Cybersecurity Solutions for Connected Vehicles

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Contents

The automobile industry faces an emerging challenge in the area of cybersecurity. For automobile original equipment manufacturers (OEMs), Tier 1 suppliers, car dealers, service providers, car owners and drivers, cyberattacks are now a reality that they have to grapple with.

Especially with connected vehicles in the era of the Internet of Things (IoT), more and more key vehicle functions rely on software rather than hardware. Unfortunately, as vehicles become increasingly automated and connected with the outside world, they tend to face growing security threats. Vulnerabilities arise particularly when just-in-time manufacturing and a faster speed to market leave less time for product testing. These vulnerabilities might not even be uncovered until after millions have been released, in which case the necessary patching procedure is all but certain to prove costly — not only to the affected carmaker's finances but also to its reputation. It's important, then, for security measures to be properly applied right from the outset of the car manufacturing process, starting in the design phase.[1]

It's a huge investment to build a complete cybersecurity solution for connected vehicles, especially one that is designed to protect critical modules with network connectivity. A couple of best-practices documents are worth mentioning in this regard. One is the series of "Automotive Cybersecurity Best Practices" launched in July 2016 by the Automotive Information Sharing and Analysis Center (Auto-ISAC), as an expansion to the Framework for Automotive Cybersecurity Best Practices published in January 2016 by the Alliance of Automobile Manufacturers and the Association of Global Automakers.[2] The other is "Cybersecurity Best Practices for Modern Vehicles," published in October 2016 by the U.S. Department of Transportation's National Highway Traffic Safety Administration (NHTSA).[3]

For its part, this Trend Micro white paper analyzes the automotive cybersecurity challenge and discusses automotive cyberthreats. It also goes into Trend Micro solutions that can help prevent and mitigate the impact of cyberattacks against connected vehicles.

[1] Sławomir Jasek. (8 October 2015). *SecuRing*. "Connected Car Security Threat Analysis and Recommendations." Last accessed on 19 September 2017 at https://www.securing.biz/wp-content/uploads/2015/10/SecuRing-Connected-Car-Security-Threat-Analysis-and-Recommendations.pdf.

[2] Auto-ISAC. (July 2016). *Auto-ISAC*. "Automotive Cybersecurity Best Practices." Last accessed on 19 September 2017 at https://www.automotiveisac.com/best-practices/.

[3] National Highway Traffic Safety Administration. (October 2016). *NHTSA*. "Cybersecurity Best Practices for Modern Vehicles." Last accessed on 19 September 2017 at http://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

Automotive Cybersecurity Challenge

The typical method of solving problems relating to information technology (IT) involves updating operation systems, patching program flaws, changing configurations or creating and restoring backups to ensure continuity of operations. With respect to IT security, there are many different solutions, tools, standards and guidelines available for IT personnel to conduct threats investigation, impact mitigation and disaster recovery.

But for the automotive industry, cybersecurity is a significantly different matter.

Because the automotive industry is highly dependent on tiered supply chains, any changes in a vehicle would often require corresponding actions from many suppliers. This, in turn, is one of the reasons that introducing a new solution in an automotive ecosystem takes time. Deploying a cybersecurity solution into that ecosystem is especially challenging, considering that what defines "connected vehicles" — connectivity — is the very thing that leads to their having more attack surfaces for hackers to take advantage of.

The cybersecurity challenge for connected vehicles have five aspects: threat intelligence, hardware security, software security, network security and cloud security. Like any other security challenge, it is about creating layers of protection, i.e., not relying on just one security mechanism, but requiring multiple security checkpoint implementation to ensure different attack surfaces are under security radar scope.

Threat Intelligence

A sophisticated threat intelligence is needed to safeguard connected vehicles and to identify and mitigate cyberattacks. Threat intelligence is one of the best ways to keep you ahead of threats. It provides real-time data queries for solution deployment with regard to cybercriminal activities. However, how you gather and interpret threat data is critical. Also, it costs a fortune to establish and maintain a threat intelligence system of immense scale. Automotive OEMs therefore have to decide on the best practice to be able to acquire such a threat intelligence system.

Hardware Security

Today's most advanced cars have around a hundred Electronic Control Units (ECUs) and even low-end ones have at least 30 ECUs.[4] The number of ECUs embedded in cars — and, by extension, the amount of bandwidth for the buses that link them — is expected to grow as advanced driver-assistance systems (ADAS) become increasingly sophisticated. Another factor driving the growth in the number of ECUs is the emerging need for connected vehicles. There is a wide range of hardware security platforms, devices and standards available from the security industry, such as Secure Elements (SEs), hardware security modules (HSMs) and Trusted Platform Module (TPM). However, the challenge in hardware security lies in the impact in supply chains and the increase in the amount of investment.

Software Security

An average modern high-end car's software is based on about 100 million lines of code. Compare that with the more or less 50 million lines of code in Windows Vista™, and you get a sense of how complex car software code can be.[5] However, the greater the complexity of car software code, the higher the probability that it has vulnerabilities. Simply put, it is impossible to guarantee that such complicated software is totally free of error. Consequently, there are existing attack methods that specifically target car software flaws, thereby affecting a considerable portion of the automotive industry.

Another difficulty is the implementation of a Secure Software Development Life Cycle (SSDLC). In the automotive industry, multiple entities encounter multiple dependencies, resulting in a longer software development life cycle and lack of software management visibility down to each module and library. A typical case is an in-vehicle infotainment (IVI) system with connectivity available on board, which can be hacked by attackers using old-school vulnerabilities because it largely depends on third-party software stacks and open-source libraries.

Network Security

Network security in connected vehicles should address the internal network as well as the external network. Common protocols such as Controller Area Network (CAN), FlexRay and automotive Ethernet have been adopted for the vehicles' internal network. Some hacking demonstrations have successfully reverse-engineered the vehicles' internal network, whereby malicious code is sent to ECU nodes. By examining the CAN bus on which the ECUs communicate, it is possible to send proprietary messages to the ECUs in order to cause them to take some action, or even to completely reprogram the ECU.[6]

[4] Robert N. Charette. (1 February 2009). *IEEE Spectrum.* "This Car Runs on Code." Last accessed on 19 September 2017 at https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code.

[5] David McCandless, Pearl Doughty-White, and Miriam Quick. (24 September 2015). *Information is Beautiful*. "Million Lines of Code." Last accessed on 19 September 2017 at http://www.informationisbeautiful.net/visualizations/million-lines-of-code/.

[6] Meriel Jane Waissman. (23 January 2015). *Wired*. "WTF! It Should Not Be Illegal to Hack Your Own Car's Computer." Last accessed on 20 September 2017 at https://www.wired.com/2015/01/let-us-hack-our-cars/.

As hundreds of millions of connected vehicles are expected to be on the road in the foreseeable future, there is also the increasing probability of attack surfaces in external network interfaces. These include the on-board diagnostics (OBD) ports, Bluetooth, Wi-Fi, mobile 4G/5G and newly proposed dedicated short-range communications (DSRC) for vehicle-to-external (V2X) communications. Researchers have been able to access the Wi-Fi access point (AP) in a vehicle using common brute-force hacking techniques. By using man-in-the-middle attacks, they have been able to tamper with the data exchanged between the vehicle and its remote control mobile app to disable the car's alarm system.[7]

Cloud Security

Automotive OEMs have begun supporting mobile apps, voice control systems and even augmented reality (AR) as the main interface of the applications connecting to the vehicle head unit or IVI. For data exchange, these applications are connected to the cloud — which has given rise to a new attack vector for hackers.

The importance of strong cloud security was highlighted in the case of a researcher who was able to look into the backend cloud service that a vehicle's mobile app was using. Subsequently, he was able to determine the vehicle identification number (VIN) by examining the URL requests sent by the app to the cloud and discover that the APIs on the server were not authenticating the user. As a result, anyone who had the credentials to use the mobile app could anonymously send requests for a vehicle to turn on its climate control, check its battery life and view its GPS data.[8]

Another issue in relation to cloud security is the delivery of firmware over-the-air (FOTA) and software over-the-air (SOTA) updates to vehicles. The majority of automotive OEMs are still relying on basic FOTA/SOTA in the service and maintenance environments. Moving forward, the trend points to a shift to direct FOTA/SOTA updates through the cloud. However, protecting the integrity of firmware or software packages should be a key consideration, given that it's typical for hackers to try to get hold of firmware or software packages for the depth of information that they can gain access to. Hackers have demonstrated the possibility of remotely controlling vehicles after rewriting the cars' firmware.[9]

[7] John Leyden. (6 June 2016). *The Register.* "Wi-Fi hack disables Mitsubishi Outlander's theft alarm – white hats." Last accessed on 20 September 2017 at https://www.theregister.co.uk/2016/06/06/mitsubishi_outlander_hack/.

[8] Tom Spring. (26 February 2016). *Threatpost*. "Total Recall: Troy Hunt Breaks Down His Nissan Hack." Last accessed on 20 September 2017 at https://threatpost.com/total-recall-troy-hunt-breaks-down-his-nissan-hack/116497/.

[9] Andy Greenberg. (21 July 2015). *Wired*. "Hackers Remotely Kill a Jeep on the Highway—With Me in It." Last accessed on 20 September 2017 at https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

Automotive Cyberthreats

As manufacturers support more technologies, the number of ECUs embedded in cars continues to grow. But since new features are often added to existing systems, these systems inherit the vulnerabilities of these technologies. With physical access to vehicles, researchers and hackers have been able to use low-cost and off-the-shelf tools to send jamming or spoofing messages over in-vehicle networks to ECUs, tamper ECU firmware, compromise ECU security keys[10] and take control of a wide range of vehicle functions.

Cyberthreats can have significant consequences. Some of the most common ones include:

Driving Safety Hazards

The victimized vehicle can cause driver distractions such as arbitrarily turning on the in-car audio and turning up its volume. A more aggressive form of attack occurs when vehicle safety functions are disabled, thereby jeopardizing human life and public safety.

Cyber Ransom

Cybercriminals have established an ecosystem in which they target connected vehicles with ransomware, which can lock out users out of their cars until ransom is paid to the hackers.

Risks to Data Privacy and Integrity

Gaining unauthorized access to data through interfaces such as USB, Wi-Fi, Bluetooth and mobile 4G/5G is becoming a relatively easy task, allowing hackers to delete or modify files on vehicles and on user devices brought into them.

[10] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage, "Experimental Security Analysis of a Modern Automobile," *IEEE Symposium on Security and Privacy (SP)*, 2010, pp. 447–462.

Physical Abuse

Consuming memory space and squandering CPU cycles are just a couple of forms of physical abuse on connected vehicles. A more aggressive example is draining a vehicle’s battery by turning on the headlight for a drawn-out period.

Stepping-stone Attacks

A compromised vehicle may be used as a sort of stepping stone for sending bogus data to others or to penetrate the home environment.

Trend Micro Solutions

Cybercriminals have more tools, time, finances and technologies at their disposal than ever before. Focused attacks on high-value targets are growing sharply. At the same time, the increasing dependence of connected vehicles on widely interconnected online systems introduces more attack surfaces that attract hacker attention.

To achieve critical modules protection, solutions against cyberattacks on connected vehicles for critical modules protection requires these major components:

- Up-to-date threats intelligence
  - Real-time threats sourcing and update ability
  - Cloud-based big-data analysis and correlation on generating threats knowledge
  - Continuous service guarantee
- Pre-build solution
  - Risk assessment
    - According to Auto-ISAC and NHTSA, a best-fit solution to protect connected vehicles
    - A built-in solution to be able to collect and detect critical modules' current health and risk status
    - Ability to detect the critical modules' abnormal condition in the system, files and network connection
    - Ability to detect system vulnerability over time
  - System protection
    - A built-in solution to perform threats prevention and threats mitigation for critical modules
    - A method to deter cyberattacks such as intrusion prevention system (IPS)
    - A method to protect system integrity such as the whitelisting for files

- Security Visibility
  - A dashboard and management console to have real-time security visibility for the immediate mitigation plan and action
  - Ability to integrate with another backend system to have a single console for the whole management ability, such as device management, device life cycle management and security management.

Founded in 1988, Trend Micro is one of the most experienced and single largest dedicated cybersecurity provider. The company has delivered over two decades of product innovation to fight cybercrime. Very few cybersecurity vendors have the multi-million-dollar research and development commitment, with many experienced data scientists and advanced big-data resources that address threats. Trend Micro remains on the forefront of fighting cyber assaults with its ever-evolving and highly flexible holistic and proactive framework. Trend Micro products have been proven to prevent, detect and eliminate cyberthreats faster than many tested systems in the industry.[11]

Trend Micro proposes a layered approach to connected vehicle cybersecurity. This reduces the probability of an attack's success and mitigates its impact with these three layers:

- Global threats intelligence
- Pre-build security SDK for critical modules
- Cybersecurity visibility management

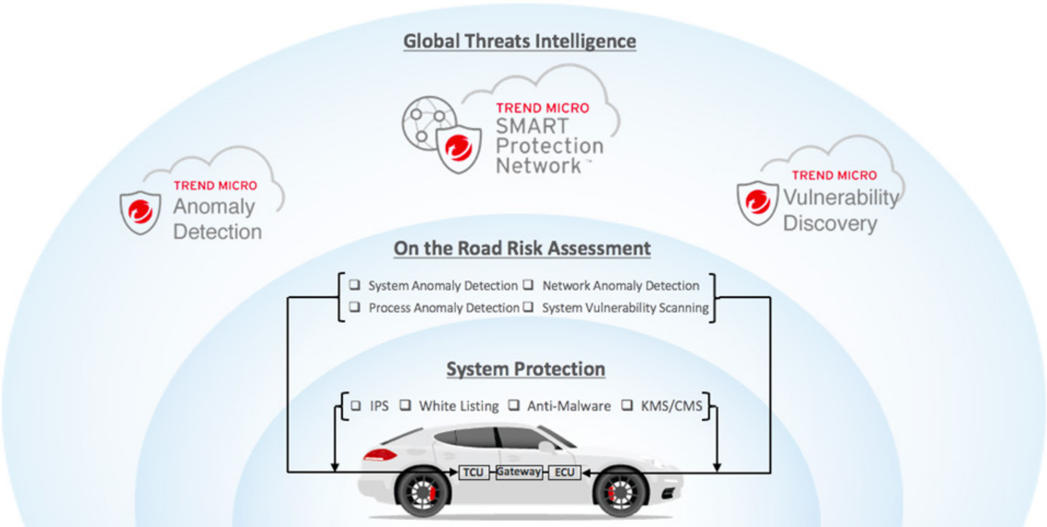

Global Threats Intelligence
TREND MICRO SMART Protection Network
TREND MICRO Anomaly Detection
TREND MICRO Vulnerability Discovery
On the Road Risk Assessment
❑ System Anomaly Detection ❑ Network Anomaly Detection
❑ Process Anomaly Detection ❑ System Vulnerability Scanning
System Protection
❑ IPS ❑ White Listing ❑ Anti-Malware ❑ KMS/CMS
TCU
Gateway
ECU

Figure 1. Trend Micro layered approach for cybersecurity for critical modules of connected vehicles

[11] NSS Labs Consumer ePP SeM tests 2009, 2010, 2014

Global Threats Intelligence

Criminal exploitation of cloud computing and the consumerization of IT, along with a rapid increase in hard-to-detect targeted attacks, put new pressure on security vendors to protect their customers' data not only throughout their physical infrastructures but in virtual, cloud and mobile environments as well. To do this, we start with a better global threat intelligence engine.

Trend Micro™ Smart Protection Network

Ongoing advances in the depth and breadth of the Smart Protection Network allow us to look in more places for threat data and respond to new threats more effectively. The Smart Protection Network works in three distinct areas: collection, identification and protection. Smart Protection Network collects more than 9TB of threat data each day from across the globe for greater visibility into the nature of attacks. Threat data is continuously gathered through a worldwide network of honeypots, submissions, feedback loops, web crawling technologies, customers and partners, and our own TrendLabs researchers.

Trend Micro pioneered the use of big-data analytics for threats intelligence when we started building the Smart Protection Network some several years ago. We host thousands of event feeds and stream billions of events in our data centers, and have become experts in the tools and techniques required to make sense of the variety of threats and attacks being perpetrated. This includes customized tools to correlate critical relationships among all the components of an attack, and model cybercriminal behavior and the environments they work in to quickly determine whether something is good or bad.

It's critical to match the velocity of attacks with an equally fast response. Our proven cloud infrastructure allows us to rapidly deliver threat intelligence across physical, virtual, cloud and mobile environments to protect data wherever it resides. We consistently demonstrate faster time to protect in independent tests. By processing threat information in the cloud rather than on individual machines, we reduce the demand on system resources and eliminate time-consuming signature downloads. Higher performance and lower maintenance reduce operating costs as well.

Cloud-Based Vulnerability Discovery Engine

Vulnerability is a major attack vector in IoT or even in connected vehicles. Trend Micro has developed a Vulnerability Discovery cloud engine to collect existing known vulnerabilities. By continually conducting the zero-day initiative (ZDI) bounty program to explore new vulnerabilities, this proactive vulnerability discovery platform feeds predictive, actionable intelligence into Trend Micro solutions for connected vehicles.

X-Gen Machine Learning Anomaly Detection Engine

It is quite difficult to predict a cyberattack in a single device. The best method is to collect necessary data within connected vehicles' critical modules and have a continuing analysis by using machine learning methods. This allows for early cyberattack prediction for the mitigation plan and action preparation.

Trend Micro launched X-Gen cross-generation machine learning in October 2016. This engine has a small footprint, thanks to the pre-build security software development kit (SDK) within connected vehicles. X-Gen modeling correlates with the Trend Micro Smart Protection Network to generate accurate threats prediction.

Pre-build Solution

Trend Micro realizes that the design philosophy for the critical modules in connected vehicle security is completely different from that of other computing systems. Signature-based blacklisting solutions are simply not suitable. Instead, ensuring critical modules integrity and operation continuity will be vital in connected vehicles security implementation. This security SDK is supported by hardware solution and OTA service providers to ensure the completion of device life cycle protection.

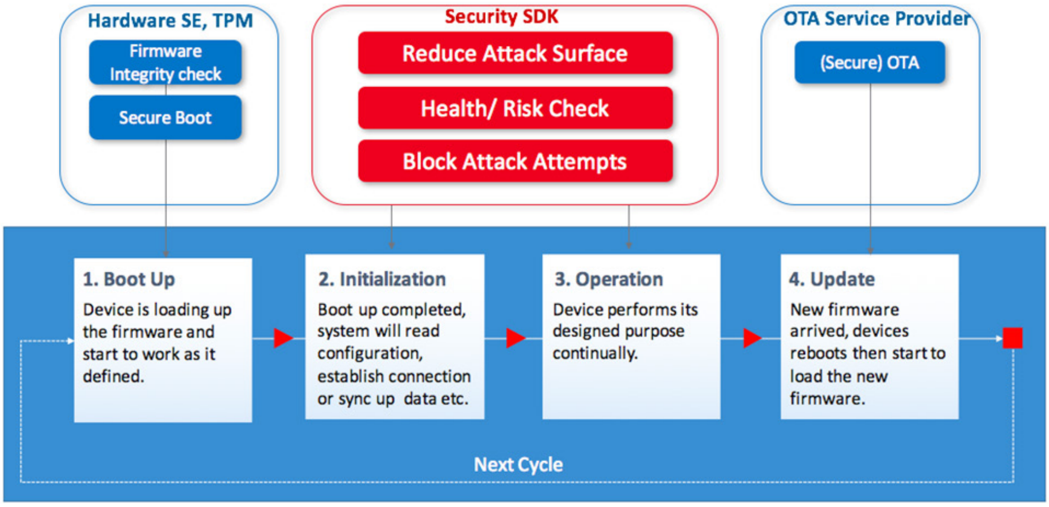

Hardware SE, TPM
Firmware Integrity check
Secure Boot
Security SDK
Reduce Attack Surface
Health/ Risk Check
Block Attack Attempts
OTA Service Provider
(Secure) OTA
1. Boot Up
Device is loading up the firmware and start to work as it defined.
2. Initialization
Boot up completed, system will read configuration, establish connection or sync up data etc.
3. Operation
Device performs its designed purpose continually.
4. Update
New firmware arrived, devices reboots then start to load the new firmware.
Next Cycle

Figure 2. SDK protection in device life cycle

Critical modules can be considered devices. As such, they can allow for the device life cycle to describe the security that should be implemented in each stage.

Boot-up stage

- Firmware Integrity Check
  To ensure that firmware has not been modified or tampered by others, the best method is to implement an integrity check by embedded checksum or secure password.
- Secure Boot
  Encrypt firmware with public key infrastructure (PKI) or public/private certification to secure the whole boot-up process.

Trend Micro Security SDK can work with hardware SE and TPM to ensure boot-up stage security.

Initialization and operation stage

Trend Micro Security SDK will perform two main functions at this stage, using risk assessment to predict and detect any abnormal behaviors in files, runtime process and network connection. Furthermore, the vulnerability discovery cloud engine will check critical modules over time for known or newly discovered vulnerabilities and present the results on the management console. OEM vendors are enabled to prepare the mitigation plan, such as releasing an OTA fix or using Trend Micro SDK System Protection IPS (Virtual Path) for deploying a rule to prevent hackers from taking advantage of those vulnerabilities.

Update stage

Trend Micro solution can work with OTA service providers to execute the mitigation action.

Security SDK Features

The best practices to plan cybersecurity for connected vehicles have three major countermeasure solutions. The first is risk assessment: to identify and prioritize cybersecurity risks that could lead to safety and data security incidents. The second solution is system protection or hardening: to build the capability to prevent and protect the system after incidents happen. The third and most crucial solution is security countermeasure continuity process for risk detection, attack prevention and vulnerability protection, since cyberattacks evolve over time.

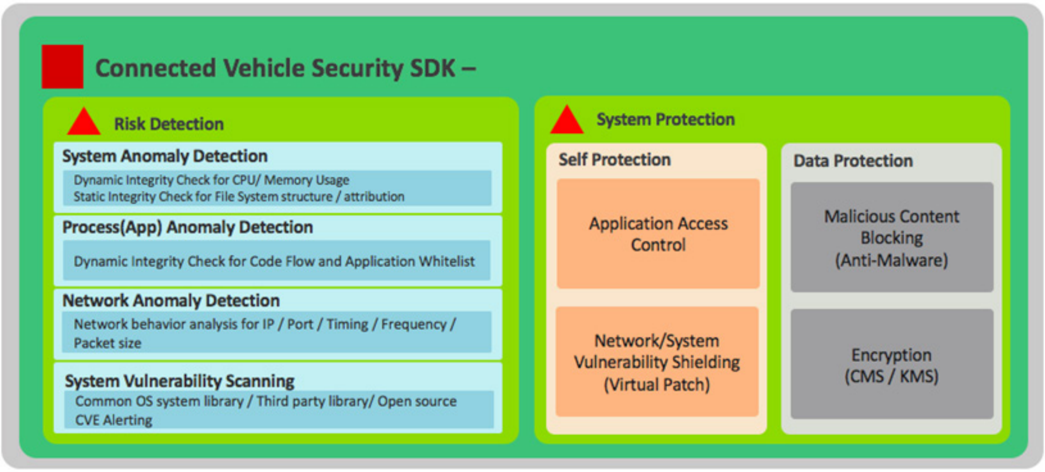

Connected Vehicle Security SDK –
Risk Detection
System Anomaly Detection
Dynamic Integrity Check for CPU/ Memory Usage
Static Integrity Check for File System structure / attribution
Process(App) Anomaly Detection
Dynamic Integrity Check for Code Flow and Application Whitelist
Network Anomaly Detection
Network behavior analysis for IP / Port / Timing / Frequency / Packet size
System Vulnerability Scanning
Common OS system library / Third party library/ Open source CVE Alerting
System Protection
Self Protection
Application Access Control
Network/System Vulnerability Shielding (Virtual Patch)
Data Protection
Malicious Content Blocking (Anti-Malware)
Encryption (CMS / KMS)

Figure 3. Connected vehicle security SDK feature diagram

Risk Assessment

Security SDK uses the Trend Micro X-Gen Anomaly cloud-based engine and Trend Micro Vulnerability Discovery cloud-based engine to accomplish continual operation.

System Anomaly Detection

- Cloud-based remote attestation method to detect the hacking attempt in system level
  - Static integrity check (file system)
    - Cloud-based technology to detect edge devices file system alteration/modification to prevent the hacking attempt
  - Dynamic integrity check (CPU/memory status)
    - Cloud-based technology to detect device running condition to prevent hacking attempt

Process Anomaly Detection

- Cloud- and device-based solution to detect running processes condition
  - Dynamic integrity check (code flow control)
    - Code-library-based solution to ensure running process flow is following designed rules
  - Dynamic integrity check (app whitelist)
    - Updated rules to contain running processes in designed/operation scope

Network Anomaly Detection

- Cloud-based big-data analysis with network behaviors machine learning
    - Multiple factors/elements sourcing IP/timing/frequency/bandwidth
    - Identifies the device abnormal network through the cloud without network performance impact on the device

System Vulnerability Scanning

- Cloud-based solution to detect devices' system vulnerability regularly
    - Integrates with Trend Micro's up-to-date system vulnerability database
    - Uses Trend Micro's Vulnerability Discovery Engine

System Protection

Host-Based IPS

- Examines all incoming and outgoing traffic for protocol deviations, policy violations or content that signals an attack
- Automatically protects against known but unpatched vulnerabilities by virtually patching (shielding) them from an unlimited number of exploits
- Provides increased visibility and control over applications accessing the network

Application Whitelisting Protection

- Monitors critical operating system and application files, such as directories, to detect, report and contain malicious and unexpected changes in real time
- Reduces administrative overhead with trusted event tagging that automatically replicates actions for similar events across the entire notes
- Simplifies administration by greatly reducing the number of known good events through automatic cloud-based whitelisting from Trend Micro Certified Safe Software Service

Anti-Malware (by request only)

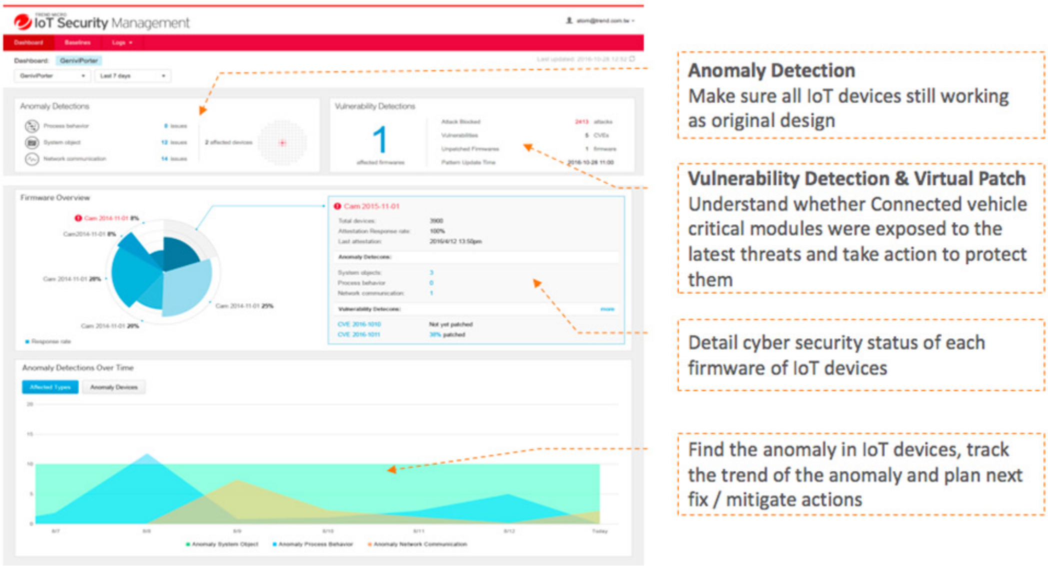
- Integrates with Trend Micro anti-malware scan engine to protect against viruses, spyware, Trojans and others malware with zero in-guest footprint
- Integrates with the Trend Micro Smart Protection Network global threat intelligence

Key Management System and Certification Management System (by request only)

Trend Micro offers Key Management System and Certification Management System for AAA protection (Authentication Authorization Accounting).

Cybersecurity Visibility Management Console

The incident response is the most critical stage for cybersecurity preparation. As Trend Micro understands the importance of threats visibility as necessary information for threats incident responses, we have provided a console that allows automotive OEMs and Tier 1 suppliers to manage cybersecurity visibility.



Anomaly Detection
Make sure all IoT devices still working as original design

Vulnerability Detection & Virtual Patch
Understand whether Connected vehicle critical modules were exposed to the latest threats and take action to protect them

Detail cyber security status of each firmware of IoT devices

Find the anomaly in IoT devices, track the trend of the anomaly and plan next fix / mitigate actions

Figure 4. Trend Micro security management console

Conclusion

The idea of connected vehicles has opened up new possibilities for automobile manufacturers and drivers alike. But the very thing that sets them apart from conventional cars, i.e., their connectivity, has also opened up new attack surfaces and threat vectors for hackers. For this reason, carmakers and car owners both need to consider taking security measures against cyberattacks on connected vehicles.

Trend Micro recommends that automotive OEMs adopt layered protection and use effective solutions to safeguard the critical modules in connected vehicles. Fueled by the belief that cybersecurity requires a tightly engaged ecosystem, Trend Micro has developed sophisticated cloud-based solutions, notably using its X-Gen machine learning engine, for connected vehicle cybersecurity protection.

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO™

Securing Your Journey
to the Cloud