The car is connected now! But are we safe? Cyber securing the connected car
The car is connected now! But are we safe?

Table of contents

01
Indian landscape: connected consumer and connected car

02
What is in it for all stakeholders?
- Connected car to help reduce range anxiety
- Connect dash camera
- Telematics help to bring down insurance claims

03
Architecture of connected cars and the risks

04
Scenarios of cyberattack:
- In-vehicle infotainment system
- WiFi hotspot
- Mobile application
- 4G SIM
- Facial recognition failure
- Tampering with OBD device

05
How can EY help?
Modern automobiles have completely changed, they are connected, available on demand and mobility is pervasive. This revolution of automotive connectivity with humans and infrastructure presents the big challenge - cybersecurity! Auto manufacturers and hackers have both demonstrated the value and perils of this connectivity and thus it necessitates a sharp focus from all stakeholders in the ecosystem - OEMs, regulators, component suppliers, insurance companies and even consumers to make the connected world safe.

The EY team is pleased to bring forward thought provoking scenarios and questions we all have to collectively answer. We live in a connected world today and in the foreseeable future, this trend is likely to increase. Historically, our experience in the industry has largely been around the use of information technology, which is now supplemented with operational technology. This combined flood of data is voluminous, instant and can be open to the outside world. This evolution opens all of us to the threats of cybersecurity, if not managed carefully.

As responsible corporate citizens we believe it is the duty of all stakeholders in this ecosystem to not only appreciate the threats of cyber but to also effectively take steps to prevent and mitigate risks. We at EY realize the enormity of the task at hand, the significant costs involved in terms of training of our people, the broader ecosystem, systems and checks and balances to be incorporated to safeguard our business.

A connected car and in-car connectivity have moved from being mere buzzwords to becoming an ubiquitous ask by the Indian consumer. The industry is already focused on multiple aspects of this transformation which include making connectivity a standard feature (as opposed to being an optional add-on), creating new business and pricing models for connectivity solutions and working with regulatory bodies to establish standards to enable a faster roll out.

We believe that the end consumer’s continuous demand for seamless in-car technology will continue to fuel innovation and collaboration between organizations spanning multiple sectors like telecom, internet service providers, automakers and component manufacturers.

Most OEMs are gradually expanding their internal organizational teams to work with these new competency areas while also solving challenges related to integrating vehicle platform development cycle time with the speed of development in the entertainment, communication and information technology space.

Alignment and collaboration across stakeholders in this connected ecosystem will be critical to ensuring that consumers continue to experience innovation in connected vehicles while also trusting the safety, seamlessness, relevance and durability of these solutions.
Section 01

Indian landscape: connected consumer and connected car
The changing Indian consumer
At confluence of aspiration and technology...

Paradigm shift in usage patterns
During 2019, it was estimated that 57.16% of the global population, or 4.3 billion people, will be using the internet.

Active mobile-broadband subscriptions have increased from 268 million in 2007 to 6.3 billion in 2019.

In 2019, average time spend 144 hours per day on social networking.

Nearly three-quarters of the world will use just their smartphones to access the internet by 2025.

Changing patterns of consumers
1. Mobile and technology-enabled
2. More sophisticated in their financial services needs
3. More demanding: expect more customization, personalization, flexibility and metricity
4. Increasingly looking towards other people for real-time recommendations
5. Fast and trouble-free solutions

"India to grow faster than China in MBB subscriptions and data traffic"
"Focus on content for enhancing customer experience"
"5G to account for 5% of total connections by 2025"
Transforming the lives of 2 billion people

India's digital and social media outlook
Growing digital media consumption, in the form of multi-play offerings, is increasing the data subscriber base for Indian telcos.

Digital opportunities to drive the next wave of growth in India
India to grow faster than China in MBB subscriptions and data traffic.

Mobile broadband subscription in India
- 2018: 0.5b
- 2024: 1.2b

Smartphone subscription to witness strong growth
- 2018: 0.6b
- 2024: 1.0b

Mobile data traffic/month to grow faster than China
- 2018: 3 EB
- 2024: 12 EB

Operators have showcased a number of 5G use cases
- Connected cars: Jio and Ericsson demonstrated 5G connected car and VR-enabled driving using 5G.
- Connected homes: Airtel and Ericsson showcased BVLOS autonomous drones over 5G networks.
- VR based 360 degree content: Airtel and Nokia demonstrated VR based 360-degree content that can be streamed in a 5G live environment.
- BVLOS autonomous drones: Airtel demonstrated how IoT can empower drivers through auto telemetry:
- Connected homes: Airtel showcased replica of modern connected home with intelligent devices and appliances.

Source: News articles, Statista 2019 Data, DMR
Source: EY knowledge

Video streaming contributes 70%-80% of mobile data traffic in India.

An average user spends up to 3.2 times more time on mobile content, than on web.

500 million people viewed videos online in 2019, a growth of 80% over 2018.

80% of the content consumed was less than a year old.

93% of time spent on videos in Hindi and other regional languages.

Source: EY knowledge

India has the largest number of Facebook users in the world
Million, Oct’19

Source: News articles, Statista 2019 Data, DMR
Connected features for connected consumers

Focus areas: stakeholder’s watch

Financial services
- Application and subscriber
- Over-the-air software updates
- Service management web portal
- Customer service helpdesk

Electric vehicles
- Battery health and charge status
- Charging location POI reservation
- Eco-trip planning and navigation
- Battery charge time scheduling

Intelligent vehicle
- Vehicle health reports and notification
- Dealer location and service scheduling
- Driver reports and coaching
- Driver monitor, limits and alerts

Infotainment delivery
- Personalized content delivery
- Driver CRM via email and SMS
- Driver smartphone app and portal
- Customer service helpdesk

Safety and security features
- Automatic crash notification
- Crash recording
- Remote alerts and theft tracking
- Remote vehicle immobilization
- Roadside assistance

OTA software management
- Policy-driven dependency, rollback and recovery
- Standards-based certification, authentication and encryption
- Dynamic data collection and upgradable analytics
- Customized consumer notifications, prompts, and consent

Connected vehicle features

- Leading automakers need to create connected car experiences that are intuitive, personalized and updatable.
- Automakers are increasingly developing electric, hybrid and plug-in hybrid vehicles to meet consumer demand and comply with current and future government fuel efficiency mandates.

What’s driving the connected car?

Intelligent mobility paves new roads for marketers

New car technologies are transforming the automotive sector, with major implications for industry players and consumers alike.

Asia Pacific and Europe
Asia Pacific & Europe are the major regions where demand for connected cars solutions and services is the highest due to various government regulations on vehicle safety.

5G and AI
The enhanced user experience for all connected cars depends on wireless connectivity. Many telecom industry players are developing 5G to increase the safety and efficiency of connected cars. According to International 5G automotive associations, 68% of accidents can be avoided with the upcoming 5G technology.

Source: EY knowledge

Continued on next page
Connected cars are poised to become a common phenomenon in India in the near future. And their relevance in the next few years is bound to increase with the expected wide-scale adoption of EVs where connectivity features will help owners locate nearby charging stations and access telematics data among several other things.

An increase in vehicle legislation and industry compliances regarding convenience features, such as navigation, remote diagnostics, etc., are driving the connected car market.

Technologies like telematics, connected and autonomous vehicles will play a vital role in transformation.

By connectivity technology: Cellular segment is expected to dominate the India connected car market.

Connected consumer puts pressure on all stakeholders for the right strategy

Right business model: stakeholder’s watch

Customer value and products portfolios value

Strategy medium/short term plans
strategy discussions amongst shareholder’s are essential to overcome frictions in the organization, because there are a number of key questions and issues to be addressed.

Technologies like telematics, connected and autonomous vehicles will play a vital role in transformation.

By connectivity technology: Cellular segment is expected to dominate the India connected car market.

An increase in vehicle legislation and industry compliances regarding convenience features, such as navigation, remote diagnostics, etc., are driving the connected car market.

Source: EY knowledge
## Key questions for all stakeholders

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer should be about</th>
</tr>
</thead>
<tbody>
<tr>
<td>What telematics services will be offered (and when)?</td>
<td>Identifying initial target market, with a view on benefits and costs</td>
</tr>
<tr>
<td>Are the telematics services technically feasible in my target market?</td>
<td>Understanding the IT landscape, its strength and weaknesses</td>
</tr>
<tr>
<td>Are the services commercially viable?</td>
<td>Building up the business plan also to anticipate issues/concerns and estimate pricing improvement</td>
</tr>
<tr>
<td>How are the black boxes/devices installed and maintained and who will bear the cost?</td>
<td>Keeping a flexible approach ready for “device independency”</td>
</tr>
<tr>
<td>Who will store and analyze the data (i.e., in-house or outsourced)?</td>
<td>Understanding the path to develop access to adequate technology and skill</td>
</tr>
<tr>
<td>What are current consumer attitudes?</td>
<td>Identifying “differentiating services” to avoid the “commodity pricing trap”</td>
</tr>
<tr>
<td>How do I attract new customers without cannibalizing my existing portfolio?</td>
<td>Comparing company’s portfolio and clients with market trends and existing threats</td>
</tr>
<tr>
<td>What strategic partnerships would add value to my proposition (e.g., car dealerships, road side assist service providers, technology partners, official bodies)?</td>
<td>Building a vision behind that of a gadget that enhance risk selection, to leverage telematics ecosystem</td>
</tr>
</tbody>
</table>

Source: EY knowledge
Connected car ecosystem

Multiplicity of services and stakeholders

Higher bandwidth
- Radio-music, news: live news feed
- Video: on-demand and real-time content
- Other in-vehicle services enabled by cloud computing

Lower bandwidth
- News, stocks and sports
- Apps store
- Multimedia, internet services, social networking, etc.

On-demand infotainment

Navigation
- Point of interest, parking
- Route optimization
- Traffic/Journey times
- Travel and traffic assistance/ off-board route guidance
- Location-based services

Diagnostics
- Vehicle health
- Scheduled maintenance
- Recall information
- Service coupons
- Service scheduling
- Electrical vehicle: battery charge monitoring/ control

Vehicle-to-vehicle
- Traffic information
- Driver warnings
- Pre-emptive actions to avoid and mitigate crashes
- Threat and hazard sensing: 360 degree awareness of the position of other vehicles

Safety and security
- Roadside assistance
- Emergency notification
- Theft tracking
- Remote control of vehicle environment/ car features
- Geo-fencing

Others
- Usage based insurance
- Fleet management
- Payment (tolling, parking, etc.)
- In-car health services
- Embedded financial GPS units

Source: EY knowledge
Connected car ecosystem (continued)

Multiplicity of services and stakeholders...

How are connected car services delivered?

- Telematics service platform/access portal
- Security services
- Content creation
- Content aggregation
- Application development
- Application delivery

User interface
- Embedded
- Tethered
- Integrated

Wireless network (connectivity)
- Low speed data services (2G)
- High speed data services (4G/5G or LTE)

Customer support/service
- Call centers
- Online support
- Subscription management
- Charging and billing

Service delivery architecture

Stakeholders

Automotive industry
- Vehicle manufacturers
- Auto component suppliers
- Repairer networks / service centers

City/State regulators
- Telecom operators

Information technology
- Packaged software vendors
- IT services companies

Telematics service provider
- Telematics service platform providers

Device manufacturers
- Smartphone manufacturers
- Portable navigation and infotainment device manufacturers

Insurance industry
- Insurance providers
- Insurance distributors (brokers and aggregators)

Others
- M2M service providers
- BPO
- Roadside assistance providers

Source: EY knowledge

Device-to-vehicle connectivity
- Visual
- Haptic
- Voice

Human-machine interface

Low speed data services (2G)

High speed data services (4G/5G or LTE)

Call centers

Online support

Subscription management

Charging and billing
We see connected vehicles as a part of the overall mobility solutions landscape

**Mobility solutions considerations: who, what, why, where and how...**

<table>
<thead>
<tr>
<th>Who and why</th>
<th>Urban (Business to consumer)</th>
<th>Regional</th>
<th>Global</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who and why</td>
<td>Ride sharing</td>
<td>Share-a-car</td>
<td>“World citizens”: people living in the various areas of the world at the same time</td>
</tr>
<tr>
<td>What</td>
<td>Car sharing</td>
<td>Autonomous driving</td>
<td>“World citizens”: people living in the various areas of the world at the same time</td>
</tr>
<tr>
<td>How</td>
<td>Brand sharing</td>
<td>Hybrid engines</td>
<td>“World citizens”: people living in the various areas of the world at the same time</td>
</tr>
<tr>
<td>Why</td>
<td>Predictive/optimized maintenance and repair</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**The audience considerations of mobility**

“Who is the mobility service designed for and why is it important to them?”

**Commercial (Business to business)**

- Corporate car sharing mobile
- Corporate BRT: mobile working space
- Integrated logistics
- Fleet cost optimization
- Mixed fleet management
- Intermodal solutions
- Hybrid engines
- Material/product logistics
- Human capital/people mobility
- Corporate dwellers

**Public (Business to government)**

- Bus rapid transit solutions
- New traffic management tools
- Dynamic space pricing
- Integration of renewable energy (with energy needs of the ecosystem)
- Tolls system
- Intermodal solutions

**What the programmatic aspects or topics within mobility**

“What needs to be considered and/or addressed in implementing a mobility strategy?”

**Where The geographic considerations**

“Where are people and things moving to and from?”

**How Some key questions for OEMs to consider**

- What do consumers value and what are they willing to pay for?
- How do we prioritize the various mobility concepts to implement?
- How do we monetize our investments in mobility (and telematics)?

- What do business and fleet customers value and what are they willing to pay for?
- How do we monetize opportunities for emission reduction targets?
- How integrated is our overall strategy for corporate clients?

- What are governments looking to accomplish?
- What is our city-focused go-to-market approach?
- How can we access new private/public business models to help finance new mobility concepts?

Source: EY knowledge
India connected car market

Emerging profit pool for the Indian automotive industry

- The key factor driving the growth of the market is the increase in the number of connected features in economy vehicles by OEMs. Additionally, an increase in vehicle legislation and industry compliances regarding convenience features, such as navigation, remote diagnostics and multimedia streaming through various platforms such as Android Auto, CarPlay and MirrorLink are driving the Indian connected car market.
- New safety norms are encouraging automakers to equip the vehicles with safety and security connected features, which in turn is increasing the demand for connected cars.
- Various technologies such as heads-up displays, smart infotainment and telematics systems are becoming an integral part of high-end automobiles.

Connected cars: market dynamics

Drivers
- Economy car manufacturers attempting to provide luxury features
- Government initiatives for implementing connected car technology

Restraints
- Lack of supporting infrastructure
- Unavailability of standard platforms

Opportunities
- Emerging profit pool for automotive industry
- Evolution of the new value chain ecosystem of the automotive industry

Challenges
- Increase in the threat of data breach and cyber security for connected vehicles
- Increase in the price of the vehicle with connected services
Section 02

What's in it for all the stakeholders:
OEMs, suppliers, insurance companies, service providers

The car is connected now! But are we safe?
OEMs challenge and opportunity

Technology, commercial and operations: are these the big questions?

Connected car mobility is the 21st century’s biggest opportunity. OEM challenge will be to find new business model for the connected services and revenue stream will the proof’’

Som Kapoor
Partner, Future of Mobility
Som works with automotive OEMs across the country

Technical challenges
“How will my connected vehicle solutions work?”

- Adopt software iteration cycles
- Standardize technology platforms
- Select partners

Integrate across vendors

Commercial challenges
“Where will we make money?”

- Define the buyer
- Enable the seller
- Optimize pricing

Operational challenges
“What’s required to deliver on our promise?”

- Deploy and operate robust solution
- Build service infrastructure
- Integrate across vendors

The car is connected now! But are we safe?”
Connected vehicles: opportunities and challenges for vehicle manufacturers

**Internet-enabled, telematics**

**From**
- Managed as feature/functionality item
- Owned by product development/engineering
- VM branded
- Unclear value proposition
- Optional item bundled in a package

**To**
- Key element of customer engagement
- Application across ownership lifecycle
- Services-driven value proposition
- Multi-vendor, multi-brand solutions
- Standard item
- Tight smartphone integration

**Many definitions exist - we propose**

- **Mobility** - moving people and things from point A to point B
- **Connected vehicles** - internet-enabled, mobile equipment
- **Telematics** - hardware and software to connect vehicles

**Challenges**
- Defining value and willingness to pay for dealers and customers
- KISS: keep it simple for users
- Organizing for success
- Operating a services business
- Managing partnerships vs. vendors
- Owning and using data

**Opportunities**
- Differentiate through the connected vehicle experience
- Build direct relationships with customers
- Use data to improve quality/reduce warranty expense
- Increase share of post warranty, customer pay parts and services spend

Success in connected vehicles requires focus and diligence in strategy and execution

**Connected vehicle strategy: Define - Develop - Monitor**

1. **Assess/Define**
   - **Strategy alignment**
     - Ensuring the alignment of telematics and mobility with overall corporate strategy across different BUs
   - **Risk management**
     - Creating an integrated and dynamic control environment for the connected vehicle strategy that balances value, cost and risk
   - **Customer definition**
     - Defining the key stakeholder and customer groups and determining key solution requirements and pricing
   - **Integration and monitoring**
     - Effectively integrating and monitoring mobility and telematics program efforts and results across BUs

2. **Design/Develop**
   - **Connected vehicle strategy**
     - After identifying one or more focus areas, the next step is to design and develop an integrated and holistic connected vehicle strategy

3. **Implement/Monitor**
   - **Technical**
   - **Commercial**
   - **Operational**

---

The car is connected now! But are we safe?
New revenue streams for all stakeholders

- Standard onboard function
- Determines vehicle chassis details, engine number, date of manufacturing and all legal attachments
- Locates the nearest OEM dealerships and workshops
- Records and shares the user feedback regarding the dealer with the OEM
- Onboard engine safety package
- Warnings include gear shift indication, rev recognition to avoid engine over revving
- End-to-end encrypted messaging system allowing users to chat with friends using the chat connect app of the same OEM and also through the vehicle's command system.

The connected car opportunity: who will provide the infrastructure and who will give the content?

- Store subscriptions allow unlimited song downloads on-board the vehicle which can be played offline
- Gives entire summary of engine usage and performance to the user
- Monitors idling, average speed, clutch usage, brake usage, acceleration, gear selection, etc. and presents in a report format to the user
- Customizes cabin light colours, instrument cluster lights and button light colours as per the desired ambience
- Includes vehicle tracking, emergency calling, location sharing and urgent member calling
- Service track records maintained by vehicle, notifying the user one week prior to the service due date. Vehicle books a service appointment with the concerned dealer by itself
- Sensors installed by default in the vehicle
- Activation of this package allows user to monitor tyre pressure
- Provides choice of setting the desired infotainment language for users unfamiliar with the generally accepted Hindi and English

Unpaid basic packages

- Vehicle information package
- Convenience package
- Warning package
- Company app downloads
- OEM chat connect

Paid add-on packages

- OEM music store
- Engine diagnostic system
- Advanced safety and security package
- Service information package
- Language package
Case study on EVs: how can being connected help reduce range anxiety?

Information at the user’s fingertips about charging infrastructure and timely alerts

Nearest charging station and availability for type of charger

To alleviate range anxiety, the electric vehicle battery will need to be safer, cheaper, have faster charging and feature a high energy density for greater range.

Current and future scenario: connected dashcam

In case of a car collision

1. No solution to notify the accident
2. During the impact, connected dashcam will send alert push notification
3. Insurance company, police, etc. have to rely on the eye witness for the sequence of events

Benefits
- Reduction in insurance premium
- In case not the driver’s fault, no premium increase
- Fleet can reward drivers based on the driving performance

Future scenario with connected dashcam

Connected dashcam, push alert notifications, geo coordinates and event video to insurance company, emergency services and family of the driver

Connected dashcam, push alert notifications, geo coordinates and event video to insurance company, emergency services and family of the driver

Case study: shared mobility connected dashcam

(|Case study 2|)
Telematics in claims provide real customer protection and drive down insurance losses

Telematics as survivor!

(Case study 3)

Real time data transmission
- Location
- Motion
- Speed
- Vin number
- Acceleration
- Force of impact
- Other external environment such weather, traffic and road conditions

Extra information via telematics devices will help manage insurance losses by enabling claims operators to determine the exact circumstance of the claim including nature, type and extent of the damage to the vehicle as well as the early indication of likely bodily injury
- Reduction in underwriting and claim fraud
- Reduces the first notice of loss process
- With two-way communication can help identify individuals involved in the accident
- Improves the accuracy of case estimation damages reducing the uncertainty in property damage and small injury claims

Telematics enables a superior seamless claims process for a more holistic protection cover for customers
- Theft
  - Theft alarm is activated
  - Theft notification to customer
- Accident
  - Instant crash / emergency notification
  - Send relevant emergency services to the confirmed location
  - Check customer record and contact family
  - Remain in contact with the customer
  - Confirm arrival of emergency service
  - Saving lives
- Breakdown
  - Instant notification and location of the vehicle
  - Direct the nearest recovery team directly to the vehicle
- Location
- Motion
- Speed
- Vin number
- Acceleration
- Force of impact
- Other external environment such weather, traffic and road conditions

Core offering of telematics insurance and connected dashcam

Managing customer needs through core offerings

1. Core UBI offering
   - Design usage-based insurance suited for the business individual insurers business and operation model including product design, IT capacity, analytical function, claim management and capital
   - As the product is still in its early stage of acceptance, lead the UBI to understand the target market and test different product offerings

2. Risk selection: driving behavior modifier
   - Continuous improvement in risk selection by capturing and analyzing increasingly accurate information about individual driving behavior
   - Actively manage claim costs through real feedback on driving behavior and instant notification of loss events

3. Product innovation: leverage through value add services, which are highly desired by the customer
   - Provide value-add vehicle services, such as emergency services, breakdown services, theft notifications and early vehicle diagnostic services
   - Additional opportunities exist around integration platforms, content provision and providing access to infotainment and navigation/traffic services
   - Portal functions for new embedded applications, such as tracking of stolen vehicles, parental control, infotainment systems and viewer of journeys
   - Requires support for single point, which is responsible for charging and billing for various services; this is a main reason for the increasing involvement of insurers in the value chain
   - For insurers looking to become more deeply involved in the value chain, strategic alliances in the development of vehicle independent services is an option

Increasing the product offering with additional services better matches the customer’s needs (emotional and logical) with the motor insurance product (traditionally, a begrudged purchase)

- Increased revenue and profitability from non-insurance product
- Increased retention for core insurance product
Section 03

Architecture of connected cars and the associated risks
The car is connected now! But are we safe?

Architecture of a connected car
Overall architecture and implementation view

Intra-vehicle network

Accessibility categories
- Application
  - V2I
- Operating system
  - V2X
- Network
  - V2V
- Firmware
  - Physical

Controller area network (CAN):

Sensors: throttle position sensor, manifold absolute pressure sensor, engine coolant temperature sensor, oxygen sensor, humidity sensors, etc.

Network communication
- LTE/GPS
- RFID

Long-range wireless
- Cloud services
- Broadcast services

Short-range wireless
- Bluetooth
- Consumer smart devices
- Vehicle
- Keyfob

Physical connection
- USB
- OBD-II
- Consumer media devices
- Programming/ diagnostic device

V2I: Vehicle-to-infrastructure
V2X: Vehicle-to-anything
V2V: Vehicle-to-vehicle
RFID: Radio Frequency Identification
The connected ecosystem of tomorrow’s mobility needs to be robust and looking at dimension of privacy and safety.

Cybersecurity has risen in importance as the automotive industry undergoes a transformation driven by new personal-mobility concepts autonomous driving, vehicle electrification, and car connectivity. The connected vehicle system will require a common technical framework for the deployment to address security implications and privacy of driver and passengers, as connected environment.

The emerging V2X landscape (V2V, V2I) calls for an approach, which takes care of drivers business use cases and as well as regulatory requirements and in achievement the players have to ensure, consumers interest of privacy at utmost while maintaining necessary hygiene of cyber security.

R Sundar
Partner, Risk
rsundar@in.ey.com
Threats and challenges to connected vehicles

Intra-vehicle network

- **Application**: V2I
- **Operating system**: V2X
- **Network**: V2V
- **Firmware**: Physical

Controller area network (CAN):

- **Sensors**: throttle position sensor, manifold absolute pressure sensor, engine coolant temperature sensor, oxygen sensor, humidity sensors, etc.

Accessibility categories

- **OEM ECU**
- **Controller area network (CAN)**

Network communication

- **Long-range wireless**
  - Cloud services
  - Broadcast services
- **Short-range wireless**
  - Consumer smart devices
  - Vehicle
  - Keyfob
- **Physical connection**
  - Consumer media devices
  - Programming/diagnostic device

- **V2I**: Vehicle-to-infrastructure
- **V2X**: Vehicle-to-anything
- **V2V**: Vehicle-to-vehicle
- **RFID**: Radio Frequency Identification

Breach at OEM data centres aimed at stealing customer’s personal files, disabling vehicle’s operation or spreading malicious activities.

Unauthorized access to vehicle internal network and infotainment system in order to steal private and corporate data, track individual vehicles or entire fleets and hijack non-safety and safety-critical function.

Physical access and tampering of OBD device leading to compromise of critical functions.
Assessment of security testing in connected car

Security oriented implementation of architecture and functions for connected cars

Common automotive processes

- Supplier and partner processes
- Security engineering
- After sales processes and tools
- Product architecture and development

EY framework for vehicle threat analysis

- Cellular data/voice
- Broadcast services (FM RDS)
- DSRC
- VANET
- Mobile phone
- Remote unlock
- OBD-II
- USB
- CANBUS

Remote threat channels

- V2I
- V2V
- V2X
- >200 ft
- 50-200 ft
- >0 ft

ECU device breakdown

- Application: Applink, CarPlay, etc.
- Operating system: QNX, Linux, Window embedded
- Firmware: Custom firmware

ECU subcomponent grouping

- Intra-car network

How big is the problem?

India ranked #1 in total number of cyber crime complaints received in 2018

Top five countries by the total number of cyber crime complaints receive

<table>
<thead>
<tr>
<th>S.no.</th>
<th>Country</th>
<th>Complaint %</th>
<th>Total number of complaints received</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>India</td>
<td>33.07%</td>
<td>4,556</td>
</tr>
<tr>
<td>2</td>
<td>United Kingdom</td>
<td>28.8%</td>
<td>3,970</td>
</tr>
<tr>
<td>3</td>
<td>Canada</td>
<td>20.90%</td>
<td>2,880</td>
</tr>
<tr>
<td>4</td>
<td>Australia</td>
<td>8.90%</td>
<td>1,227</td>
</tr>
<tr>
<td>5</td>
<td>Georgia</td>
<td>8.33%</td>
<td>1,144</td>
</tr>
</tbody>
</table>

Source: 2018 Internet Crime Report, FBI IC3

Cyber crime - major statistics - 2018

US$2.71 billion victim losses in 2018
Over 900 complaints received per day on an average
Section 04

- Attack scenarios
The car is connected now! But are we safe?

The cybersecurity market for cars is being primarily driven by the increasing connectivity of vehicles, increasing adoption of telematics services in automobiles and increasing integration of advanced features.

The automotive industry across the globe is undergoing a wave of innovation and advancements, with the emergence of ground-breaking technologies, such as the Internet of Things (IoT), enhanced GPS, location and maintenance live recording, reminders, driving assistance and Wi-Fi services, the demand for connected cars has been rapidly increasing, driving the market forward.

As all the connected vehicles are fully dependent on the connected software for all aspects of their operation, hence, they are vulnerable to a wide range of cybersecurity attacks, which increases the need for a cybersecurity solution, which is driving the market forward.

With automobiles equipped with in-vehicle infotainment systems and improved wireless network systems, have boosted the sales of the connected cars in this region, thereby, driving the overall Asia-Pacific cybersecurity market for cars.
EY cyberattack scenarios

Attacker levels and test scenarios

Attackers possess varying levels of skill which we group into four levels as shown in the table below. Against each of the four levels EY has devised a set of test scenarios that we would recommend performing to provide confidence that the component is able to withstand the associated level of attack and associated attack vectors. A process of threat assessment is used to identify the likely attacker, the attack vectors used, their motivations and typical attack targets.

### Attacker level

<table>
<thead>
<tr>
<th>Beginner (script kiddie)</th>
<th>Professional (experienced attacker)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has a basic security understanding and experience</td>
<td>Profound security understanding and experience</td>
</tr>
<tr>
<td>Is able to use public exploits or reproduce trivial security findings</td>
<td>Able to adapt existing exploits</td>
</tr>
<tr>
<td>Tries out known attack vectors against the WiFi of the headunit, e.g., breaks the WEP and brute forces easy WPA keys</td>
<td>Opens embedded devices and tries to read the memory chips</td>
</tr>
<tr>
<td>Port-scans the head unit and looks for commonly known vulnerabilities</td>
<td>Uses open debug ports to attach debuggers</td>
</tr>
<tr>
<td>Tries to get firmware images of ECUs online and looks through them directly for strings with credentials</td>
<td>Reverse engineers K-matrices</td>
</tr>
<tr>
<td>Reads car-hacking papers to reproduce findings of the past or is able to reproduce back-doors which are known on internet forums</td>
<td>Identifies simple buffer overflows in firmware which can be accessed via debug interfaces</td>
</tr>
<tr>
<td>Is able to discover multi-hop attack vectors from the car to the IT infrastructure</td>
<td>Is able to attack RF communication with known flaws in WiFi, GSM and Bluetooth, and well understood busses, e.g., CAN and LIN</td>
</tr>
</tbody>
</table>

### Example attack vectors

- **Beginner** (script kiddie):
  - Tries out known attack vectors against the WiFi of the headunit, e.g., breaks the WEP and brute forces easy WPA keys
  - Port-scans the head unit and looks for commonly known vulnerabilities
  - Tries to get firmware images of ECUs online and looks through them directly for strings with credentials
  - Reads car-hacking papers to reproduce findings of the past or is able to reproduce back-doors which are known on internet forums

- **Professional** (experienced attacker):
  - Opens embedded devices and tries to read the memory chips
  - Uses open debug ports to attach debuggers
  - Reverse engineers K-matrices
  - Identifies simple buffer overflows in firmware which can be accessed via debug interfaces
  - Is able to discover multi-hop attack vectors from the car to the IT infrastructure
  - Is able to attack RF communication with known flaws in WiFi, GSM and Bluetooth, and well understood busses, e.g., CAN and LIN

### Attack vectors: in-vehicle infotainment (IVI)

**Scenario 1**

1. **Remote attacker**
   - The remote attacker sends a malicious code masked as an entertainment file.
2. **Malicious song file**
   - The file is sent to a phone which has access to the car or is already connected to the IVI system.
3. **Passenger’s phone**
   - Unknowingly, the phone owner opens the file while the phone is connected to the IVI system and the malicious code starts running.
4. **Exploited**
   - The attacker now has gained access to the device and can control its working and can use its feature to cause different types of attacks.

**Connected car device**
- Connected via USB cable

**IVI system**
The car is connected now! But are we safe?

The device offers the feature of Wi-Fi hotspot which creates a 4G/LTE enabled secure Wi-Fi hotspot that can be used for internet by car passengers. Anyone in the car with a mobile device can now connect to the hotspot created by the device’s Wi-Fi. The passenger’s phone is vulnerable to attacks and their privacy is also at risk.

► An attacker can hijack the browsing session and snoop on the websites visited over an LTE connection using an attack called aLTEr.
► Attacker using this exploit in the LTE service can gain access to the mobile device and can use it to spy, spam, track and spoof.

Scenario 2

**Attack vectors: Wi-Fi hotspot**

**Remote attacker**

**Wi-Fi hotspot**

**Passenger’s phone**

**Wi-Fi**

**Scenario 3**

**Attack vectors: 4G SIM**

**Remote attacker**

**4G SIM**

**Device**

**Vehicle**

The 4G SIM stores the video recordings and the conversation that took place in the car. It also gives a hotspot option to the passengers of the car. The 4G SIM is introduced in the device to enable data transfer to cloud storage and to create connectivity within the car. The 4G SIM is vulnerable to attacks and their privacy is also at risk.

A remote attacker can try to remotely hack the SIM by getting the encrypted key (which can be obtained in a number of ways). The 4G SIM is introduced in the device to enable data transfer to cloud storage and to create connectivity within the car.
Attack vectors: mobile application

Scenario 4

Remote attacker
Mobile application
Owner's mobile
Connected car device

A remote attacker can hack the application of the device and get access to the device as well as the mobile phone.

The mobile application can be used by people other than the owner. The application itself may have inherent vulnerabilities which leaves it susceptible to multiple types of attacks, thus rendering the device vulnerable.

Unknowingly the phone owner opens the file while the phone is connected to the IVI system and the malicious code starts running.

Car with device
The device can have a mobile application which the owner can use to monitor the device, the car and get real time alerts.

Attack vectors: inside threat (servicing)

Scenario 5

Car whilst servicing
Device
Access to device-mounted car

Inside threat

A service personal can tamper with the device while the car has gone for repair or servicing or some other work.

They can gain access to the device and hence the car, by physically tampering with the device, the SIM and other hardware. It can also gain pathway to the software of the system.

By getting access to the device, the attacker can now has an entrance into the privacy of the owner and the fellow passengers. They also control various aspects and features of the car too.

Physical attack
Attack vectors: insider threat

**Scenario 6**

Face recognition software identifies the driver from the list of familiar drivers added to the account and then only gives him/her access to the car.

1. Face recognition software
2. Device
3. Car
4. Physical attack

The attacker can fool the software by using disguise or by sending a counter code to the device to access the facial recognition software.

Once the software mistakenly gives access to the attacker, they have the control of the car.

**Scenario 7**

Debug port contains two CAN bus ports which allows microcontrollers and devices to communicate with each other.

1. Debug port
2. Device
3. Vehicle
4. Malicious attacker
5. Gaining access to the device thus gives the attacker access to the car.

An attacker can gain access to the device by plugging in a malicious code via the debug port.

Computer needed to connect to debug port

The car is connected now! But are we safe?
In conclusion...

► The rapid increasing connectivity, the increasing number of electronic control units and lines of code have increased the complexity of products, thus, the concerns for security solutions are on the rise.
► The advancement of AI technology can seriously address cyber related issues and help companies in providing solutions.
► Developments in automobiles, such as the emergence of connected cars (internet-enabled) and predictive maintenance (using telematics), are expanding the cyberthreat surface. Also, mobility as a service (rise of shared cabs) is collecting data about drivers, passengers, destinations and routes, thereby leading to increased concerns on privacy.
► Underlying opportunities for AI in cybersecurity market include growing need for cloud-based security solutions among SMEs and increased use of social media for business functions.

Jaspreet Singh
Partner, Cyber Security
Jaspreet.Singh@in.ey.com
Section 05

How can EY help?
Connected car: how we see it!

EY capabilities
- Connected car strategy formulation
- Implementation support
- Monetization strategy
- Big data analytics
- Predictive maintenance and asset planning
- Digital risk and cybersecurity

Automotive companies can reap sustained benefits by effectively implementing a connected car strategy

<table>
<thead>
<tr>
<th>OEMs</th>
<th>Third party / others</th>
<th>Customer</th>
</tr>
</thead>
<tbody>
<tr>
<td>► Remote diagnostic and prognostic services</td>
<td>► Telematics for fleet management</td>
<td>► Advanced assisted driving capabilities</td>
</tr>
<tr>
<td>► Improve after sales and support service</td>
<td>► Content creation and management services</td>
<td>► On demand infotainment</td>
</tr>
<tr>
<td>► Leverage connected car offering as unique differentiator and improve customer loyalty</td>
<td>► Opportunities for telecom companies in machine-to-machine communication in vehicle</td>
<td>► Augmented navigation</td>
</tr>
</tbody>
</table>

► OEMs can offer significant value to its customers by combining various elements from online applications, driver assistance, call center services and solutions for the integration of mobile devices

► Services provided by the company can include vehicle management, travel and navigation, parking, entertainment, information, emergency call, vision and drive assistance

► Companies can use driving usage and car performance data to:
  ► Optimize inventory for spares
  ► Feedback into new product development
  ► Sending maintenance alert to customers and dealership
  ► Over-the-air tuning of the vehicle

► Customers can be provided with customized web portals, where they can view diagnostic reports, download directions to the vehicle or even unlock the car’s doors

► The connected car lives in the network and is open to cyber threats; companies need to have the balance between trust and risk - not just risk level, but trust level - how much assurance do they have

► Advanced assisted driving capabilities can be provided by leveraging sensors, analytics, NLP, RPA and cloud computing

To secure the connected car, cybersecurity needs to be embedded across the entire ecosystem

Our strategic partnering value
► We use knowledge to build and deploy meaningful solutions consistent with client’s objectives and expectations of EY.
► Our approach is technology and partner agnostic, we leverage the best tools and team with the industry experts to deliver a complete end-to-end service.
► The depth and breadth of our firm allows us to tap into globally renowned subject matter resources and industry leading methodologies.
► EY is known and respected for the depth and breadth of our cybersecurity practice.
► We are the market leaders in building, operating, and sustaining cyber security.
► Our approach is founded in a firm repeatable process that is capable of flexing with the unique needs of connected vehicle.

A robust connected vehicle cyber security strategy

<table>
<thead>
<tr>
<th>Strategic influences</th>
<th>Practical influences</th>
<th>Desired outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business and product strategy</td>
<td>Assessment</td>
<td>Connected vehicle cyber security strategy</td>
</tr>
<tr>
<td>IT strategy</td>
<td>Connected vehicle cyber security strategy</td>
<td>Safe customers</td>
</tr>
<tr>
<td>Compliance</td>
<td>Technical reviews</td>
<td></td>
</tr>
<tr>
<td>Risk appetite</td>
<td>Emerging technologies</td>
<td></td>
</tr>
<tr>
<td>Mobility and industry trends</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emerging technologies</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

EY’s vehicle ecosystems: cyber security and privacy framework

Car with various sensors
Connected car: how we see it!

- **Face recognition software identifies the driver from the list of familiar drivers added to the account and then only give them access to the car.**
- **Alignment with the regulatory requirements for maintaining a secure vehicle ecosystem.**
- **Design methodologies and procedures to enable secure vehicles.**
- **Processes, procedures and methods for operating the vehicle security framework.**
- **Tools to facilitate vehicle risk management governance and strategy operational processes and reporting framework.**

- **Security and privacy process, risk and control framework.**
- **Security vehicle design: Secure development, Secure integration, Secure protocols and standards, OEM security requirements, testing and validation, Privacy process and control development.**
- **Secure vehicle production: Secure development, Secure integration, Secure protocols and standards, OEM security requirements, testing and validation, Privacy process and control development.**
- **Secure vehicle operations: Risk management, Security monitoring, Change management, Incident management, Privacy, communication and preference management.**

- **Operational policies and standards that assist in achieving vehicle risk management objectives and effective management of IT risk.**

- **Compliance monitoring and reporting.**

---

**EY's vehicle ecosystems: cyber security and privacy framework.**

---

66

The car is connected now! But are we safe?
For more information please contact us. Our team will happy to serve you.

Business consulting

Vinay Raghunath
Partner
vinay.raghunath@in.ey.com

Pallav Chatterjee
Director
pallav.chatterjee@in.ey.com

Som Kapoor
Partner
som.kapoor@in.ey.com

Pratik Shah
Director
pratik.s@in.ey.com

Technology consulting

Burgess S Cooper
Partner
burgess.cooper@in.ey.com

Jaspreet Singh
Partner
jaspreet.singh@in.ey.com

Sumit Malhotra
Senior Manager
sumit1.malhotra@in.ey.com

Key Contributors

Nitin Sethi
Associate Director
nitin.sethi@in.ey.com

Amit Punjani
Associate Director
amit.punjani@in.ey.com

Kanika Sharma
Consultant
kanika.sharma@in.ey.com
The car is connected now! But are we safe?
The car is connected now! But are we safe?
The car is connected now! But are we safe?
The car is connected now! But are we safe?