CYIENT

AUTOMOTIVE SECURITY: HOW TO SECURE NEXT-GEN CONNECTED VEHICLES

Integrated security design for evolving safety threats is the way forward

CONTENTS

ABSTRACT

Connected vehicles are transforming vehicle design shining the spotlight on security features. With ever-increasing connected vehicles, automotive security has become an important factor for several reasons such as maintaining safety of vehicle occupants, protection against cyberattacks, safeguarding personal data, preventing theft and unauthorized access, protecting against malware and software vulnerabilities, compliance with regulations and standards, and preserving consumer confidence. By following strict best practices, periodic security assessments, and following standards and procedures, we can make the automotive world a safe place.

In this white paper, we discuss the significance of implementation of cybersecurity measures to secure connected vehicles and the key challenges industries face in adapting such technologies. We also share some insights into Cyient's recommendations and solutions to help the automotive industry become more scalable by following industry best practices.

INTRODUCTION

Back in the day there was no software on wheels; everything was hardware. In the '80s and '90s there was just 20% software and not much connectivity. But from 2020 onwards almost 40% - 60% of vehicles are software-based and are connected vehicles. Electronic control units (ECUs), components, protocols, systems, and backend servers are all considered software.

Increased connectivity and software-based vehicles have become a double-edged sword for even as vehicles become smarter, hackers have begun to launch sophisticated attacks like DDoS, MITM, CAN, LIN, message spoofing, Bus-off attacks, ECU reprogramming, replay attacks, eavesdropping, and ransomware. Following industry standards and best practices can prevent such attacks and ensure are secure.

Round-up of Recent Automotive Cyberattacks and Responses

Schneider Electric fixes critical vulnerabilities in EVlink electric vehicle charging stations

Mercedes-Benz USA admits some customers' credit card details and driver's license numbers were accessible for 3.5 years

Kawasaki Heavy Industries reports data breach as attackers found with year-long network access

Web-based attack crashes Tesla driver interface

Volkswagen vehicles are hacked via Wi-Fi hotspot feature

Tesla becomes latest victim of cryptojacking epidemic

Nissan Canada informs customers of possible data breach

Key Challenges of Automotive Security

As the automotive industry continues to embrace advanced technologies and connectivity, it faces several automotive security challenges.

Cybersecurity for automobiles is on the national agenda of several countries for a good reason. There are four industry trends that make modern cars vulnerable to cyberattacks and potential failures:

1 Automobiles are increasingly accessible by wireless and physical means to the outside world and bad actors.

2 Software will control all critical driving functions and if bad actors can access and modify or corrupt the software, it can lead to accidents and potential fatalities. The larger the amount of software in an automobile, the larger the attack landscape.

3 Autonomous automobiles will be driverless. By design, these automobiles will talk to each other and the infrastructure by wireless means. This further exacerbates the vulnerability problem in the number of access points through which an automobile may be breached. When this happens, the concomitant effects could be viral as one car can infect another and so on.

4 Autonomous automobiles will deploy artificial intelligence, deep neural networks, and learning algorithms. These automobiles will learn from context. This means that software that was installed as being safety- and security-certified at production will morph with time, and there need to be new ways to ensure that the automobile is still safe and secure over its lifetime.

In addition to these trends, other aspects of the automotive industry are key security concerns:

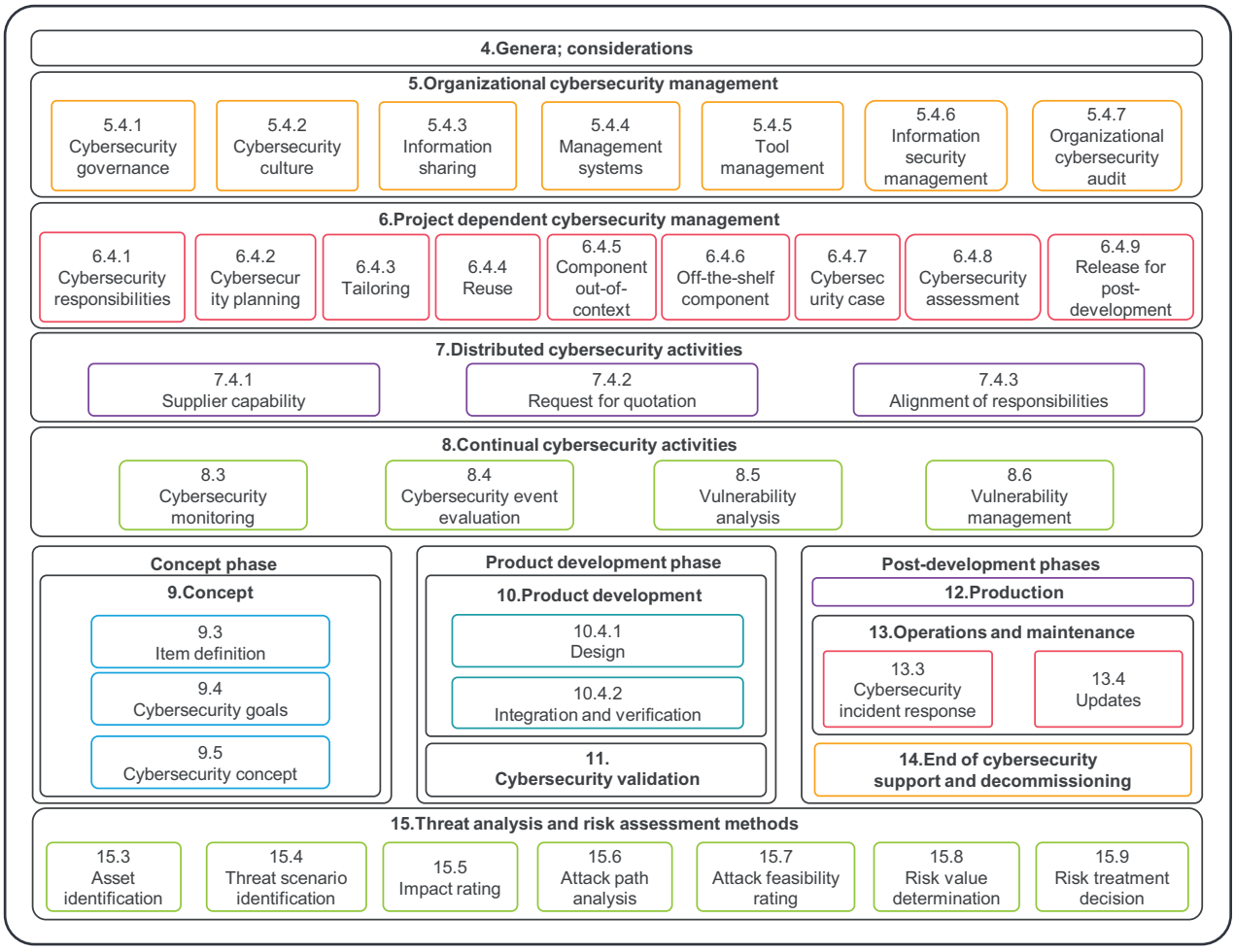
As connectivity of vehicles increases, emerging cybersecurity threats exposes them to a wide range of attacks from remote hacking and malware injection to denial-of-service.

- Complex software ecosystems in modern vehicles rely on complicated software systems to control various functions from engine management to infotainment. Managing the security of this software throughout its life cycle, including updates and patches, is challenging.
- Automotive manufacturers source components and software from global supply chains introducing potential vulnerabilities if any part of the supply chain is compromised.
- Legacy systems in many vehicles on the road today have limited security features. Retrofitting security into older vehicles can be challenging and costly.
- Human errors are the most commonly seen threats in an organization. Both drivers and service technicians can inadvertently introduce security vulnerabilities through actions such as connecting unsecured devices to the vehicle's network or mishandling software updates.
- Data privacy is vital because connected vehicles collect vast amounts of data, including location, driving habits, and personal preferences. Ensuring the privacy of this data and compliance with data protection regulations is a challenge.
- Interconnected systems in modern vehicles including infotainment, telematics, and advanced driver-assistance systems (ADAS) makes all systems vulnerable in case of an attack on any one of these.
- While over-the-air (OTA) updates offer convenience, they introduce new security challenges. Ensuring the integrity and authenticity of OTA updates is crucial to prevent malicious updates.
- Regulatory compliance is vital and fulfilling these requirements for automotive security can be challenging for manufacturers, as regulations vary by region and are subject to change.
- Often drivers and even automotive professionals may not be fully aware of the security risks and best practices. Raising awareness and providing education is thus essential.
- The cost involved in securing software-driven vehicles can be daunting. Governance teams must help in balancing the cost of implementing robust security measures with the need to keep vehicles affordable for consumers.

Manufacturers need processes in place to quickly identify, address, and communicate emerging security vulnerabilities to concerned parties. Testing and validation form a constant security loop. Ensuring that security measures work as intended and do not introduce unintended consequences requires thorough testing and validation processes.

CYIENT APPROACH AND INDUSTRY STANDARDS

Overview of the ISO/SAE DIS 21434



Section 1

Defines the scope of the norm

Section 2

Provides normative references

Section 3

Defines abbreviated terms and definition of terms used in the document

Section4

Is informative, describing the vehicle ecosystem, organizational cybersecurity management, and the related automotive life cycle

Section 5

Includes descriptions regarding the organizational cybersecurity strategy, policy, and objectives

Section 6

Defines risk management requirements, which include a plan and method to determine the extent to which the road user is threatened by a potential circumstance or event

Section 7

Deals with the concept phase and defines cybersecurity goals, resulting from threat analysis and risk assessment; and defines cybersecurity requirements to achieve cybersecurity goals

Section 8

Specifies the implementation and verification of cybersecurity requirements specific to the product development phase

Section 9

Focuses on the production, operation, and maintenance phase, specifying requirements to ensure that cybersecurity specifications are implemented in the produced item; it also covers cybersecurity activities

Section 10

Describes supporting processes, including organizational processes

Section 11

Describes the framework for validating the above-mentioned threats and vulnerabilities

Section 12

Defines a foolproof validating mechanism post production

Section 13

Talks about having a continuous process of evaluating a security cycle and a robust incident response team

Section 14

Is where the OEMs have to validate the EOLs and EOSs systems and regular patching of the hardware and software

Section 15

Talks about TARA analysis which is a method to perform risk assessments in the automotive sector

Solution Details:

Cyient has decades of experience in helping clients around the world to research, deploy, integrate, migrate, and support different networks, applications, and technologies. Our solutions offers the following steps to ensure safety automotive security:

1. Secure the supply chain

a. **Root of trust:** Ensure that every chip and electronic control unit in the automobile can be properly authenticated (via certificates) and is loaded with trusted software, irrespective of vendor tier or country of manufacture. This involves injecting every silicon chip with a private key during its manufacturing stage to serve as the root of trust in establishing a "chain of trust" method to verify every subsequent load of software. This mechanism verifies all software loaded.

b. **Code scanning:** Use sophisticated binary static code scanning tools during software development to provide an assessment which includes, file composition, the exposure of this code to security vulnerabilities, and indicators/ metrics to enable secure agile software craftsmanship. This data can be used to improve the software to reduce its security risk prior to production builds.

c. Approved for delivery: Ensure that all vendors and vendor sites are certified via a vulnerability assessment and are required to maintain an "approved for delivery" certificate. This evaluation needs to be done on a continuous basis.

2. Use trusted components

a. **Proven components with defense in depth deployment:** Use a recommended set of components (hardware and software) that have proper security and safety features and have been verified to be hardened against security attacks. Create a security architecture that is layered and deployed with defense in depth (vault within a vault). For example: Hardware (system on chips–SOCs) must be secure in architecture and have access ports protected (debug ports, secure memory, etc.). SOCs should store a secret key, as described above, and act as the root of trust for secure boot verifying software that is loaded. The operating system must have multi-level security features such as access control policies, encrypted file systems, rootless execution, path space control, thread level anomaly detection, etc. Applications should also be protected as described below.

b. **Application management:** All downloaded applications should be certified and signed by proper authorities. A signed manifest file will set permissions of those resources in the system that this application will and will not be allowed to access. The applications must always run in a sandbox and are managed over their life cycle.

3. Isolation

a. **ECU isolation:** Use electronic architecture for the automobile that isolates safety critical and non-safety critical ECUs and can also "run-safe" when anomalies are detected.

b. **Trusted messaging:** Ensure that all communication between the automobile and the external world and messaging between modules (ECUs) in the car is authentic and trusted.

4. In-field health check

a. **Analytics and diagnostics:** Ensure that all ECU software has integrated analytics and diagnostics software that can capture events and logs and report the same to a cloud-based tool for further analysis and preventative actions.

b. **Security posture:** Ensure that a defined set of metrics can be scanned regularly when the vehicle is in the field, either on an event-driven (e.g., when an application is downloaded) or periodic basis to assess the security posture of the software and take actions to address issues via over-the-air software updates or via vehicle service centers.

5. Rapid incident response network

a. **Crisis connect network:** Create an enterprise network to share common vulnerabilities and exposures (CVE) among subscribing enterprises such that expert teams can learn from each other and provide bulletins and fixes against such threats.

b. **Early alerts:** Typically, when a CVE is discovered, there is a time lag between discovery of the issue and the fix. This time lag is a "risk period" and it is necessary to alert stakeholders on what to do with advisories until a fix can be deployed.

6. Life cycle management system

a. When an issue is detected, using in-field health check, proactively re-flash a vehicle with secure over-the-air software updates to mitigate the issue. Manage security credentials via active certificate management. Deploy unified end point policy management to manage, among other things, applications downloaded over the lifetime of the car.

7. Safety/security culture

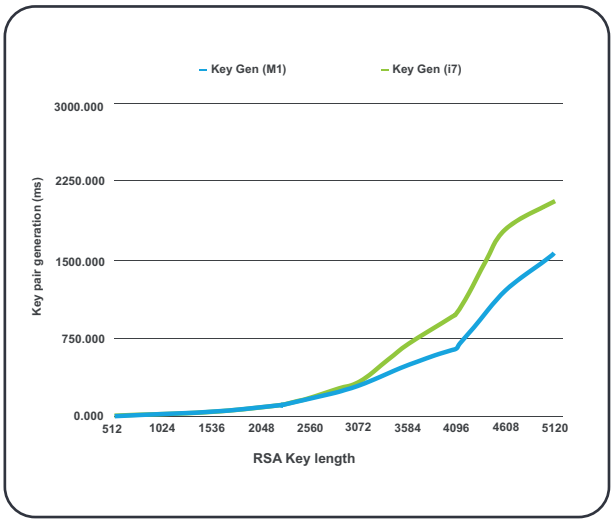
a. Ensure that every organization involved in supplying auto electronics is trained in safety/security best practices and inculcate this culture within the organization. This training includes a design and development culture as well as IT system security.

Security Mechanisms:

Relative software execution times for different public key sizes:

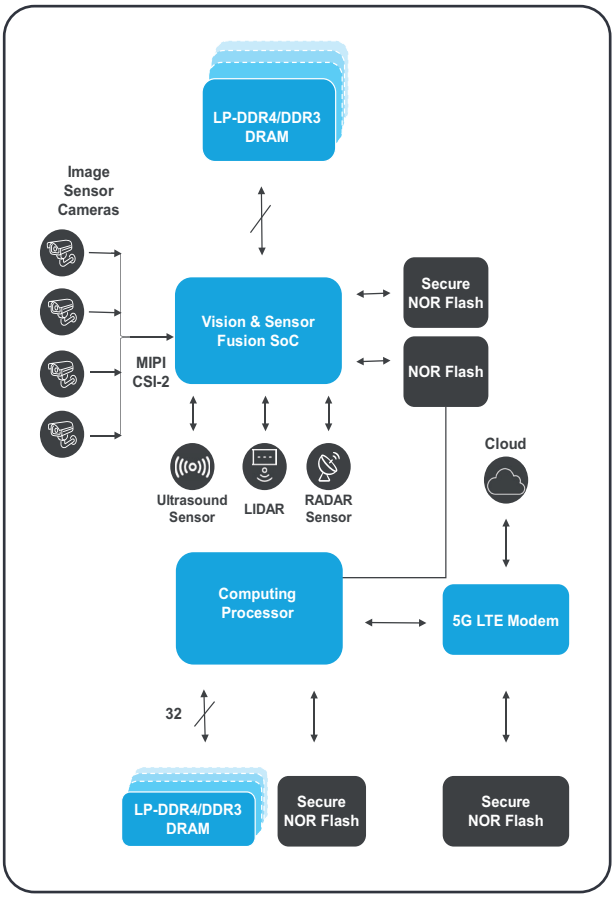
The execution times for various public key sizes can vary significantly, depending on the cryptographic algorithm used and the computing resources available. A general overview of the relative software execution times for different public key sizes in common cryptographic algorithms, with larger key sizes generally requiring more computational resources and time for encryption and decryption, is shown below.

The partitioning between hardware and software implementations must also take into consideration the types of malicious attacks to fend against. Typically, an attack will occur because malicious software has been allowed to execute during the boot process or during normal run time.



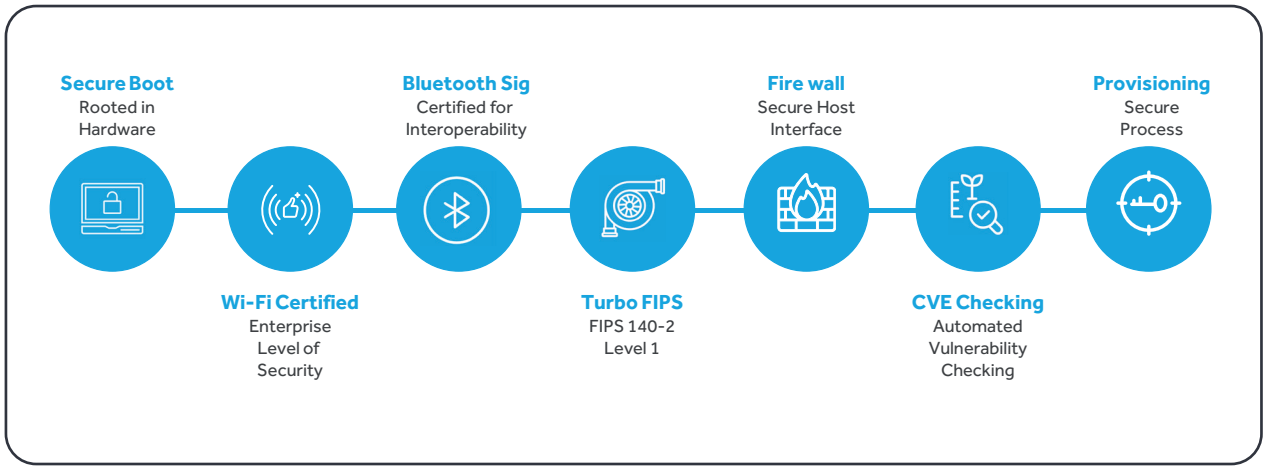
Secure flash programming

The process in which firmware or software updates are loaded onto a microcontroller's flash memory in a secure and tamper-resistant manner is crucial. This is a critical aspect of maintaining the security and integrity of embedded systems, particularly in applications where the firmware's authenticity and confidentiality are paramount.



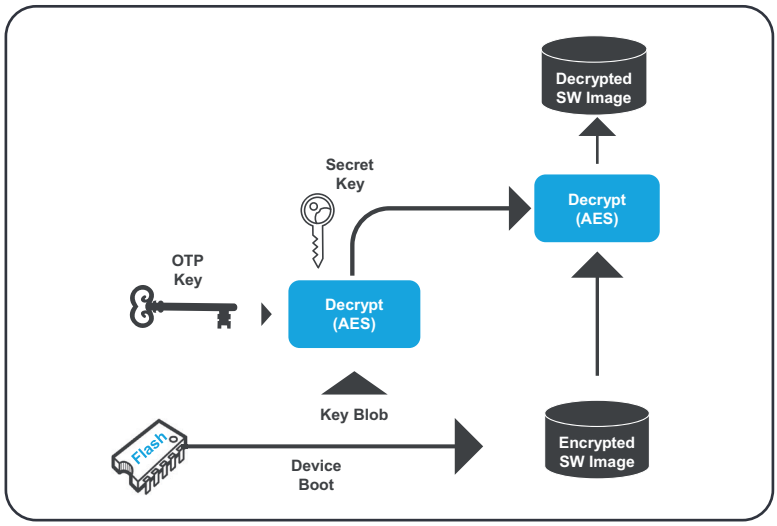
Chain of Trust

Secure boot is a fundamental security practice used in computer systems and embedded devices to ensure the integrity and authenticity of the firmware or software that is executed during the boot process. It establishes a sequence of trust between different components and entities involved in the boot process, making it more difficult for attackers to compromise the system.



Block cipher engine for external memory security

The hardware or software component designed to encrypt and decrypt data stored in external memory devices, such as external hard drives, USB flash drives, memory cards, or network-attached storage (NAS) devices, referred to as engine, should enhance the security and confidentiality of data stored in these external storage media.



CONCLUSION

In the future, it is conceivable to imagine that robust vehicle security could potentially reduce insurance rates and even lower vehicle depreciation. Integrated security design also offers the added benefit of allowing higher dollar value feature options to be delivered as an option in all vehicles, enabled by a software switch as an after-market purchase.

The continued growth in automotive security will be driven by a combination of factors. The added connectivity to the external world through entertainment portals such as Bluetooth and USB introduces an attack surface for installing malicious software or unauthorized modifications to existing software.

Another factor is the increase in safety-aware applications such as HEV and advanced driver assistance systems in the form of collision avoidance and self-parking. Moreover, emerging markets introduce a new world order to product development and manufacture. The embedded security measures described in this paper provide a way to ensure that safety is not compromised while providing the features necessary to ease product development and protecting manufacturers' investment and drivers' privacy.

ABOUT THE AUTHOR

Rachin Katti is Head of Cybersecurity at Cyient. He has 17 years of experience securing networks, infrastructure, and information for customers across multiple industries. In his current role, he provides secured, customized, tailored security solutions across all verticals.

REFERENCES

- https://blackberry.qnx.com/content/dam/qnx/whitepapers/2017/7-pillar-auto-cybersecurity-white-paper.pdf
- https://www.nxp.com/docs/en/white-paper/AUTOSECURITYWP.pdf

About Cyient

Cyient (Estd: 1991, NSE: CYIENT) is a global Engineering and Technology solutions company. We collaborate with our customers to design digital enterprises, build intelligent products and platforms and solve sustainability challenges. We are committed to designing tomorrow together with our stakeholders and being a culturally inclusive, socially responsible, and environmentally sustainable organization.

For more information, please visit www.cyient.com

Follow us on:

Contact Us

North America Headquarters
Cyient, Inc.
99 East River Drive
5th Floor
East Hartford, CT 06108
USA
T: +1 860 528 5430
F: +1 860 528 5873

Europe, Middle East, and Africa Headquarters
Cyient Europe Limited
Apex, Forbury Road,
Reading
RG1 1AX
UK
T: +44 118 3043720

Asia Pacific Headquarters
Cyient Limited
Level 1, 350 Collins Street
Melbourne, Victoria, 3000
Australia
T: +61 3 8605 4815
F: +61 3 8601 1180

Global Headquarters
Cyient Limited
Plot No. 11
Software Units Layout
Infocity, Madhapur
Hyderabad - 500081
India
T: +91 40 6764 1000
F: +91 40 2311 0352