LEADING-NAMES CLIENTS ACROSS THE VALUE-CHAIN

70% of T1 Suppliers
90% of Major Auto Semi Suppliers
70% of top OEMs

FIVE SERVICES TO COVER ALL AUTOMOTIVE OPPORTUNITIES

- Infotainment & Telematics
- Powertrain, Body, Chassis & Safety
- Autonomous Vehicles
- In-Vehicle UX
- CONNECTED MOBILITY
AGENDA

• Vehicle Vulnerability: From theft to cyber crime
• Connectivity: Status of adoption
• Automated Driving: From driver control to remote control
• Implications for Security and Law Enforcement
We need connectivity

Connectivity is a problem

We need software updates

Software updates are problematic

Automotive systems must be secure

Automotive systems will never be secure

100-150 ECUs, 7 networks, multiple gateways
The Problem: Where do I hack from?
VEHICLE THEFT MAKING A COMEBACK

On the rise in the U.S. and U.K.
Widespread perception that problem is solved – FALSE!
Most press attention to white hat hacks, stunts – Jeep hack!
Keyless entry primary point of vulnerability
Car makers struggling to respond

74.5% of stolen vehicles are autos equipped with keyless entry or remote start.

14.9% are trucks and buses, other.

$4.5 BILLION

46 SECONDS

The value of stolen vehicles and property stolen from the vehicles in 2014.

In the United States, a motor vehicle is stolen every 46 seconds.

TOP 10 STATES with highest number of auto thefts.

689,527 STOLEN VEHICLES NATIONWIDE
GUARDKNOX HARDWARE SOLUTION

Centralized

Single ECU

Certified

ISO 26262

Common Criteria CERTIFIED
AUTOMOTIVE EMBEDDED MODEMS
GLOBAL ANNUAL SHIPMENTS

50% of vehicles shipped will have embedded modems

Unit Shipments (000's)


North America
Europe
South Korea
Japan
China
India
Russia
Brazil

Source: Infotainment & Telematics Service
Global Active subscriptions will exceed 250 Million by 2022

Leading Regions:

- North America: Market Driver – Early Adoption
- Europe: Market Driver – eCall
- China: Market Driver – Biggest Global car market

Telematics 1.0

Source: Infotainment & Telematics Service
**OEM EMBEDDED TELEMATICS**
**CELLULAR MODEM SHIPMENTS - GLOBAL**

**Telematics Forecast 2015 vs. 2023 (18.8 Mil. units → 78.6 Mil. units)**

- **2.5G Network:** 7.4 Mil units in 2015 to 0K units from 2020
- **3G Network:** 8.4 Mil in 2015 units to 13.7 Mil units in 2023
- **4G/LTE Network:** 2.8 Million units in 2015 to 58 Mil units in 2023
- **5G Network:** 5.6 Million in 2023
NEXT GEN CONNECTED CAR DESIGN
→ DOMAIN & BUS CONVERGENCE

2018

Telematics 2.0

Cloud

Smart Antenna

Body ECU

Telematics ECU

Headunit

Chassis ECU

Display

Head Unit

Telematics ECU

Safety

Body

Chassis

Smart Antenna

Ethernet

Source: Infotainment & Telematics Service
COMPLEX CRITICAL SYSTEMS NEED RAPID UPDATE CYCLES…

Example is Safety - There is increasing reliance on:

- LIDAR, RADAR
- Cameras
- Contextual awareness with the objective of collision avoidance

...most of these systems have COMPLEX software...
AUTONOMOUS IS A SOFTWARE PROBLEM

Many cars with hardware: Few cars SAE L4 or above

Source: Strategy Analytics Autonomous Vehicles Service
ETHERNET AS BACKBONE?

• Today
  • High Number of ECUs each typically performing a single function
  • ECUs connected via bus systems with limited bandwidth
  • Security issues with CAN bus
  • COMPLEX!

• Tomorrow?
Assumptions:

- ~60% of global production in 2020 to feature Ethernet Diagnostics Port
- ~10% of Backup cameras to be Ethernet in 2020
- ~30% of surround view systems to be Ethernet in 2020
- ~25% of other cameras (e.g. front for LDWS etc.) to be Ethernet in 2020
- ~10% of RADARs for be Ethernet in 2020
- ~20% of premium audio & 5% of mid-range audio to be Ethernet in 2020

BMW plus one other to start using Ethernet as backbone by 2020 – BMW in lead & other only just emerging
AUTOMOTIVE ETHERNET
MARKET ISSUES

1. Timing: Exact timings of mass-market demand still unclear with many still “sitting on the fence” as to exactly what they will adopt and when
   - CAAGR of socket demand over 2015 to 2020 is around 100%
   - Means that delay/advance of market by one year could halve/double demand from expected values!

2. Current Market: We have seen less Ethernet adoption than was anticipated for camera systems. Rapid move to HD-class cameras has “forced” OEMs to choose new technologies and many have chosen LVDS.
   - HDBaseT (which can transport Ethernet traffic) also gaining support from GM, Delphi, Daimler – although momentum seems to have stalled?

3. Suppliers: Wider range of semiconductor solutions is STILL needed...
   - Integration of PHY into other semiconductor devices will be highly important in achieving mass-market adoption
   - Silicon prices were seen as hampering wider-scale adoption – but these are falling as more vendors enter market
   - Announcements such as Marvell 88Q2112 and Broadcom BCM8953x will help
Cyber Security – 2 Major challenges for Auto Industry:

1. Securing future vehicles
2. Securing the fleet of vehicles driving on roads today

- **Achieving 1**: Change to Auto industry culture, training, automotive network architecture design, and willingness to cooperate
  - A range of technical solutions exist and are actively being investigated and developed

- **Achieving 2**: Is very difficult and existing “bolt-on” methods will result in less-than-adequate security (e.g. adding intrusion detection/protection software)
VEHICLE CYBER SECURITY ‘ATTACK’ POINTS

- **Attack Surfaces**: Cellular, Wi-Fi, BT, DSRC, RKE, TPMS, USB, OBD II port, etc.

- **Interaction**: Each node can be secure in itself but is it secure when connected to the rest of the vehicle?

- **Many ECU’s**: (~50 to 100) ECUs and related processors to secure

- **CAN Protocol**: Was not designed with security in mind (no message or ECU authentication, low bandwidth, etc.)

- **Security testing**: Happening too far into production process to be effective

- **“Black box” problem**: Suppliers won’t share code due to interest in protecting IP

- **Security perception issue**: Security isn’t perceived as valuable until after a vehicle has been hacked

- **Updates**: Cannot rely on “always on” connectivity

- **Safety**: Often requires a vehicle be parked during an update

- **Auto industry security training/education**: Perceived to be not as sophisticated as in other sectors nor as much of a priority
# Vehicle Cyber Security Challenges and Threats

## Challenges

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autonomous Driving</td>
<td>Relies on connectivity and requires significant computing power to sense and perceive all manner of obstacles and driving conditions. Connectivity to control systems, safety.</td>
</tr>
<tr>
<td>Wireless Connections</td>
<td>More attack surfaces from multiple connections such as cellular, Wi-Fi, Bluetooth, and DSRC will grow considerably</td>
</tr>
<tr>
<td>Brought-in Devices</td>
<td>Smartphones, tablets, OBD dongles can be used to connect/tether the car to networks.</td>
</tr>
</tbody>
</table>

## Threats

<table>
<thead>
<tr>
<th>Threats</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Infrastructure</td>
<td>Traffic signals, ramp meters, roadside sensors, and dynamic message signs.</td>
</tr>
<tr>
<td>Remote Monitoring &amp; Control</td>
<td>Reduces maintenance or operation costs and enables new business models (i.e. car sharing), adds security challenges</td>
</tr>
<tr>
<td>Internet Companies</td>
<td>Working with the automotive industry for design, R&amp;D and manufacturing. Their competitive advantage of fast iteration and “fix-it later” mentality may cause security issues.</td>
</tr>
<tr>
<td>Over-the-Air Updates</td>
<td>Enables fast-fixes for bugs and reduces vulnerability by keeping legacy systems up-to-date, also increases the &quot;attack surface“</td>
</tr>
</tbody>
</table>
### VEHICLE CYBER SECURITY
### ORGANIZATIONS & STANDARDS ACTIVITY

<table>
<thead>
<tr>
<th>Organizations</th>
<th>Recent Activities</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAE</td>
<td>SAE has formally released its guidebook for securing automotive cyber physical systems.</td>
<td><a href="http://standards.sae.org/j3061_201601/">http://standards.sae.org/j3061_201601/</a></td>
</tr>
</tbody>
</table>
## VEHICLE CYBER SECURITY
### REGIONAL LEGISLATION

### U.S.
- **NHTSA** – The National Highway Traffic Safety Administration continues to produce guidelines and has thus far issued four reports on this subject.
- **NIST** – National Institute of Standards and Technology is developing a voluntary cyber security framework for reducing risks to infrastructure (including vehicles and transportation systems).
- **U.S. Copyright Office** – A change in the Digital Millennium Copyright Act (DMCA) now allows vehicle owners to legally access the software in their vehicles.

### E.U.
- **ENISA** – The European Union Agency for Network and Information Security is forming a group to address automotive cyber security guidelines and plans to suggest draft legislation in 2017.

### Japan
- **IAC** - Internal Affairs and Communications Ministry has created automotive cyber security guidelines designed to work with Intelligent Transportation Systems in Japan.
What are we doing?

- **Promote** - NCSC/CPNI hosted *automotive information exchange* (Feb 2017)
- **Promote** - Cyber security principles for CAV (April 2017)
- **Mitigate** - Collaborating on cyber security for *connected corridors* with EU partners
- **Mitigate** - Chairing a *task force on cyber security* within the UNECE World Forum for the Harmonization of Vehicle Regulations (draft paper 2018)
- **Respond** - Incident response and reporting mechanisms with NCSC (2017)
UNECE task force on cyber security and software updates

- The group includes trade bodies, industry and government
- The aims of the group are to:
  - Define requirements for addressing cyber threats
  - Define requirements for software update management with respect to safety type approval
  - Define guidance or measures for how to achieve this
- Aim to deliver these in 2018 to Working Party 29
  - The output may then be adopted as a regulation or resolution
- We recognize the need for agreeing something quickly
  - Standards may be instrumental but we must be agile as this is a rapidly developing area
### Example Cyber Security Solution Providers

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Argus Cyber Security</td>
<td>Certicom (owned by Blackberry)</td>
<td>Elektrobit</td>
<td>Abalta</td>
<td>Harman</td>
<td>Synopsys</td>
<td>Green Hills</td>
</tr>
<tr>
<td>Irdeto</td>
<td></td>
<td>Escrypt (owned by Bosch)</td>
<td>Arynga (owned by Wind River/Intel)</td>
<td>Irdeto</td>
<td></td>
<td>Harman (using RedBend hypervisor)</td>
</tr>
<tr>
<td>Karamba Cyber Security</td>
<td></td>
<td>Infineon Intrinsic-ID</td>
<td>Certicom/QNX (owned by Blackberry)</td>
<td>Security Innovation</td>
<td></td>
<td>QNX (owned by Blackberry)</td>
</tr>
<tr>
<td>Symantec</td>
<td></td>
<td>Qualcomm/NXP Rambus Texas Instruments</td>
<td>Escrypt (owned by Bosch)</td>
<td>Symantec</td>
<td></td>
<td>VMWare</td>
</tr>
<tr>
<td>TowerSec (owned by Harman)</td>
<td></td>
<td></td>
<td>Harman</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firewalls, White Listing, and Access Control</td>
<td>Arilou (owned by NNG) Harman</td>
<td>Runsafe Security (aftermarket) Symantec VisualThreat</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Infotainment & Telematics Service
THE SECURITY CHALLENGE

• Keyfob, OBDII, Dealerships + Denial (video)
• Limited talent pool
• Security source of cost/liability

DETECT, AND THEN WHAT?

• Suppliers to the auto industry are bringing detection and prevention systems to the market
• Will take years to implement and deploy
• No strategy for response/notification protocols – consumers, government regulators, law enforcement
VEHICLE AUTONOMY, 5G CHANGES ALL

• Remote access/control
• Inter-vehicle communication
• What does it mean?
• How will consumers, criminals react?
MORE DATA FLOWING TO/FROM CARS

• More data to and from vehicles!
  • **BUT!** Linked to wider trends than just automated driving: FOTA/SOTA; CRM/VRM; 5G for V2V/V2X etc.
  • The automated car may be gathering Gigabytes / km – but data to the cloud will be more like kilobytes / km
  • Around **90 million** active automotive data subscriptions in 2018, vs. **4.7 billion** active mobile device data subscriptions

• Key challenge - **SECURITY**
SUMMARY & RECOMMENDATIONS
SUMMARY & RECOMMENDATIONS (1/2)

• Car ownership patterns will evolve. The imminent death of car ownership is overstated, but shared cars will change traditional understanding

• Car companies are entering the fleet and B2C business space – altering the distribution channel roles

• Regulators and legislators are becoming increasingly interested in transportation generally and cars particularly
• **Mobile commerce** will play an increasing role – tolls, fuel, parking, content, services – more opportunity for criminals

• **V2X** creates **new challenges** for car companies to interact with government/municipal authorities and infrastructure companies – ultimately exposes cars to mass attacks

• **Cybersecurity** will remain a concern for the foreseeable future – can never certify vehicle security – industry response protocols/definition remains in flux – problem will only get worse – connectivity = opportunity for law enforcement