Cybellum

A REVIEW OF ENISA 2019

AUTOMOTIVE PRACTICES

INTRODUCTION

ENISA, the European Union Agency for Cybersecurity, has recently published their updated report highlighting the importance of cybersecurity for connected cars. This report is the latest in a series of industry standards and best practices around the topic of automotive cybersecurity.

In this whitepaper we review the guidelines listed in the report. We provide our insight on the challenges the industry is facing today around these areas and suggest possible solutions.

Our review of the guidelines follows the same categorization as the report. We review each category and some of the challenges it brings.

Note that our review is not intended to be comprehensive. While we cover many of the guidelines, it is not a complete review. We recommend to carefully read Chapter 4 of the report for the complete details.

So, let's get right to it.

OVERVIEW

We believe that one of the major pains in the industry right now is the multitude of available guidelines and best practices. ENISA's report provides a great overview of what's out there.

Between the EU's C-ITS, NHTSA, Auto-ISAC, UNECE, BSI, ETSI, SAE J3061 and ISO 21434, there are more than enough guidelines and regulations, repeating in many cases the same or similar requirements and recommendations. The report not only provides a great overview of these standards and best practices, but also summarizes them into very clear guidelines.

However, there are many challenges in adhering to these guidelines. In these blogs series we will address some of these challenges and offer possible solutions.

But first, let's make some order in what's ahead of us. The report suggests organizing this huge task into the following categories:

- Policies - Which procedures and policies we should have that will ensure proper automotive security.
- Organizational Practices - How should we behave as an organization that will ensure proper automotive security.
- Technical Practices - Which technical practices we should implement to ensure proper automotive security.

POLICIES

The report provides policies guidelines in four categories:

1. Security by design

Among other recommendations, the guidelines suggest a "shift left security" approach. Consider security already in early stages of the design. In addition, implement a Secure Development Lifecycle (SDL) approach and DevSecOps such that security is taken care of during each development phase.

Our experience suggests that there are two major obstacles on the way towards this goal:

- **Software obscurity through supply chain -** The reality of the automotive market is that OEMs buy subsystems from Tier-1s, and Tier-1s buy software and components from Tier-2s. This leaves OEMs with software binaries that were developed elsewhere, without enough practical controls to truly enforce security practices early in the development process.
- **Lacking tools -** Most tools available in the market only provide a partial answer for automotive software:
    - **Source-code analysis tools -** do not analyze the entire software stack including the OS or framework itself, third-party software libraries, or any other security risks that may enter the final product - the firmware.
      In addition, there are various software development standards that are commonly used in the automotive industry, but general purpose tools do not support them.
    - **Binary analysis tools -** do not support the binary formats that are in use in the industry, many of them proprietary.
      In addition, most do not support the CPU architectures that are common in automotive.

2. Privacy by design

The guidelines suggest that local and international privacy regulations must be implemented, together with Privacy Impact Assessments (PIA) and regular privacy audits.

Indeed, our own experience is that this is a serious issue. Many types of privacy information leaks are found in real world firmware. Among the findings are default passwords, plain text passwords, email addresses (for example: developers email addresses), IP addresses and more. Apparently, this information is inadvertently added during the build process and is not detected by pre-compilation security means.

As the report suggests, proper security technologies and processes should be put in place to prevent privacy information leakage. These mechanisms must validate and prevent privacy information leakage every external deliverable prior to its release.

3. Asset management

The report suggests vendors to maintain an inventory of their assets - the components and their accompanying software. In addition, vendors must implement a change management process.

Managing assets and risks is challenging. As cars and subsystems transform from mechanics and electronics to software and data, different risks are introduced.

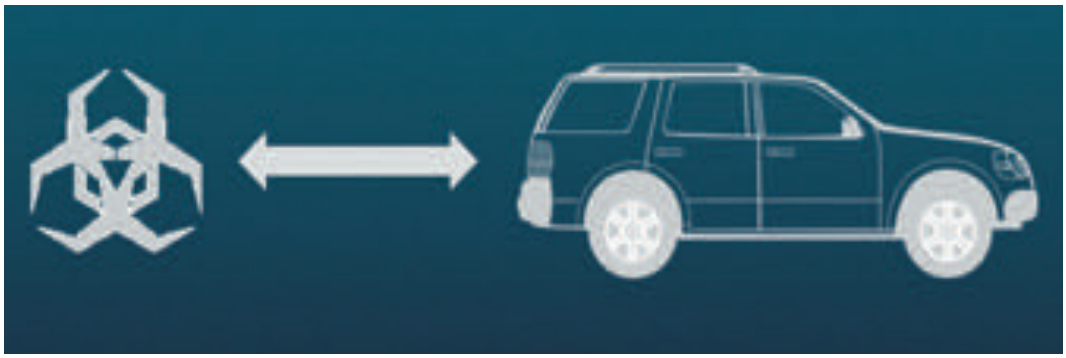
- **Cyber security vulnerabilities -** Maybe the most obvious risks. Systems are faced with publicly known vulnerabilities, zero-day hacks, and various security related hardening misconfigurations.

- **Adherence to standard industry practices -** There are many industry-specific regulations, standards and best practices related to the software design lifecycle. These practices relate to the design, development and maintenance of software. Not adhering to these practices may carry varying levels of risk to the organization.

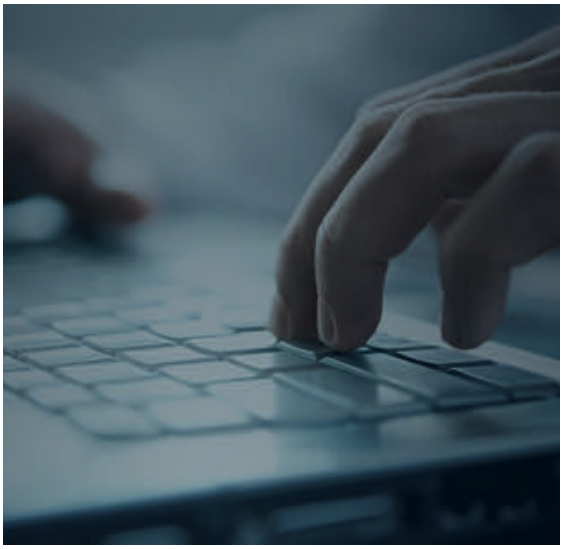
- **Software licensing risks-** Using open-source speeds up development but requires a careful review of each software library's license. With tens to hundreds of libraries used in each product, tracking licenses across the entire company becomes a tremendous challenge.

Keeping track of the above for each car model and its subsystems is a real challenge. Once a security risk or concern is identified, vendors should be able to drill-down to the exact list of on-the-road VINs affected by the risk, or in the case of suppliers, the list of product serial numbers

This mapping between physical asset types, each specific asset id, and each software revision, is the essence of a risk-focused asset management system that maintains not only the metadata about the assets themselves but also the details about the risks for these assets.



4. Risk and Threat Management



Here, the report asks vendors to “adopt an approach to risk management dedicated and suitable for the automotive sector, considering emerging threats and attack scenarios targeting smart cars” (guideline PS-11). It also asks to perform “cybersecurity risk analysis from the very early stages” (PS-12) but also to regularly (“every 6 months or more frequently”) monitor security vulnerabilities, in particular for postproduction vehicles (PS-13).

The main challenge here is indeed the frequency of vulnerabilities monitoring. Take for example an AGL based component. Just in the last three months there were 138 vulnerabilities reported for the Linux kernel, potentially affecting such a component. It is therefore irresponsible to perform this monitoring at 6 months intervals. The reason it is mentioned as an example in the guidelines is the fact that the industry is currently having difficulties in keeping up with anything more frequent.

To summarize the Policies guidelines:

To meet ENISA's guidelines in the Policy category, a solution must:

- **Manage assets, not just vulnerabilities - Keep track of vehicles, components and versions, and map them to identified risks.**
- **Analyze closed source binaries with no need for source code.**
- **Support automotive CPU architectures such as Arm®, TriCore™, Renesas and more.**
- **Support automotive binary formats.**
- **Detect cyber security and other risks automatically and continuously, from early development phases to postproduction on-the-road car fleets.**
- **Detect the privacy violations and different kinds of information leakage.**
- **Provide the facilities to become an integral part of a DevSecOps flow - namely the ability to automatically perform all of the above analysis as part of the development lifecycle.**

Note: One item that seems to be missing from the report is compliance to software coding standards - mainly AUTOSAR and MISRA, which are very common in the automotive industry. While these are not an end goal by themselves, they are very common means to reach that goal.

Cybellum Security Suite comes to the rescue

Cybellum Security Suite is a complete risk assessment solution for automotive components. It provides visibility to closed source automotive software, exposing cybersecurity threats - both publicly known and zero-day issues as well, using static and dynamic analysis engines.

It is fully automatable and integrates with software management systems and issue tracking software, enabling a DevSecOp approach to automotive security.

To summarize:

Automotive cyber security challenges can only be addressed by risk assessment software that is designed for automotive. Cybellum Security Suite provides such a solution. It enables OEMs and suppliers alike to automatically assess their existing components for an entire range of risks

ORGANIZATIONAL PRACTICES

The report provides organizational practices guidelines in four categories:

1. Relationships with Suppliers

The guidelines call for “security-related information sharing” (guideline OP-01) and cybersecurity “along the supply chain” (OP-02). However, the means to meet these guidelines are left open, since there are no clear standards on how this should be met.

2. Training and Awareness

Relevant information should be shared between all parties involved (OP-03). The model of Information Sharing and Analysis Centers (ISACs) is mentioned specifically. Employees and suppliers should be trained (OP-04), continuously and regularly (OP-05). The public awareness of security issues and prevention methods should be increased (OP-06).

The challenges for the industry as we see them are in practical and acceptable methods of sharing cybersecurity information in an industry that is now used to not share information at all. OEM cyber experts today receive pre-production units without any notion of the device internals, and when issues are found, the reporting is heavily filtered before it comes back to the supplier. The industry has to “open up” entirely from its current operational mode.

In addition, the public awareness is lacking since vendors have mostly avoided cyber security - meaning the protection against threats, as a promotable safety mechanism. OEMs are not reporting their efforts in this regard to the public. Arguably, the public is not knowledgeable enough in many cases to fully understand the technologies behind either the risks or the mitigations.

Another angle is the information sharing and education. Finding vulnerabilities is not enough. Risks must be presented as actionable results, with the necessary explanations and mitigation steps.

3. Security Management

The report recommends OEMs to establish a SOC (guideline OP-07) and define an "Information Security Management System (ISMS)" that covers the entire lifecycle of vehicles (OP-09). In addition, it calls for the obvious implementation of designated security teams (OP-08) and strategic task force (OP-10).

- **OP-07:** Consider establishing an OEM Security Operations Center (SOC) with clearly defined roles, Responsibilities and cyber security competences to centralize knowledge on cyber security, monitor and anticipate potential threats.
- **OP-08:** Designate one or several[51] dedicated security team(s) with security specialists having diversified and broad range of competencies in security related topics (e.g. risk assessment, penetration testing, secure design, etc).
- **OP-09:** Define a dedicated information Security Management System (ISMS)[52] that covers smart cars entire lifecycle.
- **OP-10:** Consider defining an internal task force, which involves board-level management, to guide security-related strategic decision and facilitate accountability.

Unfortunately, there is currently no explicit definition to an OEM SOC (or as some call it, VSOC - Vehicle SOC). The same goes with ISMS (which some call CSMS - Cyber Security Management System). As in many other cases, when there is a void, commercial parties come up with appropriate solutions.

4. Incident Management

Here, the guidelines are calling for both OEMs and third-party suppliers to establish product security teams (guideline OP-12) and processes (OP-11). From our experience, internal cross-functional security experts in the large OEMs and the largest Tier-1 suppliers are typically designated as Product Security Incident Response Team (PSIRT) and Computer Security Incident Response Team (CSIRT). This is much less the case in smaller Tier-1 and Tier-2 suppliers.

To summarize the Organizational Practices:

To meet ENISA's guidelines in the Organizational Practices category, a solution must:

- Serve as a central management for the cybersecurity relationship across the supply chain.
- Enable practical sharing of cybersecurity information between all parties.
- Support PSIRTs and CSIRTs in their day-to-day security operations.

In addition, the vendors involved must promote the information sharing, so ideally, a solution should support the distribution of this information to both internal and external parties.

In Cybellum, we are working on such a solution. Already today our products promote the sharing of security information. In addition, we are closely following the industry's reaction to the information sharing related guidelines, and we expect to evolve towards that direction.

Organizing Cyber Security with Cybellum V-Ray

V-Ray serves as an CSMS (or ISMS as related in the guidelines), providing a central access point to security and risk information for both automotive OEMs and third-party suppliers alike. Access is controlled so each party can only manage and review its relevant information.

The result is an open (yet secure) infrastructure for automotive cyber security, whereby parties can identify and share details on risks and mitigation steps with others. In other words, Cybellum Security Suite is built for a future where security sharing will be the common modus operandi, but already support today's supply chain vendor/supplier operations, where information is typically not shared through common systems.

TECHNICAL PRACTICES

The report provides technical practices guidelines in nine categories:

1. Detection

The guidelines suggest the implementation of Intrusion Detection Systems (IDS) both in vehicles and back end systems (guideline TM-01), review audit logs (TM-02) and network logs and other access controls (TM-03). It also directs that input data should be validated (TM-04). It also calls for adding the technical capabilities required for post-mortem forensics of crashes and cyber attacks (TM-05).

According to our experience, one of the key elements required for complete forensics and impact assessment is first of all maintaining a full inventory. One should maintain an updated full mapping of the software BoM at the fleet, vehicle and component levels. This mapping can then be used to identify the actual threats and how they are affecting physical assets.

Disassembly of a ŠKODA FABIA COMBI 1.2 TSI DSG after it had covered over 100,000 kilometers in a long-term test by the German magazine Auto Bild.
https://www.skoda-storyboard.com/en/skoda-fabia-combi-auto-bild-car-parts/

2. Protection of Networks and Protocols

Interfaces should be protected using authentication and access control (TM-06). Critical in-vehicle communications should be secured (TM-07), and the same goes for all external communications (TM-08). Sessions should be protected (TM-09), as well as time synchronization sources (TM-10). Radio communications should be secured (TM-11 and TM-12). Packet filtering should be used to discard illegitimate traffic (TM-13), and secure protocols for protecting the confidentiality and integrity of sensitive data (TM-14).

We believe that the major gap today is that it is difficult to implement some of the above, especially the in-vehicle systems, but even more so, the validation that these protections are in place and operating as expected.

3. Software Security

Devices and services are configured for secure operations (TM-15). Validate that only legitimate software is installed (TM-16) and booted (TM-20) and implement configuration change management (TM-17). OTA firmware updates should be secure (TM-18 and TM-19).

For the software itself, a risk assessment should be performed to identify vulnerabilities, limitations of software dependencies. The risks should be addressed and mitigated (TM-21).

Mobile apps should be protected against reverse engineering and tampering (TM-22), and sensitive data should be secured when stored on mobile devices (TM-23).

4. Cloud Security

The report suggests following cloud security providers if applicable (TM-24). Implement high-availability for cloud-based applications (TM-25) but nevertheless implement critical systems in private or at least hybrid cloud setups (TM-26). Also ensure that all data in the cloud is secured, and most notably make sure that decryption keys are not stored insecurely.

5. Cryptography

The use of encryption all around is promoted (TM-28), with well-known, standardized cryptographic schemes (TM-29). Use storage encryption (TM-30) and secure key management (TM-31), with a recommendation to use Hardware Security Modules (TM-32).

6. Access Control

The guidelines suggest applying security controls (TM-33), least privileges principle and individual access accounts (TM-34) and encourage the use of Multi-Factor Authentication (TM-36). In addition, remote communications should be controlled and monitored (TM-35).

7. Self-Protection and Cyber Resilience

Guideline TM-37 asks to implement security for Global Navigation Satellite System (GNSS). The report also recommends applying hardening in different levels (TM-38) and make interfaces more robust (TM-39). It suggests the use of trusted software technologies for application isolation (TM-40), as well as physical and logical isolation.

8. (Semi-) Autonomous Systems Self Protection and Cyber Resilience

The guidelines recommend protecting localization data and different sensors in the system and also introduce high availability and redundancy for them (TM-42 to TM-47).

9. Continuity of Operations

The report highlights the importance of easy to understand notifications of issues and their remediation (TM-48). It suggests the creation of Business Continuity Plan and Business Recovery Plan (BRP) that should also cover third-party aspects and get regularly tested (TM-49). In addition, important parameters related to business continuity should be defined.

To summarize the Technical Practices:

To meet ENISA's guidelines in the Technical Practices category, a solution must:

- Maintain an updated inventory of hardware and software - the complete configurations, operating system details and installed open-source and proprietary software BoM of each component and vehicle within the fleet.
- Validate that detection and protection mechanisms are implemented and configured correctly.
- Validate that each component and its entire software stack is configured with recommended security settings.
- Support secure software installations, in particular OTA updates.
- Validate that decryption keys are stored and managed securely.
- Validate the use of standard encryption schemes.
- Validate that remote communications are secured.
- Provide easy to use reporting of findings and remediation steps.

Cybellum V-Ray is a solution that can help OEMs and automotive suppliers meet these guidelines.

www.cybellum.com

WP-ENI2019-R1