Securing CASE: Putting the brakes on cyber threats to keep you in the fast lane

楊豐愷, 車聯網資安防護解決方案產品經理

Peter Yang
Sr. Product Manager, IoT & Connected Vehicle Security
NExT Forum: Cybersecurity Challenges in E-Vehicle

- **CASE and the risks behind**
- **Protecting CASE eco system**
- **Trend Micro can help**
CASE and The Risks Behind Hacker’s Motivation
Global Mega Trend: CASE

The Mobility Revolution

- **Connected**
  - Infotainment
  - Navigation
  - Remote diagnostics
  - FOTA/SOTA
  - Use Based Insurance
  - Fleet management

- **Autonomous**
  - Logistics
  - Cargo
  - Haling service
  - Passenger car

- **Shared**
  - Ride share
  - Car share
  - Shared parking
  - Shared energy

- **Electrification**
  - Reduce emission
  - Reduce noise
  - Lower maintenance

Global Mega Trend: CASE

© 2021 Trend Micro Inc.
The E/E Architecture is Evolving

Automotive industry is transforming into Next Data Goldmine
Behind CASE - Automotive Cyberattacks

Monetizing Cyberattacks on CASE

User PII & user data (non-PII)

- Phone contact, call history, text message, driving history, schedule...etc.
- App data & cloud data (Apple CarPlay, Android Auto), driving video recorder (Tesla's Sentry Mode)...etc.

Car itself & goods inside

- Remotely unlock the door steal the car itself or valuable goods that transport by autonomous car

Driving services

- Hacking and using cars’ services for moving contraband items, committing crimes, performing anonymous movements, and other illegal acts

Stored energy

- Stored battery energy in cars could potentially become a valuable commodity (V2G)

Network and processor resources

- Cybercriminals could install a botnet in a connected car and use network and CPU resources while the car is idle at home for the night, or they could use the car as an initial access point to hack the power grid (infra/cooperate backend).
Protecting CASE Eco System
Regulation & Standard
# Regulation, Standard and Best Practices

## Automotive Engineering

<table>
<thead>
<tr>
<th>Organization</th>
<th>Industry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNECE</td>
<td></td>
<td>WP.29 regulation on cybersecurity and software updates</td>
</tr>
<tr>
<td>NHTSA</td>
<td></td>
<td>Cybersecurity Best Practices for Modern Vehicles</td>
</tr>
<tr>
<td>VDA</td>
<td></td>
<td>Information Security Assessment</td>
</tr>
<tr>
<td>IPA</td>
<td></td>
<td>Approaches for Vehicle Information Security</td>
</tr>
<tr>
<td>MIIT</td>
<td></td>
<td>National Guidelines for Developing the Standards System of the Telematics Industry</td>
</tr>
<tr>
<td>AutoSAR</td>
<td></td>
<td>Secure Onboard Communications</td>
</tr>
<tr>
<td>ISO</td>
<td></td>
<td>ISO 21434, ISO/SAE 24089, SAE J3061, SAE J3101</td>
</tr>
<tr>
<td>SAE</td>
<td></td>
<td>ISO/SAE 24089, SAE J3061</td>
</tr>
<tr>
<td>AUTOSIG</td>
<td></td>
<td>Automotive SPICE</td>
</tr>
<tr>
<td>Auto Alliance</td>
<td></td>
<td>Consumer Privacy Protection Principles (CPPP) for Vehicle Technologies and Services</td>
</tr>
</tbody>
</table>

*Regulation/law*  *Standard*  *Best practice/framework*  *Draft/not published*
UNECE WP.29

- UNECE WP.29 regulations focus on **cybersecurity** and **software updates**.
- OEMs will need to show evidence of sufficient cyber-risk management practices **end to end**.
- This includes the demonstrated ability to deploy OTA software security fixes even after the sale of the vehicle.

5.1.1 (a) Collect and verify the information required under this Regulation through the supply chain so as to demonstrate that supplier-related risks are identified and are managed.

5.1.1 (b) Document risks assessment (conducted during development phase or retrospectively), test results and mitigations applied to the vehicle type, including design information supporting the risk assessment.

5.1.1 (c) Implement appropriate cyber security measures in the design of the vehicle type.

5.1.1 (d) Detect and respond to possible cyber security attacks.

5.1.1 (e) Log data to support the detection of cyber-attacks and provide data forensic capability to enable analysis of attempted or successful cyber-attacks.
• Currently, ISO 26262 “Road vehicles – Functional safety” is not focused on software development or detailing the cybersecurity infrastructure of car subsystems.

• ISO/SAE 21434 “Road vehicles – Cybersecurity engineering” sets standards specific to items for identification such as the use of embedded controllers, the long lifecycle of vehicles, and the safety implications of these technologies in cars.
  – The first standard that lays out clear organizational, procedural, and technical requirements throughout the vehicle lifecycle.

ISO/SAE 21434: Overall Cybersecurity Management chapter structure
Protecting CASE Eco System
Technical Implementations
NO Out-of-Shelf Security Product/Service

ISO/SAE 21434 and Trend Micro’s solution map
Solutions & Strength for Automotive

- Founded in 2005, Trend Micro's bug bounty
- Powered by over 10,000 independent researchers
- Contributing research from many different areas including Automotive and IoT
- Disclosed the most vulnerabilities in 2018/2019

250M+ sensors
2.5T+ threat queries yearly
65B+ threats blocked yearly
Cybersecurity Framework for CASE

Identify & Protect
- Attacks
- X % Blocked

Predict
- Reach in-car device
- Abnormal Behavior

Detect
- Monitoring
- Isolate/Quarantine

Respond
- Fix
- Restore full Connectivity

Recover
- OTA Update
- Original Condition

Vehicle
- Analyst
- Incident Response Team

V-SOC

OEM Backend
- RD/Vendor
- Number of Logs & Events

© 2021 Trend Micro Inc.
Protecting CASE Eco System
Behind the Scenes
Jeep Cherokee & Tesla Remote Hacking

Jeep Hack 2015

1) Telnet
   port 6667
   2) Root Head unit

3) Compromise ECUs

Tesla Hack 2016 & 2017

1) Setup Fake Hotspot
   SSID: Tesla Guest

2) Automatically connected

3) Load custom Webpage

4) Trigger WebKit Vulnerabilities

5) Root CID

6) Compromise ECUs
BMW Remote Hacking

BMW Hack 2018 A

1) Setup Fake GSM base station

Head unit
2) Hijack provisioning file
3) Change accessing URL
4) Load WebKit Vulnerabilities
5) Gain root

Send arbitrary CAN messages

BMW Hack 2018 B

Fake GSM base station

Malicious SMS

Telematics Control Box
1) Wakeup
2) Cause Buffer overflow

Send arbitrary CAN messages

LastStateCall
Generalized Remote Hacking Techniques

1) Outside Connection
   - Initiate an MitM Wi-Fi connection.
   - Configuration issues in mobile networks
   - Mobile network attacks
   - MitM with fake base station

2) In-vehicle Component connecting to outside
   - Access the head unit.
   - Exploit a vulnerability in WebKit or other software.
   - If necessary, exploit an operating system vulnerability for root privilege escalation.
   - Reprogram the CAN bus gateway.
   - Circumvent checks and upload modified firmware.
   - Access the CAN bus gateway.
   - Reprogram and/or unlock other ECUs.
   - Send arbitrary CAN messages to ECUs.
   - In 100% of cases, attackers need to create complex exploit chains to finally get access to the ECUs and then send arbitrary CAN messages remotely.

3) In-vehicle Network
   - Gateway mods required
   - Target ECU unlocking not required
   - No gateway mods required
The Jeep/ Tesla Hack MITRE ATT&CK Matrix
## The Tesla/ BMW Hack MITRE ATT&CK Matrix

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Trend Micro IoT Security for Automotive

① **System Protection**
- Vulnerability Scan
- Host Based IPS (Virtual Patch)
- Safelist
- Hypervisor Protection
- IoT Reputation Service etc.

② **Application Protection**
- Web Reputation Service
- Android App Security etc.

③ **CAN Bus Anomaly Detection**
- CAN Bus ID validation
- Frequency check
- Payload structure check
- Payload sequence check etc.
TMIS + XDR Deployment (Reduce SOC Effort)

Architecture of a distributed onboard IDS

Trend Micro Managed XDR
Threat Experts Deliver: Detection Reporting, Sweeping, Hunting, Root-Cause Analysis, Remediation Plan

Trend Micro Vision One™
Automated Detection, Sweeping, Hunting, Root-Cause Analysis

Trend Micro Data Lake

Off-Board Security Event & Log
- Mobile App
- 3rd party data
- Enterprise IT/OT
- Cloud/backend system
- OTA
- ...

- Mobile App
- 3rd party data
- Enterprise IT/OT
- Cloud/backend system
- OTA
- ...
On-Board Intelligent Sensor (Reduce Data Volume)

Big Data
(≥ 40.52PB*)
~1M USD/Y on AWS

-99.35%

Critical Evidence
(267.42TB*)

*1M cars on the road/year in U.S

**Trend Micro Vision One™**

**Delivery:**
Detection Reporting, Sweeping, Hunting, Behavior Analysis, Root-Cause Analysis, Remediation Plan

**Sensor Improvement:**
Machine Learning Model, Threat Expert Rules, HIDPS

Critical Logs - 99.35%

Legend:
- Known Good Data
- Known Bad Data
- Unknown Data

- Kernel log
- Process log
- System log
- Auth log
- Network log

TMIS Sensor

HIDPS

ML Model

Threat Expert Rule

ML Model

Threat Expert Rule

Critical Logs
Vehicle-SOC/ SIEM
Trend Micro Vision One for Vehicle-SOC
Better Together
Industry Partner & Contribution
Mindset Shift – OPEN – Better Together

• CASE Vehicle
  – is a massive system of systems
  – is transforming into super high spec mobile PC with wheels and high-speed connection
  => Transforming to system with vulnerabilities remote attacks are possible

• Plan with “CYBER security” mindset
  – Exclusivity Will Not Provide Protection
    • Work across industries to learn how incidents can affect decisions
  – Develop Automotive/IT Security Industry Partnerships
    • Leverage lessons learned, implement best practices and share intelligence on the research space
Auto Vulnerability Reported by Trend Micro

Research reports and vulnerabilities by Forward-Looking Threat Research (FTR) Team

- Volkswagen Customer-Link App Protection Mechanism Failure CAN Message Injection Vulnerability

- Connected Car Vulnerabilities Affect the CAN Standard
The Zero Day Initiative (ZDI) was created to encourage the reporting of 0-day vulnerabilities privately to the affected vendors by financially rewarding researchers.

Pwn2Own 2019 wraps up with the first successful entries in the automotive category. In all, we awarded $545,000 USD for 19 unique bug reports - and, of course, the car itself.

Tesla Vulnerability Reported by Trend Micro’s ZDI


https://www.deccanchronicle.com/technology/in-other-news/150119/take-home-a-tesla-model-3-at-this-years-pwn2own.html
Trend Micro’s Automotive Expertise

- **2017**
  - Vulnerabilities Affect the CAN
  - Cyberattack against ITS
  - ISO/SAE 21434
- **2020**
  - Threat Modeling & recommendation

Automotive Research

Research Community Engagement

PoC Record & customer

Contribution to Industrial Consortium

- Top Japanese and Chinese OEMs and Tier1s (names are confidential)
- Panasonic

and so on

- Invited talk about automotive specific vulnerability management at escar 2020
- Automotive Hacking contest with Tesla

and so on