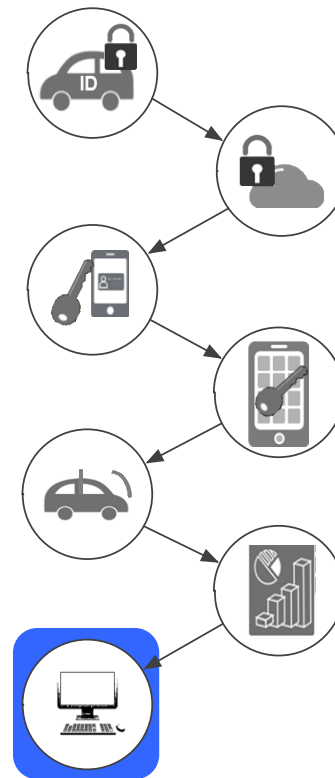
- Sixth security level
- **Content based security analytics function** that is able to supervise vehicles security status
- Supervision of **vehicle status and behavior** is key element to look for the unknown; at no time all vulnerabilities and related attacks can be foreseen during design and production of a vehicle
- Prerequisite is to collect vehicle status and communication data according continuously improved use cases



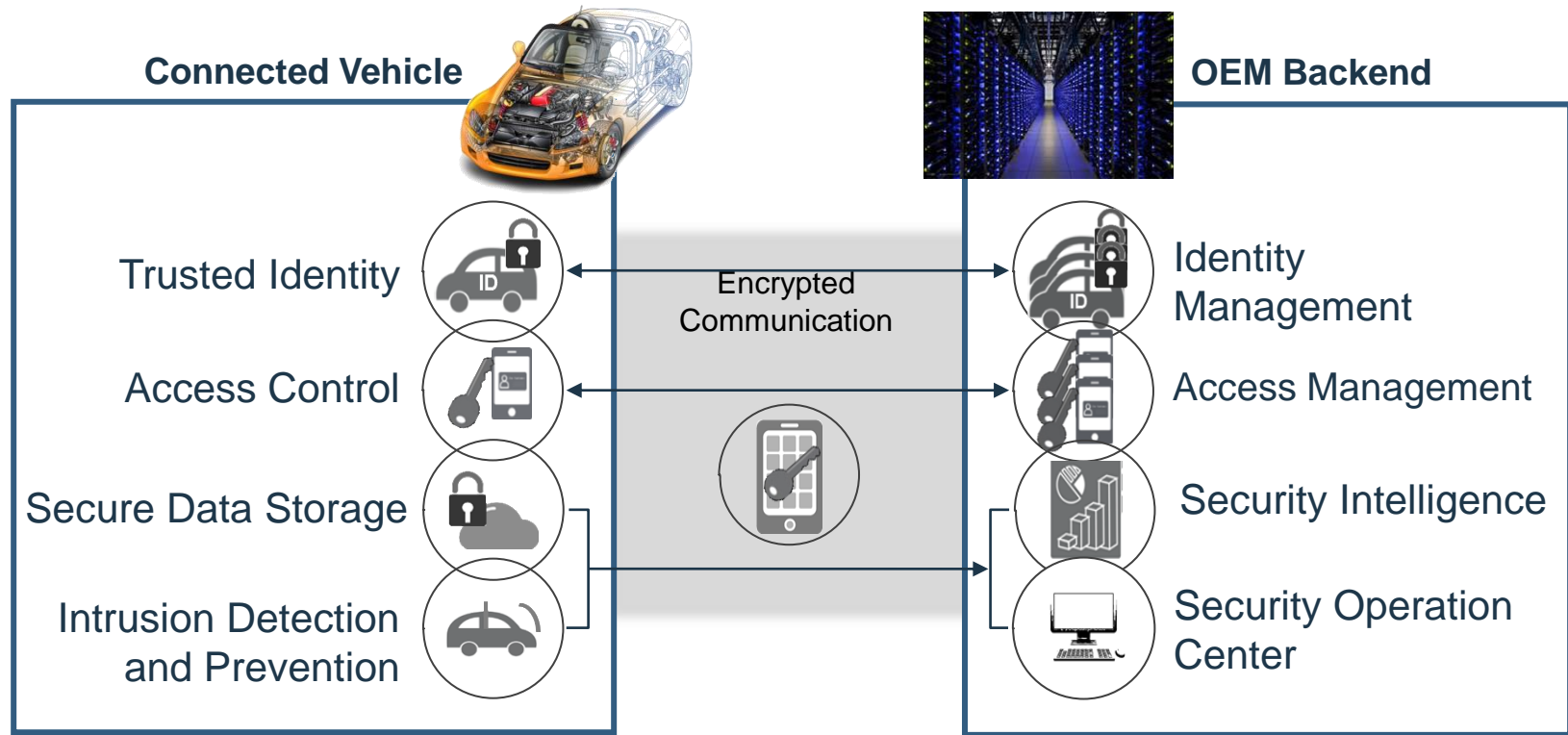
Connected Vehicle Security Elements

*Seventh and final security level **operates**, continuously **adopts and improves** Security, the living part behind all Connected Vehicle Security.*

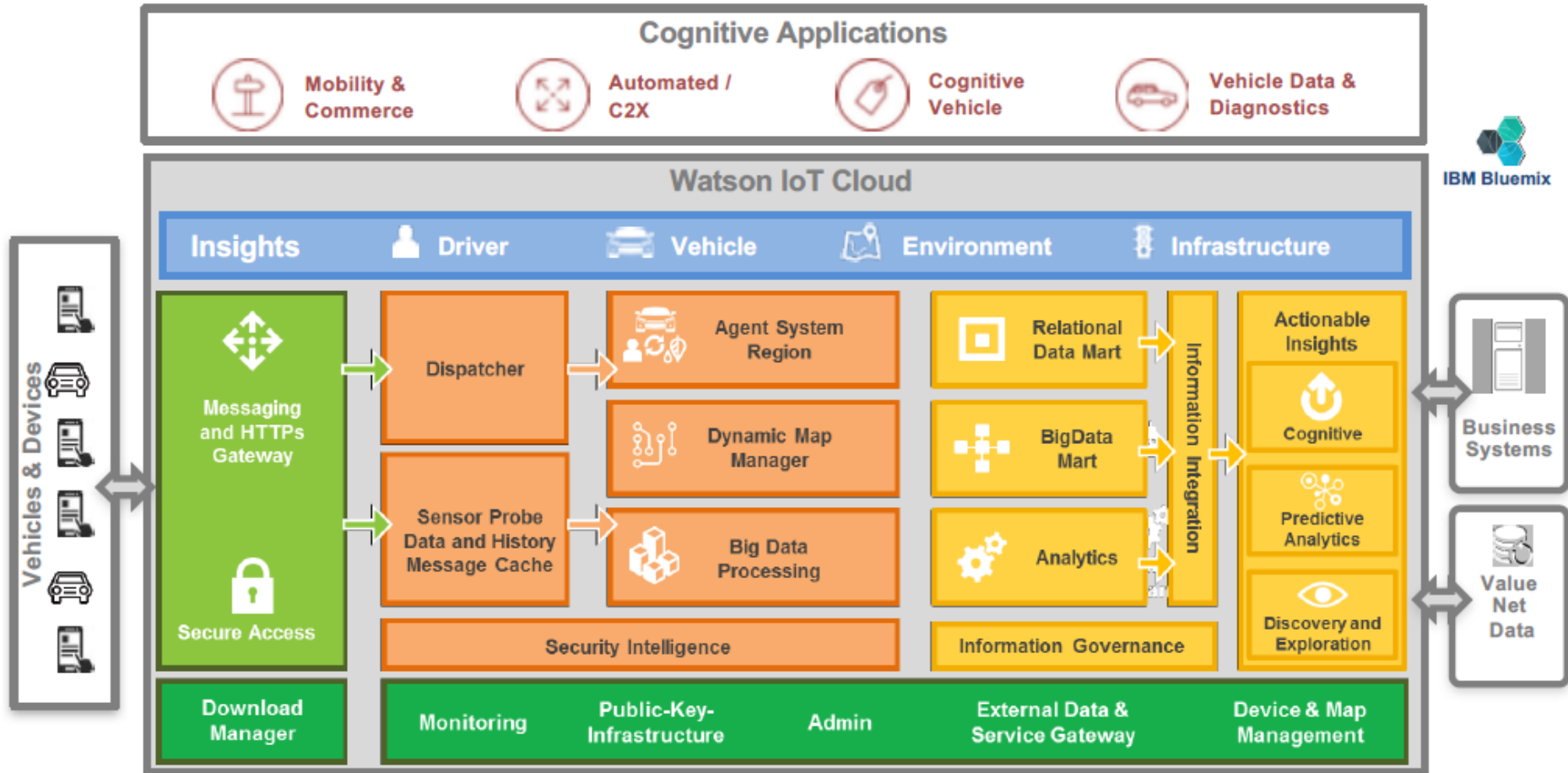
- Seventh security level
- Connected Vehicle **Security Operation**
- **Manages** and continuously **improves vehicle security** according to business strategy
- **Analyses and reacts on anomalies** in cooperation with functional departments
- **Defines and adopts rules** running in the vehicle, optimizes security analytics use cases



The architecture is designed to support Automotive OEMs and Tier-1s, from end-point (in-vehicle) devices to backend infrastructure



IBM IoT for Automotive Platform

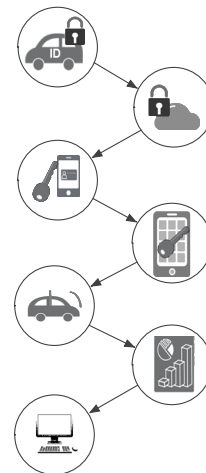


How to get started

Depending on already existing IT security considerations within recommendation is to define end to end IT security reference architecture (including variances) for future connected vehicles incl. backend.

Security work packages to start with might be

- **Reach:** end to end view (Backend, Connection, Vehicle)
 - starting point might be internet connectivity
- **Levels:** infrastructure, data, application (functionality of vehicle)
 - work items might be harden infrastructure, create/apply data model...
- **Elements:** identity and access management, communication encryption, secure storage, IDPS, analytics, operation
- **Activity:** Monitoring of end to end infrastructure and communication, triage and/or response in case of anomalies
 - proposal is to start with monitoring, use collected data for hardening and continuously improving monitoring use cases




IBM Institute for Business Value PoV Paper



<http://www-935.ibm.com/services/us/gbs/thoughtleadership/automotivesecurity/>

THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective.

IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.